LA POLICÍA JUDICIAL EN LA OBTENCIÓN DE INTELIGENCIA SOBRE COMUNICACIONES ELECTRÓNICAS PARA EL PROCESO PENAL

UNIVERSIDAD NACIONAL DE EDUCACIÓN A DISTANCIA
FACULTAD DE DERECHO
DEPARTAMENTO DE DERECHO PROCESAL

TESIS DOCTORAL

AUTOR: D. LUIS MANUEL VALLÉS CAUSADA
TENIENTE CORONEL DE LA GUARDIA CIVIL
DIRECTOR: PROF. DR. D. MANUEL DÍAZ MARTÍNEZ
MADRID, DICIEMBRE DE 2012.

A mi mujer, Carmen, Doctora en Farmacia y
Licenciada en Derecho, admirable ejemplo
de amor, capacidad de sacrificio
y afán de superación.

A mis hijos, Álvaro e Inés, por si el denuedo
de sus padres les sirviera de algún ejemplo
para impregnarse de los valores intemporales
que deseamos transmitirles.

A mi madre, Andrea, en el origen de mi vocación,
por enseñarme cuánto había que amar a España.

A mis amigos y a quienes creyeron en mí y
me sostuvieron cuando me fallaron las fuerzas.

A los guardias civiles de todos los tiempos
que sirvieron honorablemente a España.

Al Excmo. Sr. D. Vicente Gimeno Sendra,
al Teniente Coronel Dr. D. Nicolás Marchal Escalona y
al Prof. Dr. D. Manuel Díaz Martínez, por creer
que podía componer una tesis doctoral.

In memoriam

A mi padre, Luis Manuel, un hombre bueno
que murió sin concederme el consuelo
de una despedida.

A mi suegro, Poli, por su amistad y
por su lección de amor a la vida
y dignidad ante la muerte.

A todos, de corazón, muchas gracias.

"Se impone realizar un ejercicio de equilibrio.
No es posible cerrarse, de forma irracional,
a determinadas aportaciones de las nuevas tecnologías,
que enriquecen a la Policía Judicial, basándonos
en su incidencia sobre el secreto de las comunicaciones".

José Antonio Martín Pallín
Magistrado Emérito del Tribunal Supremo

ABREVIATURAS

AAN	Auto de la Audiencia Nacional
AEPD	Agencia Española de Protección de Datos
ATC	Auto del Tribunal Constitucional
ATS	Auto del Tribunal Supremo
BTS	*Base Transreceiver Station*, o estación de recepción y transmisión de comunicaciones
CC	Código Civil
CCib	Convenio sobre la Ciberdelincuencia
CDF	Carta de Derechos Fundamentales de la Unión Europea
CE	Constitución Española de 1978
CEDH	Convenio Europeo para la protección de los Derechos Humanos
CEMU	Comité Ejecutivo del Mando Unificado de las FCSE
CEPOL	Colegio Europeo de Policía
CGPJ	Consejo General del Poder Judicial
CICO	Centro de Inteligencia del Crimen Organizado
CNCA	Centro Nacional de Coordinación Antiterrorista
CNCPJ	Comisión Nacional de Coordinación de la Policía Judicial
COSI	Comité Permanente de Seguridad Interior de la Unión Europea
CP	Código Penal
CPCPJ	Comisión Provincial de Coordinación de la Policía Judicial
CRI	Comisión Rogatoria Internacional
DACE	Datos asociados a las comunicaciones electrónicas
DCD	Directiva 2006/24/CE, *sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones*
DO	Delincuencia organizada
DoS	Ataque cibernético de denegación de servicio
DP	Diligencias Previas
ELSJ	Espacio de libertad, seguridad y justicia (Unión Europea)

EM	Exposición de motivos
EOMF	Estatuto Orgánico del Ministerio Fiscal
FCSE	Fuerzas y Cuerpos de Seguridad del Estado
FFSS	Fuerzas de Seguridad
FFSSEE	Fuerzas de Seguridad del Estado
FRONTEX	Agencia Europea para la Gestión de la Cooperación Operativa en las Fronteras Exteriores
IDACE	Inteligencia de Datos Asociados a las Comunicaciones Electrónicas.
IMEI	Acrónimo del inglés *International Mobile Equipment Identity* (Identidad Internacional de Equipo Móvil)
IMSI	Acrónimo del inglés *International Mobile Subscriber Identity* (Identidad Internacional del Abonado a un Móvil)
IP	Número que determina una conexión a Internet dentro del *Protocolo TCP/IP*
ISP	Acrónimo del inglés *Internet Service Provider* o Proveedor de Servicio de Internet
ITCE	Inteligencia sobre comunicaciones electrónicas
JAI	Justicia y Asuntos de Interior de la Unión Europea
JI	Juzgado de Instrucción
LCDCE	Ley 25/2007, *de conservación de datos relativos a las comunicaciones electrónicas y de las redes públicas de comunicaciones*.
LCRIM	Ley de Enjuiciamiento Criminal
LEC	Ley de Enjuiciamiento Civil
LGT	Ley General de Telecomunicaciones
LOCFSE	Ley Orgánica de Fuerzas y Cuerpos de Seguridad del Estado
LOPD	Ley Orgánica de Protección de Datos de Carácter Personal
LOPJ	Ley Orgánica del Poder Judicial
LRJ-PAC	Ley de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común
LSSI	Ley de Servicios de la Sociedad de la Información y del Comercio Electrónico

MF	Ministerio Fiscal
MMS	Acrónimo del inglés *Multimedia Messaging System* o sistema multimedia de mensajería
OCDE	Organización para la Cooperación y el Desarrollo Europeos.
OCTA	Acrónimo del inglés *Organized Crime Threat Assessment* o Valoración de la Amenaza del Crimen Organizado, realizado por EUROPOL
OEDE	Orden Europea de Detención y Entrega
OEI	Orden Europa de Investigación
ONU	Organización de las Naciones Unidas
P2P	Del inglés *Peer to Peer* o redes de pares que permiten la conexión entre usuarios y la descarga masiva de archivos informáticos.
PE	Parlamento Europeo
PESC	Política Exterior y de Seguridad Común de la Unión Europea
PJ	Policía Judicial
PJE	Policía Judicial Específica
PJG	Policía Judicial Genérica
RDPJ	Real Decreto 769/1987, de regulación de la Policía Judicial
RLGT	Real Decreto 424/2005, *por el que se aprueba el Reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios*
RLOPD	Reglamento de la Ley Orgánica de Protección de Datos de Carácter Personal
SEPD	Supevisor Europeo de Protección de Datos
SITCEN	Centro Conjunto de Situación para el Análisis de la Inteligencia de la Unión Europea
SMS	Acrónimo del inglés *Short Message Service* o Servicio de Mensajes Cortos de telefonía móvil
STC	Sentencia del Tribunal Constitucional
STEDH	Sentencia del Tribunal Europeo de Derechos Humanos
STS	Sentencia del Tribunal Supremo
TEDH	Tribunal Europeo de Derechos Humanos

TFUE	Tratado de Funcionamiento de la Unión Europea
TIC	Tecnología de la Información y las Comunicaciones
TUE	Tratado de la Unión Europea
UCO	Unidad Central Operativa de la Guardia Civil
UE	Unión Europea
UIT	Unión Internacional de Telecomunicaciones
UMTS	*Universal Mobile Telecommunications System* o sistema de telecomunicaciones móviles
UOPJ	Unidad Orgánica de Policía Judicial
VoIP	Voz sobre IP o comunicaciones a través del protocolo de Internet

ÍNDICE:

I. CAPÍTULO PRIMERO: SITUACIÓN DE LA DELINCUENCIA GRAVE U ORGANIZADA. EL FACTOR CRIMINÓGENO DE LAS TIC: LA DELINCUENCIA COMPLEJA.

En la mayor parte de la bibliografía consultada sobre la delincuencia organizada (en adelante DO) o grave, se hacen prolijas referencias a los efectos multiplicadores de su capacidad criminal atribuidos al fenómeno social de la ***globalización***[1] y, singularmente, a la utilización masiva de las ***tecnologías de la información y las comunicaciones*** (en adelante, **TIC**)[2]; progresos que, si bien han supuesto revolucionarios avances para la humanidad[3], no han dejado de aportar a los delincuentes, al mismo tiempo, ingentes recursos para cometer sus delitos con buenas expectativas de rendimiento ilícito e impunidad.

Siendo cierto esto, no lo es menos que a estas alturas, cuando ya está bien entrado el siglo XXI, estos signos, en lo que a la delincuencia se refiere, dejan ya de ser novedosos para ser en su cotidianeidad simplemente preocupantes, en la medida en que la sociedad no ha evolucionado en la misma forma en lo que a dotación de medidas de control se refiere.

Algunos indicadores de la extraordinaria penetración en la vida social de las TIC son los siguientes[4]:

- Los españoles disponen en prácticamente todo el territorio nacional de ***banda ancha de datos*** para sus conexiones de Internet (el 60,5% de los españoles son internautas).

---

[1] Para HELD y McGREW, la definición de globalización sería la *"ampliación, profundización y aceleración de la interconexión global" o "un proceso (o conjunto de procesos) que encarna una transformación en espacial de las relaciones sociales y transacciones –evaluadas en función de su extensión, intensidad, velocidad e impacto-, generando flujos transcontinentales o interregionales de actividad, interacción y de ejercio de poder"*. Vid. Sansó-Rubert Pascual, Daniel. *Criminalidad organizada transnacional y seguridad internacional.* [aut. libro] José Julio Fernández Rodríguez, Javier Jordán Enamorado y Daniel Sansó-Rubert Pascual. *Seguridad y defensa hoy. Construyendo el futuro.* Madrid: Plaza y Valdés Editores, 2008, págs. 207-240, pág. 218. Nótese, por otra parte, que el inicio de la ***world wide web*** de Internet, como fenómeno nuclear para comprender el vertiginoso cambio social y tecnológico que vivimos, es sólo de 1992.

[2] Por todos los autores que sobre la materia se citarán en este trabajo, vid. Gómez de Liaño Fonseca-Herrera, Marta. *Criminalidad organizada y medios extraordinarios de investigación.* Madrid: COLEX, 2004.

[3] No puede reconocerse a nuestra actual sin el uso masivo por los ciudadanos de la ***VoIP*** (comunicaciones verbales a través de Internet), el correo electrónico, el acceso a las ***redes sociales*** como *Facebook, Tuenti, Hi5 o Twitter*, las descargas de contenidos P2P, la banca electrónica, la transferencia telemática de archivos de texto, imagen, video o sonido, etc. Casi la totalidad de los usuarios de redes sociales disponen de un terminal telefónico móvil avanzado con acceso a Internet. Entre estos, hay una importante presencia de móviles de última generación, con posibilidad de descargar aplicaciones y acceder a Internet de forma más avanzada.

[4] Fuente: Ministerio Turismo, Industria y Comercio. Situación del ***Plan Avanza2*** a 16 de diciembre de 2009.

- Hay más de 54,2 millones de líneas de ***telefonía móvil*** en España, de la clase **UMTS**[5] y **3G**[6] (lo que supone una penetración en el mercado del 113,6%), de las que 17,3 millones tienen acceso a la ***banda ancha móvil***.
- El número de usuarios del ***documento nacional de identidad electrónico*** supera los 13 millones (el 49% de las empresas usan la firma digital).
- Más del 70 % de los hogares cuentan con un ordenador y el número de dominios registrados en España supera el millón.
- Se ha producido un gran crecimiento del ***comercio electrónico***: de 1.530 millones de € en 2003 a 5.362 millones de € al final del 2007 (crecimiento espectacular que se debe al incremento sustancial de 3 millones de compradores *on-line*, alcanzando 8,8 millones de personas en 2008).
- Según el Instituto de la Juventud del Ministerio de Igualdad, uno de cada dos niños de más de diez años dispone de un teléfono móvil.

En datos recogidos en 2012 sobre el ejercicio anterior, las cifras se expanden y diversifican a nivel mundial respecto del 2010, con gran crecimiento de la telefonía móvil, con un 85 % de penetración, y los sorprendentes aumentos del parque de *smartphones*, tabletas, la profusión del acceso a las redes sociales, aumento de usuarios de Internet, penetración de la banda ancha, etc.[7]

Las exorbitadas cifras anteriores indican hasta qué punto forma parte de las vidas cotidianas de los ciudadanos el hecho de las TIC. Evidentemente, si están disponibles para ellos, podremos deducir que lo estarán también para los delincuentes, quienes no dudarán en hacer un uso malicioso de tan poderosas herramientas para lograr sus ilícitos fines. Consecuentemente, la Policía Judicial y todo el sistema de impartición de Justicia deberá estar preparado para garantizar la libertad de los primeros y dificultar un mal uso de la de los segundos.

Si se interpretasen los anteriores datos sólo como una amenaza y se incluyesen en un trabajo centrado en los problemas de raíz jurídico-procesal que van a ser

[5] *Universal Mobile Telecommunications System* o sistema de telecomunicaciones móviles.
[6] 3G es la abreviación de tercera generación de transmisión de voz y datos a través de telefonía móvil mediante UMTS. Permite la transferencia de archivos y la instalación de programas informáticos.
[7] Fuente: eEspaña 2012 a partir de la Organización Internacional de Telecomunicaciones ITU y *ComScore* (2012). Vid. *eEspaña 2012. Informe sobre el desarrollo de la sociedad de la información en España* de la Fundación Orange.

tratados con cierta profundidad, podría pensarse que la intención sería la de responder a una situación de inquietante excepcionalidad (un fenómeno delictivo de gran complejidad e insospechada evolución gracias un medio tecnológico en permanente expansión) con medidas de carácter extraordinario (con la presentación de un catálogo imaginativo de nuevos y vigorosos recursos legislativos orientados a la limitación de los derechos fundamentales, acompañados de unos no menos importantes recursos materiales y tecnológicos de todo tipo). Sin embargo, tal propósito quedará fuera de toda intención en el entendimiento de que el Estado de Derecho puede evolucionar en positivo sin renunciar a un exquisito respeto a los derechos fundamentales de las personas, por desconcertantes que puedan parecer las TIC.

No es el objetivo de este estudio, por tanto, la profundización o extensión de las medidas de limitación de los derechos fundamentales, pues la confianza en el Estado de Derecho no merece ser defraudada por la aportación de soluciones excesivas que ningún encaje tendrían en el sistema de libertades que se ha dado la sociedad.

En este sentido, las consolidadas garantías que se disfrutan en los países del entorno democrático de España y, junto a ellas, el amplio catálogo de derechos fundamentales[8] que asisten a todos los ciudadanos, ampliamente respaldados por la jurisprudencia, en nada tienen que sufrir porque se pretenda un mejor control de la delincuencia y la preservación de los derechos de quienes resulten ser víctimas de un delito. Por ello, cualquier solución que se propugne tendrá que hacerse en el marco de los principios generales que configuran el Estado de Derecho, buscando implementar, en todo caso, mejores medidas legislativas pero, eso sí, desprendidas del indeseable contrapeso que pudiera suponer un innecesario ahondamiento en la limitación de los derechos fundamentales.

Se ha hablado hasta ahora de la DO o grave lo que, a mi juicio, limitaría el escenario sobre el que se desea reflexionar, pues se excluiría torpemente a una

[8] Fundamentalmente, la Declaración Universal de Derechos Humanos, proclamada por la Asamblea General de las Naciones Unidas el 10 de diciembre de 1948; El Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales, hecho en Roma el 4 de noviembre de 1950; y Carta de los derechos fundamentales de la Unión Europea (2000/C 364/01).

amplísima gama de hechos delictivos que, sin ser a estas alturas novedosos, ni tener la conceptuación de ***graves***[9] a la luz de los arts. 13 y 33 del ***Código Penal*** (CP, en adelante), sí estarían observando un exponencial crecimiento que, inexplicablemente, no siempre estaría acompañado de la correspondiente ***alarma social***[10] debido, precisamente, a los efectos asociados al uso de las TIC y a la globalización.

Con la revolución de las TIC hacen su aparición el comercio electrónico ***(e-commerce)***, el acercamiento del banco a los clientes (***home-banking***), la gestión electrónica de los recursos de las empresas ***(e-management)***, la videoconferencia, el teletrabajo, el correo electrónico[11], la domótica, las redes sociales[12], etc.

Todo ello conlleva a su vez una revolución social sin precedentes, de la que los delincuentes no son ajenos. Si existe banca electrónica, se buscarán el modo de ser "atracadores electrónicos"; si existe comercio electrónico, falsificarán los datos de las tarjetas de crédito para robar bienes mediante encargos en red; si existe gestión empresarial electrónica, podrán robar los secretos industriales o los fondos de comercio; si existen redes sociales, podrán engañar a un menor para que se muestre

[9] El concepto "delito grave" no es pacífico tampoco en el derecho europeo: En el documento *Comunicación de la Comisión al Consejo y al Parlamento Europeo Panorama general de la gestión de la información en el espacio de libertad, seguridad y justicia*, de 26 de julio de 2010, se afirma que "*actualmente no existe en la UE una definición armonizada de «forma grave de delincuencia». Por ejemplo, la Decisión del Consejo que habilita a Europol para consultar el Sistema de Información de Visados (VIS) (Decisión 2008/633/JAI del Consejo, DO L 218 de 13.8.2008, p.129) define «delitos graves» haciendo referencia a lista de delitos establecidos en la orden de detención europea (Decisión 2002/584/JAI, DO L 190 de 18.7.2002, p.1). La Directiva sobre conservación de datos (Directiva 2002/58/CE, DO L 105 de 13.4.2006, p. 54) deja a los Estados miembros definir los «delitos graves». La Decisión Europol (Decisión 2009/371/JAI del Consejo, DO L 121 de 15.5.2009, p. 37) incluye otra lista de delitos definidos como «formas graves de delincuencia» que es muy parecida, pero no idéntica, a la lista de la orden de detención europea".*

[10] O, aún debiendo con todo merecimiento generar tal alarma, no sea la sociedad capaz de percibir la amenaza objetiva que presupone para su estabilidad y la dificultades para enfocar su eficaz neutralización.

[11] Según un estudio del Observatorio de Redes Sociales presentado en enero de 2010, el acceso al correo electrónico supera el 90 % de acceso diario de los internautas españoles de 16 a 45 años estudiados.
(Ver http://www.tcanalysis.com/uploads/2008/11/informe_observatorio_redes_sociales.pdf).

[12] Según un estudio del Observatorio de Redes Sociales presentado en enero de 2010, el 55% de los internautas españoles declara acceder a diario a redes sociales o comunidades *online*, aumentando este porcentaje hasta un 80% cuando se atiende a una frecuencia de acceso semanal. (Ver http://www.tcanalysis.com/uploads/2008/11/informe_observatorio_redes_sociales.pdf).

en posiciones sexuales explícitas ante la *webcam*; si existe teletrabajo, se podrá engañar con los contratos virtuales y así hasta el infinito[13].

Los hechos delictivos en este complejo ámbito no serían novedosos, pues se trataría de delitos que, en su estructura criminológica básica, estarían en su mayoría perfectamente tipificados en los sucesivos códigos penales, pero que sí habrían sufrido una inquietante evolución[14], no exenta de efectos insospechados tan sólo unos años atrás, debida precísamente a la tecnología de las comunicaciones[15].

Al estudiarlos superficialmente podría decirse de forma imprecisa que se trata de ***delitos informáticos***[16] (intercambio de pornografía infantil o captación maliciosa de las claves de banca ***telemática***, por ejemplo) como si el uso fraudulento de Internet fuese un delito en sí mismo que se consuma en un ordenador, sin trascendencia a la vida física.

Nada más lejos de la realidad: los actores de estos dramas afectan a los bienes jurídicos de siempre: la indemnidad sexual de un niño o el patrimonio de un particular, adquiriendo el ordenador o dispositivo electrónico el valor de un instrumento más o menos sofisticado, pero que es, al fin y al cabo, una mera herramienta en manos de un delincuente que la usa para atacar a su víctima.

---

[13] Para el Secretario de Estado Director del Centro Nacional de Inteligencia: *"En los últimos años, los nuevos riesgos emergentes asociados al uso masivo de las tecnologías de la información y comunicaciones (TIC), en todos los aspectos de nuestra sociedad, se han incrementado considerablemente. Esta situación, además, no es previsible que mejore en el futuro".* Fuente: Informe Anual 2007 del Centro Criptológico Nacional, perteneciente al Centro Nacional de Inteligencia en www.cni.es/ccn.

[14] Sobre la preocupación de encontrar tipos penales acordes con las nuevas formas delictivas, reflexiona VELASCO NÚÑEZ en el sentido de constatar el agotamiento de los tipos clásicos, lo que habría hecho necesario legislar para afrontar los nuevos ataques bienes jurídicos tales como la información o la seguridad en Internet. Vid. Velasco Núñez, Eloy. *Crimen organizado, Internet y nuevas tecnologías*. Conferencia impartida en la Escuela de Especialización de la Guardia Civil. Madrid, 2010.

[15] El acoso escolar, por ejemplo, tiene su expresión cibernética en el ***cyberbulling***. Según GABRIEL ALCONCHEL, del INJUVE, el 5% de los chicos entre 10 y 18 años ha manifestado un comportamiento agresivo a través de Internet. Sobre esto, afirma que "*el carácter virtual de esta nueva forma de acoso escolar, conocida como 'cyberbulling', ha supuesto que estas prácticas sean más visibles y habituales en la red que en el aula. La razón es la confidencialidad y el anonimato que provocan un mayor atrevimiento a hacer cosas que cara a cara no se atreverían*". Sobre el efecto despersonalizador de esta conducta y los problemas procesales para tratarla en sede penal girará buena parte de este trabajo. Fuente: http://www.elmundo.es/elmundo/2010/06/21/espana/1277127983.html.

[16] Para VELASCO NÚÑEZ, los delitos informáticos *"…no son un nuevo tipo de delitos, sino formas delictivas novedosas, ya que, más que hallarnos ante una nueva categoría delictiva, nos encontramos ante la irrupción de un nuevo mecanismo tecnológico que ha hecho tambalear el sistema penal".* Vid. Velasco Núñez, Eloy. *Delitos cometidos a través de Internet. Cuestiones procesales.* Tesis doctoral. Las Rozas (Madrid): La Ley, 2010, pág. 18.

A la luz de los cambios tecnológicos y de su incidencia en el mundo del delito, cabría preguntarse si un teléfono móvil es solamente un instrumento de comunicación verbal o escrita establecida en canal cerrado entre dos personas o, llegado el caso, si el terminal podría ser también un elemento por completo ajeno a las comunicaciones personales cuando se usa únicamente para detonar una carga explosiva al hacerle una llamada desde otro terminal[17]; o, tal vez, si es un acto de comunicación el uso oculto de un servidor de servicios de Internet para canalizar y apostar contra uno mismo en ***casinos on-line*** el dinero que se quiere blanquear, tras actuar a la vez como perdedor y ganador del juego.

En los ejemplos se han utilizado un teléfono móvil y una conexión a un servidor de Internet en unos claros actos de comunicación electrónica, pero debería formularse la pregunta de si estos actos estarían o debieran continuar, total o parcialmente, amparados por el art. 18.3 CE[18].

Con iguales razones, y si la respuesta a la anterior pregunta fuera negativa, podría plantearse la sistematización de las clases de comunicación electrónica distinguiendo entre las que sí suponen la transmisión de ideas en canal cerrado de aquellas otras – masivas, según puede verse – que no suponen sino un mero acto de comunicación técnico o instrumental de datos.

Finalmente, parece que, en cualquier caso, merecería una reflexión profunda la consideración sobre la intensidad de la protección constitucional para aquellos datos

[17] Un teléfono móvil o un ordenador, además de lo que se ha dicho en referencia a su uso para las comunicaciones personales, constituye también un sistema para activar dispositivos tecnológicos de cualquier género, de forma maliciosa o no (explosionar una bomba u ordenar una transferencia bancaria, por ejemplo), al mismo tiempo puede ser utilizado como un sistema para difundir públicamente informaciones, una herramienta para instalar software en otros ordenadores, un acceso a las redes sociales en canal abierto, una ventanilla bancaria, un instrumento para comerciar, un utensilio para satisfacer pasiones, un listado de posiciones GPS en tiempo real, un archivo de audio, fotografía y video, un repositorio de textos e informaciones diversas, un sistema de mensajería de voz y datos, y, en definitiva, un larguísimo etcétera de otras cosas en sorprendente evolución.

[18] Se analizarán más adelante también las comunicaciones en canal abierto, como las que se insertan en las redes sociales y chats, en los que el uso de Internet sería semejante al de un tablón de anuncios o un periódico. Recientemente, la sociedad ha asistido a la publicación en red de videos y entradas de texto relacionadas con posteriores homicidios, tales como el caso de una niña en Seseña, en marzo de 2010, o el asesinato de seis alumnos y dos adultos en Tuusula (Finlandia), en noviembre de 2007.

asociados a la comunicación[19], pero entendidos de forma ajena a la comunicación en sí misma.

Sobre todas estas reflexiones, dice SALOM CLOTET que:

> *"…esta extraordinaria expansión de las redes de telecomunicaciones trae también aparejada nuevas situaciones carentes hoy de regulación y sobre las que seguramente resulte precisa la intervención del Derecho. Las dificultades del legislador para comprender y conocer el mundo digital dificulta el proceso legislativo. La dinámica de las nuevas tecnologías sobrepasa a la dinámica legislativa. El resultado es una inadecuación o vacío legal en torno a los aspectos de la Red, que afectan a todos los órdenes del Derecho, incluido el penal"*[20].

Por todo ello, y con objeto de tratar de precisar algo más el heterogéneo ámbito de este estudio sería tanto más útil definirlo desde un punto de vista operativo como el de la ***delincuencia compleja***[21], por las razones que serán de fácil comprensión, ya que no sólo se tratarán las formas de DO o grave, cuya importancia se describe por sí misma, sino también de formas delictivas de otra naturaleza, pero muy comunes a día de hoy, para cuyo descubrimiento y tratamiento penal se necesitará de instrumentos procesales adecuados a la evolución tecnológica que los sustenta y cuya aplicación deberá, lógicamente, basarse en el ***principio de proporcionalidad***.

Se agruparán con esta terminología todos aquellos fenómenos propios de la emergente delincuencia tecnológica, junto con los demás en los que el uso de las TIC haya sido preponderante o determinante para llevar a cabo la maquinación criminal.

---

[19] Es necesario reconocer que tales datos, aunque en sí mismos sean ininteligibles para el ser humano (se trataría de series alfanuméricas sin significado directo), sí pueden ser interpretados en el marco de un tratamiento de inteligencia del que se podrían obtener conclusiones al margen de su relación con concretos actos de comunicación material. Por ejemplo, en un listado de llamadas a números de abonado telefónico puede determinarse con cuál de ellos existe una relación preferencial sin entrar en saber quién es el abonado ni cuál es el contenido de la comunicación.

[20] Vid. Salom Clotet, Juan. *Delito informático y su investigación. Delitos contra y a través de las nuevas tecnologías. ¿Cómo reducir su impunidad?* Madrid: Consejo General del Poder Judicial, 2006, Vol. III, págs. 93-129, pág. 95.

[21] No debe dejarse por ello de constatar la imprecisión del término elegido. Para algunos autores, esta terminología sería equivalente al uso de ***Delincuencia Telemática***, tratado de agrupar a aquellos delitos que, de una u otra forma, hacen uso en su dinámica criminal de la suma de la informática y las comunicaciones facilitadas por las TIC.

Las formas delictivas que se producían hasta los principios de los años noventa del pasado siglo, que es cuando se inicia el estallido y popularización de las TIC, respondían en general a formas clásicas del delito, cuyos contornos bien definidos encontraban una respuesta procesal y penal adecuada. Por el contrario, el contraste con las formas tecnificadas actuales resulta notorio.

En efecto, las modalidades comisivas clásicas exigían la presencia física del autor en el lugar del crimen, lo que aumentaba el riesgo de ser detenido por las ***Fuerzas y Cuerpos de Seguridad el Estado*** (en lo sucesivo, FCSE). Actualmente, puede actuarse a través del ***espacio virtual*** en las fases más comprometidas de la dinámica delictiva y sin la presencia del autor en el lugar de los hechos e, incluso, difuminando o enmascarando el rastro electrónico.

En las formas clásicas, los actos criminales se producían con inmediatez a la víctima (por lo que podía percibirse su aspecto o su dolor o, simplemente, sufrir sus acciones de defensa) o al objeto del crimen (dinero, robo de bienes muebles de todo tipo, drogas, armas, etc.). La probabilidad de dejar rastros aprehensibles como prueba para un futuro proceso penal aumentaba considerablemente y, con ello, el riesgo de ser detenido y enjuiciado (huellas dactilares, reconocimiento de víctimas y testigos, fibras textiles, restos orgánicos corporales, captación de imágenes, etc.). Hoy en día, sin embargo, muchas formas comisivas se basan, precisamente, en la ausencia de inmediatez con la víctima (de las que el autor se formará, en el mejor de los casos, tan sólo una imagen difusa cuyas connotaciones negativas podrá racionalizar e incluso ignorar) o el objeto del delito. La conciencia de culpa del autor se anestesia en este escenario sin mucha dificultad. Las víctimas, en bastantes ocasiones, ni siquiera tendrán conciencia de haberlo sido (robos de identidad o datos personales, uso inadvertido y malicioso de sus ordenadores por *hackers*, captación de imágenes con motivación sexual, etc.).

En las formas descritas anteriormente, se produce un desconcertante ***efecto disociativo*** entre el autor y la víctima o los objetos del delito cuando se interactúa en el ciberespacio debido a la ausencia de inmediatez entre ambos. Este efecto

disociativo ayuda a resolver el **conflicto personal del *paso al acto***[22], por poder derivar o residenciar, consciente o inconscientemente, la autoría en terceros[23] o experimentar un tranquilizador ***reforzamiento de conducta*** al constatar, no sin sorpresa, que en la red existen innumerables personas anónimas con el mismo problema[24], lo que aliviará los posibles ***sentimientos de morbidez*** o excepcionalidad de la ***conducta desviada*** propia[25], es decir, se produce un efecto de ***despersonalización de la conducta criminal***. La relación causa-efecto que puede ser observada por un individuo que interviene como actor en un escenario físico, según lo explicado, quedaría interrumpida, deformada o, al menos, anestesiada, cuando se interactúa criminalmente en el ciberespacio.

La conspiración para cometer delitos se debía hacer mediante la concertación previa de sus autores en un espacio físico[26], en contraposición a la actual coordinación dinámica sostenida por la disponibilidad, versatilidad y diversificación de las comunicaciones electrónicas con las que puede conspirarse en el mundo de las TIC[27]. Consecuentemente, la ***cultura de supresión de la prueba***[28] tenía antaño unas posibilidades mucho más reducidas para que los delincuentes evitasen la acumulación

[22] Resolver todos los obstáculos para decidirse a cometer un delito, por execrable que al autor pueda parecerle, al no tener contacto físico con la víctima ni asumir el riesgo de ser detenido por la policía.

[23] *"No cometo delitos contra la propiedad intelectual, sino que los comenten los que copian y cargan películas en la red", "son otros los que hacen fotografías o videos pornográficos en los que se abusa de los niños", "el dinero está en la red y no tiene dueño", "el ataque de hacking es un reto intelectual excitante y no un daño material o una denegación de servicio a los sistemas vulnerados"*, etc.

[24] El caso de la pedofilia resultaría paradigmático, al comprobar con sorpresa los pederastas la existencia en la red de innumerables personas de su misma condición, lo que los haría sentirse dentro de una aparente y tranquilizadora normalidad, lo que ha propiciado incluso movimientos tan inquietantes como el ***Boylover*** (Grupo de presión mediática que considera la pederastia como una inclinación sexual aceptable e incluso normal).

[25] Para SALOM CLOTET, "*Internet es un escenario en al que la persona, sujeta a los cánones sociales e incapaz de revelarse contra ellos, puede encontrar vías de escape a su despersonalización, un instrumento para ejercer el papel liberador del individuo. El entrar en el mundo virtual de la red, donde no existen los mismos patrones sociales del mundo real, permite canalizar y liberar las inquietudes sociales del individuo. Es en definitiva el individuo solo ante el ordenador, oculto tras la pantalla, no mostrando su persona y sus condicionantes, el individuo anónimo encuentra una válvula de salida en el mundo virtual, donde se libera…cualquier intervencionismo en la red por parte de los Estados, será interpretado como una amenaza a su libertad*". Vid. Salom Clotet, Juan. *Delito informático y su investigación…op. cit.*, págs. 93-129.

[26] Todo lo más mediante el uso de la telefonía fija, lo que no permitía una coordinación dinámica efectiva. En contadas ocasiones, se utilizaban de forma muy limitada los aparatos celulares de radiotelefonía.

[27] Por ejemplo, el uso de cafés-Internet, ocultación de IP, falsa identificación del propietario de teléfonos móviles, personalidades falsas en redes sociales, software de secrafonía, etc.

[28] Ver más adelante.

de evidencias en su contra por estar interactuando en un escenario físico, por más que el espacio electrónico también ofrezca medios técnicos que permiten rastrear los sucesos de tal naturaleza.

Podría añadirse, como efecto novedoso de la *cultura de supresión de la prueba,* el hecho de que la misma tecnología, maliciosamente utilizada por los delincuentes, se convertiría en sí misma, no sólo en un nuevo medio ideal para concebir formas comisivas originales, sino también en un medio para ocultar las rastros de su existencia[29].

Por todas las razones anteriores (y sobre todo por la accesibilidad, anonimato y uso absolutamente masivo de las TIC), se puede estar produciendo también un efecto colateral sin precedentes sobre la ***cifra oscura***[30] del delito. Algunos ejemplos pueden ayudar a la compresión de este efecto:

- En banca electrónica, y aunque las investigaciones policiales o los propios clientes hayan detectado casos de ***phising***[31] o ***farming***[32], se muestran reticentes las entidades a presentar denuncias para evitar frente a sus clientes una eventual pérdida de su crédito comercial y su solvencia en

[29] Según un estudio, por ejemplo, el 6% de las personas que han sido descubiertas con pornografía infantil utilizaba tecnología de cifrado, el 17% empleaba programas informáticos protegidos por contraseñas, el 3% usaba programas informáticos que eliminan las pruebas y el 2% hacía uso de sistemas de almacenamiento remoto. Vid. Finkelhor, David, Mitchell, Kimberley J. y Wolak, Janis. *Child Pornography Possessors Arrested in Internet-Related Crime: Findings From the National Juvenile Online Victimization Study.* Alexandria Va. : National Center for Missing and Exploited Children, 2005, pág. 9.

[30] La cifra oscura varía en función de la clase de estadística, policial o judicial: no todo delito cometido es perseguido, no todo delito perseguido es registrado; no todo delito registrado es averiguado por la policía; no todo delito averiguado es denunciado; la denuncia no siempre termina en juicio oral; el juicio oral no siempre termina en condena. La elaboración social y judicial del delito va haciéndose cada vez más precisa en cada nivel hasta llegar a la condena firme de una persona; pero también va aumentando en cada nivel la cifra oscura. En el lenguaje generalmente empleado se caracteriza como "cifra oscura" la relación entre la criminalidad real y la registrada oficialmente (es decir, que ha llegado a las autoridades competentes). Debe añadirse a todo ello el devastador efecto de la tardanza de, a veces, más de diez años, en producirse el acto del juicio oral.

[31] Acceso a las claves personales de banca electrónica mediante engaño (envío de correos simulando proceder del banco). El concepto de ***seguridad electrónica*** viene hoy en día relacionado con la solvencia de las entidades bancarias en soportar los eventuales fraudes de sus clientes, más que en la calidad de las contramedidas tecnológicas que aseguran, o deben asegurar, las transacciones electrónicas.

[32] Derivación del internauta a páginas *web* falsas con la intención de obtener sus datos personales y sus claves de acceso a los servicios electrónicos (normalmente, banca electrónica).

materia de seguridad y, consecuentemente, ver reducido su presencia en el mercado virtual[33].

- En los casos de pornografía infantil en red, pueden los padres no interponer denuncia[34] para preservar la estabilidad emocional y el anonimato de sus hijos abusados o, más simplemente, desconocer que se han captado sus imágenes.
- En los robos de datos de los usuarios conservados por la administración electrónica, sus gestores prefieren resolver el problema sin reclamar la intervención policial o judicial para no quebrar la confianza de los ciudadanos.

Junto a estos ejemplos, podrían añadirse otros muchos que, pese a la constatación de la ***Policía Judicial Específica*** (en adelante PJE), al menos indiciaria, se optaría por no presentar la denuncia formal, lo que entorpece considerablemente el éxito final de la Justicia. Puede hablarse en este caso de una inasumible ***extensión de la victimización***, ***doble victimización*** o ***victimización secundaria*** al derivarse la condición de víctima, no ya al usuario que fue personalmente y en primera instancia el objetivo del delincuente – y que por ello no sufrirá las consecuencias de su delito -, sino, en segundo término, a la estructura pública o privada de que se trate[35].

Evidentemente, no sólo se pierde con todo lo anterior el efecto disuasivo de la acción policial o judicial, sino que esta inquietante inhibición actúa como un estímulo o vector de crecimiento de la delincuencia compleja. No debe olvidarse que la delincuencia moderna, en franca y expansiva evolución, ha aprendido a actuar con técnicas parecidas a las que emplearía la industria o el comercio para analizar el mercado y situarse en él sin competencia o rival posibles (lo que incluye a las FCSE y la misma Justicia), estudiando las posibilidades y las vulnerabilidades ocasionadas por

[33] Según el documento correspondiente al 12º Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal *Novedades recientes en el uso de la ciencia y la tecnología por los delincuentes y por las autoridades competentes en la lucha contra la delincuencia, incluido el delito cibernético*. A/CONF.213/9, pfo. 8. Vid. Mitchison, Neil y Urry, Robin. *Crime and abuse in e-business.* [ed.] IPTS Report. 2001, págs. 19-24. Vol. 57.

[34] Por más que se trate de delitos públicos.

[35] Vid. Fernández Teruelo, Javier Gustavo. *Cibercrimen. Los Delitos cometidos a través de Internet.* Madrid: Constitutio Criminalis Carolina, 2007, pág. 33.

todos los efectos estudiados anteriormente para aprovecharse de la situación y sin que para ello hayan de asumirse demasiados riesgos[36].

SALOM CLOTET, al efecto y haciendo evidente la necesidad de que la PJE tenga un acceso de mayor dinamismo a la ***inteligencia criminal sobre las TIC*** acorde con el signo de los tiempos, ilustra diciendo que:

> *"Las técnicas de anonimato, el **IP Spoofing**[37], uso de **proxis**[38] anónimos, servidores de **correo web anónimo**[39], utilización de **anonimizadores web**, el uso de **cibercentros**[40], carentes de la más mínima regulación, el uso de telefonía móvil GPRS con tarjetas prepago para ocultar identidades o dificultar identificaciones[41,42], la conectividad a través de redes **Wi-Fi**[43] ajenas carentes de seguridad, el uso de **programas maliciosos tipo troyano**[44] que permiten el control remoto de equipos, las **técnicas de ingeniería social**[45] que permiten suplantar identidades capturando contraseñas y vulnerando el derecho a la*

[36] Por si fuera poco, para SILVA SÁNCHEZ, *"dos son las características más significativas de la delincuencia de la globalización: por un lado se trata de una criminalidad en sentido amplio, organizada. Por otro, existe una disociación entre la ejecución material directa y responsabilidad, lo que determina que el resultado lesivo pueda aparecer significativamente separado, tanto en el espacio como en el tiempo, de la acción de los sujetos más relevantes en el plan delictivo: el centro de poder"*. Vid. Sansó-Rubert Pascual, Daniel. *Criminalidad organizada transnacional…op.cit.,* pág. 219.

[37] Sistema malicioso de enmascaramiento de la dirección IP que identifica e individualiza a un terminal informático conectado en red, ofreciendo una identidad falsa.

[38] Servidores informáticos a través de cuya IP, que está enmascarada, el verdadero usuario actúa para acceder maliciosamente y de forma oculta a la red.

[39] *Id.* Nota anterior.

[40] Lugares de acceso público a la red que no exigen la identificación del cliente o usuario (Por ejemplo, los cibercafés o las Wi-Fi instaladas en aeropuertos o bibliotecas).

[41] Más adelante se explicará el fraudulento efecto que la LCDCE ha traído sobre el particular, al propiciar que determinados individuos usen su identidad para facilitar tarjetas prepago a los delincuentes.

[42] La sofisticación y diversidad llega hasta tal punto que existen en el mercado sistemas de comunicación de *VoIP* con "rasca", por el que el cliente adquiere una tarjeta con un código oculto tras una capa de pintura opaca removible. Con ese código, activa un servicio prepagado por el que su terminal contacta con un número fijo de la compañía de la Red Telefónica Conmutada, que le da acceso directo al terminal llamado. La comunicación va codificada y bajo el *Protocolo TCP/IP*, por lo que es operada por proveedores de servicios de la sociedad de la información y no por operadores de comunicaciones electrónicas o de redes públicas de comunicaciones. Los teléfonos *VoIP* se identifican con un código alfanumérico que empieza por 7.

[43] Sistema de acceso sin cable a redes abiertas o restringidas, tanto públicas como privadas.

[44] Programas que se instalan en ordenadores ajenos y que permiten su control malicioso por parte de terceros sin que el propietario se percate, lo que, entre otras muchas cosas, permite su utilización para el enmascaramiento de la identidad del delincuente cuando actúa en red.

[45] Robo de identidad (Por ejemplo, la identidad del cliente de una entidad bancaria on-line) y manipulación de los perfiles personales en redes sociales como *Twitter, Facebook, Tuenti*, etc. Sobre el concepto genérico de ***ingeniería social***, como método de influir en la voluntad de las personas para que actúen de un determinado modo, es útil la lectura del libro de Hadnagy, Christopher. *Ingeniería social. El arte del hacking personal.* Ed. Madrid: Anaya, 2011.

*intimidad de las víctimas, la explotación de **"bugs" o agujeros de seguridad mediante "exploits"**[46] diseñados al efecto para facilitar el trabajo, que permiten el control de equipos ajenos, el uso de **diccionarios y robots**[47] para ataques de fuerza bruta contra sistemas de encriptación, el envío de los famosos **virus**, bombas lógicas, gusanos, programas no deseados que causan daños a los sistemas informáticos y que se reenvían a otros **botnets**[48,49] bajo control de delincuentes informáticos, el envío de publicidad no deseada (**spam**), las **técnicas de denegación de servicios**[50] (DoS) para interrumpir la operatividad de sistemas informáticos, el mantenimiento de contenidos en "paraísos informáticos" para preservarlos de cualquier control o investigación judicial, el uso de **programas de encriptación y esteganografía**[51] para ocultar contenidos, la inserción de contenidos lesivos contra el honor o la imagen de personas, el envío de mensajes amenazantes, la utilización de productos bancarios para estafar, el engaño apoyado en contenidos falsos en red…"*[52].

[46] Procedimientos diseñados tras analizar los fallos o vulnerabilidades que los programas o sistemas operativos puedan presentar en sus códigos informáticos para que los equipos que los tienen instalados puedan ser usados maliciosamente por los delincuentes.

[47] Sistemas de envío automatizado masivo de datos para obtener nombres de usuario y contraseñas de acceso a los equipos atacados.

[48] Redes de ***ordenadores esclavos*** que se manipulan para lanzar intrusiones de alta potencia (es decir, que la *botnet* pone a disposición de los atacantes una alta capacidad computacional que es resultado de la suma de las potencias de cada ordenador individual infectado, con lo que pueden ejecutarse ataques de una extraordinaria capacidad telemática) y diversa finalidad mediante los que se pretende, entre otras cosas, realizar a ataques de denegación de servicio o DoS (ver más adelante). España, según el informe de Microsoft, ocupa el puesto más alto de Europa en número de ordenadores infectados en el segundo cuatrimestre de 2010, con 382.000 terminales. Vid. *Security Intelligence Report. Volume 9, January trough june 2010*.

[49] En el diario digital www.elconfidencial.com, de fecha 7 de noviembre de 2012, con referencia al documento de análisis *Trend Micro Incorporated Research Paper 2012 Russian Underground 101,* se afirma que *"en el mercado 'underground' de Rusia se puede contratar desde un ataque DDoS por 10 dólares la hora, 150 dólares la semana o 1.200 al mes; lanzar un millón de correos electrónicos 'spam' por 10 dólares o 'hackear' una cuenta de Facebook, Twitter o Gmail a partir de 130 dólares"*.

[50] Literalmente, bloquear los ordenadores a base de lanzarles peticiones masivas de información, lo que impide el funcionamiento normal para el que están destinados (Por ejemplo, enviar tal cantidad de peticiones a la página *web* de la Agencia Tributaria de forma que esta resulte inaccesible para los ciudadanos por saturación).

[51] Métodos para mantener oculta la información real que contienen los archivos de imagen que se envían en red. El sistema básicamente funciona mediante la creación de huecos de código binario en una imagen que se completan o rellenan con los de otra mediante el uso de un programa informático específico (Por ejemplo, el programa ***Estéganos*** permite que en una fotografía inocua se oculte una fotografía de pornografía infantil).

[52] Vid. Salom Clotet, Juan. *Delito informático y su investigación…op. cit.,* pág.98.

En definitiva, que la complejidad de las TIC arma a los delincuentes con sofisticadas e imaginativas herramientas informáticas, en constante evolución, dirigidas a la anonimización de los autores, el ocultamiento de la acción, la elminación de rastros o evidencias, la interposición de contramedidas para anular la capacidad de investigación y, como colofón, la posibilidad de alcanzar a numerosos objetivos en la escena mundial de una forma instantánea, masiva, inadvertida y altamente dañina para todo tipo de bienes jurídicos de las innumerables víctimas potenciales.

Otro de los factores que permiten el crecimiento exponencial de los nuevas formas comisivas es el de una cierta ***anomia[53] del ciberespacio***, que se produce en dos formas concurrentes: Una ***anomia aparente***, vehemente interpretada por el usuario e incluso por organizaciones sociales y políticas[54], por la que el infractor cree interactuar en un espacio ajeno al Derecho[55], defendiendo posiciones ciertamente discutibles respecto de su uso de la red; y una ***anomia real***, por no existir actualmente un cuerpo jurídico consolidado y eficaz que resuelva y supere los innumerables problemas de regulación de la actividad del ser humano en el ciberespacio y que han excedido a las previsiones más acertadas. Se ha de apostar, como no puede ser menos, por el Derecho como mejor forma de garantizar el ordenamiento de una faceta de la actividad humana tan digna de ello como cualquier otra, sin perder por ello el carácter de lugar de libertad, comunicación, creación, comercio y cultura que debe ser el ciberespacio.

A los anteriores problemas, se deben añadir los que comporta la ***extraterritorialidad de las acciones delictivas***, lo que conlleva a su vez no sólo los

[53] En su acepción del diccionario, ausencia de Ley.

[54] En Suecia el Partido Pirata llegó a ser la tercera fuerza política de su parlamento con un controvertido programa sobre el acceso a la información de los ciudadanos.

[55] Para las Naciones Unidas, *"El debate en curso en torno a la Gobernanza de Internet apunta al hecho de que Internet no es una red distinta de las basadas en la infraestructura de comunicaciones transnacionales e incluso nacionales, por lo cual la Internet debería ser también objeto de legislación, y los legisladores y las entidades encargadas de hacer cumplir la ley han iniciado ya el proceso de formular normas jurídicas en las que se preconiza un cierto grado de control central".* Vid. Documento de la Unión Internacional de Telecomunicaciones de 2009 *"El ciberdelito: guía para países en desarrollo"*, pág. 75, y Sadowsky, George, Zambrano, Raúl y Dandjinou, Pierre. *Internet governance: A discussion document.* United Nations Task Force, 2004.

consabidos problemas de jurisdicción, sino de mera operatividad de las formas de cooperación policial y judicial en la escena internacional para poder contrarrestarlas[56].

Un buen ejemplo de las dificultades que plantea la extraterritorialidad – esta vez salvadas, no sin la correspondiente discusión doctrinal - lo supondrían los ***registros virtuales del ciberespacio*** por los que la PJE, mediando el correspondiente mandamiento judicial y conociendo por otra vía igualmente legítima las claves de acceso a los servidores que contienen pruebas electrónicas, obtendrían copia de los documentos contenidos independientemente del lugar donde se halle físicamente ubicado el continente (cualquier soporte informático físico), suscitándose los evidentes problemas de extraterritorialidad y soberanía, resueltos bajo el ***principio de ubicuidad***[57,58].

[56] Este espinoso asunto, que se tratará más adelante, puede observarse al examinar los ingentes pero baldíos esfuerzos de la UE y los demás países avanzados para dotarse de instrumentos jurídicos adecuados a la magnitud del problema. Para SALOM CLOTET, *"la globalización de la sociedad, especialmente de los mercados y de las comunicaciones, lleva también aparejada una pérdida de identidad y soberanía de las sociedades y sus territorios, dado el carácter transnacional de este fenómeno"*. Vid. Salom Clotet, Juan. *Delito informático y su investigación…op. cit.,* págs. 93-129.

[57] En este sentido, dice VELASCO NÚÑEZ que *"el principio de ubicuidad, al que ya se ha hecho referencia… formulado por el Acuerdo de la Sala 2ª del TS de 3 de febrero de 2005 ("El delito se comete en todas las jurisdicciones en las que se haya realizado algún elemento del tipo. En consecuencia, el Juez de cualquiera de ellas que primero haya iniciado las actuaciones procesales, será en principio competente para instrucción de la causa"), valida, por razones de competencia judicial para España, las inmisiones y aprehensiones que por meras razones de intermediación tecnológica se hagan desde cualquier punto del territorio español con autorización judicial – y aún sin ella, para casos de extrema urgencia – aunque pasen y se vehiculicen en parte por el territorio de otros Estados, siempre que tengan relación con la investigación de un delito que en todo o en parte despliegue parte de su acción o de sus efectos en el territorio jurídico legal a que se refiere la protección recogida en el art. 23 LOPJ…el mero viaje de ceros y unos por la red internacional, o la transmisión no rectilínea de los mismos, no convierte en propietario del lugar por donde circulan en cable o magnéticamente – wireless – a nadie…el criterio de la ubicación tecnológica del prestador del servicio tampoco otorga exclusiva..."*. Vid. Velasco Núñez, Eloy. *Delitos cometidos a través de Internet…op.cit.,* págs. 123 y ss.

[58] En el caso de la OP. DRACO (Diligencias Previas núm. 1579/06 del Juzgado de Instrucción núm. 3 de Marbella), la solución jurídica para ordenar el registro virtual de un servidor privado en el extranjero, valorada previamente en forma clásica la proporcionalidad de la medida adoptada por el Juez de Instrucción, no necesitaba entrar a dilucidar el lugar en que se encontrase la evidencia digital, sino la accesibilidad virtual a la prueba, esto es, la serie de ceros y unos (código binario usado por los ordenadores) accesible a través del ciberespacio, si bien es cierto que, una vez obtenida esta por la indicada vía, se reiteró posteriormente mediante la correspondiente Comisión Rogatoria Internacional, en la que se invocó el Convenio sobre la Ciberdelincuencia de 23 de noviembre de 2001, lo que propició la obtención de una copia directa a través de los servicios judiciales y policiales del país requerido. Esta experiencia confirma el valor que tiene la inteligencia policial dentro del proceso penal para dinamizarlo, pues eso fue lo que realmente se obtuvo mediante el registro virtual y el valor que por su parte supuso la segunda acción de cooperación judicial y policial internacional, en la medida en que se consolidó procesalmente el valor de la prueba.

Las consideraciones incluidas anteriormente plantean un panorama delincuencial en el que se hace difícil la actuación de la PJE según las formas procesales clásicas, al menos, en materia de análisis del uso de las comunicaciones como parte de la maquinación criminal.

En efecto, la investigación actual tiene una faceta dominante en cuanto al análisis del factor tecnológico, no siempre relacionado con el acto de la comunicación material en sí y que hace que tal estudio, sea cual fuere su naturaleza, ocupe un lugar central en el desarrollo de cualquier labor indagatoria. Es decir, que sin la ***Inteligencia sobre las comunicaciones electrónicas*** (en adelante ITCE) resultaría prácticamente inviable cualquier planteamiento de investigación por parte de la PJE.

En este sentido, la ***trazabilidad de las comunicaciones electrónicas***, basada en su naturaleza digital y en la estructura de las redes, se convierte en la actividad troncal de los análisis de ITCE, al facilitar a la PJE diversos datos de gran transcendencia para la investigación. Lo esencial de esta actividad, como no podía ser de otra forma, es vincular un hecho delictivo con su autor de tal manera que pueda llegar a acreditarse en el acto de juicio oral.

Entre ambos se interpone un instrumento tecnológico cada vez más sofisticado, pero siempre susceptible de un análisis forense. Sin embargo, su mero análisis raramente ofrecerá por sí mismo datos determinantes que identifiquen inequívocamente a la persona penalmente responsable de los delitos que con este instrumento se hayan cometido. Pero este efecto no es, por lo demás, extraño a la dinámica probatoria clásica.

Si se recurre al ejemplo balístico, se verá que un proyectil puede relacionarse sin margen de duda con la concreta arma que lo disparó; que una huella digital sobre esta última probará que la persona que la imprimió la sostuvo en algún momento entre sus manos; que un resto orgánico pertenecerá a esta misma persona, etc. Pero lo que hasta este momento no estará aún claro, pese a todo lo anterior y por determinante que parezca, es que sea además el autor del homicidio que se investiga. Será necesario añadir aún más evidencias e indicios, normalmente de forma ajena al arma del crimen, que prueben, por ejemplo, que el sospechoso estaba además en el

lugar y el momento del crimen, que tenía un motivo, que hubo un testigo que observó la acción, etc.

Por tanto, el instrumento tecnológico deberá ser objeto de la misma consideración para lograr determinar cuál fue su papel en relación con el autor de la maquinación que se enjuicia.

Pero, en el caso que centra este trabajo, cuando las consecuencias del delito son visibles únicamente en el evanescente ***mundo virtual***[59], más allá del propio instrumento tecnológico empleado, el investigador deberá procurar la observación del ilícito para acreditar su existencia (no se debe olvidar que, al fin y al cabo, la información virtual no es sino una sucesión compleja de datos expresados en código binario, esto es, de una desconcertante sucesión de ceros y unos) y, siempre que técnicamente sea posible, obtener una copia digital para su valoración por la Autoridad Judicial.

En ello juega un papel fundamental la fe pública ejercida por el ***Secretario Judicial***[60] al conservar una copia precintada del contenido original que, por su parte, será objeto de análisis forense de la PJE. Casi todos los sistemas de copia, bien sean por *hardware* o *software*, permiten calcular como medio de salvaguarda la firma digital del soporte, lo que garantiza técnicamente la identidad entre original y copia, circunstancia esta de gran trascendencia procesal, no ajena a las controversias. Este

[59] Tanto es así, que cada día son más los internautas usan del denominado ***cloud computing*** o almacenamiento en nube de sus contenidos en servidores informáticos conectados en red. Se hace previsible que, a medida que mejore la conectividad a Internet, los ordenadores serán cada vez más sencillos, pequeños y económicos y no almacenarán en su disco duro los contenidos, sino que se alojarán en los servidores de la red, disponibles para el usuario en cualquier momento desde cualquier terminal, propio o ajeno, y aptos para compartirlos. El primer estadio de este proceso es el ***webmail*** (correo *web*), las cuentas de los grandes servidores gratuitos de correo electrónico como *Hotmail, Gmail*, *Yahoo*, etc., que almacenan nuestros mensajes de correo y a los que se accede a través de interfaces *web*. Para la ONU, junto con la *VoIP*, el *cloud computing* es uno de los nuevos retos para la investigación (Vid. 12º Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal *Novedades recientes…op. cit.,* pág. *2).* Como es de imaginar, la investigación criminal en este ámbito virtual se volverá tanto más compleja. Adviértanse, por su parte, las connotaciones procesales que todo ello puede traer.

[60] Dice SALOM, con cierto desánimo, que las deficiencias procesales al efecto son tales que *"la experiencia del GDT es que ante la anomia existente, algunos Secretarios Judiciales actúan prestando toda su colaboración y otros se amparan en la alegalidad para no aportar su valor de garante judicial".* Fuente: Documento sobre *Metodología de la investigación informática* del Grupo de Delitos Telemáticos de la Unidad Central Operativa de la Guardia Civil.

elemento de adveración se realiza mediante un algoritmo matemático llamado ***hash***[61], lo que facilitará los contrastes necesarios en el acto de juicio oral.

Se puede constatar, por tanto, un gran salto evolutivo en las formas de investigación de la delincuencia, sin que ello haya conllevado la necesidad de renunciar por completo a las formas clásicas de adquisición de la prueba por parte de la PJE[62].

Este salto se observa desde una época, aún reciente, en la que la aprehensión del dato relevante para el proceso penal se producía en un plano físico y se obtenía mediante actividades de vigilancia y seguimiento de los objetivos del caso, y llega a una actualidad en que la prueba se ha de obtener, muchas veces de forma preferente, en el espacio virtual. En cuanto a la técnica policial, se está hablando del salto de la vigilancia a la ***tecnovigilancia*** o, más acertadamente, de una mezcla equilibrada entre ambas.

En lo que interesa, se observa una notable diferencia entre estas dos técnicas ya que, contrariamente a la muy reiterada manifestación de temores por parte de la doctrina y la jurisprudencia de convertirse la PJE en un "Gran Hermano", la tecnovigilancia ofrece en términos generales un saldo de penetración en la esfera de la intimidad de los investigados notablemente menor que la vigilancia clásica.

Esto es así porque ahorra tiempo de observación de las actividades humanas que no interesan a la investigación, centrándose, además, en la obtención de datos precisos e irrefutables, por haber sido obtenidos por medios técnicos objetivos.

---

[61] Este algoritmo conjuga diversos parámetros informáticos asociados al archivo original de que se trate, haciéndolo de forma independiente a su nombre, mediante la aplicación de determinados procesos matemáticos orientados a establecer su identidad. Por lo tanto, cualquier manipulación de las copias de tales archivos conlleva una variación automática de su algoritmo *hash*, lo que la hace evidente ante un sencillo análisis forense.

[62] Como indica DOLZ, *"en rigor, lo propio de la PJE son los **actos de investigación** y no los **actos de prueba**, ya que, exceptuándose las **pruebas preconstituidas, las anticipadas** y algunas otras excepciones en que puedan adquirir la condición de **prueba documental**…", "…la doctrina procesalista, en general, destaca que la LECrim es clara en cuanto a la distinción entre actos de investigación y actos de prueba, señalando que los segundos sólo se producen en el plenario ante el Tribunal competente para conocer la causa (ex art. 741 LECrim, "pruebas practicadas en el juicio"), mientras que serían actos de investigación todos los demás (v.gr. intervenciones telefónicas, diligencia de entrada y registro, análisis clínicos, alcoholemias, etc.)".* No obstante, aún asumiendo esta visión, se usará por sencillez y comodidad la palabra *prueba* para referirse de una forma genérica a las aportaciones de la PJE al proceso penal pues, sin duda, aunque no hayan llegado a la fase de plenario, habrán sido tomadas en consideración como tales en fases procesales precedentes. Vid. Dolz Lago, Manuel-Jesús. *La aportación científico-policial al proceso penal*. Universidad Internacional Menéndez Pelayo. Seminario sobre la policía científica del siglo XXI en el marco europeo, 2008.

Un medio de seguimiento de vehículos, por ejemplo, ahorra la vigilancia de quienes lo usan cuando lo que se trata de saber es únicamente dónde estuvo. El dato, de absoluta precisión técnica, dirá irrefutablemente que el móvil (y no la persona investigada) estuvo en tal o cuál lugar. El investigador, sagazmente, sabrá combinar este dato con otros de la investigación que perfeccionen la evidencia que necesita y, a la vez, habrá preservado este tramo de intimidad en la persona concernida.

Sin embargo, debe hacerse la observación de que el dato en el plano físico está perfectamente asumido por la doctrina como válido para procurar la aportación de pruebas para el proceso penal, pero que el que se obtiene en el mundo virtual viene contaminado de una serie de prejuicios que, en mi opinión, deberían ser objeto de revisión y mejora de la legislación procesal.

Debe observarse, en lo que se refiere al estado actual de un panorama jurídico nacional e internacional claramente desbordado por los avances tecnológicos, la intensa migración que se aprecia en la prestación a los ciudadanos de los servicios de comunicaciones electrónicas, que marcadamente evoluciona desde las operadoras clásicas de telefonía – en aparente comienzo de su decadencia o, al menos, de su pérdida progresiva de competitividad frente a otras formas de comunicación -, sometidas a regulaciones más o menos afortunadas en lo que se refiere a la legal limitación del derecho fundamental al secreto de las comunicaciones, hacia los prestadores de servicios de la sociedad de la información, bajo cuyas normas inexistentes, mínimas o, incluso, de improbable encaje como consecuencia de la naturaleza de la propia tecnología, que hacen fracasar cualquier intento de imponer el Derecho, no sólo más allá de donde excede la soberanía nacional sino incluso dentro de esta misma.

La legislación internacional se centró, para mantener una operatividad procesal en materia de intervención de las comunicaciones equivalente a la conseguida en la época de la telefonía clásica – no tan lejana -, en el establecimiento de obligaciones para las compañías operadoras a través de la Ley 32/2003, de 3 de noviembre, *General de Telecomunicaciones* (en adelante, LGT) *ex* art. 33 y su reglamento de aplicación y, consecuentemente, para servicios prestados en un ámbito controlado por la soberanía nacional (allí donde se les otorgase a aquellas una licencia para operar,

admitiéndoselas en el mercado de las telecomunicaciones con registro propio), sin reparar en que estos servicios ya comenzaban a ser prestados, con diversidad de productos de comunicación de espectacular aceptación de la ciudadanía, por prestadores de servicios de la sociedad de la información a través del ***Protocolo TCP/IP***[63].

Estos prestadores de servicios de la sociedad de la información, regidos en el insuficiente ámbito nacional por la Ley 34/2002, de 11 de julio, *de servicios de la sociedad de la información y de comercio electrónico* (en adelante, LSSI), y por tanto, fuera del alcance de las obligaciones de la LGT, no facilitan sus servicios normalmente al alcance de la soberanía nacional sino a través de ignotos servidores informáticos sin ubicación física precisa sino, más bien, con probable dispersión técnico-informática, a través de diferentes territorios y estructuras de redes de compleja descripción, por lo que la imposición de medidas de orden jurídico sólo podría lograrse a través de complejos cuerpos legislativos de derecho internacional.

En su virtud, la *VoIP* sería un claro ejemplo de servicio de comunicaciones electrónicas de voz y datos que no es facilitado por operadoras de telefonía, sino por prestadores de servicios de la sociedad de la información, a los que no cabe invocárseles el art. 33 de la LGT para que faciliten la legal intervención de las comunicaciones que a su través se establezcan por no ser facilitado por operadoras del mercado de las telecomunicaciones y, ni mucho menos, se le impongan obligaciones tales como la conservación de los datos establecida en la LCDCE o el depósito de los protocolos de codificación de las comunicaciones.

Con todo ello, si el legislador internacional acertó al preparar un cuerpo jurídico que mejorase los instrumentos de investigación en el mundo de las operadoras de telefonía, fracasó estrepitosamente en hacer lo mismo respecto de los prestadores de servicio de la sociedad de la información, pese a que a esas alturas ya se trataba de un realidad perfectamente constatable y advertida desde los cuerpos policiales encargados de estar al día en las necesidades presentes y futuras de la investigación y,

[63] Este protocolo es la base de funcionamiento de Internet. Permite la comunicación de ordenadores aunque funcionen bajo sistemas operativos distintos.

consecuentemente, del máximo interés de un proceso penal propio de un estado de derecho.

Puede concluirse que la PJE debiera contar con un sólido respaldo jurídico para estar en condiciones de responder a la amenaza que supone el uso malicioso de las TIC, al menos con la misma versatilidad con que lo ha venido haciendo en el espacio físico, lo que debiera incluir además algunas previsiones para tratar la urgencia de un modo más eficiente que el actual.

Si para para el espacio físico se consolidaron a lo largo de los años cuerpos legales adecuados que, con mayor o menor éxito, se adaptaron a la amenaza, debe lograrse ahora un efecto análogo para su actuación en el ciberespacio o espacio virtual, de insospechadas posibilidades criminógenas.

II. CAPÍTULO SEGUNDO: LA POLICÍA JUDICIAL: UNA PARTE ACTIVA EN LA PRESERVACIÓN DE LAS GARANTÍAS CONSTITUCIONALES.

En el capítulo anterior se ha presentado un panorama inquietante sobre la evolución de la delincuencia moderna, en el que ha sido descrito el desfase que existe entre las capacidades de la PJE para llevar a cabo una investigación criminal, según las fórmulas clásicas sobre las que se construyó el vigente derecho procesal penal, y el cambiante y tecnificado escenario actual, en el que se hace imperiosa una renovación de los instrumentos procesales destinada a mantener un nivel equivalente de eficiencia del Estado de Derecho para afrontar los nuevos *modus operandi*.

El reto no es otro que el de mantener tales capacidades, y aún aumentarlas, sin que llevase aparejada la minoración de las garantías constitucionales sino, más bien, lo contrario, como sería la consecución de formas menos restrictivas de los derechos fundamentales de los investigados, apoyadas por la misma tecnología que maliciosamente usan.

De una manera pragmática, se han identificado alguno de estos sugerentes escenarios y mostrado las carencias del proceso penal para poder llegar a representarlos en el acto del juicio oral, dejando en evidencia, no ya el retraso en la operatividad policial respecto de los escenarios más evolucionados, sino las propias dificultades siquiera para aprehender legítimamente las evidencias criminales y para presumir que los instrumentos jurídicos existentes serán suficientes o adaptables a tan novedosa y compleja realidad social.

La doctrina, por otra parte, deja traslucir en algunas ocasiones una injustificada falta de confianza en la PJE en el ejercicio de las funciones que tiene conferidas por la Ley, ocasión tanto más acerba cuando se trata el espinoso asunto de su papel en la limitación de los derechos fundamentales. Sobre este efecto, pueden recogerse opiniones que muestran un algún recelo sobre su proceder[64], otras que hacen tabla

[64] En el Voto Particular de 1 de febrero de 2010 al Recurso de Casación 404/2009, los magistrados discrepantes critican el celo puesto en los agentes de las PJE que realizan transcripciones de las intervenciones telefónicas y llegan a poner en duda su fidelidad en las funciones de informar verazmente al tribunal. Debe aclararse además que la transcripción policial no representa sino un valor añadido que la PJE aporta para el auxilio de los Jueces y Fiscales – labor que normalmente agradecen -, pues la verdadera prueba es, precisamente, el contenido de la intervención examinado desde su continente original, a veces de un volumen absolutamente inmanejable.

rasa de conductas aisladas que son, en sí mismas, incuestionablemente reprobables en aquellos casos en que se produzcan[65] y, otras, que resultan francamente injustas[66].

Por ello, conviene redibujar los precisos contornos de una pieza esencial de la impartición de Justicia en un Estado de Derecho, de forma que encaje sin necesidad de mayores ajustes en el edificio del proceso penal. Es decir, lograr equilibrar una balanza, hoy ciertamente vencida hacia el lado de la desconfianza, para elevarla a su lugar natural, que sería el de su plena consideración como la primera y sólida salvaguarda de las garantías constitucionales que han de presidir el conjunto del proceso penal.

Consecuentemente, es preciso hacer hincapié en el estudio del instrumento al que de manera más inmediata recurre el Estado de Derecho para que, en su día, se llegue a descubrir la verdad: La PJE, llamada a proporcionar al proceso penal sus medios de prueba más sensibles. La pretensión será la de dilucidar si su actuación podrá presumirse acorde con los exigibles principios de legalidad e imparcialidad que le son imperativos, si en el ejercicio de sus actividades bajo la dependencia funcional de la Autoridad Judicial o Ministerio Fiscal - y conociendo cómo son sus concurrentes dependencias orgánica y técnica - actúa de forma autónoma y sin mediación contaminante de estas últimas y si, en definitiva, merecería una mayor consideración en el conjunto del proceso penal.

El cometido será, consecuentemente, tratar de analizar las razones por las que hay que considerar a la PJE como un elemento esencial y confiable del proceso penal en su calidad de salvaguarda de los derechos fundamentales.

---

[65] VELASCO afirma, con alguna prevención, que *"…debemos ser conscientes de que, detrás de la cortina de un confidente, frecuentemente se esconden actuaciones irregulares de la policía, ya sea por excesivo celo, ya sea por maniobras torticeras que pueden esconder intereses ilegítimos".* Vid. Velasco Núñez, Eloy. *El confidente.* Madrid: La Ley, 1993, págs. 823-830, citado por Delgado Martín, Joaquín. *Criminalidad organizada.* Barcelona: J. M. Bosch, 2001, página 45.

[66] En la STS 105/1998, de 21 de septiembre, se afirma que *"…entendemos que la esencia del control judicial de las intervenciones telefónicas ejecutadas por la Policía no es otra que la de evitar que las grabaciones puedan ser manipuladas por quienes las realizan, seleccionan o transcriben de manera que puedan servir como pruebas incriminatorias unos documentos sonoros o escritos previamente amañados".* En mi opinión, el control judicial va dirigido a garantizar la proporcionalidad de las medidas limitativas de los derechos fundamentales y su perfecta juridicidad y, sólo cuando puedan surgir indicios racionales de criminalidad de los agentes, actuar en consecuencia, lo que sin duda será absolutamente excepcional. Desde luego, nunca un cuestionamiento de la PJE como tal.
En la STS de 18 de junio de 1993 (RJ 1993/ 5191), a propósito de lo que parece ser descrito como una práctica policial cuasi deportiva en materia de las intervenciones telefónicas, se dice que *"las interferencias e intromisiones policiales…al haberse realizado de la forma más hábil y clandestina, se prodiga[n] hoy con harta frecuencia".* Sin comentarios.

A. Policía Judicial y proceso penal

En este apartado se presentarán los aspectos de índole organizativa o estructural y los principios que rigen la función de Policía Judicial. Estos aspectos fijan su posición en el proceso penal como elemento activo en la preservación de las garantías constitucionales y para la salvaguarda de los derechos fundamentales de los ciudadanos.

1. Una estructura de la Policía Judicial pensada para servir al proceso penal

a) Policía de Seguridad y Policía Judicial

La ***Policía Judicial*** es una función nacida del art. 126 CE[67], que es ejercida por todos los miembros de las FCSE, incluidos quienes desarrollan las funciones generales de ***Policía de Seguridad*** surgidas del art. 104 CE[68] y que no están asignados a las ***Unidades Orgánicas de Policía Judicial*** (en adelante, UOPJ).

Los preceptos constitucionales mencionados, sin embargo, establecen una neta diferencia entre ambas funciones por más que en el texto no se aluda expresamente a un cuerpo específico de policía judicial[69]. No en vano, los artículos 104 y 126 CE están

[67] Vid. Barcelona Llop, Javier. *Policía y Constitución.* Madrid: Tecnos S.A., 1997.

[68] Sobre la policía de seguridad, vid. Barcelona Llop, Javier. *Principios básicos de actuación de las fuerzas policiales*. *Policía y seguridad: Análisis jurídico-público.* Oñate, 1990, págs. 45-76 Barcelona Llop, Javier. *Principios básicos de actuación de las fuerzas policiales*. *Policía y seguridad: Análisis jurídico-público.* Oñate, 1990, págs. 45-76

[69] Adviértase que *"la Constitución enuncia la tarea que incumbe a la Policía Judicial, pero no atribuye la función a ningún órgano, ni efectúa la distribución material y geográfica de la competencia. En rigor, tampoco predetermina si ha de constituirse como cuerpo específico o como mera función ejercitable por los Cuerpos de Seguridad, ni si su régimen de dependencia de Jueces y Fiscales debe ser orgánico o funcional, por lo que deja en manos del legislador un extenso margen de libre configuración"* (Instrucción 1/2008 de la Fiscalía General del Estado).

incluidos en títulos distintos, el IV, *del Gobierno y la Administración*, y el VI, *del Poder Judicial*, respectivamente:

> *Art. 104.*
>
> *1. Las Fuerzas y Cuerpos de seguridad, bajo la dependencia del Gobierno, tendrán como misión proteger el libre ejercicio de los derechos y libertades y garantizar la seguridad ciudadana.*
>
> *2. Una Ley orgánica determinará las funciones, principios básicos de actuación y estatutos de las Fuerzas y Cuerpos de seguridad.*
>
> *Art. 126.*
>
> *La policía judicial depende de los Jueces, de los Tribunales y del Ministerio Fiscal en sus funciones de averiguación del delito y descubrimiento y aseguramiento del delincuente, en los términos que la Ley establezca.*

La circunstancia de la ***doble funcionalidad***, como Policía de Seguridad y Policía Judicial de las FCSE, alimenta una de las controversias más interesantes sobre el ***modelo policial español***[70] en relación con su adecuación a la función de auxilio a los Tribunales y al Ministerio Fiscal[71].

La doble ubicación en el texto constitucional es descrita con precisión por MARTÍNEZ PÉREZ, quien agrupa a la Policía de Seguridad en dos facetas: la ***administrativa*** (compuesta de la ***policía administrativa*** propiamente dicha, con funciones de control y supervisión de la acción gestora del Estado, y la ***policía preventiva***, dedicada a la evitación de ilícitos) y la ***represiva***, esto es, de la Policía Judicial[72].

---

[70] Esta aparente dicotomía es estudiada por DE LLERA SUÁREZ-BÁRCENA, quien afirma que *"respecto a la Policía Judicial la Constitución, siguiendo la tradición española y el sistema seguido en los países europeos de nuestro entorno, ha optado por esta segunda posibilidad [la coincidencia de la Policía de Seguridad con la Policía Judicial*]", lo que ha propiciado la estructuración de un cuerpo legislativo como el que se va a describir en este capítulo. Vid. de Llera Suárez-Bárcena, Emilio. *Derecho procesal Penal (Manual para Criminólogos y Policías).* 2ª Edición. Valencia: Tirant lo Blanch, 1997, pág. *92.*

[71] Ante cualquier controversia como las que se traerán a este trabajo, valórese, no obstante, la vocación de asistencia a la Justicia que se trasluce del encargo de raíz constitucional dirigido al conjunto de las FCSE.

[72] El autor comenta que *"pueden distinguirse los ámbitos de actuación policiales como Policía de Seguridad, como policía administrativa con funciones ajenas al mantenimiento de la seguridad en sentido estricto –policía sanitaria, forestal, etc. – o bien como Policía Judicial. La propia Constitución, y*

Con este comentario, ciertamente, quedan resaltadas – y, en mi opinión, perfectamente delimitadas - dos funciones notoriamente diferentes pero que, en el modelo español, se ejercen por las mismas FCSE, cuya aportación o resultado más sensible debe llevarse al terreno práctico de la complementariedad de funciones entre la Policía de Seguridad, con funciones incidentales de PJ, y la propia Policía Judicial Específica, con funciones permanentes y exclusivas en la materia, en la medida en que los frutos ofrecidos por la extensión o paso sin solución de continuidad de la función de seguridad a la de policía judicial[73], cuando la situación práctica así lo demande, en nada contamina o compromete la posición de esta última ante el proceso penal.

Expresado de otro modo, no existe obstáculo alguno que impida que la Policía de Seguridad lleve a cabo determinadas funciones de PJ en el entendimiento de que, cuando así suceda, le alcanzan todos los imperativos legales y técnicos propios del ejercicio de semejante función ante los tribunales y el Ministerio Fiscal. El resultado de esta complementariedad, materializada bajo el riguroso control jurisdiccional es, en mi opinión, el del enriquecimiento del propio proceso penal que ve de esta forma aumentada su eficacia en todos los órdenes.

Una consideración que sirve para sostener lo anterior la ofrece BLÁZQUEZ GONZÁLEZ para quien la dualidad Policía de Seguridad – Policía Judicial no resulta perturbadora de la función de policía judicial, basando sus razonamientos en el anclaje

no por casualidad, distingue entre policía gubernativa en funciones de seguridad (art. 104 en el Título IV referido al Gobierno y la Administración), y Policía Judicial (art. 126 en el Título VI relativo al Poder Judicial)". Vid. Martínez Pérez, Roberto. *Policía Judicial y Constitución.* [ed.] Ministerio del Interior. Elcano (Navarra): Aranzadi, 2001, pág. 44.

[73] MARTÍNEZ PÉREZ describe esta idea diciendo que *"la determinación del concepto de policía en todas sus manifestaciones no es clara, y menos lo es aún en cuanto al ámbito de actuación, bien como Policía de Seguridad, o como Policía Judicial. Sin embargo, lo antedicho puede servir como punto de partida para enfocar la dimensión conceptual de la policía, donde la policía opera tanto en el momento preventivo como en el represivo, como delegación del órgano jurisdiccional".* Vid. Martínez Pérez, Roberto. *Policía Judicial y…op. cit.,* pág. 50.

legislativo posterior[74], que disiparía cualquier duda sobre la sólida subordinación funcional de la PJ a las finalidades del proceso penal[75].

Sobre el difuso nexo que une a las dos funciones reflexionan algunos autores ponderando las innegables aportaciones del modelo policial español a la que sería su última finalidad: procurar la seguridad y, cuando esta falle, llevar ante la Justicia, sin dilación y con todas las garantías, a los responsables de los ilícitos penales[76]. En la misma línea de estas reflexiones, otros autores razonan sobre la íntima conexión existente entre ambas funciones[77,78].

En mi opinión, una Policía Judicial dependiente en exclusiva del Poder Judicial, perdería ese necesario vínculo con la realidad criminal del día a día policial, que en el modelo español la retroalimenta de forma que le permite interactuar en un escenario

[74] Este carácter de función viene además de forma inequívocamente reforzado por la legislación que desarrolló el art. 126 CE. Por ejemplo, en los arts. 29 y ss LOFCSE (muy especialmente en el art. 31.1), pertenecientes al capítulo dedicado a la organización de la Policía Judicial, no dejando lugar a dudas sobre qué es lo que se debe ejercer (la función de Policía Judicial) y frente a quiénes (Jueces, tribunales y Ministerio Fiscal). A lo anterior se une la exhaustiva legislación que estructura la función de PJ, principalmente a través de la LOPJ, LCRIM y el RDPJ.

[75] BLÁZQUEZ GONZÁLEZ hace una especial referencia a la promulgación de la LOPJ, afirmando que *"supuso que la PJ pasase de ser una especialidad más de las FCSE para a ser una función concreta, de acuerdo con el art. 443 LOPJ, lo que conllevó "dotar a la PJ de una sustantividad propia"… profundiza[r] en el alcance de la dependencia de la PJ al establecer que las Unidades de la PJ dependerán "funcionalmente" de la Autoridades Judiciales y del Ministerio Fiscal (art. 444.1 LOPJ). Además la dependencia deja de ser un concepto abstracto y se materializa al disponer que los Juzgados, Tribunales y MF "dirigirán" a la PJ e las funciones de investigación criminal (art. 446.1 LOPJ)…[reforzar] el estatus del personal que forma parte de la PJE al tener un carácter permanente y especial (art. 30.1 LOCFSE), estar en posesión de un diploma de especialización (art. 32 LOCFSE), dedicación exclusiva (33 LOCFSE), no poder ser removido o apartado de una investigación concreta hasta que finalice, salvo autorización del Juez (art. 34.1 LOCFSE), tener el carácter de comisionado (art. 34.2 LOCFSE)…".* Vid. Blázquez González, Félix. *La Policía Judicial.* Madrid: Tecnos, 1998, pág. 95.

[76] Para OLIVÁN, *"la Policía Judicial que procura el castigo de los delitos que no pudieron evitarse… correspondiendo esta función [la de policía judicial] en parte al orden civil o propiamente administrativo, y en parte a la justicia criminal…"*; y, por su parte, QUERALT afirma que *…"La policía gubernativa, como Policía de Seguridad, tiene la misión de prevenir la delincuencia, ello le pone en contacto con la realidad criminal en la calle…[y al hacerlo] surge la función de Policía Judicial…momento en que se propone – porque, por mandato legal, debe hacerlo - esclarecer el hecho".* Anótese, de otro lado, el valor que el autor otorga al "conocimiento de la realidad criminal" para situarse en las mejores condiciones de cumplir con la función de PJ. Vid. Oliván, A. *De la Administración Pública con relación a España.* Madrid, 1954, citado por Martínez Pérez, Roberto. *Policía Judicial y…op. cit.,* pág.50.

[77] Dice que *"la función represiva no es otra cosa que el complemento necesario de la preventiva, puesto que aquélla separa y reprime los actos y males sociales denominados delitos que no pudieron ser evitados, ya por defecto de los remedios preventivos, ya por la falsa aplicación de los mismos o ya también por la imposibilidad natural de conseguirlo".* Vid**.** Méndez Alanís, R. *La Policía. Estudio científico-jurídico de la función, órgano y elementos de acción de la policía de derecho o de seguridad.* Tres tomos. Madrid: 1913, 1925 y 1917.

[78] *"En expresión de HELIE "la policía es el ojo de la justicia" y es que, normalmente, es el primer elemento de control social que entra en contacto con el delito. Pero además la Policía Judicial es el brazo armado de la Justicia Penal". Vid.* de Llera Suárez-Bárcena, Emilio. *Derecho Procesal…op. cit.,* pág. 70.

en el que la finalidad última es estar en la mejor posición para comprender el crimen. Se ha de entender que la función de Policía Judicial no se limita a la fría aportación de técnicas sofisticadas para resolver crímenes, sino que los afronta con idea de contrarrestarlos desde el mero ejercicio de la práctica policial de seguridad.

Con las consideraciones anteriores queda resaltada una realidad muy interesante que restaría negatividad o relevancia a la dualidad en las funciones, aportando al modelo policial español el valor añadido que supone la continuidad entre una y otra función, beneficio que indudablemente se trasladará a las finalidades propias del Poder Judicial. Qué duda cabe que el conocimiento de la realidad delincuencial, sea cual fuere la faceta policial desde la que se adquiera, resultará de suma importancia para plantear una correcta investigación en sede judicial en aquel momento en que una policía que no alcanzó a evitar una determinada acción delictiva – la de seguridad -, debe ser suplida automáticamente por la judicial para tratar de esclarecer los hechos, poner al Juez en situación de conocerlos y conjurar o, al menos, disminuir, los efectos que tuvo sobre las víctimas.

Es evidente que, en todo lo anterior, un enfoque multidisciplinar basado en una sólida estructura orgánica no hará sino asegurar la completa solución del caso. No se debe olvidar, por otra parte, que la función jurisdiccional, con ser superior en muchos aspectos, no lo es todo en el mundo del delito. Baste señalar al efecto, por ejemplo, los aspectos asistenciales o de protección a las víctimas – que exigirán sin duda una actuación de la Policía de Seguridad o de los servicios sociales -, el resarcimiento económico, los aspectos de mera gestión, etc., que son ajenos, en buena medida, a la actuación judicial y que sólo pueden ser coordinados por una estructura sólida que no se limite a aspectos concretos de las necesidades surgidas tras la comisión de un delito.

En definitiva, se produce una configuración legislativa de la función de Policía Judicial de tal naturaleza que ha permitido a los Jueces y Fiscales liberarse de su dirección orgánica e incluso técnica para poder servirse de todas sus potencialidades y concentrase sin impedimento alguno en el desarrollo de sus instrucciones judiciales o de las investigaciones que se llevan a cabo en las sedes de las respectivas Fiscalías.

Algo se añadirá más adelante sobre las inmensas posibilidades que este modelo de Policía Judicial ofrece a quien ha de impartir Justicia, que es como decir a la misma sociedad democrática, sosteniendo que, aunque no haya un pro sin su contra, se trataría de un modelo consolidado y que ha servido eficazmente a las altas expectativas nacidas desde el mismo texto constitucional.

Por ello, profundizando aún más en las características del modelo español, y dado que el ejercicio de la función de policía judicial es tarea o cometido universal para todos los miembros de las FCSE a la luz del art. 547 LOPJ, es necesario distinguir con claridad cómo la ejercen sus agentes dependiendo de la unidad a la que estén adscritos.

b) Policía Judicial Genérica y Policía Judicial Específica

En un principio, se deberá establecer una distinción básica entre la ***Policía Judicial Específica***[79] - que será de forma preferente el objeto de este estudio - de la ***Policía Judicial Genérica*** (en adelante PJG)[80], que es la desarrollada cotidianamente y sin diferenciación alguna por todos los miembros de las FCSE no adscritos a las UOPJ o, expresado de otro modo, por los miembros de las FCSE no destinados en la PJE.

Esquemáticamente, podría presentarse la base jurídica de la PJ del siguiente modo:

POLICÍA JUDICIAL[81] **ART. 126 CE**	**PJ GENÉRICA**	**PJ ESPECÍFICA**	
		UOPJ	**Unidades Adscritas**

[79] Entendiendo como tal a la compuesta por los funcionarios de las FCSE destinados en las diferentes UOPJ de acuerdo con lo establecido en los arts. 548 LOPJ, 30 LOCFSE Y 7 RDPJ.
[80] Art. 547 LOPJ y art. 1 RDPJ.
[81] Vid. Corral Escáriz, Vicente. *Problemática de la Policía Judicial: composición, dependencia y funciones.* Madrid, 2010 (En imprenta).

Arts.	**LCRIM**	283		
	LOPJ	547	548	
	LOFCS	11.1.g), 29.2, 38.2.b, 46, 53.1.e	30.1	30.2
	RDPJ	1, 4	7, 10 al 22	23 al 30

Una distinción básica entre ambas formas de prestar la asistencia requerida en el art. 547 LOPJ, a identificar en el terreno de lo práctico, que ayudará a entender las peculiaridades surgidas del mandato constitucional, queda determinada por el momento en que se produce un hecho que presente ***indicios racionales de criminalidad*** y que aconseje la intervención reactiva de la Policía de Seguridad y su concomitante actuación como PJG o, alternativamente, por el conocimiento diferido del hecho delictivo por parte de la PJE, como resultado, en este último caso, bien de la transferencia para su continuidad de lo inicialmente actuado por la PJG, bien de la propia dinámica investigativa de las UOPJ[82] o, alternativamente, por haber recibido el encargo de investigar de un Juez o un Fiscal[83].

Una primera conclusión que de todo ello puede deducirse es que, por un lado, la función realizada por las unidades de la Policía de Seguridad es primariamente preventiva y, secundariamente, reactiva frente a hechos de naturaleza delictiva, siguiéndose de este último aspecto una penetración puntual y delimitada en la esfera de la función de Policía Judicial, por lo que ha merecido, cuando la ejerce, el apelativo de "genérica".

[82] En lo que se debe incluir para más precisión la cesión de las investigaciones complejas cuyo primer conocimiento lo haya sido por parte de la PGE.

[83] Lo que no excluye que la PJE en el transcurso de una investigación evite la comisión en tiempo real de un nuevo hecho delictivo por la simple razón de que responda a la materialización de la dinámica criminal de la persona o grupo delictivo que está siendo objeto de la investigación. En este caso, se reconocería su actuación, no como la de la PJE *sensu stricto,* sino más bien, como una actuación eventual o sobrevenida como Policía de Seguridad. Una cuestión interesante en este punto se suscita al valorar aquellas ocasiones en que el interés de la investigación exige la omisión de la reacción inmediata, con las consecuencias jurídicas que son de imaginar.

Esta circunstancia en ningún momento desluce su función como propia de la Policía Judicial, pues desarrollando cualquiera de sus cometidos, por breves, limitados o modestos que sean, actúa en plenitud de lo que dispone ordenamiento jurídico al efecto, tratándose de una actuación genuina de la Policía Judicial. Se puede afirmar, por tanto, que esta función se ejerce indistintamente, tanto por la PJG, como por la PJE, siendo las labores de esta última normalmente ajenas a la prevención de la delincuencia[84,85], al menos en la acepción más policial del término[86].

No obstante lo anterior, y en sentido contrario, se recogen algunas opiniones que, según mi parecer, no tendrían cabida en el concepto de PJE[87], tales como la expresada por la Fiscalía General del Estado (en adelante, FGE), sobre la habilitación del Ministerio del Interior para encargar a las UOPJ tareas preventivas[88].

Una segunda conclusión que también puede extraerse de las anteriores observaciones, de alta transcendencia para comprender la forma en que la PJE interviene en el proceso penal, viene derivada del mero hecho de su irrupción en este,

[84] Podría inferirse que la labor de la PJE no tiene una finalidad preventiva frente a la comisión de hechos delictivos más allá del factor disuasorio que pueda seguirse del público conocimiento de su prudente y eficaz ejercicio cotidiano. Sin embargo, algunos autores quieren ver en las distintas leyes un factor preventivo primigenio, del que, obviamente, participaría la PJE en el sentido indicado. Así se pronuncia MORENO CATENA sobre la LCDCE, de la que no debe perderse de vista el valor preventivo que su mera existencia consigue como disuasión de quienes piensen hacer un uso delictivo de las comunicaciones, cuyos datos de tráfico se conservarán a disposición de la Justicia. Vid. Moreno Catena, Víctor. *Ley de conservación de datos y garantías procesales.* [ed.] Agencia Española de Protección de Datos. *La protección de datos en la cooperación policial y judicial.* Madrid: Aranzadi S.A., 2008, págs. 163-172.

[85] Otros autores argumentan algo más en favor del efecto preventivo, en la medida en que pueda delimitarse o no como parte de las funciones de la PJE, el desarrollo de una faceta prejudicial o precaucional – la prevención -, junto con la propiamente judicial o auxiliatoria – la represión -. Aunque diversos autores se decantan por el evidente peso de esta última, no deja de ser reseñable el factor preventivo de su actuación. Vid. Blázquez González, Félix. *La Policía Judicial…op. cit.,* pág. 141, con citas a AGUILERA DE PAZ y DE LLERA SUÁREZ- BÁRCENA.

[86] Sobre el carácter permanente de la PJE, vid. de Llera Suárez-Bárcena, Emilio. *Derecho Procesal…op. cit.,* pág. 92.

[87] La redacción del art. 33 LOCFSE, entre confusa y contradictoria, contiene conceptos jurídicos indeterminados, pues al término "exclusividad" no puede seguirle, en mi opinión, un amplio catálogo de excepciones como las que se anuncian en el texto de este artículo, redactado cual norma en blanco, que admitiría el empleo de las UOPJ para todas las modalidades policiales existentes o por existir. No opera en la práctica.

[88] La Fiscalía General del Estado, en su Instrucción 1/2008, considera que la Policía Judicial puede compatibilizar sus funciones con las de prevención, otorgando al Ministerio del Interior la iniciativa de ordenar a la PJE estas u otras prestaciones. En mi opinión, esto contradice frontalmente "*el estatus del personal que forma parte de la PJE, al tener un carácter permanente y especial (art. 30.1 LOCFSE),…dedicación exclusiva (33 LOCFSE), no poder ser removido o apartado [el agente] de una investigación concreta hasta que finalice, salvo autorización del Juez (art. 34.1 LOCFSE), tener el carácter de comisionado (art. 34.2 LOCFSE)".* Vid. Blázquez González, Félix. *La Policía Judicial…op. cit.,* pág. 97. Finalmentel el art. 549.2 LOPJ impide la realización de otras funciones que no sean las propias de la PJE.

ya que, a diferencia de lo que sucede con la PJG, se produce siempre con posterioridad a la consumación de los hechos delictivos.

Esta cuestión no es menor, ya que sugiere la completa ausencia de una modificación de la escena del crimen derivada de la intervención de la PJE, ya que esta no ha actuado en el momento de producirse los hechos para intentar impedirlos sino tras su finalización y al ser requerida para su esclarecimiento, lo que, por su lado, sí sería propio de la intervención policial contemporánea con aquella de la PJG.

En efecto, esta última interviene como un actor esencial en la escena del crimen, tratando de impedirlo o paliarlo, participando de forma activa en la configuración de unos acontecimientos en su condición primigenia de Policía de Seguridad y que, por ser de naturaleza delictiva, en su día deberán ser sometidos al acto de juicio oral[89]. Por ello, y salvo que mediase una actuación espuria, la PJE jamás tendrá la posibilidad de modificar ninguna de las circunstancias que los rodearon sino, más bien, la vocación de desentrañarlos hasta sus últimas consecuencias de modo que el proceso penal alcance sus más altos fines, esto es, la impartición de Justicia con arreglo a un ordenamiento jurídico propio de un Estado de Derecho.

Puede resumirse de lo afirmado sobre el momento de la intervención diciendo que, con todas las salvedades hechas, la PJE no interviene en el cuadro criminal salvo cuando este ya pertenece al pasado, por lo que la dinámica de la investigación que a partir de ese momento se inicie no interfiere en su realidad, tanto si se llega finalmente a desvelar la verdad como si no, o si este desvelamiento resulta completo o parcialmente conseguido.

c)Dependencias funcional, orgánica y técnica

[89] Un ejemplo sería la frustración de un homicidio en curso por la acción de la Policía de Seguridad presente en el escenario de los hechos, reduciendo a la persona que de forma inequívoca se disponía a cometerlo mediante el uso de un arma contra su víctima. Es evidente que, junto con su condición de Policía de Seguridad, se producirá una actuación de la PJG que deberá ser representada en el acto de juicio oral. Nótese, por último, que la valoración jurídica de los hechos y, consecuentemente, la responsabilidad penal y civil de su presunto autor variaría considerablemente de no haber intervenido la Policía de Seguridad y actuado al mismo tiempo como PJG.

Cuando, por los motivos que se han expuesto, la PJE inicia la actividad investigativa para averiguar qué sucedió y quiénes serían penal y civilmente responsables, desde la estructura orgánica de las FCSE de la que dependen se produce una completa transferencia de la dirección de la investigación de sus agentes especializados adscritos a la UOPJ quienes, a partir de ese momento, dependerán plena y funcionalmente del concreto Juzgado o Fiscalía ante los que recaiga la dirección de la investigación.

Esta transferencia, pese a la solvencia que puede atribuirse al modelo policial español, sigue suscitando algunas dudas sobre si, una vez asignados los efectivos de la PJE a un determinado Juzgado o Fiscalía, puede presumirse que ejercen sus funciones con el adecuado ***grado de autonomía***. La discusión puede plantearse aún con mayor precisión en torno a la presumible colisión de la ***dependencia funcional de la PJ*** con sus ***dependencias orgánica y técnica***, en la media en que pudieran distorsionar o interferir en el ejercicio autónomo de la función de Policía Judicial.

Por ello, se tratará ahora de realizar una tarea de prospección en las notas de autonomía que respaldan la actuación de una PJE que, aunque se encuentre inserta en una ***estructura policial jerárquica*** y, por tanto, sujeta a una cadena de mando perfectamente identificable y efectiva en sus cometidos[90], no es menos cierto que los mandos de las unidades de PJE se preservan de interferir en las investigaciones que son conferidas a los instructores policiales por más que sean ellos mismos los que, en primera instancia, los designen[91].

En este sentido se pronuncia el ordenamiento jurídico al conjugar con claridad meridiana el principio de jerarquía con los imperativos nacidos del principio de

[90] Lo que vendría a suponer un reforzamiento de la imparcialidad, pues se hace inconcebible que una estructura jerárquica soporte conductas desviadas o actuaciones carentes de rigor profesional. El hecho de que una estructura policial enfoque su actividad a tratar determinadas formas de delincuencia no exige, en modo alguno, "finales de diseño" para las investigaciones policiales.

[91] Siempre sujeta a la definitiva anuencia judicial. El nombramiento por parte de los mandos de la PJE de un Instructor Policial, un Secretario y la asignación de un determinado número de especialistas tiene siempre el carácter de propuesta, que puede ser aceptada o no por la Autoridad Judicial o Fiscal, quienes tienen, no sólo esa potestad, sino también la de impedir su remoción.

legalidad en la actuación de la PJE, sin interferencia entre ellos, produciéndose como consecuencia la actuación autónoma que se pretende reivindicar en este párrafo[92].

Así, se ha logrado una fuerte interiorización de este aspecto en el devenir diario de la PJE, de modo que las órdenes impartidas bajo la dependencia funcional de los Jueces y Fiscales se hacen imperativas de un modo absoluto frente a cualesquiera otras que se les puedan impartir desde la cadena de mando policial, lo que confiere a los Instructores Policiales una situación de completa autonomía en el desarrollo de la encomienda que hayan recibido de juzgados y fiscalías. El resto de la estructura de mando se volcará en que esto sea así sin impedimento ni obstáculo de ninguna clase, tanto si la actuación nació del ejercicio de la función de Policía de Seguridad, en su calidad de PJG[93], como si se trata de una investigación iniciada por la PJE[94].

Es también de resaltar la vinculación del ***Instructor Policial*** a su caso, incluso en aquellas situaciones en que las vicisitudes administrativas pudieran imponer otra cosa, por ejemplo, por un cambio de destino o unas vacaciones. En estos casos, lo común es comunicar a la Autoridad Judicial o Fiscal el cambio de Instructor o Secretario a propuesta del mando orgánico, lo que normalmente es admitido sin reparo alguno.

---

[92] Para MARTÍNEZ PÉREZ, *"…los principios de dependencia y jerarquía implican una situación de subordinación que supone el respeto y la obediencia a las autoridades y superiores tanto funcionales como orgánicos, sin que ello suponga el cumplimiento de actos que sean contrarios a la ley o constitutivos de delito, tal y como se dictan en los arts. 5.1º.d, 11.1ºa LOFCS, arts. 2 y 5 del Código de Conducta para funcionarios encargados de hacer cumplir la Ley, y los apartados 1 a 9 de la Declaración sobre la Policía de 1979 (Del Consejo de Europa)".* Vid. Martínez Pérez, Roberto. *Policía Judicial y…op. cit.,* pág. 77.

[93] La nota esencial de la PJG es la inmediata reacción ante la flagrancia de un hecho delictivo, procurando evitar su consumación y, en todo caso, asegurando pruebas y autores y minimizando en lo posible las consecuencias del crimen. Frente a las críticas que se puedan hacer sobre las actuaciones de la PJG, nótese, con carácter previo, que no sólo habrán de actuar de modo reactivo, sino que además habrán de hacerlo de una forma escrupulosamente conforme a Derecho, lo que no será fácil si se toma en consideración la compleja casuística del crimen y el comportamiento de los delincuentes, a veces extremadamente violento.

[94] La PJG se limita a actuar en estos casos - que podrían describirse como altamente protocolizados -, en los que la sencillez de la actuación policial es su primer signo, cediendo si es posible y de manera inmediata la continuidad de las acciones a la PJE. Esto puede observarse de forma muy común desde la estructura de mando orgánico de las FCSE que, si de algo se ocupa, es de ordenar la inmediata transferencia de lo actuado a la PJE tan pronto como los hechos adquieren una mínima complejidad, siendo estos últimos quienes los continúen investigando tras comparecer ante la Autoridad Judicial o Fiscal, poniéndose a su plena e inmediata disposición tras haber adquirido la completa gestión del caso. Es evidente que, desde este preciso momento, el mando orgánico cede por completo el control del caso al Instructor Policial de la PJE quien, a su vez, alcanza una completa autonomía para su desarrollo.

Es relativamente frecuente que las autoridades mencionadas, en casos de extrema complejidad, se dirijan a los mandos orgánicos para que mantengan a los agentes en su calidad de Instructores policiales hasta la resolución de los casos, lo que normalmente sucede sin el más mínimo obstáculo, consagrándose con ello esa especial relación de subordinación e identificación con las finalidades de las autoridades judiciales, muy ajeno a cualquier suerte de confrontación o contaminación de tan necesarias y productivas vinculaciones profesionales en beneficio de la pureza del proceso penal.

Para argumentar las anteriores aportaciones, es necesario profundizar un poco más en los tres tipos de dependencia que afectan a la compleja estructuración de la PJE, todo ello con el objeto de dilucidar si suponen algún quebranto a la confianza que el Estado de Derecho puede dispensarle en relación con su adecuación a las necesidades del proceso penal.

Estas dependencias pueden ser de tres tipos: ***orgánica, técnica y funcional***.

La ***dependencia orgánica***, establecida en el art. 29.1 LOCFSE, y en lo que interesa a esta explicación, supone la mera ***adscripción administrativa de las UOPJ*** a las respectivas estructuras jerarquizadas de los cuerpos policiales de cuyos miembros se nutre[95], con dedicación exclusiva a la función y ubicándose genéricamente[96] en las comisarías del Cuerpo Nacional de Policía y en las comandancias de la Guardia Civil.

La ***dependencia técnica***, íntimamente relacionada con la orgánica[97,98], cuya legitimación se halla en el art. 285 LCRIM, supone una vinculación jerárquica de las respectivas jefaturas de la PJE y se centra exclusivamente en, precisamente, la

[95] Vid. de Llera Suárez-Bárcena, Emilio. *Derecho Procesal…op. cit.,* pág. 91.

[96] Existen otras adscripciones de las UOPJ y, naturalmente, unidades pertenecientes a las policías autonómicas, según los respectivos estatutos de autonomía.

[97] Para BLÁQUEZ existen dos niveles, el orgánico y el funcional, resumiendo en el primero todas las facultades de los órganos superiores de la PJ relacionadas con la dirección, inspección y ordenamiento de los servicios, esto es, lo que se ha denominado "dependencia orgánica y técnica". Vid. Blázquez González, Félix. *La Policía Judicial…op. cit.*

[98] A este propósito, y abundando sobre las afirmaciones de BLÁZQUEZ sobre la interrelación entre las dependencias técnica y orgánica, MARTÍNEZ PÉREZ dice que *"y aún cuando el interés son las relaciones funcionales dentro del proceso penal entre la Policía Judicial y la autoridad judicial y/o Fiscal, no olvidamos que junto a este nexo jerárquico, y la inevitable relación orgánica respecto de sus mandos naturales y de las autoridades políticas, existe una tercera que condiciona decisivamente cualquier planteamiento al respecto, que es la de carácter técnico en relación con el propio cuerpo de pertenencia del que precisan los elementos propios para llevar a cabo la investigación, lo que genera en definitiva una relación en el ámbito orgánico".* Vid. Martínez Pérez, Roberto. *Policía Judicial y…op. cit.*, pág. 313.

dirección técnica de determinados aspectos de la investigación, lo que no interfiere en la iniciativa del Instructor Policial si se observa con exactitud el precepto contenido en el art. 11 RDPJ, que prohíbe de forma contundente que la directrices técnicas de los mandos contraríen las de los Jueces y Fiscales[99], al depender funcionalmente como comisionados de tales autoridades[100]. Esta relación debe constar en el atestado policial de acuerdo con el art. 293 LCRIM.

Respecto de las dependencias orgánica y técnica, BLÁZQUEZ, cuando analiza la evolución de las relaciones de jerarquía entre el Poder Judicial y las FCSE respecto del ejercicio de las funciones de PJE, sostiene que con la redacción vigente del art. 288 LCRIM[101] queda solucionado el conflicto que antaño solía producirse entre la Autoridad Judicial y Ministerio Fiscal con la jerarquía policial sobre el curso de sus investigaciones[102], de lo que se seguiría un reforzamiento de la posición de tales autoridades frente a quienes ostenten el mando jerárquico de la PJE y, consecuentemente, de la expresión más genuina de la dependencia funcional. Esto seguirá siendo así por más que haya asuntos que puedan "admitir espera", lo que no tendrá en la práctica más valor que el de un mero formalismo o atenta deferencia hacia las autoridades policiales, sin efecto real alguno, ya que, en cualquier caso, el resultado final será el de la asignación de especialistas de la PJE plenamente obligados por las directrices de las Autoridades Judicial o Fiscal[103].

A este mismo propósito, QUERALT añade que *"…la [eventualmente superior] diferencia en la escala administrativo-protocolaria [de algunos policías] en nada minora la superioridad jurídico-política que distingue a los Jueces del resto de los funcionarios; de ahí que todos los policías en función de Policía Judicial les estén*

[99] Sin pretender establecer comparación alguna entre la PJE y el Ministerio Fiscal, se puede decir que no existe para los primeros una norma del carácter imperativo como la contenida en el art. 25 EOMF, que obligue a sostener en sus dictámenes las órdenes que recibiere por su conducto jerárquico.
[100] Art. 34.2 LOFCSE y 13 RDPJ.
[101] Art. 288 LCRIM: *"El Ministerio Fiscal, los Jueces de Instrucción y los municipales, podrán entenderse directamente con los funcionarios de Policía Judicial, cualquiera que sea su categoría, para todos los efectos, de este título; pero si el servicio que de ellos exigiesen admitiese espera, deberán acudir al superior respectivo del funcionario de Policía Judicial, mientras no necesitasen del inmediato auxilio de éste".*
[102] Vid. Blázquez González, Félix. *La Policía Judicial…op. cit.,* pág. 105.
[103] En la práctica, esta cuestión se sustancia mediante la emisión de un Auto Judicial que se dirige normalmente al mando más caracterizado de la UOPJ local. Los autos judiciales contienen órdenes que adquieren el inmediato carácter de ejecutivas para la PJE, a ser cumplidas sin dilación ni reserva alguna.

subordinados y que, en consecuencia, llámense como se quiera, lo que reciben de aquéllos con la mayor de las cortesías son órdenes"[104]. Y, puede añadirse, órdenes de carácter absoluto que no admiten dilación ni discusión alguna. Su incumplimiento, siquiera parcial, puede acarrear gravísimas consecuencias jurídicas para los agentes de la PJE en las que la inhabilitación profesional pende de un hilo sobre la cabeza del presunto infractor, tras años de procesamiento en que su vida personal y profesional quedará suspendida.

En ocasiones, el celo profesional, mediando el pleno convencimiento moral e intelectual del Instructor Policial sobre las necesidades de una concreta investigación – y aún asumiendo cabalmente la superior posición y exclusividad jurisdiccional de la Autoridad Judicial o la del Fiscal - lleva a procurar la solución más favorable de su caso intentando hacer valer sus razonamientos.

La ***dependencia funcional***[105] de las UOPJ, exhaustivamente tratada en la legislación nacional, nace de manera específica en el art. 126 CE y se desarrolla fundamentalmente a través de los arts. 548 y 550.1 LOPJ, lo que se materializa en una absoluta subordinación del Instructor Policial a las finalidades que le señalen la Autoridad Judicial o Fiscal[106] y que, de forma especialmente expresiva, se resume, entre otros, en el art. 286 LCRIM:

> *"Cuando el Juez de Instrucción o el municipal se presentaren a formar el sumario, cesarán las diligencias de prevención que estuviere practicando cualquiera autoridad o agente de la policía; debiendo éstos entregarlas en el acto a dicho Juez, así como los efectos relativos al delito que se hubiesen recogido, y poniendo a su disposición a los detenidos, si los hubiese".*

[104] Vid. Queralt Jiménez, Joan Josep. *Introducción a la Policía Judicial.* 3ª Ed. Barcelona: J.M. Bosch Editor, 1999, pág. 22. También, vid. Queralt Jiménez, Joan Josep. *El policía y la ley.* Barcelona, 1986.

[105] Independiente por completo de la orgánica, ya que, una vez iniciada la dependencia funcional de Jueces y Fiscales mediante la asignación de concretos especialistas de la PJE, esta pasa a ser exclusiva de los asistidos. Vid. Queralt, Joan Josep. *Derecho Procesal…op. cit.,*91 y ss.

[106] BLÁZQUEZ expone la dependencia funcional basándose en tres aspectos: La subordinación de la PJ (atribuyendo a la Autoridad Judicial y Ministerio Fiscal la potestad directiva y la obligación de dación de cuenta para la PJ), las facultades de los anteriores respecto del personal de la PJ y la figura del comisionado. Vid. Blázquez González, Félix. *La Policía Judicial…op. cit.,* pág. 106 y ss.

Para completar el grado de autonomía del Instructor Policial, conferido por la legislación respecto de la estructura en la que se incardina, puede señalarse el también expresivo contenido del art. 34 LOFCSE:

> "*1. Los funcionarios de las Unidades de Policía Judicial no podrán ser removidos o apartados de la investigación concreta que se les hubiera encomendado, hasta que finalice la misma o la fase del procedimiento judicial que la originara, si no es por decisión o con la autorización del Juez o Fiscal competente.*
>
> *2. En diligencias o actuaciones que lleven a cabo, por encargo y bajo la supervisión de los Jueces, tribunales o Fiscales competentes de lo penal, los funcionarios integrantes de las Unidades de Policía Judicial tendrán el carácter de comisionados de dichos Jueces, tribunales y Fiscales, y podrán requerir el auxilio necesario de las autoridades y, en su caso, de los particulares."*

Es evidente que el carácter que el Instructor Policial tiene en su calidad de *"**comisionado de dichos Jueces, tribunales y Fiscales**",* en mi opinión, le reportará un grado notable de autonomía, estabilidad y respaldo jurisdiccional que tan útil resultará finalmente para que se alcance la verdad judicial en el acto de juicio oral. No obstante, la figura del comisionado, al menos desde un punto de vista estrictamente jurídico, no ha resultado ser pacífica en el ordenamiento pues, aún apreciando algunos autores el esfuerzo del legislador por dotarla de alguna operatividad, otros la consideran vacía de contenido[107].

No por ello se debe dejar de otorgarle mérito a esta controvertida figura jurídica en lo que tiene de útil para el mejor desempeño de la función jurisdiccional ex art. 17 LOPJ y la de policía judicial en la medida en que, por un lado, dota a sus miembros de una importante capacidad de actuación al poder requerir el ***auxilio de autoridades y particulares*** (arts. 34.2 LOCFSE y 13 RDPJ) y, por otro, hace que los

[107] Dice BLÁZQUEZ que *"no tenemos que olvidar que la actuación de la PJ es por encargo o mandato de las Autoridades Judiciales y del Ministerio Fiscal, en ningún caso, por delegación o comisión. En el acuerdo del Comité Técnico de Policía Judicial, de 3 de enero de 1990, se criticaba la figura del Comisionado, tanto por no encontrarle contenido, como por chocar con el principio de indelegabilidad de la jurisdicción…Lo anterior nos lleva a pensar que la regulación del Comisionado ha buscado más la dignificación de los funcionarios de PJ que el refuerzo de los Jueces, Tribunales y el MF…y reforzar la dependencia funcional".* Vid. Blázquez González, Félix**.** *La Policía Judicial…op. cit.,* pág. 114. Por su parte, QUERALT comenta criticamente la parquedad legislativa de la figura del comisionado. Vid. Queralt, Joan Josep. *Introducción a la Policía Judicial…op. cit.,* pág. 28 y ss.

atestados que presenten gocen de una especial consideración derivada de la adscripción de los comisionados a Jueces, Tribunales y Fiscales (art. 14 RDPJ).

Por ello, en mi opinión, esta figura merecería un desarrollo legislativo autónomo de mayor calidad y enjundia, ya que podría usarse para reparar muchas de las insuficiencias procesales que son objeto de crítica en este trabajo. Si así fuere, podrían solventarse las lagunas que la lacra del hipergarantismo y las arcaicas leyes procesales van dejando abiertas en el sistema español de Justicia, especialmente, para la intervención de la PJE en los casos de ***urgencia vital*** o para tratar de resolver las necesidades de afrontar los retos emergentes de la delincuencia compleja.

Frente a estas notas de autonomía, por un lado, podrían oponerse algunas críticas haciendo exégesis del art. 285 LCRIM[108], en cuanto a la ***preeminencia de un funcionario de la PJ de superior categoría***, y las salvedades del 288 LCRIM en lo que se refiere a la remisión de Jueces y Fiscales al mismo funcionario superior *"…si el servicio que ellos exigiesen admitiese espera"* (ciertamente, sería una decisión a adoptar más bien en el terreno de las formalidades[109] y, desde luego, con muy poco efecto en el de lo práctico si se atiende a la clarísima potestad que en el proceso penal tienen sobre la PJ cualquiera de estas autoridades, lo que de ninguna manera se pretende criticar).

Pero, por otro lado, debe tenerse también en cuenta que el art. 11 RDPJ dice de forma perfectamente clara que:

> "*Los funcionarios policiales comisionados por la autoridad judicial o Fiscal con arreglo al artículo 21 para la práctica de alguna concreta investigación se atendrán en el desarrollo de ésta a las órdenes y directrices que hubieren recibido, sin que las instrucciones de carácter técnico que obtuvieren de sus superiores policiales inmediatos puedan contradecir las primeras*".

[108] Art. 285 LCRIM: "*Si concurriere algún funcionario de Policía Judicial de categoría superior a la del que estuviere actuando, deberá éste darle conocimiento de cuanto hubiese practicado, poniéndose desde luego a su disposición.*" Esta norma, cuya redacción no ha sufrido cambios desde el año de la promulgación de la Ley, responde obviamente a un limitado concepto sobre las elementales facultades de la PJ de aquella época.

[109] Es muy común que Jueces y Fiscales se dirijan mediante auto a los jefes de las UOPJ ordenándoles determinadas prácticas procesales. En ocasiones, visto el contenido de los autos, lo redirigen a aquellos otros jefes de UOPJ que a su juicio están en mejor posición de intervenir en el asunto, a lo que habitualmente las autoridades requirentes no ponen impedimento alguno, iniciándose con toda normalidad la instrucción en sede policial con remisión posterior de lo actuado a la autoridad competente.

Es decir, que el reducido abanico de acciones investigativas que el "superior policial" puede dirigir, siempre a través del Instructor Policial, se limita, aun no siendo poco, a impartir las órdenes e instrucciones de naturaleza estrictamente técnica dirigidas a conseguir la mayor calidad del conjunto de la investigación, por lo que en poco o en nada podrán condicionar otro tipo de resoluciones de contenido decisivo que pueda adoptar el Instructor Policial en el marco de una investigación sometida al directo control jurisdiccional[110].

d) Legalidad, imparcialidad y neutralidad como principios de la policía judicial. Perspectiva ética y deontológica

Si bien se ha apostado decididamente por el modelo español de policía judicial, no se dejan por ello de constatar algunas de sus posibles tachas. Aunque se ha atribuido a la PJE una actuación imparcial y autónoma, no deja de inquietar el hecho de que la ***dirección política***[111] posea un conocimiento actualizado del estado de las investigaciones dirigidas desde las FCSE y, entre ellas, de aquellas que pudieran afectar a los intereses puramente partidistas.

No hay que olvidar que en España la estructura orgánica de la PJE[112] es dependiente del Ministerio del Interior a través de la Secretaría de Estado de Seguridad y que su alta dirección política es ejecutada por el partido o partidos políticos que tengan a su cargo las responsabilidades de gobierno en cada momento.

Pero sobre todas las consideraciones que se han ido hilvanando hasta ahora sobre la idoneidad del la estructura de la PJ para el cumplimiento de la función

[110] Cuando la orden del jefe policial entraña un contenido reseñable, el Instructor Policial simplemente lo hace constar de forma expresa en el atestado, incluso incorporando los documentos que aquel valide con su firma.

[111] Apunta con alguna prevención DOLZ al respecto que *"como se ha indicado, la problemática de la prueba policial, básicamente, se orienta hacia el establecimiento de aquellos requisitos jurídicos que permitan dotar de una mayor objetividad e imparcialidad a esta prueba, desde el reconocimiento de la dependencia gubernamental de la policía y de su pertenencia al Estado, que, por otra parte, es el que ejerce el ius puniendi y frente al cual se concibe el Derecho Penal y Procesal Penal, como instrumentos jurídicos de garantía del individuo frente al propio Estado".* Vid. Dolz Lago, Manuel-Jesús. *La aportación científico-policial…op. cit.,* pág. 6.

[112] Entendiendo como tal la cadena profesional compuesta por policías y guardias civiles.

encomendada por el art. 126 CE, se debe añadir su firme sujeción a los principios del Estado de Derecho.

En efecto, y como argumento general que oponer a la inmensa mayoría de las críticas que se hacen sobre la fiabilidad de la PJE, conviene afirmar que tiene las mismas notas de sujeción a los ***principios de legalidad e imparcialidad*** en el desarrollo de sus investigaciones que las que se presumen en Jueces, Secretarios Judiciales y fiscales, así como una acusada fidelidad y lealtad a los propósitos de estos últimos, con quienes busca y desea la mayor inmediatez.

Pues bien, pueden reclamarse estas mismas notas de confianza para una PJE que no tiene capacidad alguna de llevar al atestado policial ningún tipo de actuación procesal que no se atenga a la verdad[113] y, con esta, a las notas de cientificidad que acompañan a sus actuaciones periciales o, incluso, de mera técnica policial. Es decir, que el necesario control jurisdiccional que se ejerza sobre sus actuaciones carece por completo de connotación inquisitiva alguna, deviniendo únicamente en un examen de su adecuación al principio de legalidad que permita el desarrollo de un proceso penal con todas las garantías posibles, sin que su finalidad expresa sea la de detectar conductas desviadas merecedoras de sanción disciplinaria o penal[114].

No se alcanza a comprender cómo puede concebirse que el resultado final de una investigación policial en sede penal sea consecuencia de los deseos inconfesables de la PJE de quebrar su imparcialidad al investigar un caso, ni con qué torticeros medios puede perturbar a la Justicia para conseguirlo sin perfeccionar al mismo tiempo algún reprensible tipo delictivo.

Sobre la cuestión de la imparcialidad[115] de la PJE, DOLZ dice que:

---

[113] La única diligencia valorativa que se incluye en el atestado policial, de forma potestativa, con meridiana separación del resto del contenido y sin valor procesal alguno, es la denominada "Diligencia de Informe". En ella, el Instructor Policial, dejando claro que se trata "de la opinión que se formado sobre cómo pudieron producirse los hechos", con escrupulosa apoyatura en los posibles elementos de prueba, prudentemente ofrece su parecer. Siendo esto así, no es difícil colegir el efecto que puede tener para formar a su vez la opinión de Juez Instructor.

[114] Es necesario insistir en que se habla de los miembros de la PJE que diariamente cumplen pundonorosamente su labor bajo criterios profesionales muy exigentes y no aquellos de sus miembros que, excepcionalmente y dado el bajo nivel de corrupción de la PJ española, sean simultáneamente infractores o delincuentes.

[115] Sobre la imparcialidad de la PJE, el art. 5 LOCFSE ordena su *"adecuación al ordenamiento jurídico, especialmente: a) Ejercer su función con absoluto respeto a la Constitución y el resto del ordenamiento*

"Es cierto que en algunos supuestos se ha cuestionado la parcialidad de tales peritos-testigos en tanto son funcionarios de cuerpos y fuerzas de seguridad del Estado, interesados en la persecución y castigo de los delitos, o en el caso de los Inspectores de Hacienda, funcionarios de las Agencias Tributarias, a cuya instancia se persigue penalmente el fraude fiscal. Pero reiteradamente se inclina la jurisprudencia de esa Excma. Sala por afirmar la imparcialidad que se presupone a los funcionarios (Sentencias 1688/2000, de 6 de noviembre de 2000, 20/2001 de 28 de marzo, 776/2001, de 8 de mayo), incluso cuando en la causa estuviera personado como acusación particular el Abogado del Estado (Sentencia 1368/1999 de 5 de octubre).

Por su parte, la Sentencia dictada el 21 de mayo de 2004 por la Sala conformada en el Tribunal Supremo con arreglo al art. 61 de la LOPJ, en recurso electoral 2 /2004, de conformidad con lo que ya había señalado la ya dictada por la misma Sala con fecha 27 de marzo de 2003 que hay que atribuir naturaleza de prueba pericial cualificada a los informes emitidos por las fuerzas y cuerpos de seguridad del Estado, porque el Ordenamiento jurídico español alberga un acabado diseño del estatuto jurídico al que se encuentran sometidos los funcionarios de los Cuerpos y Fuerzas de Seguridad del Estado en garantía de que en su actividad de colaboración y servicio a la justicia actúen con plena imparcialidad y sometimiento no menos pleno a la Ley y al Derecho. Esa realidad no supone sino una particularización de la regla más general de sujeción a la legalidad de todos los poderes públicos españoles, como único cauce viable para conseguir un verdadero reinado del Estado de Derecho"[116].

El resultado de una investigación, tanto si resulta esclarecedor para el proceso penal como si fracasa en su contribución para la demostración de los hechos, es

jurídico y b) Actuar, en el cumplimiento de sus funciones, con absoluta neutralidad política e imparcialidad".

[116] Continúa DOLZ diciendo que *"esto permite precaver cualquier desviación de aquel mandato de plena sujeción a la legalidad y de imparcialidad. Así, el artículo 9.1 de la misma Constitución expresa que tanto los ciudadanos como, en lo que ahora interesa, los poderes públicos, están «sujetos a la Constitución y al resto del Ordenamiento jurídico». En parecida dirección, el artículo 103.1 de esa misma norma suprema previene que la Administración Pública (en la que sin duda alguna quedan insertos los funcionarios policiales) «sirve con objetividad los intereses generales y actúa (...) con sometimiento pleno a la ley y al Derecho». El apartado 3 de este mismo precepto previene que la ley regulará el estatuto de los funcionarios públicos y, dentro de éste, «las garantías para la imparcialidad en el ejercicio de sus funciones»".* Vid. Dolz Lago, Manuel-Jesús. *La aportación científico-policial…op. cit.,* pág. 31 y ss.

consecuencia exclusiva de la transparente, profesional y proporcionada actuación policial que, desde parámetros estrictamente técnicos y periciales, los acopie y presente de forma fidedigna ante la Autoridad Judicial.

Como parte de esta actividad, y como no podría ser menos, el Instructor Policial no se determina a sí mismo de forma obsesiva a conseguir que su sospecha adquiera carta de su naturaleza, sino también a comprobar si lo que la desmiente puede verificarse.

Sobre la cuestión de la ***inmediatez*** o no a Jueces y Fiscales, en absoluto pretende la PJE un alejamiento de la acción jurisdiccional que le permita llevar a cabo sus investigaciones "sin intromisiones", lo que sería radicalmente contrario a sus principios de actuación y, desde luego, perturbador del proceso penal. Antes bien, la fórmula impuesta por el modelo policial vigente – que conlleva la dependencia funcional del Poder Judicial -, hace que los miembros de las UOPJ sean asignados de una forma dinámica a las investigaciones, tanto si son de iniciativa propia como si han sido ordenadas verbalmente o por escrito por Jueces o Fiscales, lo que supone una adscripción temporal al juzgado o Fiscalía de que se trate en tanto dure la investigación.

Esta adscripción no se produce en exclusiva, ya que lo normal es que el equipo de investigación, dada la elevada cifra delictiva, lleve a su vez otros casos con dependencia funcional de otros juzgados o Fiscalías, que demandarán la acción policial de una manera a veces totalmente imprevisible[117]. No es necesario insistir, de otro lado, en la cuestión de la disponibilidad que ello acarrea y que ocasiona no pocos conflictos cuando uno de los Jueces o Fiscales exige atención preferente o exclusiva. No se dejan de constatar, por tanto, los defectos del sistema.

Por todo lo anterior, si algo busca el Instructor Policial es, precisamente, el respaldo de la Autoridad Judicial – su inmediatez -, especialmente en aquellas

[117] Por ejemplo, una fase de detenciones y registros domiciliarios embeberá durante días todos los recursos humanos y materiales disponibles, lo que impedirá, con toda evidencia, atender otras necesidades, por más que la vocación y disponibilidad de la PJE pueda de una forma u otra paliar estas deficiencias.

investigaciones complejas en que un dictamen jurídico previo haya de orientarlas desde un principio[118].

Es necesario también dilucidar si los agentes de la PJ actúan desde una fuerte motivación profesional para reducir la delincuencia de tal intensidad que pudiera comprometer su posición en el proceso penal, al verse contaminada su imparcialidad.

Cierto es que la vocación última de cualquier miembro de las FCSE, pertenezca o no a la PJE, es la de conseguir una sociedad libre de delitos y delincuentes[119], tarea en la que vuelcan todos sus esfuerzos[120]. Con injustificada lógica, podría pensarse que esta lucha condiciona su imparcialidad a la hora alcanzar sus fines. Sin embargo, nada más lejos de la realidad. Sin embargo, el art. 5.1 LOCFSE, como no podía ser menos, hace imperativo el principio de legalidad como criterio de actuación de sus miembros, ordenando el absoluto respeto a la Constitución y el resto del Ordenamiento jurídico, a actuar con imparcialidad y colaborar con la Administración de Justicia[121].

Sobre la "voluntad de éxito" de los investigadores, que pretendidamente condicionaría su imparcialidad, no puede sino atribuirse también a cualquiera de los demás operadores jurídicos del proceso penal, de lo que no se sustraen tampoco los Jueces y Fiscales, quienes desean finalizarlas con el pleno esclarecimiento de los hechos.

---

[118] Esto es muy común en el tratamiento de la delincuencia económica y, particularmente, de la corrupción, donde es necesario estudiar con gran detenimiento los complejos indicios de criminalidad que se observen ya que, normalmente, la maquinación criminal consistirá en la vulneración artificiosa de diversos cuerpos jurídicos con interposición de testaferros, falsedades documentales, uso de paraísos fiscales, etc. Consecuentemente, el Instructor Policial necesitará tempranamente consolidar tales indicios desde un plano jurídico contando con la opinión del Juez o el Fiscal.

[119] Sumándose con ello a la función atribuida al MF de actuar para *"la defensa de los derechos de los ciudadanos y del interés público"* de acuerdo con el art. 124.1 CE, lo que, según GIMENO, lo diferencia de la función asignada a los Jueces. Vid. Gimeno Sendra, Vicente. *Propuestas para una nueva Ley de Enjuiciamiento Criminal. La reforma de la LECRIM y la posición del MF en la investigación penal*. Revista del Poder Judicial. Madrid, 2006.

[120] Este efecto, es tanto más visible en el modelo policial español en la medida en que unas mismas FCSE ejercer las funciones de Policía de Seguridad nacidas del art. 104 CE y las de Policía Judicial consagradas en el art. 126 CE.

[121] En relación con el mandato legal que impera sobre la Policía Judicial, de intenso enraizamiento constitucional, acertadamente señala MARTÍNEZ PÉREZ que "l*as FCS se encuentran vinculados a las disposiciones que con carácter general rigen la actividad pública, sometidos los principios de eficacia, jerarquía, descentralización y coordinación, con sometimiento pleno a la ley, al Derecho (arts. 9.1 y 103 CE) y, en particular a los derechos y libertades fundamentales reconocidos en el Capítulo Segundo del Título I del texto constitucional (art. 53 CE).* Vid. Martínez Pérez, Roberto. *Policía Judicial y…op. cit.,* pág. 53.

En relación con otro de los elementos en juego, el de la ***neutralidad*** de la Policía Judicial, dice la Instrucción 1/2008 de la Fiscalía General del Estado que:

> *"La existencia de una estructura de Policía Judicial no sólo refuerza la independencia del Poder Judicial, sino que permite realizar la actividad policial con la denominada "neutralidad del investigador" - STS 1207/95, de 1 de diciembre*[122] *- y con la necesaria proyección jurídica para alcanzar validez en el proceso penal; proporcionando, además, en virtud de su especialización, mayor eficacia en la labor policial en el orden criminal".*

En mi opinión, el sistema actual de instrucción hace que el Juez y el Fiscal, sin perder de vista la faceta de preservación de las garantías, muestren idéntico interés en la resolución del caso que el que pueda tener el Instructor Policial. Todos ellos ansían "llegar al fondo del asunto", sin que por ello se les pueda tachar de parciales.

Por tanto, si se identifican los imperativos comunes a los cuatro operadores del Sistema de Justicia Español contenidos en el ordenamiento jurídico nacido de la Constitución Española (En adelante, CE), veremos que estos son, precisamente, los de actuar con absoluta ***imparcialidad, neutralidad y sujeción al principio de legalidad***, hallado en la legislación y que obliga plenamente a Jueces, Fiscales, Secretarios Judiciales y Policías Judiciales.

A estos factores se unen además las cualidades específicas de la PJ que, de una forma resumida son: La ***adecuación del modelo policial español*** a las finalidades del proceso penal, la ***inmediatez*** de la PJ a Jueces y Fiscales y su completo ***grado de autonomía*** para el ejercicio de la función consagrada en el art. 126 CE. Finalmente, y para todos ellos, hay que añadir otros dos factores esenciales – y no precisamente menores - y que son o deben ser comunes a todos ellos: su exigente ***formación técnica y científica*** y la estricta ***perspectiva ética y deontológica***[123] que ha de acompañar a todos sus actos. Todo lo anterior, en mi opinión, configura una PJ merecedora de la más alta consideración dentro del proceso penal español.

---

[122] En este mismo sentido se pronuncia la STC 36/1995, de 6 de febrero.

[123] Sobre esta compleja cuestión, vid. Garrido Roca, Pedro. *Corrupción policial y tráfico de drogas* en Marchal Escalona, Nicolás (Director). *Manual de lucha contra la droga.* ISBN: 978-84-9903-003-6. Cízur Menor (Navarra): Aranzadi. 1ª Edición, 2011, pág. 345 y ss.

2. ¿Una Policía Judicial dependiente en exclusiva del Poder Judicial?

Las dudas que se han planteado sobre la adecuación del modelo policial español a las necesidades del proceso penal motivan una breve reflexión sobre la necesidad de que la PJE fuera dependiente en exclusiva del Poder Judicial y no de estructuras orgánicas dependientes de las autoridades gubernativas. En este sentido, es frecuente en la doctrina la preocupación por el modelo español de Policía Judicial en caso de que estuviese sometida a contrapoderes de tal fuerza imperativa que condicionasen su posición frente a los tribunales y al Ministerio Fiscal[124].

Algo se ha avanzado con las aportaciones anteriores sobre la autonomía, neutralidad e imparcialidad de la PJE y, aunque no se pretenda dejar sentado paragón alguno en este punto con el Poder Judicial[125], sí se puede concluir que tales notas son suficientes para el estricto cumplimiento de la función encomendada por el art. 126 CE, más allá de su adscripción orgánica al Poder Ejecutivo y de las dudas que ello pueda suscitar.

Sin embargo, interesa en este punto que se profundice algo más en las opiniones contrarias, pues pueden hallarse en la doctrina posiciones a favor de la dependencia plena de la PJ del Poder Judicial[126] basadas, en mi opinión, en

[124] En efecto, MARTÍNEZ PÉREZ muestra sus dudas respecto de su validez frente al Poder Judicial *"si el instrumento fundamental con el que cuenta para realizarla, la PJ, le resulta un instrumento ajeno, sometido a vínculos de disponibilidad y fidelidad a otros poderes, sino también si con ello atiende a exigencias cuando menos extrañas a la ley".* Vid. Martínez Pérez, Roberto. *Policía Judicial y…op. cit.,* págs. 82 y 83. No he podido desentrañar a qué puede referirse el autor con lo de *"atender a exigencias cuando menos extrañas a la ley"*. La PJ está plenamente sometida al principio de legalidad y sus mandos absolutamente concernidos por las exigencias del Estado de Derecho.

[125] Para el Tribunal Constitucional, *"la estricta imparcialidad e independencia de los órganos del poder judicial no es, por esencia, predicable en la misma medida de un órgano administrativo"* (STC de 15 de febrero de 1990).

[126] Es evidente que este modelo debe incluir la dependencia orgánica del poder judicial, lo que JIMÉNEZ VILLAREJO anota cuando dice que *"la mejor garantía de la dependencia funcional hubiese sido el reconocimiento de la orgánica, que la coexistencia de las dos implica forzosamente una dualidad de lealtades…"*. Vid. Jiménez Villarejo, José. *La Policía Judicial: Una necesidad, no un problema.* Poder Judicial. Número Especial II, Justicia Penal. Madrid, 1988, págs. 175-188.

impensables incumplimientos del art. 35 LOCFSE, cuya redacción es de una reseñable claridad y carácter imperativo para la PJ[127,128]:

Art. 35 LOCFSE:

"Los Jueces y Tribunales de lo Penal y el Ministerio Fiscal tendrán, respecto los funcionarios integrantes de Unidades de Policía Judicial que le sean adscritas y de aquellos a que se refiere el número 2 del artículo 31 de esta Ley, las siguientes facultades:

a. Les darán las órdenes e instrucciones que sean necesarias, en ejecución de lo dispuesto en las normas de Enjuiciamiento Criminal y estatutos del Ministerio Fiscal.

b. Determinarán, en dichas órdenes o instrucciones, el contenido y circunstancias de las actuaciones que interesen a dichas Unidades.

c. Controlarán la ejecución de tales actuaciones, en cuanto a la forma y los resultados.

d. Podrán instar el ejercicio de la potestad disciplinaria, en cuyo caso emitirán los informes que puedan exigir la tramitación de los correspondientes expedientes, así como aquellos otros que considere oportunos. En estos casos recibirán los testimonios de las resoluciones recaídas".

Sin embargo, pese a tan diáfana prescripción y en línea con otros autores citados, MARTÍNEZ PÉREZ insiste en la desconfianza en la PJ con la frase *"es francamente difícil imaginar un funcionario de policía que desobedeciendo las órdenes de sus superiores jerárquicos, atienda por gusto el requerimiento de colaboración que le haga un Juez o Fiscal y mantenga una rectitud de principios que son los que deben regir esta colaboración. La perplejidad alcanzaría un plus añadido si se tratara de un*

[127] Sostiene GONZÁLEZ MONTES que *"lo propio de una verdadera Policía Judicial sería atribuir una dependencia plena de las autoridades judiciales, con lo que la situación actual de doble dependencia, lo único que puede originar son disfunciones en el normal discurrir de la Administración de Justicia, con relación a la posibilidad de dar órdenes y el efectivo cumplimento de las mismas, cuestionándose el contenido del art. 35 LOFCSE"*. Vid. González Montes, José Luis. *Instituciones de Derecho procesal. Parte General.* Granada, 1990, pág. 321. Ciertamente, no se alcanza a comprender cómo puede la PJE sustraerse del cumplimiento del art. 35 LOFCSE sin situarse escandalosamente por encima de una ley orgánica de firme anclaje en los arts. 104 y 126 CE.

[128] Vid. Prieto Castro y Gutiérrez de Cabiedes, Eduardo. *Derecho Procesal Penal.* Madrid, 1987.

miembro perteneciente a un cuerpo de estructura militarizada o de cuerpos o servicios secretos dependientes del Ejecutivo".

Este desalentador comentario, que me merece todo el rechazo, supone atribuir a la PJE y, en especial, a sus mandos, un olímpico desprecio del principio de legalidad que debe presidir todos sus actos. Sin necesidad siquiera de acudir a la inexorable responsabilidad penal personal que se asociaría a tales conductas, en el muy improbable caso de que se produjeran, se debe proclamar la irracionalidad de tales temores, especialmente en el caso de los *"cuerpos de estructura militarizada"* y de sus tan temidos mandos[129].

Las afirmaciones de quienes desde la doctrina han argumentado la imposible lealtad de la PJE al Estamento Judicial y Ministerio Fiscal[130,131] atribuidas a las insuficiencias del modelo actual, quedan en mi opinión disipadas por la fuerza de los hechos, asentados por el estable devenir del ejercicio cotidiano de las facultades conferidas a la PJE por el ordenamiento constitucional nacido en 1978, esto es, ya más de treinta años atrás.

La dependencia funcional de la PJE respecto de Jueces y Fiscales se renueva día a día y caso a caso, verificándose con toda naturalidad y diligencia sea cual fuere su

[129] Hay que colegir que el autor se está refiriendo al Cuerpo de la Guardia Civil, de estructura militar (y no "militarizada", pues no se trata de ningún adorno jurídico que se le sobreponga), que si por algo se distingue es, precisamente, por dar la mayor exactitud al cumplimiento de la legislación vigente, todo ello de forma completamente ajena a cualquier signo de politización, como es público y notorio, lo que se hace especialmente visible en el ejercicio de la función de Policía Judicial. Los mandos de la Guardia Civil jamás dan órdenes que puedan contrariar al Derecho, en cuyo caso sus subordinados tendrían la obligación legal de desobedecerlas y de denunciar a continuación tan reprensibles conductas. Defenderé vehementemente esta posición, así como serán objeto de crítica, por injustos, los comentarios al efecto. Vid. Martínez Pérez, Roberto. *Policía Judicial y…op. cit.,* pág. 322. En términos similares se pronuncia PEDRAZ al ver la "militarización" como un aparente impedimento natural o incompatibilidad para ejercer funciones policiales, lamentándose de que "*sigue sin resolverse el tema de la militarización de la Guardia Civil que no favorece la exclusiva dedicación de su PJ".* No sólo la favorece, sino que, además, puede llevarla, bajo la estricta dependencia de los Jueces, al escenario de la guerra si es necesario, cosa que no podría hacer el CNP, por ejemplo. Vid. Pedraz Penalva, Ernesto. *Notas sobre policía y justicia penal*. Revista Jurídica de Castilla y León. 2008, pág. 44.

[130] Para MENA ÁLVAREZ *"resulta quimérico pretender una eficaz dependencia funcional de la Policía Judicial*". También opina que *"la independencia del Poder Judicial estará en razón inversa a la dependencia real que tenga la Policía Judicial respecto del Poder Ejecutivo"*. Vid. Mena Álvarez, José María. *La Policía Judicial. Los comunistas y la reforma de la Administración de Justicia.* Madrid, 1981, págs. 35-44, pág. 36.

[131] FERRAJOLI proclama que *"la Policía Judicial, encargada de la investigación de los delitos y de la ejecución de las decisiones judiciales, debería estar rígidamente separada de los demás cuerpos de policía y dotada de las mismas garantías de independencia frente al ejecutivo que el poder judicial del que debería depender en exclusiva".* Vid. Martínez Pérez, Roberto. *Policía Judicial y…op. cit.,* pág. 322

duración o complejidad, por imperativo del principio de legalidad y de todas las disposiciones que la obligan.

Lo anterior se manifiesta sin tacha alguna con total normalidad a través de la dinámica adscripción funcional de unidades pertenecientes a la PJE a los Jueces y Fiscales, dotándolas con una composición adecuada a las necesidades específicas de cada caso y disponiendo los apoyos genéricos y técnicos de todo tipo que puedan suscitarse, lo que se constituye en un proverbial respaldo al más exacto cumplimiento de las necesidades manifestadas por tales autoridades que, por lo demás, raramente expresan indisposición alguna con los servicios que se les prestan sino, antes bien, manifiestan su gran satisfacción al efecto.

No existe, consecuentemente, polarización alguna entre la dependencia orgánica y la dependencia funcional de la PJE, nacida del desarrollo legislativo posterior, fundamentalmente mediante diversas leyes orgánicas, de los arts. 104 y 126 CE[132], lo que sería interpretado como un acto fallido de construcción de un modelo constitucional de PJ enteramente dependiente del Poder Judicial[133].

Pero, tras expresar la apuesta por una Policía Judicial dependiente en exclusiva del Poder Judicial, no llega este sector doctrinal a indicar cómo debiera estar estructurada en un plano práctico, limitándose a proclamar la consabida necesidad de la *"plena dependencia del Poder Judicial"*, pero sin que se conozcan siquiera alguna de las líneas maestras que desarrollarían sus alternativas o propuestas.

En su expresión más genuina, y si hay que atenerse a la independencia de los Jueces, puede pensarse que cada titular necesitará disponer en su juzgado de una unidad de policías judiciales a su plena disposición, para preservar su actuación sin contaminación de estructuras "ajenas al Poder Judicial" y sin que compromisos de ningún género perturbasen su plena disponibilidad y autonomía para cumplir los mandatos de su Juez Titular. Mandatos como, por ejemplo, auxiliar en caso de apuro a

[132] Para MARTÍNEZ PÉREZ, *"la constitucionalización de esta nota de dependencia no puede entenderse de otro modo sino como reforzamiento de la relación entre Jueces y Fiscales y Policía Judicial, que sin embargo no ha sido tal con el desarrollo legislativo postconstitucional"*. Vid. Martínez Pérez, Roberto. *Policía Judicial y…op. cit.,* pág. 317.

[133] Aunque como señala BLÁZQUEZ GONZÁLEZ, *"la falta de un modelo de Policía Judicial, al margen de la situación actual en el modelo policial, tiene su explicación en la coexistencia de una normativa post-constitucional fragmentaria, y en la discutible vigencia de algunos artículos de la LCRIM"*. Vid. Blázquez González, Félix. *La Policía Judicial…op. cit.,* pág. 100.

los compañeros del juzgado adyacente, lo que supondría, entre otras cosas, asumir complicadas tareas de gestión del horario laboral compartido o de la complicada logística policial (sin que pretenda ser exhaustivo en la enumeración de las posibles incidencias). Se ha de entender que las posibilidades presupuestarias harían imposible además la asignación de tales puestos en suficiente número como para cubrir siquiera medianamente esta configuración, con tantos Juzgados de Instrucción y Fiscalías repartidos por el territorio nacional, sin contar con cubrir las necesidades logísticas inherentes a la función.

Un modelo como el anterior mutilaría a la PJ de toda su eficacia actual, pues se vería privado de la visión de conjunto que proviene del acceso a los sistemas de gestión de la inteligencia policial compartidos, la disponibilidad de los laboratorios forenses, el apoyo de unidades de intervención policial, la proyección internacional de las investigaciones, de gestión de los recursos logísticos, de los centros de formación, etc.

Se haría impensable además la iniciativa en la apertura de investigaciones surgidas de la observación directa de la realidad delincuencial, lo que se constituye en todo un signo de identidad del modelo actual de policía. Y, por lo demás, ¿Cómo se gestionarían las funciones de la PJG si estas se atribuyen masivamente a la Policía de Seguridad?[134]

Se admite, por tanto, la necesidad de disponer de una estructura orgánica y de una dirección técnica que ampare a la PJ, en lo que parecen coincidir los autores mencionados, que facilite y gestione todos estos recursos de una forma dinámica para cubrir las necesidades concretas de la investigación policial que planteasen las diversas autoridades judiciales y fiscales y, se supone, que cubra con holgura cualquier necesidad de intervención por compleja y alargada en el tiempo que resulte, sin escatimar recursos. Siguiendo a los autores mencionados, esta estructura debiera, como sostienen, ser dependiente en exclusiva del Poder Judicial. La pregunta inmediata sería: ¿De qué estructura del Poder Judicial?

[134] En este sentido, vid. Jar Couselo, Gonzalo. *Jueces-Policías: problemas de relación entre Poderes Judicial y Ejecutivo,* en Rechea Alberola, Cristina (dir.) et al. *La criminología aplicada II.* Consejo General del Poder Judicial. Madrid 1999, citado a su vez por Corral Escáriz, Vicente. *Problemática de la Policía Judicial…op. cit.,* pág. 95.

En la respuesta debe descartarse al Ministerio de Justicia, por ser un ente que ejecuta la política del Gobierno de turno en la materia, en la misma medida en que hace lo propio el Ministerio del Interior con respecto a la política de seguridad, lo que merecería todas y cada una de las tachas reiteradamente expuestas por los autores. Y, mucho me temo, por similares razones, habría que descartar también al Consejo General del Poder Judicial, cuya composición responde también a criterios de elección de sus miembros revestidos de un innegable componente político, deducidos de la forma en que la Ley lo dispone al efecto[135,136].

En suma, y por lo que es conocido, el modelo actual de PJ no suscita en el plano real las preocupaciones que muestran los autores estudiados en el plano doctrinal, recibiendo los Jueces y Fiscales con sumo agrado, y podría decirse en general que con total confianza y despreocupación, los servicios que regularmente les prestan la PJE desde una amplísima carta de sofisticados servicios. El liberarse de la carga que supondría su gestión no es motivo sino de un gran alivio en su complicado quehacer diario.

Por ello, soy de la opinión de que la estructura en funcionamiento en España, pese a sus deficiencias, ha superado ampliamente los estándares de eficiencia, autonomía e imparcialidad que serían exigibles en un Estado de Derecho.

Por lo tanto, si la dependencia orgánica tiene una naturaleza eminentemente administrativa; si, por su parte, la dependencia técnica se ocupa asépticamente de resolver sobre aspectos operativos, procedimentales, periciales o de técnica policial[137]; y si, finalmente, la actuación de la PJE se hace mediante la estrecha dependencia funcional de la Autoridad Judicial o Fiscal, actuando como sus comisionados; debe

[135] Arts. 112 y 113 LOPJ. El consenso político que se presume de la obligación de la elección de los candidatos por acuerdo de las tres quintas partes de las cámaras del Parlamento Nacional no empece para que se hayan suscitado numerosas dudas sobre su politización.

[136] Sobre los aspectos de interés relativos al Poder Judicial y, en particular, sobre los peligros de la politización de la Justicia, vid. Andrés Ibáñez, Perfecto y Movilla Álvarez, Claudio. *El Poder Judicial.* Temas claves de la Constitución Española. Madrid, 1986.

[137] Por ejemplo, una entrada y registro no es sólo un acto procesal relacionado con la limitación del derecho fundamental recogido en el art. 18.2 CE sino, también, una operación policial que debe planificarse meticulosamente para que alcance todos sus fines. Incluirá una táctica de entrada y aseguramiento de pruebas y personas, una inspección ocular, una recogida de pruebas que preserve su cadena de custodia, la práctica de detenciones, volcados de equipos informáticos, pericias, etc. Es evidente que una actuación de esta naturaleza, por simple que parezca, necesita de una organización fuertemente jerarquizada que soporte las acciones propuestas por el Instructor Policial.

concluirse que las notas de autonomía e imparcialidad de la PJE, al menos en un plano práctico y real[138], están lo suficientemente asentadas como para presumirse que nada debe temerse de actuaciones contaminantes del proceso penal por parte del Instructor Policial en su relación con el mando orgánico[139].

3. El atestado policial: una relación veraz de la intervención policial

La forma material con que la PJ presenta sus actuaciones ante la Autoridad Judicial es el ***atestado policial*** (cuya primera regulación se sitúa en el art. 292 LCRIM), al que la jurisprudencia y la doctrina atribuyen, de una manera un tanto destemplada, un "mero valor de denuncia" siguiendo lo preceptuado en el art. 297 LCRIM[140], de obsoleta descripción de lo que en realidad representa para el proceso penal si se observas a la evolución técnica que ha sufrido con el paso del tiempo.

---

[138] Debe excluirse de esta acepción cualquier similitud con la consagrada independencia de los Jueces, de altísimo blindaje constitucional. No se pretende comparar a Jueces con policías judiciales por este aspecto.

[139] CORRAL, que aporta una amplia e interesante descripción de los diversos y polarizados pareceres jurídicos que pueden encontrarse en la doctrina sobre la dependencia de la PJ, en opinión a la que me adhiero, afirma que, *"urge, por lo tanto, encontrar una solución de compromiso, que bien podría ser mantener la situación actual de inexistencia de un cuerpo específico [de policía judicial] y por lo tanto de doble dependencia, pero adoptando las medidas necesarias para garantizar la salvaguardia de la independencia judicial como prioridad absoluta, evitando que la dependencia funcional pueda resultar subordinada a la dependencia orgánica. En resumen, como se ha dicho en alguna ocasión, "prima en todo caso sobre cualquier otra consideración, la llamada dependencia funcional, y si existen problemas derivados de la dependencia orgánica que directa o indirectamente afecten a la funcional, deben solventarse siempre a favor de la función constitucional expresamente referida en el artículo 126 citado"".* El autor se apoya en Sala i Donado, Cristina. *La Policía Judicial.* Aravaca (Madrid): McGraw Hill, 1999, pág. 11 y, en la inserción literal *in fine,* en Boix Reig, Francisco Javier. *Policía y Administración de Justicia,* en el I Seminario de colaboración institucional entre la Universidad Internacional Menéndez Pelayo y la Dirección General de la Policía, *Policía y Sociedad.* Dirección General de la Policía. Santander, 1989, pág. 141. Vid. Corral Escáriz, Vicente. *Problemática de la Policía Judicial…op. cit.,* pág. 98. Sobre la naturaleza de las diversas dependencias, vid. Moreno Catena, Víctor. *Dependencia orgánica y funcional de la Policía Judicial.* Poder Judicial. Núm. Especial VIII. Madrid, 1988.

[140] *Artículo 297.*

"Los atestados que redactaren y las manifestaciones que hicieren los funcionarios de Policía Judicial, a consecuencia de las averiguaciones que hubiesen practicado, se considerarán denuncias para los efectos legales.

Las demás declaraciones que prestaren deberán ser firmadas, y tendrán el valor de declaraciones testificales en cuanto se refieran a hechos de conocimiento propio.

En todo caso, los funcionarios de Policía Judicial están obligados a observar estrictamente las formalidades legales en cuantas diligencias practiquen, y se abstendrán bajo su responsabilidad de usar medios de averiguación que la Ley no autorice".

Con esta crítica no se pretende restar independencia al ejercicio de la jurisdiccionalidad como consecuencia de haber recibido de la PJE un atestado o, aún menos, colonizar el proceso penal en su conjunto, otorgándole a este instrumento, de naturaleza estrictamente policial, un valor de tal fuerza determinante de su resultado que, en un sistema democrático basado en el ***principio acusatorio***, no resultaría procedente.

El ***principio de libre valoración de la prueba***, que respalda a la actuación de quien realiza una actuación jurisdiccional, hace que el contenido del atestado, junto con los demás elementos de juicio, se sometan al imparcial escrutinio del juzgador, quien otorgará a sus concretas aportaciones el valor probatorio que estime procedente.

Sin embargo, y siguiendo a MARCHAL[141], mucho habría que decir del valor real del atestado[142] para el moderno proceso penal y que trasciende a lo que sería una *"mera comunicación verbal o escrita de hechos presuntamente delictivos"*[143], con un innegable y exponencial crecimiento en su calidad técnico-científica y carácter determinante para la formación de la opinión judicial desde que la anciana LCRIM entrase en vigor en 1882 (en que difícilmente se pudiera hablar de una Policía Judicial siquiera aproximada al concepto actual y, menos aún, de una Policía Científica), antes incluso de que la naciente ***ciencia de la criminalística***, aunque revestida de extraordinario mérito científico, diese sus primeros y tambaleantes pasos de la mano de los fracasados estudios de los ***antropometristas*** Lombroso, Bertillón, Gall o Cubí i Soler o los hoy perfectamente válidos y vigentes hechos por Vucetich sobre la identificación de las personas mediante el estudio de sus huellas digitales[144].

---

[141] Vid. Marchal Escalona, Nicolás. *El atestado. Inicio del proceso penal.* 8ª Edición. Pamplona: Thomson Aranzadi, 2010. También, vid. Álvarez Rodríguez, José Ramón. *El atestado policial completo.* Madrid: Tecnos, 2007 y Martín Ancín, Francisco, Álvarez Rodríguez, José Ramón. *Metodología del atestado policial. Aspectos procesales y jurisprudenciales.* Madrid: Tecnos, 1999 y Alonso Pérez, Francisco. *La Policía Judicial. Legislación, comentarios, jurisprudencia y formularios.* 3ª Ed. Madrid: Dykinson, 1998, págs. 57 y ss.

[142] Falto, por lo demás, de valor como prueba documental, tal y como se proclama en las SSTC 100/1985, 217/1989, 303/1993, 51/1995 ó 157/1995), otorgándosele el menor de testifical.

[143] Según el diccionario *"Documento en que se da noticia a la autoridad competente de la comisión de un delito o de una falta"*.

[144] El mismo año de 1882 BERTILLÓN exponía sus primeras conclusiones basadas en los estudios antropométricos de diversos delincuentes (el llamado "bertillonaje"), pretendiendo con ello, aún sin éxito, explicar el comportamiento criminal. Menos afortunados, pero igualmente meritorios, fueron los

Desde la promulgación de la LCRIM, la evolución de la técnica policial y la criminalística puede calificarse de espectacular[145] por dos motivos esenciales: porque la apoyatura de la investigación en el método científico es absoluta y porque no se trata de unas materias reservadas a las investigaciones policiales más sofisticadas, trascendentes o complejas, sino que son parte de la labor cotidiana que realizan con perfecta solvencia todos los miembros de la PJ en sus quehaceres más nimios.

Así, en el transcurso de una inspección ocular en el lugar de los hechos (un robo con fuerza en un domicilio, por ejemplo), pueden recogerse huellas digitales que permitirán un cotejo posterior con los sospechosos mediante su contraste con los datos contenidos en las bases policiales. Un fluido o resto corporal del sospechoso, como la saliva o el pelo, permitirán un análisis de DNA de gran valor identificativo. Podrá analizarse la voz del sospechoso, tomarse audio, video o imagen de sus movimientos, analizarse el contenido de sus comunicaciones y los datos de tráfico y localización, estudiarse sus interacciones en el sistema económico-financiero o social, reconstruirse sus movimientos físicos, etc. Todo ello, además, podrá contrastarse con las declaraciones y acciones de testigos, cómplices o víctimas, cuyo resultado quedará indubitadamente reflejado en los informes periciales facultativos acompañados de las consistentes pruebas materiales que se han mencionado. Estos elementos tendrán el valor probatorio que la Autoridad Judicial prudentemente les atribuya en el acto de juicio oral, poniendo en relación unos hechos de naturaleza delictiva con las personas penal y civilmente responsables, determinando unas concretas consecuencias jurídicas, naturalmente, caso de haber estimado la suficiencia e irrefutabilidad de las pruebas examinadas.

En este marco, tendrán el carácter de ***prueba preconstituida*** y, por lo tanto, sin sujetarse a los principios de inmediación y contradicción, las que recojan datos de naturaleza objetiva, tales cmo las aprehensiones, la ocupación de efectos, croquis,

---

intentos posteriores de GALL y CUBÍ I SOLER de desentrañarlo mediante la frenología, pretendida ciencia que se fundamentaba en la relación entre la morfología del cráneo de los delincuentes y su comportamiento criminal. Tendría que ser VUCETICH quien en 1891 (esto es, nueve años después del nacimiento de la LCRIM) estudiase con acierto el valor individualizador de las huellas digitales para determinar indubitadamente la identidad de la persona a quienes pertenecían y, con ello, facilitar la demostración de los actos criminales en cuya escena hubieran estado. Sobre cuestiones de orden criminológico, vid. Serrano Maíllo, Alfonso. *Introducción a la criminología.* Madrid: Dykinson, 2005.

[145] En un muy considerado comentario de GIMENO, *"la policía en tres días hace mucho más trabajo que los Jueces en meses o incluso años".* Vid. Gimeno Sendra, Vicente. *Propuestas para una nueva…op. cit.*

fotografías, alcoholemia, etc. Lo único que se exigirá es que estén realizadas, con mayor o menor proximidad, bajo la supervisión del órgano jurisdiccional[146].

En cualquier caso, se necesitará la ratificación de los componentes de la PJ, en calidad de testigos o de peritos, en el juicio oral[147], aunque este requisito no minora el principio de libre valoración de la prueba que corresponde al órgano jurisdiccional (art. 741 LCRIM).

El corolario que puede deducirse de todo ello es de una extraordinaria simpleza pero, a la vez, de una gran trascendencia para la impartición de Justicia en un Estado de Derecho, en una doble expresión: De un lado, y en términos generales, las pericias practicadas por la PJ no tienen contradicción científica posible y, por imperativos de orden técnico, no contienen cláusulas valorativas del instructor o facultativo, salvo que contengan errores inadvertidos o se trate de atestiguar hechos que, por diversas circunstancias, no hayan podido ser suficientemente contrastados, lo que de forma clara se precisará en el cuerpo del informe policial[148]; y, de otro lado, permiten una libertad total del juzgador para situarlas en el contexto de los hechos y permitir su más exacta valoración en el acto de juicio oral, bajo los principio***s de publicidad, inmediatez, contradicción y oralidad***[149], deduciéndose de estas dos afirmaciones, que la parte esencial y determinante de un proceso penal habrá sido elaborada y puesta a disposición del juzgador, con todas las garantías posibles, precisamente, por la PJE.

De la lectura del segundo párrafo del art. 297 LCRIM, y respecto de los testimonios de los funcionarios de la PJ, MARCHAL hace unas interesantes precisiones sobre el peso jurídico real que merecería dentro del proceso penal, proclamando que están revestidos de *"una especial presunción de certeza, en orden a la futura*

[146] Vid. Ruiz Vadillo, Enrique. *El proceso penal en el estado social y democrático de derecho*. Cuadernos de la Guardia Civil. Madrid, 1993, pág. 14.
[147] Vid. *El atestado policial.* Gordillo Álvarez-Valdés, Ignacio. *El atestado policial*. Revista de documentación. Madrid, 1996, pág. 19.
[148] Naturalmente, se excluyen de este comentario las actuaciones maliciosas de la PJE, que serían a su vez, materia delictiva, lo que se puede descartar en cuerpos policiales como los españoles que presentan unos índices de corrupción extraordinariamente bajos y no relacionados normalmente con la praxis de la función de Policía Judicial. La anulación de pruebas practicadas por la PJE hay atribuirla en su inmensa mayoría a la falta de una regulación procesal adecuada, lo que las hace inválidas o vulnerables a la contradicción. Caso paradigmático de esta afirmación podría comprobarse, precisamente, tras el análisis de las causas de anulación de las intervenciones telefónicas en determinados procesos penales, materia que excede el propósito de este estudio.
[149] Véanse las SSTC 1281/2006; 127/1990; 137/1988; 22/1988; 150/1987; 80/1986; 31/1981.

apreciación judicial de la prueba", estableciendo al respecto un sustento en los preceptos jurídicos incluidos en el art. 5 EOMF y el 14 RDPJ[150].

Las críticas de algún sector de la doctrina a las anteriores afirmaciones parecen resumirse en la no jurisdiccionalidad de la actividad PJ en su estructuración actual, a su no adscripción al Poder Judicial y al carácter meramente preliminar del atestado.

Sin embargo, el propio Alto Tribunal, considerando anacrónica la redacción del art. 297 LCRIM, hace variar al alza la valoración actual de los atestados según se trate de:

1) *Opiniones o informes de los imputados, aunque se les haya instruido de sus derechos constitucionales y hayan gozado de la asistencia de un letrado, declaraciones de testigos, diligencias de reconocimiento en rueda o de otras semejantes no se les puede atribuir más que el de meras denuncias.*
2) *Dictámenes o informes prestados por gabinetes policiales, al menos, el de dictámenes periciales y especialmente si se ratifican a la vista del juicio oral, con posibilidad a las partes de pedir aclaraciones, formular observaciones a los miembros de los indicados gabinetes (prueba pericial[151]), y*
3) *Tratándose de diligencias objetivas y de resultado incontestable, como la aprehensión en el lugar de los hechos de los delincuentes, los supuestos en que son sorprendidos en situación de flagrancia o cuasi flagrancia, la ocupación o recuperación de los efectos o instrumentos del delito, armas, drogas o sustancias estupefacientes, los que se hallaren en el transcurso de diligencias de entrada y registro, cumplidas las formalidades procesales, el*

[150] Art. 5 EOMF: *"Todas las diligencias que el MF practique o que se lleven a cabo bajo su dirección, gozarán de presunción de autenticidad".*
Art. 14 RDPJ: *"Las diligencias y actuaciones llevadas a cabo por las UOPJ tendrán el valor reconocido en las Leyes y gozarán de la especial consideración derivada de la adscripción y del carácter de comisionados de Jueces, Tribunales y Fiscales".*

[151] Al analizar el valor jerárquico de las diferentes clases de prueba admisibles en el juicio oral, GUERRERO dice que *"en un plano inferior [respecto de la prueba documental], pero también de mucha preponderancia, se sitúa, por su propia naturaleza, la prueba pericial, pues la misma ilustrará al Juez en una materia (científica, artística o técnica) que el Juez desconoce, pudiendo incluso ser tenida como prueba de cargo, si la misma no es impugnada, cuando estamos ante periciales elaboradas por "organismos oficiales" sobre cuestiones de índole científico (SSTS de 14 de junio de 1991, 12 de abril de 1994 o 1 de febrero de 1995)".* Habrá que volver sobre este asunto cuando se trate la cuestión de la prueba pericial de inteligencia o los informes policiales de inteligencia. Vid. Guerrero Palomares, Salvador. *La denominada "prueba de inteligencia policial" o "pericial de inteligencia".* Revista de Derecho y proceso penal, Núm. 25, 2011, pág. 77.

valor de verdaderas pruebas, sometidas como las restantes, a la libre valoración de las mismas, cuya competencia corresponde a los tribunales de instancia.

Pero el atestado tiene otros caracteres que interesa resaltar y que se suman a la especial consideración que ha quedado reflejada en los párrafos anteriores:

En primer lugar, no es un acto administrativo regulado por la LRJ-PAC y, por tanto, resulta a extramuros de la vía contencioso-administrativa.

En segundo lugar, el atestado es un acto procesal, en la medida en que forma parte del proceso penal, esto es, un acto nacido con vocación de servir a un procedimiento[152].

En tercer lugar, el atestado es un documento público en la forma en que se describe en el art. 1216 CC, ya que su inexactitud podría considerarse delito de falsedad en documento público a tenor de los arts. 390.1 y 391 CP[153].

En el origen de su concepción, el atestado, como elemento de constancia cronológica de los sucesos objetivamente interesantes para la indagación[154], sirve al investigador para ir recogiendo una suma de indicios criminales que, en una fase normalmente temprana de la actividad policial, le llevan a construir una más o menos fundada sospecha[155]. Esta no es otra cosa que una ideación o figuración intelectiva, basada en indicios, sobre la forma en que pudieron producirse los hechos y todas las circunstancias que los rodearon y que habrá que demostrar o refutar.

El paso de la sospecha a la certeza no tiene otra vía que la de la comprobación inequívoca de su naturaleza, para lo que habrá de buscarse el concurso de una depurada técnica policial y pericial, como herramienta profesional, junto con una acrisolada actitud ética y deontológica del investigador para su logro. La sucesión de

---

[152] En palabras de MARCHAL, *"no creemos que lo que le otorgue carta de naturaleza sea su origen [ajeno a la sede judicial], sino el hecho de que se incluya en un proceso".* Vid. Marchal Escalona, Nicolás. *El atestado... op. cit.,* pág. 44.

[153] Vid. Marchal Escalona, Nicolás. *El atestado... op. cit.,* pág. 44.

[154] Tal es la precisión del Instructor Policial que llegará a reflejar meticulosamente en su atestado sucesos aparentemente irrelevantes pero que, en su momento, puedan adquirir una trascendental importancia.

[155] Según el diccionario, "*aprehender o imaginar algo por conjeturas fundadas en apariencias o visos de verdad".*

comprobaciones y refutaciones propiciará finalmente el conocimiento de la verdad, muchas veces completamente ajena a lo que en principio se sospechó.

Por otra parte, debe huirse, por ser por completo ajena a la realidad actual, de la imagen de una PJ que ejecuta pulcramente, pero sin iniciativa ni reflexión alguna, las sucesivas órdenes y resoluciones puntuales que va concibiendo el Juez para desarrollar su instrucción, lo que respondería a la equívoca concepción que se trasluce de la lectura de la antiquísima LCRIM y que parece trasladarse a los tiempos actuales.

Muy por el contrario, son mayoría los expedientes policiales (atestados) que contienen investigaciones llevadas a cabo de principio a fin exclusivamente por la PJE y cuyas sucesivas diligencias son el fruto de una depurada técnica policial. Esto exige inequívocamente la permanente búsqueda, no sólo de las pruebas de cargo que puedan incriminar al investigado, sino aquellas otras que puedan exculparlo (art. 2 LCRIM), en un ejercicio de exigente imparcialidad que no se conforma con la acreditación de la sospecha sin someterla a la debida crítica[156].

Caso paradigmático de lo anterior sería la práctica de aquellas diligencias policiales de comprobación, a incluir de forma diferenciada en el atestado, que resulten procedentes tras las declaraciones en sede policial[157] y realizadas en su descargo por los propios concernidos (Por ejemplo, la negación de hallarse físicamente en el lugar de los hechos que se les imputan, lo que puede comprobarse hoy en día con solventes medios de prueba tales como el examen de testigos, trazabilidad de rastros electrónicos, archivo de imágenes de cámaras de seguridad, etc.). Esta actitud, perfectamente interiorizada por los miembros de la PJ, que es permanente durante todo el proceso investigativo[158], no sólo debe responder a estrictos criterios deontológicos, sino a evidentes exigencias de orden técnico-procesal.

[156] A propósito de la dependencia funcional de la PJE del Ministerio Fiscal, CONDE-PUMPIDO hace notar la obligación de los investigadores de recoger indistintamente todos los vestigios que incriminen o exculpen. Vid. Conde-Pumpido Ferreiro, Cándido. *La Policía Judicial: Sus relaciones con el Ministerio Fiscal.* Cuadernos de la Guardia Civil. Madrid, 1990, pág. 30.

[157] En cumplimiento a los estrictos preceptos contenidos en el art. 520 LCRIM.

[158] Como hace imperativo el art. 2 LCRIM. Sobre esta cuestión, relacionada con la actuación imparcial de la PJE, vid. Fernández Villazala, Tomás y García Borrego, José Antonio. 2010. *Derecho procesal penal para la policía judicial.* Madrid: Editorial Dykinson S.L., 2010, pág. 60.

4. Garantismo, hipergarantismo y seguridad.

a) El derecho garantista y su exceso

Una aproximación al concepto de ***derecho garantista*** la ofrece GASCÓN ABELLÁN, en sus comentarios sobre la obra *Derecho y razón* de LUIGI FERRAJOLI[159], afirmando que *"un Derecho garantista [es el que] establece instrumentos para la defensa de los individuos frente a su eventual agresión por parte de otros individuos y, sobre todo, por parte del poder estatal; lo que tiene lugar mediante el establecimiento de límites y vínculos al poder a fin de maximizar la realización de esos derechos y minimizar esas amenazas"*[160], asunto este, el del garantismo, sobre el que el prologuista de la mencionada obra, N. BOBBIO, dice que *"[Esta teoría es la que inspira y promueve] la construcción de las paredes maestras del Estado de Derecho que tienen por fundamento y fin la tutela de las libertades del individuo frente a las variadas formas de ejercicio arbitrario del poder, particularmente odioso en el Derecho penal". E*stos valores, en mi opinión y pese a los eventuales fallos que hayan podido producirse, están perfectamente interiorizados en la vida diaria de la sociedad y de sus operadores jurídicos, valores de los que no es ajena la PJE.

Así, los redactores de la CE de 1978, con el masivo refrendo del pueblo español, optaron por extremar este genuino sentido del garantismo constitucional[161]. A modo

---

[159] Vid. Gascón Abellán, Mariana. *La teoría general del garantismo, a propósito de la obra de L. Ferrajoli "Derecho y razón"*. Anuario del Departamento de Derecho de la Universidad Iberoamericana, número 31, Sección de Previa, 2001. Sobre el paradigma de la violencia estatal, también vid. Ferrajoli, Luigi. *La legalitá violenta*. Cuadernos de Política Criminal. Madrid, 1990, págs. 305-319

[160] Vid. Gascón Abellán, Marina. *La teoría general…op. cit.* Para esta autora, *"…el garantismo no es simple legalismo; o, si se quiere, no es compatible con la falta de limitación jurídica del poder legislativo, pues la mera sujeción del Juez a la ley puede convivir con las políticas más autoritarias y antigarantistas".* Esta idea evoca el cimero papel que corresponde al Juez en un Estado de Derecho, situando su función por encima del mero legalismo para proteger y extender las más estrictas garantías en la impartición de Justicia.

[161] Esta determinación garantista la refleja GONZÁLEZ-CUÉLLAR al decir que *"nuestra Norma Fundamental ha adoptado [en referencia a las órdenes de limitación de los derechos fundamentales] una rígida posición garantista, a diferencia de otros ordenamientos europeos, como el alemán, en el que se permite a la Fiscalía y sus Ayudantes acordar la limitación de los DF en casos en que exista peligro por el retraso que pudiera perjudicar a la investigación, dando inmediata cuenta al Juez*". Vid. González-Cuéllar Serrano, Nicolás. *Proporcionalidad y derechos fundamentales en el proceso penal.* Madrid: Colex, 1990, pág. 129.

de ejemplo y en relación con el propósito de este trabajo, puede comprobarse que la limitación del derecho fundamental al secreto de las comunicaciones representa en la legislación un plus de garantismo ya que, efectivamente, y a la luz del art. 18.3 CE, solamente se puede verificar mediante resolución judicial, algo que no sería exigencia de la jurisprudencia del TEDH[162].

El problema asociado a este efecto surge cuando no se encuentra el equilibrio o se desplaza injustamente hacia un lado o a otro de la balanza. Es decir, que se plantee una difícil ponderación – el complicado hallazgo de un punto medio - entre el ***hipergarantismo*** y la ***arbitrariedad del Estado*** frente a los derechos individuales de los ciudadanos.

Se debe identificar como una exigencia para el Estado de Derecho el que sea capaz de hallar una fórmula que estabilice esta balanza, pues ninguno de los desplazamientos descritos es admisible en su seno[163].

Sin embargo, el hipergarantismo parece tener la batalla ganada de antemano en España. La proclamación de cualquier paradigma con esta etiqueta servirá como argumento-mordaza frente a cualquier otro que pretenda la proclamada búsqueda del equilibrio entre las garantías constitucionales de los victimarios y la protección de los derechos fundamentales de sus víctimas – que de alguna forma alcanza a toda la sociedad -, consiguiendo inexorablemente sacrificar las primeras en perjuicio de las segundas. Lamentablemente, cualquier intento de establecer mejoras procesales que tiendan a mejorar la seguridad está con gran probabilidad condenado al fracaso pues, a día de hoy, no hay contestación posible a un argumento de corte hipergarantista.

---

[162] GONZÁLEZ-CUÉLLAR afirma que *"la jurisprudencia del TEDH no considera imprescindible la previa autorización judicial para la autorización de comunicaciones telefónicas, e incluso ni siquiera entiende ilegítima la supresión del control judicial posterior…siempre que existan otras salvaguardas [STEDH, DE 6 de septiembre de 1978, Caso Klass]*". Se profundizará más adelante en este asunto. Para muchos países de nuestro entorno, estas salvaguardas serían: Un soporte tecnológico homologado, una legislación procesal bien construida y, naturalmente, una PJE en la que confiar. Vid. González-Cuéllar Serrano, Nicolás. *Proporcionalidad…op. cit.,* pág. 111.

[163] QUERALT, al comentar las causas de justificación penal de la legítima defensa y el estado de necesidad, apunta que *"la desmesurada amplitud es contraria a la idea de la proporcionalidad y especialidad de Derecho ablativo del Estado en materia de libertades y derechos públicos subjetivos; la estrechez supone caer en una indefensión de la sociedad y de los individuos y grupos que la integran*" y que *"el Estado de Derecho encuentra dificultades a la hora de conciliar los criterios de igualdad y de libertad con los de seguridad y orden, lo que obliga al legislador a no escatimar recursos para buscar el equilibrio entre ambos conforme a los presupuestos de legalidad constitucional"*. Vid. Queralt, Joan Josep. *Introducción a la Policía Judicial…op. cit., p*ágs. 45 y 60, respectivamente.

Esto lleva a preguntarse nuevamente si la hiperextensión de la capacidad limitativa de los derechos fundamentales por parte del Estado conduce a la arbitrariedad y al abuso de los poderes públicos sobre los individuos y si la falta de determinación y la laxitud en su definición conduce a la indefensión de aquellos o, expresado de otra forma, tratar de dilucidar dónde se halla el punto de equilibrio perfecto entre garantía y seguridad.

Ciertamente, no se hallan respuestas claras a estas cuestiones, pues la proposición de una medida sugestiva de una más ponderada capacidad limitativa del Estado de los derechos fundamentales, ha provocado un enrocamiento de la postura garantista, como se trasluce de muchas de las aportaciones traídas a este trabajo, sin que la necesidad haya apremiado al postulador para ofrecer la justa contrapartida en forma de propuestas que equilibren los dos brazos de la balanza.

Si la respuesta se decantara hacia el lado del hipergarantismo, resultaría extraordinariamente atractivo semejante desequilibrio para las formas más complejas de la delincuencia, ocasionando graves perjuicios al conjunto de la sociedad y a los poderes públicos[164]. En este sentido, el hipergarantismo propiciaría la conversión de las democracias occidentales en un cálido refugio para una delincuencia extraordinariamente perversa, que se aprovecharía de estas aparentes debilidades como si se tratasen un seguro de pervivencia dotado de magníficas expectativas de futuro.

Pero si, contrariamente, se observara alguna reacción medianamente firme de los poderes públicos, surgirían inmediatamente reacciones claramente decantadas hacia el lado de las garantías y de la preservación sin contrapeso definible de los derechos conquistados en las democracias[165], poniendo de manifiesto una

[164] Para SANSÓ-RUBERT *"la delincuencia, en aras de una mayor y más eficiente autoprotección, ha optado por asentarse en aquellos países que presentan características más favorables en contraposición con sus naciones de origen. Son candidatos predilectos los Estados dotados de ordenamientos jurídicos laxos, excesivamente garantistas si se prefiere, con leyes de extranjería permeables y políticas criminales infradesarrolladas o desfasadas que les permiten operar al amparo de los beneficios reportados por el marco de legalidad descrito"* Vid. Sansó-Rubert Pascual, Daniel. *Criminalidad organizada transnacional…op.cit.*, pág. 222.

[165] RODRÍGUEZ MOURULLO afirma con preocupación que *"…la política criminal del mundo occidental sufre una profunda conmoción a partir de los atentados de las torres gemelas de Nueva York. Desde entonces el fin de prevención lo invade todo y entra en pugna con el Derecho penal garantista, que tan trabajosamente se fue forjando en especial durante la segunda mitad del Siglo XX, con el riesgo de*

preocupación, a mi juicio excesiva, por la supervivencia de los derechos fundamentales puestos en peligro por la necesidad de defenderse de la criminalidad.

Pero no puedo dejar de preguntarme: ¿Qué derechos fundamentales les quedarán a los ciudadanos si el tratamiento de la tumoración criminal excede a la capacidad quirúrgica del Estado?[166] ¿Se está preservando el Estado de Derecho o, más bien, alimentando una polémica artificiosa con resultado de impunidad criminal que en nada le favorece?

b) El derecho penal de lucha

Las reflexiones introducidas en el apartado anterior abren el camino a una discusión que estaría de una forma trascendental en la esencia de este estudio y que, precisamente, se centraría en lo que se ha denominado el ***Derecho penal de lucha***, expresión que apuntaría, en la opinión de importantes sectores doctrinales, a una evolución – no del todo indeseable - del derecho penal destinado a exceder los límites del garantismo para restaurar una seguridad puesta en peligro por la evolución de la DO y el terrorismo. Lo anterior lo expresa DONINI diciendo que:

> *"El Derecho penal de lucha constituye un ataque frontal que las instituciones europeas han levantado contra el garantismo…, pero también contra la criminalidad, de modo que, al mismo tiempo, aquél contiene algunos momentos del todo legítimos aunque desagradables de la acción de contraste del Estado contra fenómenos seguramente graves y peligrosos. La diferencia*

---

dejarlo definitivamente maltrecho. Es como si el "Derecho Fundamental a la seguridad" hubiese devorado a los demás derechos". Vid. Prieto Navarro, Evaristo. *Excepción y normalidad como categorías de lo político* en Cancio Meliá, Manuel y Pozuelo Pérez, Laura. *Política criminal en vanguardia. Inmigración clandestina, terrorismo, criminalidad organizada.* Cízur menor (Navarra): Editorial Aranzadi S.A., 2008, págs. 77-136. Prólogo de Rodríguez Mourullo en la pág. 11.

[166] En un libro-entrevista al que fuera Juez Antimafia italiano, GIOVANNI FALCONE, luego asesinado por su extraordinario valor y firmeza en imponer la Ley, reitera hasta la angustia que la mafia habría alcanzado tal poder que se trataría de igual a igual con el Estado, haciendo que los italianos cabales dudaran al elegir de qué "Estado" ser ciudadanos. Vid. Falcone, Giovanni y Padovani, Marcelle. *Mafia.* Barcelona: Ediciones B, S.A., 1992. En este mismo sentido, SHELLY dice que *"el crimen organizado se ha convertido en algunos Estados o regiones donde logra establecerse como un forma de control social alternativo al oficial en una nueva forma de autoritarismo político no estatal, que se traduce en un debilitamiento del Estado democrático y la violación de derechos humanos".* Vid. Prieto Navarro, Evaristo. *Excepción y normalidad…op. cit.,* pág. 453 y ss.

respecto del Derecho penal del enemigo[167]*, sin embargo, es que este último, per definitionem, es no-Derecho o Derecho ilegítimo"*[168,169,170].

Sobre la primera idea contenida en la cita que se acaba de incluir, se pregunta DONINI que *"si el Derecho es visto como un "arma", ¿Cómo podrá servir de garantía? ¿Cómo podrá el Derecho penal tutelar al ciudadano frente al Estado, si es visto sólo como un medio para golpear a los enemigos, antes aún de que sean confirmados como tales?"*[171], dando lugar a la clásica cuestión sobre si de tal discusión saldrían indemnes el conjunto de las garantías constitucionales[172]. Sin embargo, si se lee atentamente la segunda parte, puede comprobarse que el autor da cierta salida a la necesidad de afrontar la criminalidad[173].

La cuestión, por tanto, puede resumirse en mi opinión en que, efectivamente, pueden explorarse caminos para la lucha – por inapropiado que pueda resultar el

[167] Esta interesante discusión sobre el Derecho penal del enemigo excede a los propósitos de este estudio, en la medida en que en ningún caso se plantearán soluciones que tengan el más mínimo encaje en esta figura. No está de más su mención, en cuanto a que los tratadistas consultados lo han mencionado como excesivo en un Estado de Derecho, incluyendo referencias a cuerpos legislativos de derecho comparado ciertamente inquietantes. Vid. Prieto Navarro, Evaristo. *Excepción y normalidad…op. cit. y* Ávila Gómez, Enrique. *Derecho Penal del Enemigo. Un análisis comparado en los sistemas penales de EEUU y España*. 2ª Edición. Ed. Lulu.com, 2010.

[168] Vid. Donini, Massimo. *Derecho penal de lucha. Lo que el debate sobre el derecho penal del enemigo no debe limitarse a exorcizar* en Cancio Meliá, Manuel y Pozuelo Pérez, Laura. *Política criminal en vanguardia. Inmigración clandestina, terrorismo, criminalidad organizada.* Cízur Menor (Navarra): Aranzadi S.A., 2008, págs. 29-76, pág. 31.

[169] En este sentido, también vid. Prieto Navarro, Evaristo. *Excepción y normalidad... op. cit.,* pág. 451.

[170] Un ejemplo, entre muchos, de la reactividad mostrada por el legislador europeo frente al avance del terrorismo puede verse en el considerando décimo de la directiva de conservación de datos donde se valora que "*el 13 de julio de 2005, el Consejo reafirmó en su declaración de condena de los atentados terroristas de Londres la necesidad de adoptar cuanto antes medidas comunes sobre conservación de datos de telecomunicaciones".*

[171] Vid. Donini, Massimo. *Derecho penal de lucha…op. cit.,* pág. 30.

[172] DONINI añade cierto efecto perturbador sobre los jueces que condicionaría su papel en el proceso penal, al sumar a su función jurisdiccional un inapropiado papel de "luchadores", algo a lo que se ha aludido anteriormente al discutir su implicación en los casos que investigan. Dice: "*El juzgador se siente bajo dos fuegos, en conflicto entre dos lógicas contrapuestas: la dimensión serena de las garantías, por una parte; la idea de finalidad y de lucha contra la criminalidad, por la otras, como objetivos conjuntos del instrumento penal, que ha absorbido en sí hay también funciones de policía: arma y derecho, lucha y garantía sobre el límite de emergencia de los estados de excepción".* Vid. Donini, Massimo. *Derecho penal de lucha…op. cit.,* pág. 39.

[173] DONINI hace notar que en la legislación de la Unión Europea y de las Naciones Unidas es incontable el número de textos que reclaman actuaciones contra el racismo, la xenofobia, abuso sexual de menores, trata de seres humanos, etc., en los que se insiste en términos como "lucha" o "combate". Al respecto afirma que *"la lucha y el combate jurídicos no pertenecen más, por tanto, a los preámbulos de las leyes y a los fines publicitarios de una acción de gobierno…éstos son objetivos incorporados a textos legislativos internacionales fundamentales, y han adquirido la naturaleza de verdaderos y propios conceptos normativos".* Vid. Donini, Massimo. *Derecho penal de lucha…op. cit.,* pág. 33.

término[174] - contra las más execrables formas de la delincuencia moderna, perfectamente admisibles en un Estado de Derecho y, no debe olvidarse, de una forma adaptada al escenario en que se mueve (con el consiguiente adorno de la tecnología).

Por mi parte, trataré de incorporar a la discusión el punto de vista de las víctimas (que son las grandes olvidadas de la sociedad, pese a los grandes esfuerzos que se reconocen a la moderna criminología para corregir esta situación), en torno a la percepción sobre qué ha de hacerse para conseguir una mejor respuesta, entre otros, a los retos procesales planteados por la delincuencia compleja[175], y no sólo en relación con el victimario, sino también, con idéntico entusiasmo, con sus víctimas.

c)El garantismo como equilibrio

Siguiendo a GARCÍA-PABLOS, debe reclamarse un papel ponderado para la víctima de tal naturaleza para el que *"habrá de conjurar tres tentaciones: el antigarantismo tendencial de muchas de sus propuestas, símbolos y lenguaje; el insaciable y desmedido rigor punitivista, que vicia y desacredita cualquier política criminal fiel a sus dictados; y, finalmente, el victimismo rentable de una mal entendida política asistencial que consolida y perpetua a la víctima en su estatus, que cronifica éste"*[176]. Es decir, adhiriéndome a la opinión del autor, "*no oponer un antigarantismo*

[174] La palabra "lucha" aparece con gran frecuencia en los textos normativos producidos por los órganos legislativos de la UE y en los documentos de las diferentes instituciones de la UE, como EUROJUST, EUROPOL u OLAF. El término "combate" es también usado en ocasiones como alternativa al anterior o en su refuerzo, cuya contundencia sugiere una gran necesidad de afrontar resueltamente un problema. Sin duda, la carga semántica de ambos términos nace de los consensos alcanzados para conjurar la preocupación de los veintisiete estados de derecho que forman parte de la UE, de los muchos que ajustan sus estándares democráticos para merecer ser sus miembros y de todo el entorno de terceros países democráticos que desean lograr un control eficiente del terrorismo y de la delincuencia de todo tipo.

[175] Para GARCÍA-PABLOS *"…la víctima dejará de ser un personaje neutro, pasivo, fungible, aleatorio, irrelevante en la génesis y prevención del delito"* y será objeto de redefinición el rol de la víctima *"que reclama enteramente una nueva formulación global de su estatus y de las relaciones de la víctima del delito con su infractor, con el sistema legal, la sociedad, los poderes públicos y las diversas políticas (económica, social, asistencial, político-criminal, etc.)".* Vid. García-Pablos de Molina, Pablo. *Los retos de la moderna criminología empírica.* [aut. libro] J.C. Carbonell Mateu, y otros. *Constitución, derechos fundamentales y sistema penal.* Valencia: Tirant lo Blanch, 2009, págs. 693-716.

[176] GARCÍA-PABLOS ofrece con esta lúcida frase la mesurada contraparte que presidirá todo el contenido de este trabajo, es decir, el sustento conceptual por el que en nada se atacará a la consolidación de un garantismo bien entendido y mejor dirigido a la preservación de los derechos fundamentales

irracional como forma de contrarrestar a un garantismo que se presume exacerbado hasta ser hiriente, sino procurar una respuesta político-criminal proporcionada y basada más en el propio garantismo que en soluciones desmesuradas; huir con determinación de cualquier concepción retribucionista de la pena, entendida esta como venganza; y, por último, no estatuir la condición perpetua de víctima ni convertirla en una profesión o modo de existencia que corrompería la misma dignidad como ser humano"[177].

Esta sería, en esencia, la prudente motivación de este estudio, desde el que se tratarán de deducir algunas conclusiones y propuestas útiles para el proceso penal, aspecto en lo que se apuesta con firmeza. Las soluciones así pensadas se basarán, entre otras cosas, en la acción de una PJE perfectamente inserta en un proceso penal, en el que actúa bajo los principios de legalidad, proporcionalidad, autonomía e imparcialidad, con inmediatez a Jueces y Fiscales y sometida por propia vocación a irrenunciables criterios éticos y deontológicos.

Por ello, el respeto por la libertad y los derechos de los ciudadanos debe, a su vez, liberar de los complejos que se esconden tras el rechazable hipergarantismo. La Justicia en una democracia no se dirige sino contra quien justificadamente lo merece por sus actos reprensibles, lo que hará, eso sí, con el uso más comedido de las facultades legales de restricción de los derechos fundamentales. El proceso penal, consecuentemente, debe ir revestido de todas las habilitaciones legales para la PJE.

Uno de los más sensibles problemas que acucian a la PJE en el ejercicio diario de sus funciones se debe a la carencia de una sólida legislación procesal que, en términos generales, ampare eficazmente su actuación en el marco de las garantías constitucionales que debe presidirla. Estos problemas no guardan relación alguna o, al menos de una forma relevante, ni con inexistentes problemas derivados del modelo

---

reconocidos en la Constitución, sin que ello haya de ser obstáculo para disponer de una mejor normativa procesal que permita afrontar los retos de la delincuencia compleja. Vid. García-Pablos de Molina, Pablo. *Los retos de la moderna…op. cit.*

[177] Aún siendo comprensibles estas reacciones enumeradas con evidente preocupación por GARCÍA-PABLOS DE MOLINA, deben los poderes públicos reaccionar desde un principio para tratar de atemperarlas. En la mente de todos pueden estar los dramáticos casos de víctimas o sus familiares, debidamente manipulados por algunos medios de comunicación social poco escrupulosos, que durante años se exhibieron como tales deformando públicamente su propia condición y, en algunas ocasiones, también con un perceptible interés económico o mediático. El caso de las niñas de Alcàsser podría ser un paradigma de lo anterior.

policial, ni con carencias de orden profesional, ni mucho menos con los más que improbables problemas de inmediatez o lealtad con el estamento Judicial y Fiscal, desafección del principio de legalidad, parcialidad o falta de autonomía o neutralidad.

En consecuencia, se sostendrá con absoluta convicción que buena parte de sus problemas y deficiencias son de una naturaleza procesal[178,179,180]. Baste indicar para ello que la Ley de Enjuiciamiento Criminal fue promulgada en 1882 -, asistiendo con preocupación a las graves insuficiencias en la adecuación de la normativa a una realidad cambiante que evoluciona con gran dinamismo, en ocasiones incluso de forma absolutamente insospechada[181].

d) La necesidad de amplias reformas procesales

Desde un punto de vista estrictamente policial, las sucesivas y caóticas reformas que han sufrido la LCRIM y los demás instrumentos procesales, dejando al mismo tiempo grandes vacíos legales, no han venido adornadas precisamente de la calidad necesaria como para afrontar los problemas reales de la intervención de la Policía Judicial y, muy por el contrario, lo que sí han creado con total eficiencia son importantes riesgos jurídicos que acompañan al día a día del ejercicio profesional de sus agentes[182], sin beneficio reseñable para el proceso penal y las finalidades últimas

[178] Dice CORRAL ESCÁRIZ de manera genérica, que no se conseguirá una mejora "*…mientras la materia de Policía Judicial esté regulada por un cuerpo normativo en el que caben la propia CE, una norma preconstitucional como es la LCRIM, dos leyes orgánicas (LOPJ o LOFCS) y una norma de rango reglamentario cual es el RDPJ, y que por lo tanto no merece otra calificación que la de fragmentario y disperso".* Vid. Corral Escáriz, Vicente. *Problemática de la Policía Judicial…op. cit.,* pág. 162.

[179] La Fiscalía General del Estado afirma que *"no obstante, si bien la regulación de la Policía Judicial contenida en la Ley de Enjuiciamiento Criminal de 1882 no ha sido derogada, sí ha quedado superada, de un lado, por el desarrollo social, económico y tecnológico, y de otro, por el modelo establecido por la Constitución de1978 y por el desarrollo legislativo posterior"* (Instrucción 1/2008).

[180] *"La falta de un modelo de Policía Judicial, al margen de la situación actual en el modelo policial, tiene su explicación en la coexistencia de una normativa post-constitucional fragmentaria, y en la discutible vigencia de algunos artículos de la LCRIM".* Vid. Blázquez González, Félix. *La Policía Judicial…op. cit.,* pág. 100.

[181] Sobre la materia, vid. González-Cuéllar Serrano, Nicolás. *La reforma de la ley de enjuiciamiento criminal: necesidad de su reforma y examen de las sucesivas reformas parciales.* El proceso en el siglo XXI y soluciones alternativas, 2006, ISBN 84-8355-035-0, págs. 69-84.

[182] En este particular, me remito a modo de ejemplo al contenido de la tesis doctoral de GÓMEZ RODRÍGUEZ. Vid. Gómez Rodríguez, Serafín Rafael. *Los agentes policiales antidroga: Riesgos penales de su actuación en España.* Tesis doctoral. Madrid: Universidad Complutense, 2004.

de la impartición de Justicia, en contraste con los instrumentos procesales más eficientes que, en general, gozan otros países del entorno democrático de España.

Cuando se hable genéricamente de la *"adaptabilidad de la ley a las cambiantes circunstancias de la moderna delincuencia"* no me estoy refiriendo, de otro lado, a obtener del legislador una reacción subsiguiente a la detección de una concreta necesidad procesal o penal, con toda los problemas que esto conllevaría en un Estado de Derecho, ni a un ejercicio compulsivo de la facultad legislativa, sino que, antes bien, a que se dispusiese de un cuerpo legal de tal calidad que acogiese sin problemas el tratamiento jurídico de los nuevos retos.

La antiquísima LCRIM ha sido reescrita o complementada con nuevas – y a veces fallidas - instituciones procesales para tratar de adaptar la respuesta jurídica a la realidad del crimen, especialmente cuando la sociedad mundial se vio desbordada por complejos fenómenos delictivos transnacionales como el narcotráfico y sus fenómenos asociados, el blanqueo de capitales o la corrupción, y, también, por el auge de todo tipo de redes terroristas o por grupos con gran capacidad de desestabilización (lo que en términos vulgares se denominarían "mafias", por extensión y agudización del fenómeno bien conocido sufrido por Italia[183]).

Sobre esta falta de sintonía legislativa entre la evolución de la DO y la propia posición de la PJE en el proceso penal, cuyo sumatorio ha de expresarse en términos de inseguridad jurídica, y opinando en línea también con las críticas que se han manifestado al hipergarantismo, sostiene GÓMEZ RODRÍGUEZ que:

[183] En este sentido, constatando sus fallos, como indica GÓMEZ RODRÍGUEZ*, "España ha aumentado los instrumentos jurídicos de investigación policial en las exigencias operativas fundamentales a que obligaba tanto la Convención de Viena de 1988, contra el tráfico ilícito de Estupefacientes y sustancias sicotrópicas, como la Convención de Naciones Unidas de Nueva York contra la DO Transnacional de diciembre de 2.000 — la entrega vigilada, el agente encubierto, los testigos protegidos y los arrepentidos o colaboradores de la justicia —, con lo que nuestro país ha entrado, formalmente, en el club internacional de fuerzas policiales con patrones investigadores reconocidos por la comunidad internacional. Sin embargo, la materialización normativa de tales herramientas en nada se parecen a las adoptadas por los países de nuestro entorno socio-económico, no sólo en las garantías jurídicas con que debe dotarse al agente policial que se atreva a emplearlas, sino, incluso, en la inaplicabilidad operativa de las mismas por el simple hecho de estar construidas con ausencia casi absoluta de criterios profesionales emanados del operador policial".* Se anota aquí la tímida y testimonial participación de la PJE en los foros de todo tipo donde se analizan las necesidades político-criminales y la aparente ajenidad del legislador al asesoramiento de los expertos policiales, a quienes parece no necesitar. Vid. Gómez Rodríguez, Serafín Rafael. *Los agentes policiales antidroga…op. cit.,* pág. 500.

"…y en los tiempos actuales, en que parece inevitable reconocer definitivamente como compañera de viaje del desarrollo social esa «expansión penal», es preciso que queden englobadas también las medidas de cobertura para los operadores policiales, que son los van a investigar realmente y a materializar su cumplimiento.

Y ello, porque el Estado no puede limitarse a crear o ampliar nuevos tipos penales contra riesgos y actividades de organizaciones delictivas complejas, anticipando la responsabilidad penal a estadios iniciales de la acción, sin explicitar también, con la misma minuciosidad y rango normativo, las coberturas y responsabilidades de los que van a actuar contra esas actividades o grupos organizados, generalmente con técnicas encubiertas y de infiltración. De lo contrario, es decir, si se mide y examina al agente policial, por las actividades de lucha que realice contra la organización criminal, sin más protección y perspectiva que la superada Parte general del Código penal, sí se caería en una «expansión irrazonable» del Derecho, al operar esa expansión directamente en contra de los agentes policiales, por no instaurarse mecanismos de corrección"[184].

La opinión GÓMEZ RODRÍGUEZ, aunque centrada en el mundo de la lucha contra la droga y en las figuras de los ***arrepentidos judiciales***, las ***entregas vigiladas y controladas***, los ***agentes encubiertos*** y los ***confidentes policiales***, pone de manifiesto el riesgo y la inseguridad jurídica que comporta un cuerpo legal no orientado a la lucha contra la delincuencia sino a la recuperación social del delincuente, situando en un plano similar a los mismos agentes que lo persiguen, con grave inseguridad jurídica de estos últimos, para los que no se espera indulgencia alguna caso de actuación irregular[185].

[184] Vid. Gómez Rodríguez, Serafín Rafael. *Los agentes policiales antidroga... op. cit.,* pág. 499.

[185] A propósito de la responsabilidad de los agentes por su presunto exceso de celo, invoca el autor el nulo efecto que tuvo sobre la legislación española el art. 5.2 de la Convención de Nueva York de 15 de noviembre de 2000 contra la delincuencia transnacional organizada, por el que se establecían consideraciones sobre la modificación de la responsabilidad penal del autor en relación con "*el conocimiento, la intención, o la finalidad, requeridos como elementos de cualquiera de los delitos enunciados en el párrafo 1 del presente artículo [penalización por participación en organización delictiva] podrán inferirse de las circunstancias objetivas del caso"*. Vid. Gómez Rodríguez, Serafín Rafael. *Los agentes policiales antidroga…op. cit.,* pág. 501.

Los cambios legislativos operados en España presentan una tendencia regresiva, primando el garantismo exacerbado frente a soluciones jurídicas efectivas y aceptables para la función de Policía Judicial, pese a que van implementándose normas de derecho internacional que tratan de ofrecer una respuesta proporcional y adecuada al signo de los tiempos. En mi opinión, existe una clara fractura entre las tendencias de la legislación internacional y las que se desarrollan en España.

Compartiendo en lo fundamental las opiniones de GÓMEZ RODRÍGUEZ, puede comprobarse que las más recientes figuras procesales, como la del Agente Encubierto del art. 282 bis LCRIM[186], nacidas de la exigencia de los compromisos internacionales de afrontar la lucha contra la DO, desde un punto de vista policial, resultan fallidas o mínimamente operativas y con graves riesgos, no sólo físicos para el agente de la PJE –único que puede ser señalado como tal -, sino también jurídicos[187].

Insuficientes son también las previsiones para la protección de testigos y peritos en causas criminales[188], que ninguna protección real reciben, así como la existencia de un peligroso limbo jurídico sobre la figuras de los confidentes y colaboradores, tan necesarios para el conocimiento de la maquinación criminal, y cuya regulación debiera ser objeto de una normativa especial, hoy inédita.

Sobre todos estos elementos, por si fuera poco, sobrevuela la no regulación del ***secreto*** en materia de tratamiento de la DO, que no puede acogerse a la Ley 9/1968, de 5 de abril, *reguladora de los secretos oficiales*[189]*,* como sí sucede con la materia terrorista (sostengo que la DO representa un peligro parangonable para la sociedad).

---

[186] Redacción según Ley Orgánica 5/1999, de 13 de enero, *de modificación de la Ley de Enjuiciamiento Criminal en materia de perfeccionamiento de la acción investigadora relacionada con el tráfico ilegal de drogas y otras actividades ilícitas graves*.

[187] Vid. Vallés Causada, Luis. *Análisis crítico de los instrumentos procesales para la lucha contra la criminalidad organizada. Especial referencia a la figura del Agente Encubierto.* Madrid, 2009.

[188] Ley Orgánica 19/1994, de 23 de diciembre, *de protección de testigos y peritos en causas criminales*.

[189] Nada puede considerarse secreto si un tercero tiene la potestad jurisdiccional de levantarlo. Cuando se redactó la preconstitucional Ley de Secretos Oficiales, en el año 1968, se tenía una noción clara de cuáles eran las amenazas contra *"la seguridad y defensa del Estado"*, según reza su art. 2, lo que podría identificarse, entre otras, con cualquier forma o expresión coetánea del terrorismo, pero presumiblemente nunca con la por entonces prácticamente inexistente DO y, mucho menos, con la potencialidad que hoy exhibe para amenazar la estabilidad del Estado. Se puede, por tanto, atribuir a las anteriores razones el que en el art. 2.4 del Decreto 242/1969, del Reglamento de la Ley de Secretos Oficiales, se apreciasen como objeto de protección de la Ley *"…los conocimientos [informaciones] de cualquier clase de asuntos o los comprendidos como materias clasificadas en el citado artículo segundo de la Ley"*. Esto sin duda propició que las calificaciones de secreto del art. 3 del reglamento se aplicasen,

Cualquier idea de adecuar los instrumentos jurídicos procesales sería visto por el hipergarantismo, sin duda, como un ataque a los derechos a la tutela judicial efectiva y a la defensa proclamados en el art. 24 CE, ataque que nada de perturbador representaría si un ***Juez de Garantías***[190] validase los hallazgos de la PJE para el proceso penal[191], sin que por ello hubiese de sufrir la legítima posición del justiciable y su derecho a defenderse con todas las garantías constitucionales intactas.

Se hace imperioso, por tanto, que los miembros de la PJE sepan cuáles son los límites y sus atribuciones en el marco de un proceso penal del que inequívocamente forman parte[192].

Se detecta un especial temor en la sociedad cuando los avances tecnológicos se aplican a los dispositivos, técnicas y procedimientos dirigidos a cumplir con las medidas limitativas relacionadas con el secreto de las comunicaciones o con los datos que le están asociados, y no sólo cuando estás son ordenadas por la Autoridad Judicial sino, especialmente, cuando lo que se utiliza es un medio técnico de investigación no precisado de tal autorización.

Además, las insuficiencias procesales que acompañan a la intervención de las comunicaciones son ciertamente notorias, habiendo resultado las innovaciones de una

---

por Acuerdo del Consejo de Ministros de 28 de noviembre de 1986 y según su ordinal primero, apartado cuarto, a "*la estructura, organización, medios y procedimientos operativos específicos de los servicios de información, así como sus fuentes y cuantas informaciones o datos puedan revelarlas"*. Sin embargo, una redacción más ajustada en mi opinión debiera extenderse, teniendo en cuenta el razonamiento anterior, *a "…las Unidades de Policía Judicial encargados de la lucha contra la delincuencia organizada o grave…"*. Sobre la cuestión se hace interesante la lectura de Sacristán París, Francisco. *La inteligencia en el tratamiento de fuentes* en *Manual de lucha contra la droga.* ISBN: 978-84-9903-003-6. Cízur Menor (Navarra): Aranzadi. 1ª Edición, 2011, págs. 681-736.

[190] Resulta sugerente a los efectos la figura del Juez Especial del Tribunal Supremo que propugna la Ley 11/2002, de 6 de mayo*, sobre el Centro Nacional de Inteligencia*, que llevase a cabo el control jurisdiccional de los medios de tecnovigilancia usados para el proceso penal.

[191] Lamentablemente, muchas de las piezas doctrinales y jurisprudenciales se convierten en perfectos compendios o manuales donde los delincuentes pueden saber con qué métodos lícitos se les persigue y cómo eludirlos.

[192] Los limbos jurídicos propician, junto a otras que se estudiarán en su momento, SSTS como la 605/2007, de 23 de enero, y la 523/2008, de 11 de julio, en las que las referencias al uso de balizas para el seguimiento de móviles no cooperantes (vehículos de todo tipo usados por los delincuentes) son meramente valorativas del tribunal, que las adecúa, tímidamente – sin gran acopio de enjundiosos argumentos jurídicos -, a criterios de proporcionalidad y de no afectación a los derechos fundamentales de los concernidos, pero sin referencia a precepto legal alguno. Otro ejemplo de parecida naturaleza, sobre la obtención del IMI e IMEI, puede encontrarse, entre otras, en la STS 130/2007, de 19 de febrero, que será objeto de análisis más adelante.

ínfima calidad, aún después de los varapalos proporcionados por el TEDH a España a través de sendas STEDH[193] por vulneración del CEDH en su art. 8.

Así, aún sobre la reforma de 1988 del art. 579 LCRIM[194], en la que hubo ocasión de legislar con mayor precisión, se siguen recogiendo críticas relativas a la indefinición de las personas sobre las que se pueden autorizar las intervenciones telefónicas, los plazos de duración de las intervenciones, las infracciones que pueden motivarlas, las formas de constancia documental, el protocolo policial a aplicar, las precauciones sobre la integridad de los contenidos, la forma de control jurisdiccional, los tiempos de conservación o destrucción de los soportes, la forma de acceso de la defensa, etc.[195,196], a las que se puede añadir el entusiasmo de ciertos sectores por desacreditar el SITEL, por centrarlo en el sustrato tecnológico, cuya efectividad en la defensa de los derechos fundamentales no merece tacha alguna[197].

Íntimamente relacionado con lo anterior, se puede mencionar también la regresión que trajo la promulgación de la LCDCE que, aunque será objeto de un profundo estudio en este trabajo, sí merece adelantar su insuficiente calidad desde un punto de vista de las necesidades policiales, entre otras cosas, en la medida que

[193] Se citan al efecto las STEDH sobre los casos *Prado Bugallo* (18 de febrero de 2003) y *Valenzuela Contreras* (30 de julio de 1998), de las que se tratará con mayor detenimiento algo más adelante.

[194] Operado mediante Ley Orgánica 4/1998, de 25 de mayo, de reforma de la Ley de Enjuiciamiento Criminal.

[195] Nótese que no se reclama con este comentario una legislación laxa que permita una fácil restricción de los derechos fundamentales sino, antes bien, una Ley bien hecha que conjure cualquier riesgo jurídico asociado a su aplicación, tanto para el investigado como para la propia PJE. Conocer bien los límites significa usar bien la Ley en defensa de la Justicia.

[196] DÍAZ MARTÍNEZ, sumándose a los autores que comentan las evidentes deficiencias de la normativa, lamenta la ocasión perdida de introducir reformas procesales tras la promulgación de la Ley 22/2003, de 9 de julio*, Concursal*, ya que *"tratándose de la intervención de las comunicaciones telefónicas, el artículo primero, apartado 4 de la LORC, sorprendentemente efectúa una remisión en bloque a lo previsto en la LECrim., habiendo desaprovechado el legislador la oportunidad que se le ofrecía de incorporar a nuestro derecho interno, en el ámbito específico del proceso concursal, la doctrina que tanto el TEDH, como el TC han elaborado a propósito de la intervención telefónica acordada judicialmente en el curso de un proceso penal"*. Según este autor, además de la jurisprudencia del TEDH, podría haberse recogido la del TC (SSTC 259/2005, 165/2005, 167/2002, 14/2001, 236/1999, 49/1996) y TS (SSTS núms. 957/2005, de 18 de julio, 841/2005, de 28 de junio, 864/2005, de 22 de junio, 1489/2004, de 18 de diciembre, 999/2004, de 19 de diciembre, 322/2004, de 12 de marzo, 343/2002, de 7 de marzo). Vid. Díaz Martínez, Manuel. *La dudosa constitucionalidad de la regulación legal de las medidas limitativas de derechos fundamentales del deudor en el proceso concursal*, en Estudios de Deusto, Vol. 59/2, Julio/Diciembre 2011, págs. 259-276.ISSN: 0423-4847.

[197] El SITEL cumple con el estándar europeo de interceptación legal de las comunicaciones del ETSI ES 201 671 V.3.1.1. (ETSI es el acrónimo de *European Telecommunications Standards Institute* o Instituto Europeo de Estándares sobre las Telecomunicaciones).

desatiende amplios sectores del ámbito de las comunicaciones electrónicas que serían del máximo interés para nuevas formas de investigar.

Estas deficiencias se subliman cuando se trata de hablar de la adaptabilidad de la Ley a la evolución tecnológica y, singularmente, en materia de obtención de ITCE. Se puede decir, a estos efectos, que la brecha o desfase tecnológico abierto entre el investigador y el delincuente ocasionado por las deficiencias procesales podría llegar a hacer impracticable su perseguibilidad.

En mi opinión, a tan desfavorable situación se añade el indeseable efecto de sanarse las deficiencias procesales que se han mencionado a golpe de casación[198], creándose una jurisprudencia a veces contradictoria o, al menos, poco pacífica, que lejos de ayudar a la correcta interpretación y uso del instrumento procesal por parte, no ya de la PJE, sino del mismo Juez que ha de aplicarlo, pone en riesgo tanto la viabilidad procesal de la investigación, como su alcance y eficacia. Al mismo tiempo, coloca al agente de la PJE en una inaceptable situación de riesgo jurídico, al verse más amenazado por las posibles responsabilidades penales o disciplinarias que en su contra pudieran exigírsele que por los propios riesgos físicos que provengan de los criminales.

En la actualidad, los avances que la tecnología va aportando a la función de Policía Judicial, a falta de derecho positivo, vienen introduciéndose en el proceso penal de una forma inestable, admitiéndose al albur de la eventual consolidación de

[198] En este sentido, LLAMAS y GORDILLO dicen que *"hay un evidente retraso en la acomodación del derecho positivo al uso de los medios técnicos, lo que ha provocado que sea frecuente que se tenga que esperar a que, vía casacional, se consiga validar su uso, en el mejor de los casos, cuando no que, después de años de trabajo con un medio técnico en uso, se cuestione éste como lícito y se echen a perder decenas de causas e investigaciones que han tenido en el empleo de tales medios la principal de las herramientas de investigación. Y si bien, el daño que una declarada nulidad de actuaciones, por el ilegal empleo de medios que se han entendido contaminantes de todas las pruebas obtenidas a partir de aquella intervención, siempre provoca cierto desaliento, mucho más preocupante nos parece que este "desafortunado" empleo de medios se pueda entender relevante a efectos penales para los funcionarios actuantes, como recientemente se ha insinuado nada veladamente en alguna sentencia de la Sala Segunda del TS"*. (Nota: se refiere a la STS de la Sala 2ª, de 19 de febrero de 2007).
Continuan afrimando que *"no se nos escapa que en este contexto no faltará quien vea en este escenario una capacidad inmensa de control social que potencialmente ponga en riesgo los derechos y libertades individuales más básicos, pero creemos que una buena regulación del uso de las nuevas tecnologías de la información y un buen sistema de garantías judiciales, equilibrado y razonable, que no haga inoperante para las Fuerzas de Seguridad el enorme campo de medios tecnológicos para la defensa del Estado de Derecho, eliminará el lógico temor al "Gran Hermano""*. Vid. Llamas Fernández, Manuel y Gordillo Luque, José Miguel. *Medios técnicos de vigilancia.* [ed.] Consejo General del Poder Judicial. *Los nuevos medios de investigación en el proceso penal. Especial referencia a la tecnovigilancia.* Madrid, 2007, Vol. II, págs. 207-249.

determinadas líneas jurisprudenciales, cosa que llegará tras muchos años de reiterados procesos de valoración y contradicción de la prueba.

El procedimiento será mediante la proposición de su uso a la Autoridad Judicial, la cual, recabado el informe del Ministerio Fiscal[199] y mediante la emisión de una resolución motivada[200] y atendiendo al principio de proporcionalidad, dispondrá su activación.

Recibida la orden de proceder, los hallazgos propiciados por la nueva herramienta se aportan al proceso penal mediante el atestado policial de forma objetiva y acompañados de los correspondientes análisis, valoraciones periciales y, llegado el caso, de las estimaciones subjetivas no vinculantes de los investigadores.

La controversia surgirá cuando esta herramienta sea puesta en duda en el acto del juicio oral y genere el correspondiente proceso de casación que puede culminar con la anulación de la prueba, que provocará los devastadores efectos que ello representa para la impartición de Justicia, y que llegarán, además, tras largos años de aplicación del procedimiento técnico de que se trate en diversas investigaciones, ocasionando nuevos e inaceptables descalabros del Estado de Derecho frente a la delincuencia.

Por tanto, la inadaptabilidad de la Ley, su falta de calidad o sus clamorosas omisiones se constituyen, en mi opinión, en el alimento esencial que nutre las expectativas de la delincuencia más perniciosa para la sociedad, es decir, la que más puede desestabilizarla y dañarla, haciendo atractivo nuestro país a las más complejas formas de criminalidad.

---

[199] Cuando por razones de prudencia policial se evacúan consultas a Jueces, Fiscales o expertos en derecho sobre la idoneidad de los nuevos procedimientos surgen opiniones contradictorias, que varían de la aceptación ("de alguna forma tendrá la PJ que intervenir, vistos los tiempos") al hipergarantismo ("es desproporcionado y vulnera el derecho a la defensa por…"). Al final, la proposición es del Instructor Policial y, la resolución, de la mezcla de audacia y solvencia jurídica de quien realiza el acto jurisdiccional, lo que de ninguna manera debiera producirse, sino por la de haberse invocado concretas normas de derecho positivo en las que residenciar tales decisiones jurisdiccionales. Decisiones de este tipo que, de otro lado, vienen condicionadas en su fortuna por otras que las confirmen o rechacen posteriormente desde instancias procesales superiores.

[200] A veces con gran enjundia jurídica, no exenta de creatividad, que hace que el esfuerzo intelectual de apreciar la constitucionalidad de una medida no pueda basarse en la concreta aplicación de cuerpos legales inexistentes que, en su estricto desarrollo, hubieran dado con las debidas fórmulas jurídicas que proporcionasen acomodo a tales progresos sin menoscabo de la más leve garantía constitucional.

Resulta llamativa, por tanto, la falta de flexibilidad y capacidad de la Ley para prevenir o asumir pronta y eficazmente sus retos, exceptuándose la extrema diligencia con que reacciona cuando se trata de tutelar los derechos de los delincuentes, lo que en sí mismo no debe ser materia de la más mínima crítica.

Pese a la alarma social[201] que generan muchas formas de delincuencia moderna, no se produce la subsiguiente reacción de los poderes públicos introduciendo las medidas y cambios legislativos que le doten de la necesaria capacidad de respuesta. Es decir, que la política criminal se dirige más a precaverse de las posibles desviaciones de la PJE que a dotar a los investigadores de unas herramientas procesales abiertas a los tiempos y respetuosas con las garantías constitucionales.

De una forma intuitiva, podría colegirse que la sociedad descansa todo el peso de su confianza en el estamento judicial y poca o ninguna en el policial. La discusión en este territorio, estéril por definición, podría llevarse *ad infinitum* sin llegar a conclusión alguna. La consecuencia de todo puede ser un ejercicio defensivo – y por tanto ineficaz – de los profesionales cuya responsabilidad personal es exigida con extraordinaria prontitud y rigor, lo que por otra parte tampoco debe ser materia de mayor crítica.

No se discute, por tanto, la necesidad de contar con un exigente control jurisdiccional, sino de adecuarlo al dinamismo que la propia delincuencia impone a la sociedad.

Se trata, no de dotar al derecho procesal penal de instrumentos de mayor capacidad restrictiva de los derechos fundamentales sino, muy por el contrario, de aplicar soluciones legislativas bien ponderadas y apoyadas en los más adecuados recursos materiales (con especial referencia a la tecnovigilancia y a su uso bajo el debido control jurisdiccional), de tal calidad que incluso reduzcan el nivel de injerencia en los derechos fundamentales. Esta pretensión debe orientarse a que la penetración en la esfera de la intimidad por los poderes públicos sea la mínima imprescindible y que la validez de lo obtenido esté, a su vez, revestida de tan inequívoca capacidad

[201] La referencia a la "alarma social" será en su acepción criminológica, pues la jurídica queda excluida como tal al carecer de base legal en el ordenamiento jurídico, según se proclama en las SSTS de 17 de febrero de 1996 y 7 de noviembre de 1997, entre otras.

probatoria que pueda ser debidamente valorado en el proceso de enjuiciamiento de los hechos.

Por ello, no puedo en este punto estar de acuerdo con lo expresado por DELGADO MARTÍN al referirse a la forma en que los poderes públicos reaccionan frente a la criminalidad organizada "*mediante la admisión de medios cada vez más agresivos contra las organizaciones criminales, con grave quiebra de los derechos fundamentales, sin que muchos de ellos determinen una eficacia real, a largo plazo, en la lucha contra la DO*"[202]. La sociedad, bajo el imperio de la Carta Magna, si en algo viene siendo celosa es en motivar que los poderes públicos reaccionen preservando las garantías constitucionales cuando se trata de legislar en materia procesal y no al contrario.

Algún ejemplo de la anterior posición, que demuestran una menor penetración en la esfera de la intimidad, ceñido al ámbito de la ***tecnovigilancia***, sería el de la obtención de inteligencia sobre la localización geográfica de un teléfono móvil mediante el análisis de determinados datos conservados por las operadoras de telefonía (geoposicionamiento), lo que haría innecesario, como antaño, acudir a la intervención de las comunicaciones establecidas por los investigados en canal cerrado[203] o, de una forma por su frecuencia más cercana a la vida diaria, serviría el caso de los arcos detectores de metales, que evitan los registros corporales cuando se desea acceder a una dependencia sujeta a determinadas medidas de seguridad física[204].

---

[202] Vid. Delgado Martín, Joaquín. *Criminalidad…op. cit.,* pág. 31.

[203] Vid. Delgado Martín, Joaquín. *Criminalidad…op. cit.,* pág. 21. La vía no invasiva del derecho al secreto de las comunicaciones que se pretende realzar frente a procedimientos precedentes, hoy obsoletos, se efectuaría por la PJE mediante la solicitud de una resolución judicial amparada por el art. 6.1 LCDCE, con la que se obtendrían los datos de localización de celda conservados por la compañía operadora de telecomunicaciones de acuerdo con el art. 3.1.f LCDCE, al que seguiría un análisis de las BTS activadas por el terminal telefónico móvil para conocer su ubicación relativa. De no existir esta posibilidad técnica y su apoyatura legal, se haría necesario acudir a la intervención telefónica para intentar obtener esta misma información. Es evidente que el procedimiento descrito representa, en este concreto campo, un incuestionable avance legislativo, en cuanto a las posibilidades que ofrece de no tener que limitar el derecho fundamental al secreto de las comunicaciones establecido en el art. 18.3 CE.

[204] El documento de evaluación de la Directiva 2006/24/CE reconoce que *"algunos Estados miembros alegaron asimismo que el uso de datos conservados contribuyó a absolver a personas sospechosas de delitos sin tener que recurrir a otros métodos de vigilancia, como las escuchas telefónicas y los registros domiciliarios, que podrían considerarse más intrusivos".* Vid. *Informe de la Comisión al Consejo y*

En igual manera, de contar con medidas procesales más evolucionadas, un análisis inteligente de los datos de tráfico de llamadas o la introducción de determinados parámetros de riesgo en el tráfico bancario permite evitar farragosos análisis de datos personales que supondrían una evidente e innecesaria indagación en la privacidad de los sujetos y, con seguridad, en la de otras personas que nada tienen que ver con lo que se investiga, pero cuyos datos se han pedido al carecerse de una inteligencia previa que precise con exactitud el objeto de la indagación y que permita descartar a estas personas desde un principio o, al menos, en el tiempo real en que dura el examen de la base de datos.

Otros ejemplos, de lo que me ocuparé en detalle más adelante, en el que el exceso de garantismo se hace patente por considerarlos por completo ajenos a la protección del art. 18.3 CE, serían los que he denominado ***usos no comunicativos o instrumentales de las comunicaciones electrónicas***, en los que las tarjetas SIM o el direccionamiento IP se utilizan, no para establecer una comunicación en canal cerrado entre dos personas, sino para hacer un uso instrumental del teléfono preordenado a la obtención de un lucro (vaciamiento patrimonial), a conducir ataques informáticos (lanzamiento de un ataque de DoS), a geoposicionar víctimas o a iniciar cargas explosivas.

Sobre cualquier investigación en la que se usan medios tecnológicos, las directrices técnicas de la PJE en el curso de una investigación suelen ser por lo demás extremadamente prudentes. En ocasiones, y dada la necesidad de que el Juez de Instrucción haya interpretado extensivamente la deficiente legislación procesal que ampara la intervención de las comunicaciones[205], tras una solicitud de medidas limitativas de derechos fundamentales en este concreto campo, se dé la circunstancia de no utilizarse provisionalmente sus hallazgos por la PJE cuando se sostenga la razonable duda de que, pese a el innegable respaldo del mandato judicial, pueda en un futuro discutirse o anularse la prueba en el acto de juicio oral. Es decir que, por esta

Parlamento Europeo. Informe de evaluación sobre la Directiva de conservación de datos (Directiva 2006/24/CE), COM(2011) 225 final, pág. 27.

[205] Por ejemplo, un registro virtual o la instalación de programas informáticos mediante intrusión en los elementos informáticos del investigado (troyanos), donde el esfuerzo interpretativo de la Ley y del principio de proporcionalidad es ciertamente complejo para la Autoridad Judicial, lo que puede producir causas de nulidad de la prueba al someterse a criterios de revisión más estrictos en otras instancias.

razón, tales hallazgos pasarán provisionalmente a considerarse únicamente como mera inteligencia desde un punto de vista policial, hasta tanto pueda refrendarse la prueba por otra vía distinta.

Sobre la posición de la PJE en todas estas cuestiones que hasta ahora se han tratado, es necesario proclamar que no tiene otra forma de actuar contra la delincuencia que la de contribuir lealmente a que queden firme e inequívocamente probados los hechos delictivos en el acto del juicio oral, para lo cual no existen los atajos en un Estado de Derecho que la hagan ser merecedora de la desconfianza de los operadores jurídicos.

Por todo lo anterior, se puede afirmar que la PJ, bajo la observancia estricta del principio de legalidad, interviene en el proceso penal de una forma autónoma, neutral e imparcial bajo la dependencia funcional de un Juez de Instrucción que ejerce de forma permanente el debido control jurisdiccional de sus actuaciones, sin compromiso procedente de las estructuras orgánica y técnica.

A estos efectos, la PJE se sirve de procedimientos técnico-policiales y científicos puestos en práctica bajo un exigente marco de actuación ético y deontológico, constituyéndose, por su inmediatez al justiciable y por su posición intermedia entre este y el juzgador, en la primera y más sólida salvaguarda de sus derechos fundamentales y, con especial dedicación, de los de las víctimas.

El campo de actuación de la PJE en la limitación de los derechos fundamentales es, por otra parte, extraordinariamente estrecho, no dando lugar – por economía de medios e innecesaridad procesal – a las intervenciones o vigilancias de naturaleza prospectiva. Sus pesquisas, bajo el principio de proporcionalidad, se dirigen exclusivamente sobre quienes existen fundados indicios racionales de criminalidad.

Es a esta PJ a la que se referirán las explicaciones que formen parte de este trabajo.

B. La delincuencia organizada y la delincuencia compleja

1. Insuficiencia conceptual de la expresión "delito informático".

Como paso previo a iniciar el análisis de la delincuencia moderna, es necesario hacer una breve referencia al concepto y alcance real del denominado ***delito informático***[206] en su calidad de factor emergente que la ha hecho evolucionar espectacularmente hasta llegar a su estadio actual en un proceso que, sin duda, permanece inacabado. Esta denominación, poco afortunada, contribuye sin duda a la ceremonia de la confusión que reina en los foros internacionales, donde a falta de consensos sobre su misma definición, aún con menor fortuna si cabe se acierta a la hora de concebir las posibles soluciones en el orden penal o procesal.

En efecto, como señala DAVARA, no existe la calificación jurídica de delito informático[207], al que define conceptualmente como *"la realización de una acción que, reuniendo las características que delimitan el concepto de delito, sea llevada a cabo utilizando un elemento informático y/o telemático, o vulnerando los derechos del titular de un elemento informático, ya sea hardware o software"*[208].

En mi opinión, la informática no propicia por sí misma la creación de nuevos tipos penales, sino que facilita una nueva e inquietante dimensión a los ya conocidos mediante la ideación de nuevos *modus operandi* de insospechadas posibilidades tecnológicas para perfeccionar el hecho punible, lo que obviamente debe conducir a una urgente reflexión sobre las posibles mejoras en la definición de los tipos y de las

[206] Vid. Davara Rodríguez, Miguel Angel. *Manual de derecho informático.* 9ª Edición. Cízur Menor (Navarra): Editorial Aranzadi SA, 2007, pág. 364 y ss.
[207] Este autor anota, antes de proponer una definición formal, que *"aceptamos la expresión "delito informático", por conveniencia, para referirnos a determinadas acciones y omisiones dolosas o imprudentes, penadas por la Ley, en las que ha tenido algún tipo de relación en su comisión, directa o indirecta, un bien o servicio informático"*. Afirma a renglón seguido también que *"la interpretación analógica tampoco es posible, ya que implicaría la creación de nuevos delitos, lo que a su vez iría en contra del principio de legalidad"*. Vid. Davara Rodríguez, Miguel Angel. *Código de Internet.* Colección de códigos profesionales. 3ª Edición. Cízur Menor (Navarra): Editorial Thomson Aranzadi SA, 2007, págs. 361 y 362.
[208] Vid. Davara Rodríguez, Miguel Angel. *Código de Internet…op.cit.,* pág. 364.

consecuencias jurídicas de su perfeccionamiento[209] que, además, asuman tales dinámicas hasta tal punto que su tipificación tienda a ser jurídicamente estable frente a la propia evolución del fenómeno.

Puede resultar muy atractivo denominar "delito informático" a la creación de una *botnet* – que en sí misma carece de utilidad - capaz de servirse de un sinnúmero de ordenadores *zombies* maliciosamente infectados y ubicados a escala internacional para destinarlos a finalidades criminales propias o para ponerlos a disposición de terceros, pero, al fin y al cabo, tal maquinación no será sino el instrumento que permita a sus manipuladores lucrarse, revelar secretos, causar daños a otros sistemas telemáticos o atacar la indemnidad sexual de un menor, por reiterar algunos ejemplos[210,211].

Así al menos parece reconocerlo VELASCO, cuya clasificación de los delitos informáticos conduce inexorablemente a la identificación de conductas que no son novedosas para el derecho penal:

- *"Delitos Económico-Patrimoniales o ciberdelincuencia económica: Suponen la utilización de la informática para robar, estafar, defraudar, usar indebidamente o dañar medios informáticos, estragos, vulneración de los*

[209] Sobre la urgencia de actualizar la legislación procesal por imperativos de la TIC, sin olvidar la preservación de las garantías constitucionales, dice PÉREZ GIL que *"hoy por hoy nuestro ordenamiento jurídico en relación con las medidas de investigación penal en las que la tecnología ocupa un papel relevante no cumple, ni aun en la más benevolente de las interpretaciones posibles, las condiciones exigidas por el art. 8.2.º del Convenio Europeo de Derechos Humanos para las injerencias en la intimidad… A mi juicio ha de considerarse inaplazable, y no puede hacerse esperar hasta la elaboración de una nueva Ley de Enjuiciamiento Criminal, la introducción de normas expresas que posibiliten que los Jueces autoricen concretas y novedosas medidas de investigación lesivas de la intimidad personal y familiar o del derecho a la protección de datos personales".* Vid. Pérez Gil, Julio. *Investigación penal y nuevas tecnologías: Algunos retos pendientes*. León, Revista jurídica de Castilla y León. 2005, Vol. 7, pág. 220.

[210] Hablar de delito informático equivaldría a hacerlo, por ejemplo, de "delitos de cuchillo", por ser un instrumento con el que se puede cometer un homicidio, o de "delitos de cámara", si se usa para tomar una fotografía sexualmente explícita de un menor.

[211] Reflejos de esta idea parecen subyacer en las sucesivas reformas del código penal operadas en tiempos recientes, por ejemplo, mediante la Ley Orgánica 15/2003, de 25 de noviembre, por la que se introdujo en el art. 286 el concepto de los programas informáticos supresores de las medidas de acceso condicionado a los contenidos protegidos por la propiedad intelectual, el reconocimiento implícito del potencial lesivo de la distribución de pornografía infantil a través de las TIC que se deduce de la reforma practicada en el art. 189 mediante la Ley Orgánica 5/2010, de 22 de junio, o mediante esta misma norma y la Ley Orgánica 3/2011, de 28 de enero, por la que por similares razones se redefinieron las tipologías del descubrimiento o la revelación de secretos contenidas en el art. 197, dando cabida a la evolución de las formas comisivas.

derechos de propiedad intelectual e industrial, espionaje informático, blanqueo de capitales, falsedades documentales, etc.

- *Atentados contra la intimidad y la privacidad o ciberdelincuencia intrusiva: Mediante ataques a los derechos fundamentales recogidos en el art. 18 CE. Incluyen delitos de amenazas, coacciones, distribución de material pornográfico y pornografía infantil, descubrimiento y revelación de secretos, injurias y calumnias y cesión inconsentida de datos ajenos.*
- *Ataques por medios informáticos contra intereses supraindividuales o ciberterrorismo y ciberespionaje: Son ataques a los intereses generales de la población"*[212].

Además del uso directamente delictivo de las TIC, parece poco menos que imposible que, de un modo u otro, en la inmensa mayoría de las maquinaciones criminales actuales no hayan jugado un papel relevante como instrumento imprescindible para la concertación, por lo que se ahonda más en la indefinición del concepto[213].

Por ello, PÉREZ GIL acierta al comentar que *"puesto que casi todos los delitos (valga la exageración) pueden constituir delincuencia informática, casi toda la investigación penal lo será sobre nuevas tecnologías en la medida en la que habrá sistemas o datos informáticos que sirvan de soporte a información relevante (un teléfono móvil, una agenda electrónica, la utilización de un cajero automático, etc.: todos ellos contienen sistemas informáticos). En esa tesitura lo lógico será configurar un marco legal que, debidamente encajado en el núcleo jurídico fundamental, posibilite la traducción al proceso penal de las características que definen las profundas transformaciones que ha impulsado la sociedad de la información: a) desmaterialización de los bienes objeto del tráfico jurídico; b) desterritorialización e irrelevancia de fronteras o distancias geográficas; c) horizontalización, en la medida en que los mecanismos de comunicación y de intercambio de información toman por base la existencia de redes, tanto abiertas (Internet) como cerradas, y d) transparencia,*

[212] Vid. Velasco Núñez, Eloy. *Delitos cometidos a través de Internet…op.cit.,* págs. 41 y ss.
[213] En este sentido, vid. Pérez Gil, Julio. *Investigación penal y nuevas…op.cit.,* pág*s. 223 y ss.*

dado que los actos de personas y organizaciones se hacen visibles y pueden interrelacionarse".

Es evidente, por tanto, que estas modificaciones operadas por las TIC donde verdaderamente han de alcanzar son al derecho procesal y, especialmente, a la eficiencia en la perseguibilidad internacional de los delitos, lo que incluye la mejora de las facultades en la obtención de la prueba y la posibilidad de exigir la adopción de medidas cautelares.

Dado que por las características que por su naturaleza material vienen revestidos estos nuevos *modus operandi*, se exige también un nuevo enfoque para la legítima limitación de los derechos fundamentales de aquellas personas de las que se sospeche fundadamente que hayan utilizado las TIC para alcanzar sus fines criminales, estando por ello justificado que pueda accederse al análisis del instrumento tecnológico independientemente de la gravedad de la conducta, atendiendo de este modo al enfoque jurisprudencial que toma en consideración su singularidad y su potencial lesividad.

En consecuencia, la Unión Europea previó una expansión en la afectación al sector privado de las telecomunicaciones que, trascendiendo a las operadoras de telefonía de red fija o móvil, debía alcanzar a los prestadores de los servicios de la sociedad de la información, no sin antes expresar las dificultades de implicar a la iniciativa privada en un marco globalizado donde la soberanía nacional no podía alcanzar[214].

El examen de la definición de la UE sobre qué es la delincuencia informática tampoco ayuda mucho a percibir una categoría penal nueva, ya que resulta confuso y parece más orientado a describir el fenómeno criminal en sí mismo que para referirse a la tipología penal. El concepto es ofrecido por la Comisión al indicar que *"[en esta Comunicación] se aborda la delincuencia informática en el sentido más amplio;*

[214] *"En caso de que los Estados miembros introduzcan nuevos requisitos técnicos sobre interceptación para los operadores de telecomunicaciones y los proveedores de servicios de Internet, la Comisión opina que estas normas deberán coordinarse a escala internacional para prevenir la distorsión del mercado único, minimizar los costes para el sector y respetar los requisitos de protección de los datos y de la intimidad*". Vid. *Comunicación…Creación de una sociedad de la información más segura…op.cit.*

cualquier delito que de alguna manera implique el uso de tecnología de la información".

De forma críptica y aparentemente ajena a los consensos, pretendiendo distinguir los delitos en los que el uso de la informática sea un fin de los que haya sido tan sólo su instrumento, la Comisión, incurriendo en mi opinión en referencias expresas inapropiadas al concepto de delito informático o cibernético, afirma a continuación que *"sin embargo, existen distintos puntos de vista sobre lo que constituye la "delincuencia informática". Suelen utilizarse indistintamente los términos "delincuencia informática", "delincuencia relacionada con la informática", "delincuencia de alta tecnología" y "delincuencia cibernética". Cabe diferenciar entre los delitos informáticos específicos y los delitos tradicionales perpetrados con ayuda de la informática*[215]*…Mientras que los delitos informáticos específicos requieren una actualización de las definiciones de los delitos en los códigos penales nacionales, los delitos tradicionales perpetrados con ayuda de la informática requieren una mejora de la cooperación y de las medidas procesales"*[216].

Vista la amplitud de la definición, no se alcanza a comprender el sentido de la última frase del texto anterior pues, dada su aparente ubicación extrapenal, no se puede hablar en propiedad de los delitos informáticos como concepto autónomo sino meramente operativo, lo que exige, sin duda, identificar las nuevas modalidades de comisión que hayan surgido por su irrupción en la vida social e independientemente del instrumento que se haya utilizado para su perpetración, así como revisar su tratamiento penológico, y, sobre todo, mejorar o construir la herramienta procesal que permita su persecución cuando se hayan aprovechado las facilidades proporcionadas por las TIC.

---

[215] VELASCO afirma a este respecto que *"en la dogmática actual se incluye en el concepto de delito informático tanto el delito tradicional cometido a través de ordenador, como el propiamente tal, delito contra la informática"*. Ciertamente, no se alcanza a comprender cómo se puede haber un "delito contra la informática" sino es causando modificaciones o daños físicos o lógicos en el *hardware o software* de los sistemas telemáticos con un determinado fin de los que son perfectamente conocidos por el derecho penal actual y con toda la gravedad o trascendencia que se quiera apreciar. Vid. Velasco Núñez, Eloy. *Delitos cometidos a través de Internet…op.cit.,* pág. 41.

[216] Vid. *Comunicación al Consejo, al Parlamento Europeo, al Comité Económico y Social y al Comité de las Regiones, sobre la Creación de una sociedad de la información más segura mediante la mejora de la seguridad de las infraestructuras de información y la lucha contra los delitos informáticos. COM(2000) 890 final*, de 26 de enero de 2001.

Examinado todo lo anterior, y constatadas por la experiencia profesional práctica las ineludibles exigencias de la investigación criminal actual, lo más interesante de la irrupción de las TIC en el mundo del delito viene de la mano de sus propias ***peculiaridades criminológicas***[217], lo que a los efectos que centran el interés de este trabajo – y que serán objeto de un estudio más detallado - se materializan en las siguientes y especialísimas circunstancias, que condicionan la viabilidad policial de las investigaciones:

- Existe un recurso permanente a las comunicaciones electrónicas protegidas por el art. 18.3 CE para llevar a cabo las acciones de concertación y desarrollo instrumental del ***iter criminis***[218], especialmente cuando la finalidad delictiva se centre en el uso ilícito de las TIC.
- Necesidad de hacer una redefinición o revisión del concepto de dato y de su cesibilidad al proceso penal, particularmente en lo que se refiere a los ***datos asociados a las comunicaciones electrónicas*** (en adelante DACE)[219] y su tratamiento diferenciado del ***contenido material***[220] de estas[221].
- La leve penalidad de muchas de las expresiones de los delitos complejos exige revisar el concepto de gravedad de forma que no sea obstáculo para hacer procesalmente accesibles a la investigación las nuevas modalidades

[217] Comisión a distancia e instantánea, resultado de delitos masa, desconocimiento de la víctima, componente internacional, a veces por meros usuarios (muchas veces jóvenes), afectación a diversos bienes jurídicos (información, propiedad, intimidad, sistemas informáticos, seguridad, fe pública, confianza en la red, violación de la dignidad de las persona o su desarrollo sexual libre), etc. Vid. Velasco Núñez, Eloy. *Delitos cometidos a través de Internet…op.cit.,* págs. 46, 55 y ss, y 76. Se puede añadir en muchos casos el bajo o nulo perfil criminal de los autores y la escasa idoneidad o imperfección de las formas de agrupamiento delictivo en el sentido de su configuración o calificación jurídico-penal.

[218] Vid. Velasco Núñez, Eloy. *Delitos cometidos a través de Internet…op.cit.,* pág. 73.

[219] Al escoger el término "asociados" se pretende introducir un concepto que integre la ya evidente evolución y diversa utilidad de los DACE, no siempre relacionados directamente con la transmisión de mensajes, como función primaria de los dispositivos de comunicaciones electrónicas, pero no única, cuestión que es objeto de este trabajo (como, por ejemplo, la adquisición de los datos de cobertura o la revelación del IMSI o el IMEI de los terminales mediante análisis del espectro radioeléctrico y fuera de los actos de comunicación).

[220] Por contenido material, GONZÁLEZ LÓPEZ define *"la información cuya transmisión motiva el proceso de comunicación"*. Vid. González López, Juan José. *Los datos de tráfico de las comunicaciones electrónicas en el proceso penal.* Móstoles (Madrid): La Ley, 2007, pág. 48.

[221] VELASCO considera que la evolución tecnológica "*obliga a reinterpretar la protección de ciertos derechos fundamentales (la intimidad, la propia imagen, el secreto de las comunicaciones, la intimidad informática, la protección de los datos tratados automatizadamente, la privacidad y las libertades de expresión e información)"*. Vid. Velasco Núñez, Eloy. *Delitos cometidos a través de Internet…op.cit.,* pág. 52. En este mismo sentido, vid. Pérez Gil, Julio. *Investigación penal y nuevas…op.cit.,* pág. *221.*

comisivas, centrándolo más en las necesidades inherentes a las TIC que en límites cuantitativos objetivos de orden penológico[222].

En efecto, baste observar el contenido de cualquiera de los casos complejos que investiga la PJE para percatarse de algunos aspectos de interés que han hecho variar la escena del crimen a consecuencia de lo anterior ya que, en definitiva, la complejidad de las comunicaciones electrónicas actuales no se ve compensada por la calidad de las medidas procesales que pueden activarse para alcanzar un nivel análogo de eficacia al que puede obtenerse en el mundo físico.

Parece, en suma, que el proceso penal español, instalado en la morosidad en cuanto a la necesaria reforma de su normativa, se resigna a no tratar una fuente de prueba indispensable para llegar al completo esclarecimiento de determinadas formas delictivas hoy día muy comunes en nuestra sociedad.

---

[222] Sostiene VELASCO que *"la constante necesidad de aplicar medidas restrictivas de algunos de los derechos fundamentales recogidos en el art. 18 CE, en delitos de leve penalidad, es otra característica de la investigación de este tipo de delitos que debe vincularse más a la esfera de utilización sobre la que recaen las nuevas tecnologías que a consideraciones innecesarias sobre la gravedad penológica…El Tribunal Constitucional aleja la caracterización de la "gravedad" necesaria para injerir derechos fundamentales en este tipo de investigaciones de meras consideraciones matemáticas como las consignadas a otros efectos en el art. 33 CP y las residencia en la afección a la relevancia jurídica penal de los hechos, su bien jurídico protegido y la trascendencia social afectados"*. Vid. Velasco Núñez, Eloy. *Delitos cometidos a través de Internet…op.cit.,* pág. 73. Vid. Martín Pallín, José Antonio. *El equilibrio entre la conservación de datos y el secreto de las comunicaciones: implicaciones en el proceso penal.* [ed.] Agencia Española de Protección de Datos. *La protección de datos en la cooperación policial y judicial.* Madrid: Aranzadi S.A., 2008, págs. 153-162, pág. 154. Sería tanto más razonable entender el término "grave" en su expresión estrictamente semántica de transcendencia o importancia de acuerdo con el daño que se cause o se pretenda causar, aplicándose el principio de lesividad según la interpretación jurisprudencial con el que se extiende el concepto relacionándolo con *"…la relevancia social del hecho o del bien jurídico protegido",* según se proclama, entre otras, en las SSTC 299/2000, de 11 de diciembre; 14/2001, de 18 de enero; 202/2001, de 15 de octubre y 167/2002, de 18 de septiembre. Con la STC 104/2006, de 3 de abril, se extiende el concepto a *"…la potencialidad lesiva del uso de instrumentos informáticos para la comisión del delito".* Sobre esto último, vid. Rodríguez Lainz, José Luis. 2008. *Dirección IP, IMSI e intervención judicial de las comunicaciones electrónicas.* Córdoba, 2008 y Rodríguez Lainz, José Luis. *El principio de proporcionalidad en la nueva Ley de conservación de datos relativos a las comunicaciones.* Diario La Ley, 7062/2007, Nº 6860, Sección Doctrina, 14 Ene. 2008, Año XXIX, Ref. D-10, Editorial LA LEY. En esta última referencia, dice este autor que *"tal criterio [el de la potencialidad lesiva de los instrumentos informáticos] se basa en dos razones muy concretas, como son tanto la posibilidad de expansión de determinados delitos por las redes de comunicaciones, y la grave dificultad de su persecución por los medios tradicionales de investigación; de suerte que la implicación del principio de necesidad de la medida y la lucha contra auténticos santuarios de impunidad, abren un campo hasta ahora inescrutado para el empleo de técnicas de investigación basadas en la injerencia sobre contenidos o datos de tráfico de comunicaciones, y por ende, sin duda sobre los datos almacenados por mandato de la LCDCE. El Tribunal Constitucional llega a reconocer por primera vez de forma abierta la necesidad de dar una respuesta jurídica específica a la adaptación del mundo de la delincuencia organizada o transnacional al fenómeno expansivo de las comunicaciones electrónicas; y lo hace abriendo las puertas de la utilización de técnicas de injerencia en el secreto de las comunicaciones"*.

A los anteriores efectos, de forma clarividente, afirma PÉREZ GIL que:

> *"Por situarnos nuevamente ante un ejemplo, diremos que por definición toda investigación penal tiene por objeto la búsqueda de datos. Hoy, en plena sociedad de la información y el conocimiento, las medidas que implican tratamiento (automatizado o no) de los datos personales son uno de los pilares sobre los que se asienta cualquier indagación, con lo que también podríamos hablar de la digitalización de la instrucción. Pero nuestra normativa procesal penal no sólo se halla anclada en un mundo analógico, sino que lo está en uno superado ya por el curso de los tiempos, sin alcanzar a ver la trascendencia de la protección de datos. Ello hace que nos enfrentemos constantemente a dudas sobre cómo trasvasar los conceptos de tratamiento o de cesión de datos al proceso penal, máxime cuando se trata de datos que pueden haber sido recogidos antes de la comisión de los hechos y para finalidades absolutamente diversas"*[223].

Es decir, en términos prácticos, que el proceso penal en este campo está urgido de cambios legislativos o, entretanto, a servirse de la adaptación de interpretaciones doctrinales como la contenida en la ***prueba pericial de inteligencia*** o ***prueba de inteligencia policial*** (término este último que propongo como más adecuado según los razonamientos que se expondrán en un apartado posterior), siempre dentro del principio de proporcionalidad, de forma que se faculte como proceda a la PJE para desarrollar labores de inteligencia en el marco de las comunicaciones electrónicas[224].

En los apartados siguientes se va a presentar un breve panorama de la DO o grave según los parámetros evolutivos que ofrece la realidad criminológica de los tiempos actuales. Si en algo ha incrementado la grave amenaza que supone es, en términos generales y respecto a cómo era la situación de no demasiados años atrás, su carácter marcadamente transnacional, la sofisticación de sus maquinaciones y los

[223] Vid. Pérez Gil, Julio. *Investigación penal y nuevas…op.cit.,* pág. *221.*

[224] No deja de inquietar a algunos autores *"el progresivo incremento de las facultades policiales"*, como teme PEDRAZ, pero lo cierto es que a esta situación no viene generada por los afanes expansivos de la PJE sino por la evolución de un exigente panorama criminal cuyos operadores figuran en él con nombre propio y cuyo tratamiento no puede atribuirse con exclusividad al estamento judicial. Vid. Pedraz Penalva, Ernesto. 2008. *Notas sobre policía…op. cit., p*ágs. 91 y ss.

ambiciosos objetivos delictuales, lo que incluye la pretensión en algunos casos de socavar y sustituir al mismo Estado de Derecho.

Pues bien, súmese ahora a los fenómenos de DO que se van a describir el factor modificativo que supone lo que se ha relatado en este apartado respecto de la investigación policial en el ámbito de las TIC y los problemas procesales que todo ello conlleva.

2. La delincuencia organizada

Según el diccionario, por "definición" debe entenderse la *"proposición que expone con claridad y exactitud los caracteres genéricos y diferenciales de algo material o inmaterial*". Por ello, es necesario recurrir a las definiciones para centrar el asunto que se va a tratar.

Naturalmente, las consecuencias jurídicas de un acto deben sobrevenir si este está perfectamente descrito – definido - en la Ley[225]. Por tanto, aún asumiendo el riesgo de la imprecisión y con único propósito descriptivo, se incluyen a continuación algunas definiciones sobre qué es la DO:

a) Algunas definiciones doctrinales

Para HERRERO *"es la que se realiza a través de un grupo o asociación criminal, revestidos de las siguientes características: carácter estructurado, permanente, autorrenovable, jerarquizado, destinado a lucrarse con bienes y servicios ilegales o a efectuar hechos antijurídicos con intención sociopolítica. Valedores de la disciplina y de toda clase de medios frente a terceros con el fin de alcanzar sus objetivos"*[226].

[225] En este sentido se pronuncia GÓMEZ DE LIAÑO, resaltando la necesidad de que el investigador sepa qué ha de perseguir y cómo. Vid. cita de Sansó-Rubert Pascual, Daniel. *Criminalidad organizada transnacional…op.cit.,* pág. 212.

[226] Vid. HERRERO HERRERO, citado por Sansó-Rubert Pascual, Daniel. *Criminalidad organizada transnacional…op.cit.,* pág. 213

Esta meritoria definición, de contenido eminentemente criminológico, describe con bastante acierto lo que podría entenderse como DO, pero le faltarían aspectos tales como concretar el número de personas que se consideraría que forman un grupo o asociación o restar fuerza de caracterización a aspectos tales como la estructuración o la permanencia ya que, por su parte, y sin dejar de valorarlas en su justo término como señas de identidad, tampoco pueden considerarse signos absolutos de la DO, pues la estructuración puede ser difusa e incluso caótica, sin perder por ello capacidad criminal de alcanzar los fines del grupo, y este, a su vez, constituirse en el tiempo con vocación de caducidad.

Una crítica parecida puede hacerse a la definición de SANSÓ-RUBERT, cuyo concepto criminológico es estructurado a través de los siguientes elementos:

- *"Existencia de un centro de poder.*
- *Distintos niveles jerárquicos y estructuración estanca.*
- *Aplicación de tecnología y logística. Profesionalidad.*
- *Fungibilidad o intercambiabilidad de sus miembros de la empresa criminal que actúan en los escalones inferiores.*
- *Sometimiento a las decisiones que emanan del centro de poder y férrea disciplina.*
- *Movilidad internacional.*
- *Apariencia de legalidad y presencia en los mercados como medio de transformación de los beneficios ilícitos".*

En mi opinión, la precisión en la enumeración de las características conlleva el efecto colateral de restar, llegado el caso, aplicabilidad jurídica a la definición, sobre todo si se ha de entenderse que tienen carácter acumulativo – lo que por otra parte no se indica en esta propuesta -, ya que reduciría sensiblemente el número de grupos que adquirirían la categoría de pertenecientes a la DO, sin alcanzar a dar una respuesta al fenómeno, si como se dice tan rígidamente hubieran de cumplir todas y cada una de ellas.

Por todo ello, el verdadero valor de una definición debiera ser el de informar la opinión de quien ha de aplicar justamente una Ley penal, aconsejándole desde un

punto de vista político-criminal su invocación para establecer las medidas apropiadas de las incluidas en la propia norma.

Como aportación de SANSÓ-RUBERT se destaca el aspecto de la ***apariencia de legalidad*** como efecto más conseguido de un sinnúmero de organizaciones delictivas actuales, sobre todo en materia de delincuencia económica o de influencia socio-política, tales como las redes de defraudación fiscal o los negocios fraudulentos de la delincuencia urbanística que afectan a la corrupción de los ayuntamientos, por poner algunos ejemplos. La ya mencionada *cultura de supresión de la prueba*, en estos casos, adquirirá la consistencia necesaria para que esa apariencia de legalidad alcance el virtuosismo.

b) Definiciones en el derecho internacional

La Convención de Palermo de las Naciones Unidas de 2000 contiene su propia definición, de redacción notoriamente más genérica, en el art. 2 a): *"Por grupo delictivo organizado se entenderá un grupo estructurado de tres o más personas, que exista durante cierto tiempo y que actúe concertadamente con el propósito de cometer uno o más delitos graves o delitos tipificados con arreglo a la presente Convención, con miras a obtener, directa o indirectamente un beneficio económico u otro beneficio de orden material"*[227].

Esta definición, que adolece de precisión, permitiría, en lo positivo, un más amplio margen de aplicación pero, en lo negativo, ocasionaría una mayor inseguridad jurídica. Además, presenta algunas características demasiado rígidas, como es el número mínimo de elementos (tres), superado por la actual legislación europea (dos), o la referencia a la comisión de delitos graves, según los limites objetivos señalados en el apartado b). Esta última circunstancia excluiría el tratamiento de los tipos que no conllevasen tales penas, considerando tanto más merecedor de reprensión, no el delito de que se trate, sino la capacidad de generación de formas delictivas

[227] Vid. Convención de las Naciones Unidas contra la DO transnacional, adoptada por la Asamblea General de las Naciones Unidas el 15 de noviembre de 2000 (Convención de Palermo).

organizadas en sí mismas, lo que, en mi opinión, merece un tratamiento procesal y penal autónomo.

Para intentar aportar alguna flexibilidad a la categorización, EUROPOL estableció una serie de requisitos, en el orden policial[228], para que se considerase que el fenómeno que se investiga reviste la apariencia de DO:

1. *"Colaboración de dos o más personas.*
2. *Especialización (reparto de tareas).*
3. *Pervivencia definida en el tiempo.*
4. *Recurso a alguna forma de disciplina y control.*
5. *Comisión de delitos graves.*
6. *Proyección internacional.*
7. *Empleo de la violencia o determinadas formas de intimidación.*
8. *Estructura empresarial para el desempeño de sus actividades.*
9. *Implicados en el lavado de dinero.*
10. *Búsqueda de influencia en la esfera política, los medios de comunicación, la administración pública y el poder judicial.*
11. *Afán de lucro".*

Como aportación o hallazgo más notorio podría señalarse que las anteriores características no son acumulativas, sino adaptadas a un estándar básico en el que deben producirse inexcusablemente las conductas incluidas en los números 1, 3, 5 y 11 y verificarse simultáneamente un mínimo de dos de las demás contenidas en el listado, siendo también reseñable la consideración contenida en el punto 1, que reduce a dos el número de personas que, como mínimo, se constituirán en "organización criminal".

Ciertamente, con este sistema se llegaría a cubrir un amplio abanico de la fenomenología actual, pero es necesario insistir en que, en lo negativo, se reproducen los efectos contenidos en otras definiciones dentro de los puntos de obligado cumplimiento. Así, el apartado 3 induce a confusión en la medida en que no determina de una forma clara si ha de considerarse únicamente la permanencia en el tiempo de la organización o basta que durante un periodo sensible de tiempo esta actúe como

[228] Nótese que no se trata de un instrumento de valor jurídico, sino orientativo de la actuación policial desde un punto de vista estrictamente criminológico y policial.

tal, lo que, en su caso, dejaría un margen indefinido de apreciación a esta circunstancia.

En igual medida, vuelve a reproducirse la invocación de los delitos graves, cuestión que me merece la opinión reflejada en párrafos anteriores, a lo que además se sumaría un insuficiente apartado 11, donde la definición de ***lucro*** no es pacífica, ya que puede interpretarse de forma estricta como la obtención de una ganancia económica, en contraposición a una más amplia de "obtención de una ventaja", sin especificar su naturaleza, lo que parece más acertado, pues no siempre se busca el lucro económico, sino la usurpación de los más variados bienes jurídicamente protegidos.

Notorio, y creo que injustificado, es el número mínimo de participantes en la red, que es de dos, lo que nos aleja de la interpretación semántica del término de "organización" que, indudablemente, requiere la concertación de varias personas para conseguir un determinado fin, ilícito en este caso.

Se llega con esto a la definición contenida en el art. 1 de la *Decisión Marco 2008/841/JAI del Consejo de 24 de octubre de 2008, relativa a la lucha contra la DO,* que establece lo siguiente:

> *"1) «organización delictiva»: una asociación estructurada de más de dos personas, establecida durante un cierto período de tiempo y que actúa de manera concertada con el fin de cometer delitos sancionables con una pena privativa de libertad o una medida de seguridad privativa de libertad de un máximo de al menos cuatro años o con una pena aún más severa, con el objetivo de obtener, directa o indirectamente, un beneficio económico u otro beneficio de orden material;*
>
> *2) «asociación estructurada»: una organización no formada fortuitamente para la comisión inmediata de un delito ni que necesite haber asignado a sus miembros funciones formalmente definidas, continuidad en la condición de miembro, o exista una estructura desarrollada".*

La mayor virtud de esta definición es la de su carácter comprensivo de la mayoría de los fenómenos delictivos organizados actuales, sin que por ello se pierda la

necesaria precisión conceptual en la categorización. Esto es así, bien porque mantiene el número mínimo de miembros en lo imprescindible para considerar que se trata de la actuación concertada entre personas, lo cual sólo podría producirse si participasen al menos tres, como indica la lógica; bien porque los rasgos de la estructuración señalados en el apartado segundo son notoriamente laxos, pues no se relacionan con la estabilidad o permanencia en el tiempo de la organización criminal, la calidad o complejidad de la propia estructuración o la adhesión estable que recibe de sus miembros. Vuelve el concepto de delito grave o, al menos, el del establecimiento de un límite objetivo e las penas asociadas a los hechos que protagonice el grupo, lo que, en mi opinión, obliga a excluir conductas reiteradas y bien preparadas que no generarían la penalidad establecida.

c)Definiciones en la reforma del Código Penal del 2010

En la reforma operada en el Código Penal mediante la Ley Orgánica 5/2010, de 22 de junio, *por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal*, se reconoce en su exposición de motivos la insuficiencia del art. 515 y ss, de asociación ilícita, para el tratamiento de la delincuencia organizada, cuya potencialidad lesiva ha ido en aumento. De forma inquietante, proclama que la DO *"se caracteriza en el aspecto cualitativo por generar procedimientos e instrumentos complejos específicamente dirigidos a asegurar la impunidad de sus actividades y de sus miembros, y a la ocultación de sus recursos y de los rendimientos de aquéllas, en lo posible dentro de una falsa apariencia de conformidad con la ley, alterando a tal fin el normal funcionamiento de los mercados y de las instituciones, corrompiendo la naturaleza de los negocios jurídicos, e incluso afectando a la gestión y a la capacidad de acción de los órganos del Estado"*.

Por todo ello, incluye en su articulado una nueva definición de ***organización criminal***[229], que se encuentra en el art. 570bis.1:

[229] VELASCO NÚÑEZ considera esta aportación en la línea de la DM 2008/841/JAI, de 24 de octubre, sobre la lucha contra la DO. Vid. Velasco Núñez, Eloy. Crimen organizado, Internet…*op. cit.*

> *"A los efectos de este Código se entiende por organización criminal la agrupación formada por más de dos personas con carácter estable o por tiempo indefinido, que de manera concertada y coordinada se repartan diversas tareas o funciones con el fin de cometer delitos, así como de llevar a cabo la perpetración reiterada de faltas"*.

La principal novedad de esta definición, de un lado, es la de considerar que un grupo delictivo organizado no tiene por qué dedicarse exclusivamente a las grandes conspiraciones criminales, cuyos delitos alcancen la consideración de graves, sino que también puede serlo si su dedicación es a los delitos menores o faltas.

Es decir, que la sugestiva actividad "profesional" de dedicarse a los ataques a bienes jurídicos de transcendencia menor – sin duda muy lucrativa y perturbadora del orden - que se cuida de no irrumpir en las formas graves de delito, también va tener su respuesta penal proporcionada a la reprensibilidad de las conductas asociadas. En este sentido, se establece la respuesta penal proporcionada a la trascendencia de tales hechos.

De otro lado, queda resuelta la cuestión de la permanencia en el tiempo de la forma DO, dejando en manos del prudente arbitrio jurisdiccional el considerar cuándo tiene "carácter estable", lo que sin duda permitirá un enfoque ajustado a la necesidad de valorar e individualizar los efectos jurídicos que deberán ser instaurados.

Se añade una nueva categorización criminal en el art. 570ter CP sobre la consideración de ***grupo criminal***, como una organización de menor integridad y cohesión, para considerar, según la exposición de motivos *"otros fenómenos análogos muy extendidos en la sociedad actual, a veces extremadamente peligrosos o violentos, que no reúnen los elementos estructurales" de la organización criminal"*, flexibilizando o extendiendo de esta manera la consideración de estructura criminal a fenómenos ciertamente amplios o inespecíficos, cuyas amenazas encontrarán tratamiento a través de este artículo.

La compleja estructuración de la nueva norma penal hace evidente la necesidad de que el juzgador halle la expresión precisa para la forma de DO que esté

examinando, de manera que pueda establecer con la mayor exactitud las diversas consecuencias jurídicas explicitadas en los tipos.

Sobre los concretos delitos que hayan protagonizado sus miembros – a los que corresponderá una concreta pena – aparece la necesaria valoración político-criminal en razón de su integración en la organización más allá de la comisión de aquellos, tanto si se les pueden atribuir como si no. Es decir, que se hará preciso valorar la calidad de la organización delictiva en sí misma y la individualización de la responsabilidad contraída por cada uno de sus miembros, todo ello con independencia de los delitos que cometa por más que les correspondan una u otra pena o las demás consecuencias jurídicas según la gravedad de los que eran su objetivo delictual[230].

En esto, y desde el punto de vista de la PJE, se configura un plus de exigencia para alcanzar en el acto de juicio oral la acreditación de las características criminológicas de la red y que, de forma indubitada, habrán de generar la convicción judicial sobre la existencia de una red de DO merecedora del tratamiento jurídico-penal establecido en los nuevos tipos mencionados.

Por ello, la investigación criminal deberá ir orientada de forma muy exigente a desentrañar una faceta que se extiende más allá de los delitos subyacentes y que de forma autónoma e individualizada deberán también llegar a probarse.

Se puede concluir que el juzgador, con los nuevos tipos penales para el tratamiento de la DO, se encontrará con un amplio margen de valoración en el que extender sus apreciaciones político-criminales algo más de lo que sería habitual en aquellos casos en que se enjuician otros tipos delictivos.

Se ha de entender también que la singularidad criminal de cada red variará sensiblemente en cada caso, dando lugar a una valoración específica e individualizada

[230] Se constata la extrema complejidad del nuevo sistema punitivo instaurado con la reforma del 2010, según se trate de una organización o un grupo criminal y estas en relación con la gravedad objetiva de los hechos cometidos, así como de los roles de sus miembros que se acrediten durante la investigación y posterior juicio oral: promotor, constituyente, organizador, coordinador, dirigente, participante activo, integrante, cooperador económico o activo, líder, etc. Se hará evidente la necesidad de contar nuevamente con la consolidación de criterios jurisprudenciales para afrontar debidamente la valoración de una u otra consideración, lo que no parece precisamente fácil dada la disparidad de las apreciaciones político-criminales que suelen proclamarse en las STS y el tiempo en que se acumulen de tal forma que se puedan considerar constantes y pacíficas. Vid. Velasco Núñez, Eloy. *Crimen organizado, Internet…op. cit.*

para cada uno de sus miembros según su forma de participación. Por ello, ha de constatarse la dificultad que tendrá para llegar a conclusiones justas y proporcionadas[231], para lo que deberá sin duda contar con las aportaciones de la PJE en lo que se ha venido en denominar la prueba pericial de inteligencia o prueba de inteligencia policial y que será tratada más adelante.

3. La dimensión transnacional de la delincuencia

La evolución de la delincuencia desde el último cuarto del siglo pasado hasta la actualidad, en términos generales, ha pasado del hecho delictivo producido en precisas áreas locales a adquirir una grave dimensión transnacional.

Así lo ha advertido la ONU al afirmar que:

> *"La delincuencia organizada transnacional es una amenaza para el Estado y la sociedad. Atenta contra la seguridad del ser humano y la obligación fundamental del Estado de mantener el imperio de la ley. La lucha contra la delincuencia organizada no sólo reduce esa amenaza directa a la seguridad del Estado y el ser humano sino que constituye un paso necesario en la tarea de prevenir y resolver los conflictos internos, combatir la proliferación de armamentos y prevenir el terrorismo"*[232].

Esta preocupación ha llegado a trascender de los responsables de la seguridad pública interior para alcanzar directamente a los de la defensa, tanto desde sus

[231] Consciente de estas dificultades, la Fiscalía General del Estado, en su Circular 2/2011 sobre la reforma del Código Penal por Ley Orgánica 5/2010 en relación con las organizaciones y grupos criminales, valorando el hecho de que tales conceptos se extiendan a fenómenos hasta ahora considerados menores y que estos, a su vez, sean difíciles de distinguir de los graves, orienta a los Fiscales en sentido de examinar su peligrosidad en función de elementos concretos, tales como la complejidad de su estructuración, la profesionalidad con actúen sus miembros, su implantación geográfica, incluido el carácter transnacional, etc.

[232] Vid. *"Un mundo más seguro: la responsabilidad que compartimos". Documento del Quincuagésimo noveno período de sesiones. Tema 55 del programa. Seguimiento de los resultados de la Cumbre del Milenio. A/59/565.*, pfo. 165, y que puede consultarse en la página *web* http://www.un.org/spanish/secureworld/. En él se recogen aspectos tan inquietantes como el dinero que se blanquea en el mundo anualmente (de 300.000 a 500.000 millones de dólares sólo por los narcotraficantes o la estimación total para el año 2000 de 500.000 MM $ a 1,5 miles de millones de dólares).

estructuras nacionales como internacionales[233]. De esta forma se pronuncian, por ejemplo, los secretarios generales de la OTAN[234] sobre el terrorismo y la DO y, especialmente, en la cooperación y vínculos financieros entre ambos fenómenos, en los que está presente, entre otros inquietantes fenómenos, la droga, la corrupción y el blanqueo de capitales[235,236].

La lectura de los diversos documentos estratégicos consultados dejan traslucir un cierto poso de impotencia ante la extraordinaria dimensión del problema[237] – que nace desde la misma falta de consenso en las definiciones de términos como "terrorismo" - y sobre las formas en las que los estados de derecho podrían afrontarlo, sin que, por otra parte, lleguen a definir dónde empieza y dónde acaba una u otra amenaza, y dónde dejaría de ser materia policial para necesitar los instrumentos y mecanismos propios de la defensa[238].

---

[233] En el Ministerio de Defensa se afirma que *"también es necesario considerar que, aunque aisladamente el crimen organizado, es en esencia un problema policial propio de la esfera de la Seguridad Interior del Estado, sin embargo, la relación creciente entre sus actividades delictivas, llevadas a cabo en los espacios vacíos de Estados con déficit de gobernabilidad o de estabilidad institucional y recurriendo al terrorismo o a la subversión como forma de acción política, cambia radicalmente el panorama estratégico ubicando esta amenaza en la esfera de la Seguridad Nacional, ya sea en el interior del Estado, o en su consideración como conflictos internacionales cuando éstos adquieren una dimensión transnacional".* Vid. "*Hacia una estrategia de seguridad en España"* en el Documento de Seguridad y Defensa núm. 25 del CESEDEN, de febrero de 2009.

[234] Asumiendo esta visión, el antiguo Secretario General Lord Robertson, ya se refirió al cambio de paradigma en el tratamiendo doméstico del terrorismo y la delincuencia organizada a cargo de la policía para exceder a este escenario y a sus capacidades, adquiriendo una dimesnión internacional necesitado de enfoques más ambiciosos *("Terrorism was then, by and large, a national threat, requiring a domestic response. Defeating it was largely the responsibility of law-enforcement and intelligence personnel. Organized crime, too, was a threat without real international security implications - a challenge for police officers and crusading judges")*.
Vid. *"A new security network for the 21st Century"*, Discurso del Secretario General de la OTAN, Lord Robertson, en 2002.

[235] Vid. *"NATO and Russia: a new begining"*. Discurso del Secretario General de la OTAN, Anders Rassmusen en el Carnegie Endowment de Bruselas (Bélgica) el 18 de septiembre de 2009.

[236] El G-8 también se pronuncia en este mismo sentido. Vid. *"G-8 Leaders Statement on Countering Terrorism".* Declaración de 26 de junio de 2010.

[237] En el *Informe Albright* se afirma lo siguiente: *"Between now [2010] and 2020, the international security environment will change in ways both predictable and unforeseen. Certainly, the forces that come under the general heading of globalization can be counted upon to intensify. This will result in a rapid, if uneven, growth in cross-border flows of goods, services, people, technology, ideas, customs, crime, and weapons."* Vid. *"NATO 2020: Assured security; dynamic engagement. Analysis and recommendations of the group of experts on a new strategic concept for NATO" (Informe Albright),* de 17 de mayo de 2010.

[238] Hay que anotar, con finalidad ilustrativa, que los actos de guerra trascienden ya al uso del armamento convencional o nuclear, para llegar a lanzar ciberataques con consecuencias similares para las infraestructuras industriales críticas. El gusano informático *Stuxnet* se utilizó para dañar las instalaciones nucleares de Irán mediante la alteración de los sistemas informáticos que regían el

En todos los documentos, junto a las consabidas referencias a la necesidad de controlar los aspectos de corrupción, de financiación y blanqueo de los capitales procedentes del delito, así como los efectos intensificadores y diluyentes de la responsabilidad real asociados a la globalización y el uso de las tecnologías de la información y el conocimiento, se menciona recurrentemente la necesidad del intercambio de inteligencia entre los países y la falta de implementación de mejores recursos legislativos.

En el documento de la ONU se afirma que :

> *"Los Estados y las organizaciones internacionales no han reaccionado con rapidez suficiente a la amenaza que plantean la delincuencia organizada y la corrupción. Las declaraciones sobre la gravedad del problema rara vez han sido acompañadas de las medidas correspondientes. Hay tres obstáculos básicos que impiden una respuesta internacional más eficaz: una cooperación insuficiente entre los Estados, la falta de coordinación entre los organismos internacionales y un incumplimiento inadecuado por parte de muchos Estados…La agilidad con que operan esas redes contrasta marcadamente con el laborioso intercambio de información y la inadecuada cooperación entre los Estados en materia de investigaciones y enjuiciamientos penales"*[239].

A la exigencia de afrontar mejor el fenómeno de la delincuencia organizada, se une la sugerente propuesta de las Naciones Unidas de "*…establecer una autoridad central que facilitara el intercambio de pruebas entre las autoridades judiciales nacionales, la prestación de asistencia judicial mutua entre las Fiscalías y el cumplimiento de los pedidos de extradición".*

Por ello, el intercambio de inteligencia deviene una de las necesidades más imperiosas para afrontar la lucha contra la DO, cuestión está no baladí en la medida en que supone, en primer lugar, tener la capacidad de obtenerla y distribuirla por medios tecnológicamente eficaces usados bajo normas procesales adecuadas; en segundo

---

funcionamiento de las turbinas, acelerándolas más allá de sus límites y causándoles daños irreparables, cual si hubieran recibido el impacto de un misil. Fuente: Diario el Mundo en las fechas: 27/09/2010 y 23/11/2010.

[239] En este documento se recogen y resumen las razones centrales de las que trata este trabajo: Agilizar la accesibilidad a los datos que puedan conducir al esclarecimiento de los hechos que son materia del interés del proceso penal. Vid. *"Un mundo más seguro…op. cit.,* pfo. 170.

lugar, tener la posibilidad de superar las barreras impuestas por el carácter fuertemente territorial de las diversas legislaciones penales en la escena internacional; y, en tercer lugar, poder asumir la cesión de soberanía que supone toda esta actividad, máxime cuando la disparidad de las legislaciones de otros países supone una incertidumbre sobre su aplicación acorde con el acervo democrático que respalda a las actuaciones en el espacio soberano propio.

Evidentemente, los espacios supranacionales para la cooperación penal, como es o debiera ser el de la Unión Europea, suponen una meritoria aproximación a este concepto[240], aun revestidos de todos los problemas y defectos que también serán objeto de atención. Esto supone una previa equiparación de la calidad de los estados de derecho constituidos en cada uno de los países miembros, lo que, desde luego, no es a día de hoy exportable a una gran mayoría de los demás miembros de las Naciones Unidas.

En mi opinión, no se puede sino constatar la certeza de las aseveraciones contenidas en el informe de la ONU y lamentar la falta de reactividad de los gobiernos para concertarse en la lucha contra la DO y el terrorismo, donde deben ocupar un lugar distinguido – que no único – los instrumentos del derecho procesal penal. Más difuso, y desde luego más controvertido, es el papel que habrían de jugar los recursos de la defensa nacional y de los organismos internaciones para afrontar la lucha contra el terrorismo y la DO[241].

En relación con esto último, en la Cumbre de Estrasburgo – Kehl, celebrada el 4 de abril de 2009, los jefes de Estado y de Gobierno de la OTAN aprobaron la Declaración sobre Seguridad Aliada –basada en su concepto estratégico de 1999, y revisado en 2010 en el que se afirma que *"…los aliados reconocen que deben hacer frente no sólo a amenazas militares, sino también a otra serie de factores…el*

[240] El Tratado de Maastricht, de una forma ciertamente artificiosa, estableció un tercer pilar para la Unión Europea dedicado a un "espacio de libertad y seguridad común", muy débil en la práctica, en el que la cooperación judicial, policial y aduanera deberían tener su acomodo. Esta estructura, superada hoy día por el Tratado de Lisboa, responde a un trabajoso esfuerzo – muy contestado e inconcluso – para conseguir un espacio europeo donde ejercer la soberanía en materia penal, al menos para afrontar las amenazas más inquietantes a que está sometida la sociedad: el terrorismo y la DO.

[241] En este inconcreto espacio que se dibuja en la escena internacional se podrían situar los esfuerzos de la comunidad de naciones en afrontar algunas formas singulares de la DO, como la Operación "Atalanta", contra la piratería en el Océano Índico, o la presunta extensión de la lucha contra el terrorismo islámico a países como Irak o Afganistán.

terrorismo, el crimen organizado, los problemas en el suministro de recursos energéticos y los movimientos masivos de población pueden afectar a la estabilidad"[242].

En esta declaración se sientan las bases para la elaboración de un nuevo Concepto Estratégico, del que sería parte España[243]. En relación con el ámbito nacional, la Ministra de Defensa afirma que "*el tradicional enfrentamiento entre bloques, basado en una estrategia de bipolaridad, ha dado paso a nuevas amenazas y riesgos para nuestra seguridad, como son el terrorismo internacional*[244]*, la posibilidad de obtención de armas de destrucción masiva por individuos o por* organizaciones *terroristas, los estados fallidos o en descomposición*[245]*, la delincuencia y crimen organizado o la irrupción de conflictos de carácter asimétrico. Estamos por tanto ante un escenario cuyas características fundamentales son su complejidad, su incertidumbre y su alta peligrosidad"*[246].

La profundización en los documentos estratégicos de defensa proporciona una visión trascendente del fenómeno de la DO transnacional que, si en una faceta nacional se encontraría una respuesta dentro del proceso penal o de medidas más o menos ambiciosas de política criminal, obliga a tratar de percibir además cómo habría de ser esa respuesta en un escenario internacional en el que el proceso penal interno

[242] Vid. *"Nuevo concepto estratégico"* del Ministerio de Defensa en 2009.

[243] En este mismo sentido, pueden verse los conceptos estratégicos del Reino Unido y de los Estados Unidos, en los documentos respectivos del año 2010 *"A Strong Britain in an Age of Uncertainty: The National Security Strategy"* y *"National Security Strategy"*. Ambos documentos incluyen insistentes referencias a las amenazas de las redes de DO y, particularmente, de los potenciales peligros del uso malicioso de las TIC. En la página 39 del documento estadounidense se recoge una especial preocupación por los efectos de desestabilización de los gobiernos y quebrantos en el sistema financiero global.

[244] Los escenarios bélicos pasan de visualizarse en los documentos estratégicos como enfrentamientos entre ejércitos regulares de potencias en pugna a actuaciones difusas de terroristas cuyos ataques se encubren en la propia sociedad y sirviéndose de sus mismos instrumentos, a los que poca táctica o estrategia militar pueden oponerse. El factor financiero o empresarial, convenientemente usado por el terrorismo, por ejemplo, dificulta cualquier maniobra de represión desde este concreto ámbito.

[245] Pueden mencionarse el extraordinario efecto que tuvo la descomposición de la antigua Yugoslavia y la caída de los regímenes comunistas del este europeo en términos de incremento de la delincuencia en varios países de la UE y, singularmente, en España, donde las bandas de albano-kosovares, rumanos, búlgaros, ucranianos, rusos, etc., brillan con luz propia en las estadísticas policiales, en ocasiones, además, caracterizados por una gran violencia en sus formas de actuación. Sobre los estados fallidos puede consultarse la página *web* del Fondo para la Paz http://www.fundforpeace.org/global/?q=fsi.

[246] Comparecencia para informar del desarrollo de las Operaciones de Paz en el exterior (Congreso de los Diputados,10 de diciembre de 2008).

ninguna respuesta puede dar[247], todo dirigido a conseguir para los ciudadanos no sólo una seguridad real sino una percepción psicológica de que, en verdad, están seguros. Naturalmente, todo esto, excede y trasciende al propio ejercicio de la jurisdicción penal para alcanzar a conceptos estratégicos relacionados con la seguridad integral[248].

Un buen ejemplo de lo anterior se puede encontrar en investigaciones sobre determinados tráficos ilícitos o algunos de los usos de las TIC, donde no es fácil distinguir dónde termina la acción de una organización de delincuentes, dónde se entra en materia de terrorismo o, directamente, en qué puede afectar a la seguridad nacional e internacional.

Así, se pueden analizar algunas investigaciones como las que se proponen a continuación:

- En un caso criminal, la UOPJ de la Comandancia de la Guardia Civil de Madrid detectó lo que en un principio parecía un mero delito contra la propiedad industrial. Su presunto autor, un empresario del ramo del metal, se dedicaba a fabricar repuestos falsos para aeronaves de guerra[249]. Esto plantearía dos preguntas iniciales básicas: La primera, sobre la seguridad de unas piezas cuya posible falta de calidad pudiera ocasionar un accidente aéreo, además de cualquier otra consideración sobre la correcta tutela de los derechos de propiedad industrial vulnerados. Pero la segunda, mucho más alarmante, habría que formularla al saber que estas piezas eran para aeronaves de guerra de países de Oriente Medio sujetos a estrictas restricciones de derecho internacional que limitan este tipo de comercio de

[247] Se ha de recordar en este punto lo que se aportó en su momento sobre el derecho penal del enemigo, por su ilicitud, y el derecho de lucha, que tantos interrogantes plantea en la doctrina sobre su idoneidad para servir al proceso penal. En el documento de la ONU *"Un mundo más seguro…op. cit.,* pfo. 147 se afirma que *"los gobiernos y las organizaciones de la sociedad civil expresaron preocupación por el hecho de que la actual "guerra contra el terrorismo" había vulnerado en algunos casos precisamente los valores que los terroristas pretendían conculcar: los derechos humanos y el Estado de Derecho"*.

[248] Para SANSÓ-RUBERT *"…las perspectivas sobre el crimen transnacional organizado se han ido asociando con aspectos de seguridad internacional. La floreciente eclosión de diversidad de tráficos ilícitos, especialmente el narcotráfico y la inmigración ilegal, sumado al creciente número de conflictos interesadamente alimentados por una actividad criminal con proyección internacional, han sido cruciales para reformular el problema de las redes criminales transnacionales en el contexto de la seguridad e incluso de la defensa".* Vid. Sansó-Rubert Pascual, Daniel. *Criminalidad organizada transnacional…op.cit.,* pág. 208.

[249] DP 416/2009 del Juzgado Central de Instrucción Nº 5 de los de la Audiencia Nacional (Madrid). Véase también la nota de prensa sobre la Operación CUREÑA, de 11 de julio de 2007, en www.guardiacivil.org.

materiales de defensa y doble uso en razón de la amenaza que suponen para la estabilidad mundial.

- Otro interesante ejemplo lo representa una investigación sobre una red de ordenadores (llamados *zombies*) que, en número superior a los 12 millones y sin que sus propietarios se percatasen, habían sido infectados por la red "Botnet Mariposa" para lanzar su ataques informáticos por sí o bien ofreciéndoselos a terceros, hechos investigados en la escena internacional por el Grupo de Delitos Telemáticos de la Unidad Central Operativa de la Guardia Civil[250]. Lo interesante de esta investigación hay que situarlo en varias de sus circunstancias: En primer lugar, anotar que los ordenadores se podían utilizar para realizar devastadores ataques DoS a los sistemas informáticos mundiales, incluyendo el ciberterrorismo, tanto los de ciudadanos particulares como de instituciones públicas o privadas o, incluso, de infraestructuras o recursos críticos[251]; En segundo lugar, que este ataque fue ejecutado tan sólo por seis personas comunes, sin una especial vinculación entre ellas[252]; En tercer lugar, la sofisticación de las herramientas de las TIC, con el uso de programas llamados "troyanos" (*malware* o *software* malintencionado, si es utilizado para finalidades ilícitas, destinado a dañar o usar los ordenadores ajenos como medio para cometer delitos, sin el conocimiento de sus usuarios) y, en cuarto lugar, la accesibilidad a dichas herramientas y la aparente sencillez de su diseminación por parte de los imputados, que llegó a alcanzar nada menos que a 190 países, incluyendo importantes estructuras gubernamentales que se pusieron en riesgo sin que sus gestores se apercibieran de ello[253].

---

[250] Véase la Nota de Prensa sobre la "*Botnet* Mariposa", de 3 de marzo de 2010, www.guardiacivil.org. Entre otras entrevistas realizadas con miembros del GDT, merecen resaltarse las realizadas con el Teniente Coronel D. Juan Salom Clotet, Comandante D. Óscar de la Cruz Yagüe y Capitán D. César Lorenzana González, en cuya excelente labor e inestimable ayuda se residencian buena parte de los conocimientos que he adquirido para realizar este estudio.

[251] Se produjo un ataque de denegación de servicio a una importante empresa de Canadá, por ejemplo, que ocasionó la desactivación de los ordenadores de universidades y administración de ese país.

[252] Nótese también las dificultades para considerar la condición de DO donde faltan unos claros signos de concertación para delinquir según las diferentes definiciones que se han aportado.

[253] En el documento nº 10 sobre *Cybercrime* de las Naciones Unidas, incluido en el TOCTA 2010, sobre esta importantísima operación de la Guardia Civil, se afirma que *"los propietarios de la recientemente descubierta "Mariposa Botnet" (una red de ordenadores "esclavos"), quizá la más grande de la historia,*

En este sentido, se hace especialmente amenazador el capítulo de la desestabilización de los países que pueda provenir de la poderosa acción de las redes de DO. Se ha adelantado algo sobre las impresiones de FALCONE respecto de la equiparación al Estado lícito de las estructuras mafiosas ilícitas, con las evidentes secuelas sociales de todo tipo[254].

Todo esto conduce a realizar una reflexión sobre un derecho penal centrado en el tipo delictivo[255], lo que en materia de corrupción o, más genéricamente, en materia de la delincuencia económica tomada en consideración como un sustrato esencial de cualquier actividad delictiva organizada moderna, no tendría un correlato jurídico efectivo que permitiese un tratamiento unificador de la respuesta a través del mero catálogo de tipos a aplicar. Cuando menos, por su efecto real, estos tipos y sus penas y medidas de seguridad asociados alcanzarían inofensivamente únicamente a determinados elementos de la red que, con bastante probabilidad, resultarían ser los menos relevantes[256] – que por su posición en la maquinación criminal y en la propia red se harían amortizables -, sin que esta siquiera se tambalease.

---

no tenían habilidades avanzadas como hackers". Sin embargo, fueron capaces de lanzar demoledores ataques cibernéticos sumando las capacidades computacionales de millones de ordenadores, tal y como se reconoce en el mismo documento. Vid. *The Globalization of Crime: A Transnational Organized Crime Threat Assessment (TOCTA),* pág. *204.*

[254] A este respecto, opina SANSÓ-RUBERT *que "el incremento exponencial de la actividad criminal organizada, caracterizada por la ostentación de un fuerte poder económico y el ejercicio del liderazgo político a través del empleo expeditivo de la violencia, la práctica sutil de la manipulación y la corrupción de amplios sectores del sistema económico y político a nivel mundial, resulta hoy un fenómeno altamente productivo y cada vez más sofisticado, que arroja unas cifras de beneficios extraordinariamente lucrativas. El crimen organizado crece, muta y fruto de la transformación continua se perfecciona, consolidado por todo el orbe una modalidad empresarial delictiva que proyecta su dominación sobre Estado y sociedad con un poder depredador…En cuestión de años, un problema que por tradición había sido interno – local o nacional- de orden público, se ha transformado en una amenaza que puede poner en peligro la viabilidad de las sociedades, la independencia de los gobiernos, la integridad de las instituciones financieras, el funcionamiento de la democracia y los equilibrios en las relaciones internacionales".* Vid. Sansó-Rubert Pascual, Daniel. *Criminalidad organizada transnacional…op.cit.,* págs. 209-210.

[255] Para SANSÓ-RUBERT, *"pretender combatir esta modalidad delictiva propia de una sociedad postindustrial con idénticos planteamientos arbitrados para la delincuencia común, además de un despropósito, resulta absolutamente inoperante"*. Vid. Sansó-Rubert Pascual, Daniel. *Criminalidad organizada transnacional…op.cit.,* pág.232. Por su parte, dice QUINTERO OLIVARES que *"las clásicas explicaciones sobre autoría y la complicidad, la inducción o la autoría mediata, la tesis del dominio del hecho como modo de fundamentar la responsabilidad criminal, saltan en pedazos cuando se intentan aplicar en el campo de la criminalidad organizada"*. Vid. QUINTERO OLIVARES citado por Sansó-Rubert Pascual, Daniel. *Criminalidad organizada transnacional…op.cit.,* pág.232.

[256] Se ha de considerar la existencia de una disociación entre la ejecución material de los hechos delictivos y la estructura delincuencial superior que los determina, consiguiendo establecer una distancia con aquellos de tal sofisticación que llega a preservarla de sus consecuencias, permitiendo no

La vocación de pervivir de la DO se cimenta, precisamente, en la solidez de este sustrato de orden económico de tratamiento incierto en un Estado de Derecho. Puede resumirse, aun con poca precisión, que las formas más inquietantes de la DO moderna – los más profusamente generadores de la cifra oscura - resisten sin mayores convulsiones la acción de los sistemas penales propios de los estados democráticos.

Por ello, se hacen extremadamente necesarias otras medidas de orden administrativo que dificulten los progresos de la DO, tales como planes contra de gestión del fraude, normas mercantiles contra la constitución de sociedades por testaferros o sin cumplimiento de la normativa fiscal o de viabilidad mercantil, normas para que los notarios consignen los instrumentos de pago, legislación sobre descargas de Internet, etc. Es necesaria, consecuentemente, una visión pluridisciplinar de la política criminal.

Para LUPSHA, en relación con la inserción de la DO en el sustrato de las sociedades democráticas, supone *"el desarrollo de una interacción corruptora con los sectores legítimos de poder [que] permite amasar recursos, capitales, información y conocimiento empresarial, hasta alcanzar la etapa simbiótica. Estadio en el que los sectores políticos y económicos se hacen dependientes de los monopolios y redes delictuales. En esta cúspide evolutiva del poder criminal, es ilusorio discernir de las disimilitudes entre Estado y crimen organizado"*[257].

LUPSHA identifica tres etapas o estadios en la evolución global de las organizaciones criminales transnacionales:

- *Grupos de influjo emergentes.*
- *Organizaciones transnacionales o de vínculo.*
- *Organizaciones consolidadas o corporativizadas (incrustadas en los sistemas políticos y económicos, y sus vastos recursos les habilitan para atenazar a la Estado).*

---

sólo su pervivencia sino, también, su progresiva integración en las estructuras sociales no delictivas. En este sentido, Vid. SILVA SÁNCHEZ citado por Sansó-Rubert Pascual, Daniel. *Criminalidad organizada transnacional…op.cit.,* pág. 219.

[257] Vid. Lupsha, P. *Transnational organized crime versus the nation-state.* Transnational Organized Crime. 1: 21-48, 1996: 21-48, citado por Sansó-Rubert Pascual, Daniel. *Criminalidad organizada transnacional…op.cit.,* pág. 219.

Es evidente que, en el tercer escalón, la presencia de la DO se hace indistinguible del Estado, haciéndose difícil su reacción para recuperar el espacio democrático contaminado por aquella.

4. Panorama real de la delincuencia compleja

Las formas modernas de DO dejan obsoleto el esquema clásico "un hecho, un delincuente, un lugar" que claramente preside el espíritu de la anticuada legislación criminal y, particularmente, de su normativa procesal.

En efecto, las redes no cometen un solo hecho delictivo sino que a veces encadenan decenas, cuya naturaleza será frecuentemente pluriofensiva; obviamente, se cometerán desde organizaciones difusamente estructuradas y jerarquizadas, con diferenciación de funciones entre sus miembros; y, finalmente, no se limitarán a un determinado punto geográfico, sino que, en las más de las veces, se producirá en la escena internacional.

Y por si fuera poco, en mi opinión, si la legislación española está pobremente estructurada para el tratamiento procesal de unos fenómenos delictivos que, en expresión seguramente poco afortunada, pueden definirse como "inteligibles", es decir, los robos, homicidios, los secuestros, el narcotráfico, etc.; menos preparada lo está aún para la investigación de aquellos otros, menos inteligibles, propios de la delincuencia tecnológica, la económica, la corrupción, el blanqueo de capitales, etc., que necesitarán de herramientas procesales para investigaciones funcionalmente más sofisticadas.

La evolución legislativa en el ámbito europeo, lenta pero progresivamente, va dando acuse de recibo de la necesidad de cambios que hagan más eficaz la lucha contra la DO. En su Decisión Marco 2008/841/JAI del Consejo, de 24 de octubre de 2008, *relativa a la lucha contra la delincuencia organizada*, transpuesta a la legislación nacional, extiende y amplia el concepto de organización delictiva incluido en su artículo 1.1 hasta convertirlo prácticamente en una norma en blanco, haciendo

además que para se considere que una asociación está estructurada sea bastante el cumplir con los requisitos ciertamente laxos contenidos en su artículo 1.2[258].

A esta DM le han precedido otras que han mejorado sensiblemente en tiempos recientes la cooperación policial y judicial internacional, al menos, en la escena europea. Entre estas podemos mencionar, sin ánimo de exhaustividad, las que facilitan recursos tan importantes y eficaces como los nacidos de la Decisión Marco 2002/584/JAI del Consejo, de 13 de junio de 2002, *relativa a la orden de detención europea y a los procedimientos de entrega entre estados miembros* (que dio lugar a la Ley 3/2003, de 14 de marzo, *sobre la orden europea de detención y entrega*, y a la Ley Orgánica 2/2003, de 14 de marzo, complementaria de la anterior)[259], la Ley 18/2006, de 5 de junio, *para la eficacia en la Unión Europea de las resoluciones de embargo y de aseguramiento de pruebas en procedimientos penales* o el Acto del Consejo de 29 de mayo de 2000 por el que se celebra, de conformidad con el artículo 34 del Tratado de la Unión Europea, el *Convenio relativo a la asistencia judicial en materia penal entre los Estados miembros de la Unión Europea* (2000/C 197/01).

En contraposición, pese a la evolución positiva de la legislación comunitaria, aún debe padecer España concretas insuficiencias procesales como las que se describen en este trabajo o, en mi opinión, lamentables pérdidas de la oportunidad de legislar adecuadamente, como la que sucediera recientemente con la transposición en la Ley 25/2007, *de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones, de 18 de octubre*, de la Directiva 2006/24/CE, *sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones* (En adelante DCD).

Para que la Justicia conozca de los hechos protagonizados por las redes de DO, de los que indudablemente tendrá una información fragmentaria al principio, antes de invocar el uso de determinadas medidas procesales, se tropieza con un problema

[258] Esta conceptuación es notoriamente menos exigente que la incluida en el artículo 282bis.4 LCRIM a efectos de la aplicación de la figura procesal del agente encubierto según los tipos delictivos expresamente enumerados en el mismo párrafo.
[259] Vid. Vallés Causada, Luis. *Aspectos policiales en la aplicación de la Orden Europea de Detención y Entrega.* Madrid: UNED, 2009.

desde su mismo origen, ya que se habrá de servir de las, como poco, ineficaces normas de competencia para el conocimiento de unos hechos[260] que, aunque desde el principio se atisbe su más que probable enjundia, sólo tras penetrar en ellos se comprobará la falta de recursos y competencia para afrontar su adecuada investigación[261]. Se complicarán tanto las cosas, que el Juez de Instrucción y el Fiscal que reciban informaciones sobre hechos propios de la DO, deberán simultanear su exigente conocimiento con los incontables asuntos propios de su día a día, lo que en sí mismo resultará absolutamente desaconsejable.

En más ocasiones de las deseables, se produce incluso un conflicto previo de naturaleza pre-procesal, bien conocido en la práctica, cuando es el propio Instructor Policial quien, temiéndose el conflicto de competencia que se avecina, intenta determinar por sí mismo dónde puede residir, iniciándose a continuación un calvario para conseguir que su interés por investigar sea atendido por juzgados que le rechazan, no ya la competencia, sino la mera recepción de las diligencias policiales[262].

En todo este interludio, y en atención a los artículos 8 y ss LCRIM, se habrá planteado sin duda en el Juzgado de nstrucción que haya recibido las diligencias la cuestión de la competencia, buscando probablemente la inhibición en otra jurisdicción a la que habrá de darse traslado de todo lo actuado (lo que se debe suponer de urgente resolución).

La realidad en estos casos enseña que, pese a las previsiones del artículo 25 LCRIM, la pérdida de eficacia ocasionada por las dudas competenciales condicionará la calidad de la investigación en la medida en que se acabe resolviendo poco o nada desde la sede judicial para no contaminar un asunto que parece destinado a no ser tratado como propio. Todo terminará de complicarse si se plantea un conflicto de competencias para ser resuelto por la instancia superior que proceda, en cuyo caso la pérdida de eficacia policial en la práctica estará más que garantizada[263].

[260] Probablemente se trate de una mera faceta de unos hechos delictivos que tendrán otras innumerables expresiones.
[261] Recuérdese lo dicho sobre la obsolescencia del esquema “un hecho, un delincuente, un lugar”.
[262] Por razones que no vienen al caso, en alguna ocasión ni siquiera se les recibirá personalmente para atender a sus necesidades.
[263] Es lo que en términos coloquiales policiales se llama la “fase de limbo judicial”, dicho sea con todos los respetos, bastante frecuente y cuya duración puede contarse incluso por meses, en la que se sigue

Por tanto, y a falta de una mejor redacción, se detecta desde un punto de vista práctico un primer problema o insuficiencia procesal grave, de naturaleza claramente subjetiva, por la falta de aplicación del precitado artículo 25 LCRIM, que dice:

> *"…Entretanto no recaiga decisión judicial firme resolviendo definitivamente la cuestión promovida o aceptando la competencia, el Juez de Instrucción que acuerde la inhibición a favor de otro de la misma clase seguirá practicando todas las diligencias necesarias para comprobar el delito, averiguar e identificar a los posibles culpables y proteger a los ofendidos o perjudicados por el mismo."*

Las herramientas procesales cuyo análisis se trae a este trabajo, de conseguirse que fuesen realmente eficaces, supondrían el núcleo de lo que necesitaría la Policía Judicial para ejercer correctamente su labor sin menoscabo de los derechos y garantías constitucionales de aquellos a quienes investigue.

Aunque todas van dirigidas a la legítima obtención de pruebas, desde un punto de vista policial se podrían distinguir *grosso modo*, entre otros, dos tipos de herramientas procesales: las que van dirigidas esencialmente a la obtención de inteligencia criminal[264] y las que propiamente se constituyen en una forma de obtención directa de pruebas.

Entre las primeras se pueden distinguir las siguientes:

- Intervención de las comunicaciones.
- Utilización de colaboradores, confidentes y arrepentidos.
- Utilización de medios de Tecnovigilancia.
- Obtención de inteligencia de fuentes restringidas.

Y entre las segundas, incluimos:

- El agente encubierto.

---

investigando heroicamente con los muy limitados recursos de una fase pre-procesal que, a esas alturas, se halla absolutamente agotada, por lo que se necesitará angustiosamente acceder al uso de las herramientas procesales en plenitud y, naturalmente, actuar bajo el debido control jurisdiccional como mejor garantía de la eficacia de la investigación. En ocasiones, los juzgados prohíben incluso, más o menos abiertamente, siquiera la mera entrega de oficios u otros documentos que el celo policial produzca. Son evidentes, por tanto, los riesgos jurídicos que para el investigador comporta esta fase tan anómala y de tan felices pronósticos para el delincuente, aunque ignore lo que sucede en ese momento.

[264] Naturalmente, la inteligencia criminal no tiene otro propósito que el de la localización de las pruebas cuando estas no están al directo alcance del investigador.

- Los testimonios de los testigos y peritos protegidos.
- Las entregas vigiladas.

a) Bandas organizadas que generan gran alarma social

Desde hace varios años, se han asentado en España una serie de bandas de delincuentes extranjeros dedicados al robo, que han hecho de esta actividad delictiva su *modus vivendi* y, en muchos casos, se han especializado en un tipo determinado de delito patrimonial, habiendo alcanzado una alta sofisticación. Los lugares más afectados por este tipo de delitos son: domicilios, comercios de todo tipo (electrodomésticos, textiles, perfumerías, estancos, joyerías, naves industriales, entidades bancarias, centros de enseñanza, etc.), asaltos a vehículos de carga, etc.[265]

Como se ha expuesto con anterioridad, estas bandas no llevan a cabo hechos aislados, sino que cometen numerosos robos en una determinada zona, siendo el número de perjudicados muy elevado, con lo que estos delitos causan una enorme ***alarma social***.

Esta sensación de inseguridad se incrementa en los casos en que se ejerce violencia sobre las personas, caso de los robos en domicilios con los moradores en su interior, secuestros *express*, atracos a viajantes de joyería, etc. Todavía aumenta más esta sensación cuando la violencia afecta a otros miembros del núcleo familiar. Uno de los hechos más significativos ocurridos en los últimos años fue el asalto a la familia Ferri en la localidad de Canals (Valencia), en el que resultaron muertos dos componentes del grupo asaltante por los disparos realizados por el propietario de la vivienda o el caso similar del intento de asalto al chalet de la familia Tous en Barcelona, en el que resultó muerto uno de los que pretendían cometer el robo por los disparos efectuados por un vigilante de seguridad.

[265] Entre otras fuentes consultadas para elaborar este apartado deben figurar diversas entrevistas con el Teniente Coronel D. Antonio Cortés Ruiz, como Jefe del Departamento de Delincuencia Organizada de la UCO. Un análisis muy interesante de la DO actual puede leerse en Requena Espada, Laura. *Delincuencia Organizada: Perfil criminológico de una muestra de miembros activos en organizaciones criminales que han actuado en España entre 1999 y 2010.* Tesis Doctoral. Facultad de Psicología. UAM. Madrid, 2011.

El número de delitos de estas características cometidos hace pensar en la existencia de numerosos grupos de delincuentes dedicados a esta actividad. La experiencia indica que se trata de grupos que actúan de forma independiente, aunque mantienen contactos de forma puntual, con un número de miembros variable, entre cuatro y ocho personas y con especialización funcional, características que permiten encuadrarlos perfectamente en la tipología de la criminalidad organizada, dado que su forma de vida es el delito. Salen casi todas las noches a delinquir y lo habitual es que en cada una de estas salidas realicen sustracciones de vehículos, varios robos en domicilios o establecimientos comerciales y que sea vean implicados en alguna persecución con alguna patrulla policial.

Los componentes de estos grupos criminales, en un porcentaje muy elevado, son delincuentes extranjeros (rumanos, albanokosovares, colombianos, magrebíes, etc.) que mantienen los vínculos con sus países de origen, a los cuales envían los beneficios obtenidos y a donde regresan de forma temporal para descansar o cuando se ven sometidos a una intensa presión policial.

La incidencia de esta clase de delitos es especialmente notoria en todo el arco mediterráneo por la concurrencia de una serie de factores, como son: zona de alto nivel de inmigración y de desarrollo turístico que permite pasar desapercibidos a los integrantes de estas organizaciones delictivas; alto potencial económico que les permite tener una amplia gama de objetivos.

Los *modus operandi* más habituales son los siguientes:

- Robos en domicilios con violencia sobre los moradores para obtener el mayor beneficio económico.
- Robos en domicilios por el procedimiento silencioso, es decir, sin que los propietarios detecten la intrusión[266].
- Robos en naves industriales durante las horas nocturnas practicando butrones para acceder al interior donde sustraen dinero en efectivo (*modus operandi* empleado por las bandas de albanokosovares).

[266] En algunas ocasiones llegan a narcotizar a los moradores.

- Robos en establecimientos comerciales violentando de forma brutal la entrada o los escaparates, mediante el lanzamiento de tapas de alcantarilla o empotrando vehículos (*modus operandi* conocido como "alunizaje").
- Robos con violencia en entidades bancarias durante las horas nocturnas en pequeñas localidades que carecen de Fuerzas de Seguridad, forzando las cajas fuertes o cajeros automáticos. Cuando se instalan sistemas de anclaje y refuerzo de los cajeros, emplean vehículos industriales pesados para arrancarlos y abrirlos en otros puntos[267].
- Robo en joyerías y a representantes del ramo (casi todos los años varios industriales resultan muertos cuando hacen frente a los atracadores, generalmente de nacionalidad colombiana).
- Bandas de delincuentes de nacionalidad chilena cuya actividad consiste en la comisión de robos con intimidación a personas que acaban de realizar extracciones de efectivo en entidades bancarias, sobre las cuales han ejercido un control previo para determinar la operación que han realizado en el banco (*modus operandi* conocido como "cogotazo").
- Robos con violencia y hurtos cometidos sobre turistas que se desplazan en sus automóviles por el territorio nacional, que son obligados a detenerse por individuos que se hacen pasar por policías (*modus operandi* conocido como "policías ful").
- Sustracciones de placas solares o maquinaria industrial, generalmente instaladas en explotaciones agropecuarias, realizadas por delincuentes magrebíes que posteriormente las trasladan a Marruecos.
- Robo de vehículos de gama alta y todo terreno, empleando sofisticados medios tecnológicos para evitar las medidas de seguridad instaladas (los delincuentes búlgaros son los grandes especialistas en esta actividad delictiva) o bien, empleando violencia o intimidación sobre los conductores con la finalidad de obtener la llave original.

[267] Hay bandas organizadas que preparan el terreno para la huída mediante la corta de árboles o torretas de cualquier tipo para obstaculizar la persecución policial.

- Robo de mercancía de alto valor transportada en camiones, aprovechando los descansos en estaciones de servicio (*modus operandi* conocido como "teloneros").
- Grupos de delincuentes franceses de origen magrebí que trasladan partidas de hachís (en torno a los 500 Kg) desde el sur de España hasta Francia en vehículos todo terreno o monovolumen que circulan a muy altas velocidades sin detenerse en los controles policiales (*modus operandi* conocido "*go fast routier*").
- Grandes organizaciones internacionales de narcotráfico[268], capaces de fletar cargueros de altura que portan toneladas de droga, con bases logísticas situadas en países de difícil acceso a la acción policial, redes de distribución a gran escala, uso de aviones, blanqueo de capitales, uso de la violencia, etc.

El ámbito de actuación de estos grupos delictivos es bastante amplio, puesto que residen en un determinado lugar pero se trasladan a puntos distantes, a veces trescientos o cuatrocientos kilómetros, para llevar a cabo los robos. En prácticamente todo el territorio nacional se están produciendo hechos de las características reseñadas con anterioridad, lo que indica la elevada incidencia de la criminalidad organizada, si bien, sólo del simple conocimiento de un hecho delictivo, no se puede deducir la participación de esta clase de bandas.

En las intervenciones telefónicas y controles de actividades que se mantienen sobre los integrantes de las bandas organizadas se puede deducir claramente los procedimientos que utilizan para cometer los robos (preparativos, medidas de seguridad, instrumental, etc.), frecuencia de comisión, zonas de trabajo, actitud ante las patrullas policiales, contactos con el resto de miembros del grupo y con otras bandas, hábitos de vida, destino de los beneficios que obtienen con su actividad ilícita, etc.

Todo lo anteriormente expuesto da una idea bastante clara del nivel de organización y peligrosidad, así como de la necesidad de disponer de mecanismos legales suficientes, así como de recursos de tecnovigilancia para luchar adecuadamente contra esta nueva delincuencia.

[268] Cannábicos, cocaína, heroína, sustancias de diseño, etc.

Por otra parte, es innegable que estos grupos de delincuentes adoptan medidas de seguridad para evitar la acción de las Fuerzas de Seguridad (uso de transmisores, contramedidas para anular alarmas, contravigilancias para detectar seguimientos, circulación en vehículos a altas velocidades, por caminos o por carreteras poco frecuentadas, etc.[269]); suelen ser asistidos por los mismos abogados que les informan de los procedimientos utilizados por la policía para conseguir su detención; hacen un uso intenso de las nuevas tecnologías (telefonía móvil de tercera generación, telefonía satelital, inhibidores de frecuencias de alarma, comunicaciones policiales o celulares, comunicación por correo electrónico, uso de microcámaras de vigilancia; dispositivos para control de flotas, etc.). Todo esto hace necesario que las Unidades de Investigación utilicen también numerosos medios técnicos para contrarrestar los procedimientos utilizados por los delincuentes.

Por tanto, para la lucha contra la criminalidad organizada es necesaria una centralización de la información a nivel nacional, análisis operativo, intercambio inmediato de los datos obtenidos por las unidades de investigación, especialización de la investigación, sobre todo, a nivel central, etc.

En resumen, se puede decir que la criminalidad organizada es una de las principales amenazas para la sociedad actual, por ser la seguridad uno de los principales logros alcanzados y también uno de los principales requerimientos que se realizan a los poderes públicos

Las principales dificultades en la lucha contra la DO son:

- Carecen de vínculos estables en España, no tienen domicilio fijo, no tienen lazos familiares, no frecuentan lugares habituales, usan de documentación falsificada, a veces circulan indocumentados, etc. Por tanto, la dificultad de localización es muy grande, debido a su movilidad y a no tener un vínculo con un domicilio identificable, un puesto de trabajo, un grupo familiar, etc.
- El comportamiento de esta clase de delincuentes similar a los inmigrantes que se dedican a cualquier actividad lícita. Vienen a España a realizar una campaña

[269] Se ha observado en ocasiones cómo para impartir unas brevísimas instrucciones verbales a un cómplice los delincuentes se han desplazado cientos de kilómetros para evitar las escuchas policiales de sus medios de comunicación (por ejemplo, para indicarles la dirección a la que tienen que dirigirse, lo que supone una comunicación de no más de diez segundos de duración).

delictiva, mantienen lazos con su país de origen, envían dinero a su país de origen (algunos viven con muy poco dinero), regresan de vacaciones, invierten los beneficios en pequeños negocios[270] o adquieren viviendas o terrenos. Entre estos grupos, hay delincuentes dedicados al fraude con tarjetas que critican a los grupos dedicados al robo en domicilios, puesto que hacen daño a las personas y, en cambio ellos "sólo quitan dinero a los bancos".

- El llamado "efecto llamada" que se detecta en las numerosas conversaciones telefónicas espontáneas en las que los delincuentes hablan de la permisividad judicial-policial en España que hace "que en España estaban muy a gusto por ser un lugar muy bueno para hacer negocios".
- Esta clase de bandas mantienen contactos con otros grupos delictivos de su misma nacionalidad asentados en otros países, ya que, anteriormente, habían pasado por estos países antes de llegar a España.
- Gran movilidad, incluso entre distintos países. Hay datos concretos sobre delincuentes que residen en un país distinto del suyo y que se desplazan a España para llevar a cabo sus campañas criminales.

La investigación de este tipo de redes representa el paradigma de la necesidad de intervenir policialmente para desentrañar las actividades de concertación que los delincuentes necesitan establecer entre sí para cometer sus crímenes, esto es, conocer en profundidad cómo se producen sus comunicaciones internas y externas.

El elemento clave de la investigación, el que permitirá de una manera efectiva conocer la estructuración de la red, no es otro que la ITCE. Sin embargo, más que sus contenidos verbales o escritos, interesará obtener inteligencia oportuna mediante el análisis de los datos de tráfico, localización e identificación. De esta manera, conociendo cómo establecen las medidas de concertación y cómo estas se materializan desde los diversos terminales de comunicaciones electrónicas de que hagan uso, podrá la PJE establecer sus medidas de investigación y reacción.

Algunas de estas medidas irán directamente dirigidas a la actividad delictiva en sí, esto es, a anular la concreta maquinación criminal, reiterada o no, de la que se

[270] Puede decirse que se buscan "una inversión inicial" que les permita conseguir un trabajo en su país de origen.

sirvan para conseguir sus ilícitos objetivos. Otras, deberán tener su fundamento en el conocimiento de la misma estructura de la organización y de los apoyos externos que puedan recibir, incluido el plano legal, como, por ejemplo, la canalización o blanqueo de los capitales obtenidos, la receptación, los refugios, el transporte, la corrupción, el empleo de influencias, el uso del sistema económico-financiero, las falsedades de todo tipo, la colaboración con otras redes, etc.

Es evidente que, con la reforma operada en el Código Penal de diciembre de 2010, se exigirá de los investigadores un plus en la determinación de la condición de organización, de modo que el juzgador pueda valorar con la mayor exactitud la adecuación a las tipologías enunciadas en los arts. 570 bis, ter y quáter.

b) Bandas organizadas que generan una alarma social difusa

Junto a las peligrosísimas bandas de crimen organizado que se han presentado en el apartado anterior, podemos situar un segundo grupo cuyas actividades ilícitas son poco o nada conocidas por los ciudadanos. Se trata de una forma de delincuencia sorda, capaz de pervivir por más que se desmantelen algunas de sus menos conseguidas expresiones. De ahí el haber elegido, seguramente de forma poco académica, la expresión ***alarma social difusa*** porque, ciertamente, aunque su presencia se intuya, raramente preocupan a la opinión pública.

Bajo esta denominación hay que referirse a aquellas redes fuertemente estructuradas dentro de lo que se podría denominar, no sin cierta imprecisión, la ***delincuencia económica***, bajo dos grandes conceptos: la ***economía sumergida***[271] y la ***economía criminal***, entendida esta última como aquel conjunto de actividades, frecuentemente protagonizadas desde países con legislaciones permisivas, que desestabilizan los mercados alterando la libre competencia y poniendo en riesgo la

[271] Entendida en general como factor criminógeno o, en sí misma, cuando para actuar en el mercado ilícitamente sea además necesario cometer delitos de cualquier género.

salud pública, sirviendo como vector de crecimiento de cualquiera de las demás formas que presenta la DO.

En la superficie, el ciudadano, como mucho, llegará a percibir algún daño criminal que se le hará más o menos ajeno pero, las más de las veces, su actitud podrá llegar más allá de ser comprensiva para, incluso, ser tolerante o francamente entusiasta.

Como ejemplos, puede mencionarse las vulneraciones de los derechos de propiedad intelectual e industrial, las defraudaciones de todo tipo de impuestos, el contrabando, etc. Algunos ejemplos podrían ser los siguientes[272]:

- Defraudaciones del IVA asociadas a la comercialización de vehículos de lujo, material informático de alta demanda, soportes magnético-ópticos, etc.
- Defraudación de impuestos especiales, tales como los hidrocarburos, el alcohol[273] y el tabaco[274].
- Estafas de todo tipo, que llegan a afectar a la estabilidad económica de las personas y a la actividad empresarial.
- Vulneración de los derechos de propiedad intelectual e industrial, como faceta patrimonial en razón de los derechos económicos de los derechohabientes o como faceta socioeconómica en relación a su condición de motor del progreso.
- Vulneración de la normativa sobre consumo, tales como el tráfico y falsificación de medicamentos, adulteración o falsificación de alimentos, etc.
- Vulneración de la normativa de comercio exterior, tales como los regímenes económicos aduaneros, del sistema de preferencias generalizadas de la UE, etc.
- Fraudes a los intereses financieros de la Unión Europea mediante ataques a su presupuesto en su capítulo de ingresos (aranceles[275], IVA[276], IVA de

[272] No obstante, si nos atenemos a la lista cerrada incluida en la Ley Orgánica 5/1999, muchos delitos de los mencionados no merecerían la calificación de DO, como sería el caso del fraude fiscal.
[273] Recientemente, tras varios años de intensas investigaciones, se desarticuló por la UCO una complejísima red que desviaba alcohol absoluto (sujeto a elevados impuestos especiales) para la financiación del grupo terrorista IRA Auténtico (RIRA o *Real Irish Republican Army*).
[274] La complejidad de las redes de contrabando es tan excepcional como la pérdida de ingresos que ocasiona a las arcas públicas, así como los problemas de salud pública que pueden ocasionar.
[275] Mediante la comisión de cualquiera de los fenómenos relacionados con el contrabando.
[276] Pérdidas Fiscales que generan desestabilización de la libre competencia y de leal ocupación del mercado.

importación, etc.) o gastos (aplicaciones de la política agraria común, fondos estructurales, fondos sociales, etc.[277]).

- Extorsiones, corrupción, tráfico de influencias, etc.
- Delitos urbanísticos.
- Blanqueo de capitales[278] en todas sus formas.

Para el investigador no es difícil de adivinar detrás - pero prácticamente imposible de probar - la presencia de los grandes grupos delictivos internacionales como las mafias chinas, las mafias rusas, la Camorra, la N'Drangheta e, incluso, antiguos grupos terroristas[279], que se caracterizan por su presencia en el mercado y en la vida social enmascaradas tras la facilitación de servicios de alta demanda del ciudadano.

Para que esto sea así, el delincuente se cuidará de que su cara más amable no se relacione con sus intensas actividades de corrupción, amenazas, lesiones, asesinatos, drogas, blanqueo y un largo etcétera de actividades criminales. Es decir, que se tratará de una delincuencia que se mueve en el mercado y en la sociedad con naturalidad y que tiene recursos para que todo quede razonablemente opaco.

La faceta más peligrosa de estas redes, junto con la imprudente complacencia de algunos sectores sociales e incluso políticos, es su posibilidad de construir sólidas infraestructuras económicas permanentes dotadas de una solvente capacidad de resistir la acción de la Justicia en los países en los que impera el derecho y la libertad. La argamasa para conseguirlo, entre otras cosas, viene dada por las deficiencias de una legislación procesal y penal anticuada, con escasa capacidad resolutiva y enmarcada en un excesivo garantismo que en nada ayuda a la Justicia misma.

[277] Debilitación de amplios sectores económicos de exigente regulación frente a otros cuya actividad tiene origen en economías criminales, tales como la agricultura, sectores textil y del calzado, fondos para las infraestructuras, capacitación laboral, lucha contra el paro, mejora de la competitividad, etc.).
[278] Nótese las extremas dificultades para probar el blanqueo de capitales cuando el delincuente no es nacional y ha de recurrirse a países terceros para valorar el delito precedente, dada la falta de efectividad de la colaboración internacional o, más domésticamente, cuando el origen de los fondos esté en un complejo fraude fiscal sustentado en infraestructuras societarias dirigidas por testaferros.
[279] Las operaciones dirigidas a la desarticulación de estas formas de DO inexorablemente dañan a infraestructuras delictivas menores y aún perfectamente prescindibles para la propia organización criminal. Suena a inalcanzable el que el Estado de Derecho llegue a anular su capacidad criminal.

La política criminal, si alguna producción le puede ser reconocible en la sociedad española, es consecuencia de la observación de los fenómenos que se han agrupado bajo el epígrafe de "bandas organizadas que generan gran alarma social" y de la subsiguiente – y muchas veces tímida - reacción.

Roberto Saviano[280] a propósito de este concepto, llega a afirmar, con profusión de datos y experiencias, que las redes mafiosas de criminalidad económica no están formadas por delincuentes que cometen los tipos penales propios de esta especialidad criminológica sino, y he aquí lo sorprendente, empresarios que cometen delitos económicos. Un simple examen de esta afirmación permite colegir las dificultades de intervenir en un ámbito en el que no se respira criminalidad propiamente dicha, sino una potencialidad económica ilícita que perfunde y desdibuja el escenario donde se desarrolla con normalidad la vida económica de los demás ciudadanos.

Descrito así el concepto de alarma social difusa, su evidente y grave potencial lesivo para importantes bienes jurídicos de interés público y privado no tiene un contrapeso definible y unificado en cuanto a la respuesta penal, lo que permite colegir que sus posibilidades de supervivencia y crecimiento en el seno de la sociedad son tan altas como su posible y sórdida influencia en los poderes públicos.

c) La intervención de urgencia.

Existe una tercera categoría definida por aquellos delitos sobre los que ha de reaccionarse de una manera inmediata, bien porque se trata de emergencias de riesgo catastrófico (atentados terroristas, amenazas a estructuras críticas, ciberataques, etc.),

[280] Sobre su libro "Gomorra", el autor de este estudio, incrédulo sobre su contenido y sobre la certeza de que el escritor hubiera sido testigo de tan inquietantes hechos, tuvo la oportunidad de entrevistarse con el Fiscal Antimafia de Nápoles Sr. Falcone durante una reunión en sede de Eurojust sobre el tema del blanqueo de capitales en la Costa del Sol, quien le comentó que todo era cierto y resultado de un profundo estudio realizado por Saviano de los expedientes antimafia archivados en la Fiscalía. Vid. Saviano, Roberto. *Gomorra.* Barcelona: Debate. Random House Mondadori S.A., 2007. Sobre otro de los ya demasiados fenómenos mafiosos más inquietantes de la actualidad, a título meramente ilustrativo, vid. Forgione, Francesco. *'Ndrangheta. La mafia menos conocidad y más peligrosa del planeta.* Barcelona: Ediciones Destino S.A., 2009.

bien porque suponen una urgencia vital por estar amenazadas la libertad y la integridad de las personas (Inminencia de asesinato, secuestro *express*, desaparición de personas y, singularmente, de mujeres y menores, actuación de personas desequilibradas, etc.).

El derecho procesal tiene este problema insuficientemente resuelto. Cuando fueron estudiadas las formas actuales de materializar el mandato judicial para la limitación de los derechos fundamentales, se vio que su disponibilidad, sujeta a un protocolo discorde con las necesidades de actuar de forma inmediata, tomaba plazos de tiempo inasumibles. Tan inasumibles como pudiera serlo también el que dichas medidas se adoptasen fuera del principio de proporcionalidad y, en este caso, al margen de los requisitos extrínsecos de motivación y judicialidad.

Sin entrar por el momento en mayores profundidades, se ha de anotar que, por término medio, el tiempo de activación de las intervenciones telefónicas en un caso de secuestro o desaparición de personas viene a ser de unas cuatro horas. Este tiempo, dado el dinamismo con que actualmente actúan los delincuentes, supone perder un tiempo precioso para la feliz resolución del caso.

Se puede decir, en frase lapidaria, que lo que se hace durante la investigación en tiempo real de un secuestro o, en general, ante cualquier hecho delictivo en curso, no se atiene únicamente a satisfacer lo que en su día deberá representarse en el acto de juicio oral, sino que, más perentoriamente, deberá de protegerse eficazmente la vida, la libertad o cualquier otro bien jurídicamente protegido que tan injustamente haya sido puesto en peligro por los delincuentes, por lo que el derecho procesal deberá ofrecer las aceptables respuestas.

C. La respuesta a la delincuencia organizada y compleja

En capítulos anteriores se ha hablado de dos conceptos interesantes e íntimamente relacionados: el que se ha referido a una más que aparente ***anomia*** sobrevenida como consecuencia del desarrollo en un mundo globalizado de las tecnologías del conocimiento o, al menos, de las insuficiencias que se han vislumbrado para el efectivo imperio del Derecho en este ámbito; y, de otro lado, el de una de la formas con las que el Derecho, con discutible éxito, ha tratado de compensar o paliar este efecto: el ***Derecho Penal de Lucha*.**

Lo anterior representa una dinámica de acción-reacción de la que nace la inadecuación del derecho actual a los problemas que insistentemente se vienen describiendo y que se tratarán de explicar a través del inestable – y seguramente cuestionado - concepto actual de ***soberanía***, en su acepción primigenia de *autoridad suprema del poder público* – es decir, el ejercido por cada uno de los estados -, y en de ***soberanía nacional***, que es la *que reside en el pueblo y se ejerce por medio de sus órganos constitucionales representativos*[281].

Si el primero no siempre es ejercido en plenitud por ningún país[282], el segundo carece de virtualidad cuando su legítima acción no puede cumplirse en ocasiones por exceder al ámbito territorial donde esta se manifiesta. Pues bien, el efecto de las tecnologías del conocimiento y la globalización han desdibujado aún más estos conceptos y los han llenado de nuevos e inesperados matices, cuando no evidenciando importantes lagunas en su necesaria efectividad, una de cuyas expresiones más singulares no es otra que la de garantizar la seguridad de los ciudadanos y, como parte esencial de esta obligación, la de ejercer el legítimo poder coercitivo.

Algunos autores se han referido a este efecto como sugestivo del agotamiento del Estado con el consiguiente surgimiento de la necesidad de experimentar una adaptación si se desea continuar con la gestión de los asuntos públicos[283]. Las formulas

[281] Diccionario RAE.
[282] Así lo reconocen las Naciones Unidas: "Ningún Estado, por más poderoso que sea, puede hacerse invulnerable, por sí solo, a las amenazas actuales". Vid. *"Un mundo más seguro…op. cit.,* pág.11.
[283] Beltrán, Francisco y Molina, Ignacio. *Retos y transformaciones actuales del Estado.* Barcelona: Universitat Oberta de Catalunya, 2010.

de adaptación conducen a lo que ha denominado el ***vaciamiento del estado***, según dos direcciones distintas: Una a favor de entidades superiores o inferiores, llamado ***vaciamiento vertical***; y otro, que interesa ahora más, que es el que supone el cuestionamiento de la soberanía dentro del propio territorio, cuando esta se ve contestada por otras fuerzas y relaciones sociales, que se denomina ***vaciamiento horizontal***[284].

Evidentemente, de lo que se habla en realidad es de una ***cesión de soberanía***, bien por imperativo de necesidades insoslayables (Ej: Planeamiento de la defensa frente a un enemigo común a través de organizaciones supranacionales como la OTAN), bien por convenir a una mejor gestión de los asuntos públicos (Ej: Regulación económica a través del Banco Central Europeo).

Junto al concepto de vaciamiento, y como su primera consecuencia, se debe introducir también el de ***gobernanza*** por el que se entendería *"la renuncia al poder exclusivo en beneficio de los consensos con la ciudadanía y el mercado"*[285,286] y que será de gran trascendencia para comprender el alcance de los retos que tiene la sociedad actual.

Como premisa inicial, y desde un punto de vista estrictamente policial, la extensión de la acción criminal fuera de las fronteras de cualquiera de los estados legítimos conlleva inexorablemente la pérdida de la iniciativa, oportunidad y capacidad

[284] Este vaciamiento horizontal deviene espurio cuando se impone por la fuerza de los hechos por grupos de presión, de marcado carácter desestabilizador, como los fenómenos que han propiciado oscuras iniciativas de las redes sociales como *Anonymous* (http://anonymousespaña.es/), *Lulzsec* (http://twitter.com/#!/lulzsec) o *Wikileaks* (http://wikileaks.org/), que sin duda pretenden condicionar la acción de los gobiernos excediendo a cualquier consenso democrático que pueda producirse en el seno de la sociedad por el efecto de vaciamiento que se ha comentado. *Anonymous* o *Lulzsec* se expresan normalmente mediante ataques de denegación de servicio para exhibir su poder (DoS), lo que distingue el ***hacktivismo***, de naturaleza delictiva y muy agresiva (sin duda con derivación a la DO), del ciberactivismo, dentro absolutamente de los deseables cánones de participación ciudadana democrática en la gobernanza de los estados de derecho.

[285] Scharpf, Fritz W. *Apuntes para una teoría del gobierno multinivel de Europa*. [aut. libro] Agustí Cerrillo i Martínez (Coordinador). *La gobernanza hoy: 10 textos de referencia*: Instituto Internacional del Governabilitat de Catalunya. Estudios Goberna. Ministerio de Administraciones Públicas, 2005, págs. 173-202.

[286] Un ejemplos lo constituyen la llamada del Ministerio de Industria, Energía y Comercio para la participación ciudadana a través de un foro digital, que puede verse en la *web* http://www.agendadigital.gob.es/, en el que se realiza una *"Consulta pública sobre la propuesta de Agenda Digital para España"*. Vid. *Propuesta de Agenda Digital para España;* o la consulta a los ciudadanos hecha por la Comisión Europea a través de la *web* http://ec.europa.eu/justice/opinion/your-rights-your-future/index_en.htm.

de acción investigativa frente a la delincuencia, todo ello pese a los meritorios esfuerzos de la comunidad internacional en materia de cooperación policial y judicial para minorar este efecto. Todo ello representa una sólida posibilidad de éxito para cualquier delincuente que platee sus crímenes en la escena internacional.

Todos estos conceptos ayudan a introducir y situar las aportaciones que a continuación se incluyen, al entrar con alguna profundidad en cómo se ha organizado la comunidad internacional para afrontar los retos planteados. Interesa más ahora analizar los instrumentos jurídicos y de todo tipo establecidos para afrontar la lucha contra una delincuencia transnacional ayudada por la globalización y las tecnologías del conocimiento, tratando de predecir sus tendencias evolutivas y, algo menos, su enfoque genérico sobre el fenómeno de la DO, ya suficientemente tratado por diversos autores. Particularmente, conviene penetrar con mayor detenimiento en aspectos esenciales relativos al intercambio de inteligencia en la escena internacional y en su efectividad para aportar al proceso penal pruebas válidas que corrijan la presumiblemente alta cifra oscura que ha ocasionado la delincuencia compleja.

1. Las Naciones Unidas

Al final de la Segunda Guerra Mundial, la comunidad internacional, horrorizada por la dimensión que habían adquirido los conflictos humanos de la primera mitad del Siglo XX y pretendiendo resolver en común los futuros problemas de seguridad que sin duda excederían por completo a las capacidades de acción de cada uno de estados considerados individualmente, sentaron en el art. 1.1 de la ***Carta de las Naciones Unidas***, de 26 de junio de 1945, la necesidad de conseguir, por imperativo de la concordia entre las naciones, que nada llegase en el futuro a quebrantar la paz y la seguridad internacionales.

Desde aquel momento, estos dos conceptos básicos han evolucionado mucho en su naturaleza. Si en 1945 se pensó en la guerra clásica como el mayor problema a resolver, hoy en día, sin abandonar este concernimiento, se extiende de forma preocupante a la prevención y anulación de cualquier problema seguridad que pueda

llegar a afectar o condicionar la estabilidad de la comunidad internacional, sin que ningún estado pueda considerarse ajeno a unas amenazas de carácter global[287].

Si en aquella época el fenómeno de la delincuencia tenía un carácter perfectamente descriptible y un ámbito de incidencia local o, como mucho, regional, es evidente que, a día de hoy, el problema ha trascendido también a las fronteras de los estados deviniendo un problema transnacional de emergente y compleja solución.

Por ello, años después de la promulgación de la Carta, el entonces Secretario General de las Naciones Unidas KOFI A. ANNAN, con ocasión de la que se denominó la ***Convención de Palermo de 2000***, preocupado por la evolución de la DO transnacional, sostuvo que *"los mismos medios tecnológicos que fomentan la mundialización y la expansión transnacional de la sociedad civil también proporcionan la infraestructura para ampliar las redes mundiales de la sociedad "incivil", vale decir, la delincuencia organizada, el tráfico de drogas, el lavado de dinero y el terrorismo."*

Posteriormente, en el prefacio de la ***Convención de las Naciones Unidas contra la delincuencia organizada transnacional y sus protocolos***, de 11 de noviembre de 2004, o ***Convención de Nueva York***, manifestó que "l*os grupos delictivos no han perdido el tiempo en sacar partido de la economía mundializada actual y de la tecnología sofisticada que la acompaña. En cambio, nuestros esfuerzos por combatirlos han sido hasta ahora muy fragmentarios y nuestras armas casi obsoletas"*, adhiriéndose así al sinnúmero de personas que apuntan estos efectos indeseables asociados a uno los avances más revolucionarios de la historia de la humanidad.

Este organismo internacional ofrece su enfoque genérico de los retos planteados por la criminalidad a través de la Oficina de Drogas y Crimen[288] y adoptó su

[287] Así se reconoce repetidamente en el documento de las Naciones *Unidas "Un mundo más seguro…doc. cit.*, pág. 16 (por todas). Nótese, por otro lado, que ya no se trata de la agresión de un Estado a otro o, ni siquiera, de un conflicto interno de un Estado que le cause inseguridad a él mismo o a la comunidad internacional, sino de una amenaza difusa de imposible catalogación o sistematización como lo sería la DO transnacional o el terrorismo.

[288] Vid. http://www.unodc.org/unodc/index.html. Las declaraciones de la Asamblea General de las Naciones Unidas de Viena, de 4 de diciembre de 2000, y de Bangkok, de 24 de abril de 2005, son significativas al respecto. En esta última se afirma además en su punto 16 que *"observamos que, en esta era de la globalización, la tecnología de la información y el rápido desarrollo de nuevos sistemas de telecomunicaciones y redes informáticas se han visto acompañados del uso indebido de esas tecnologías con fines delictivos. Por consiguiente, acogemos con beneplácito los esfuerzos por aumentar y complementar la cooperación existente para prevenir, investigar y juzgar los delitos informáticos y de*

principal instrumento jurídico tras los mencionados acuerdos de Palermo, esto es, mediante la ***Convención de las Naciones Unidas contra la delincuencia organizada Transnacional***, de 15 de noviembre de 2000[289]. El documento contiene en su art. 1 un llamamiento a la cooperación internacional para afrontar la lucha contra la DO trasnacional[290,291], tarea para la que propugna un compromiso de cooperación judicial internacional recíproca en su art. 18[292], que se configura como uno de los elementos claves para garantizar que la Justicia alcance más allá de las limitaciones de la acción soberana de los estados.

Sin embargo, las medidas establecidas en el convenio quedarían reservadas a la comisión de delitos graves, entendiéndose por tales, de acuerdo con el art. 2b, *"las conductas que constituyan un delito punible con una privación de libertad máxima de al menos cuatro años o con una pena más grave"*, lo que, a mi juicio, constituye una constricción inapropiada, establecida mediante un inoportuno límite objetivo que condicionará, sin duda, los avances del régimen jurídico en materia de aplicación de medidas adecuadas para contrarrestar la delincuencia compleja. Las opciones

---

alta tecnología, incluso desarrollando la asociación con el sector privado". En la Declaración de Salvador, de 19 de abril de 2010, se reiteran todas las prevenciones incluidas en este texto (Ver los pfos. 39, 41 y 42).

[289] Este convenio fue adoptado por la Unión Europea mediante la Decisión del Consejo de 29 de abril de 2004, relativa a la celebración, en nombre de la Comunidad Europea, de la Convención de las Naciones Unidas contra la DO Transnacional (2004/579/CE).

[290] Según el art. 3.2: *"A los efectos del párrafo 1 del presente artículo, el delito será de carácter transnacional si:*

a) Se comete en más de un Estado;
b) Se comete dentro de un solo Estado pero una parte sustancial de su preparación, planificación, dirección o control se realiza en otro Estado;
c) Se comete dentro de un solo Estado pero entraña la participación de un grupo delictivo organizado que realiza actividades delictivas en más de un Estado; o
d) *Se comete en un solo Estado pero tiene efectos sustanciales en otro Estado".*

[291] En el documento de las Naciones *Unidas "Un mundo más seguro…doc. cit.*, pág. 20, se añade un complemento a la definición al decir *que "cualquier suceso o proceso que cause muertes en gran escala o una reducción masiva en las oportunidades de vida y que socave el papel del Estado como unidad básica del sistema internacional constituye una amenaza a la seguridad internacional".*

[292] *Asistencia judicial recíproca:*

1. Los Estados Parte se prestarán la más amplia asistencia judicial recíproca respecto de investigaciones, procesos y actuaciones judiciales…delito…carácter transnacional.

29. El Estado Parte requerido:

a) Facilitará al Estado Parte requirente una copia de los documentos oficiales y otros documentos o datos que obren en su poder y a los que, conforme a su derecho interno, tenga acceso el público en general;

b) Podrá, a su arbitrio y con sujeción a las condiciones que juzgue apropiadas, proporcionar al Estado Parte requirente una copia total o parcial de los documentos oficiales o de otros documentos o datos que obren en su poder y que, conforme a su derecho interno, no estén al alcance del público en general.

alternativas basadas en la trascendencia social de los hechos o en la interpretación semántica del término "grave" que les pueda acompañar, parecen más adecuadas para lograr la adaptación de la Ley a la necesidad evidente de que el Derecho Penal llegue a intervenir en muchas de las tipologías criminales actuales[293].

Es de hacer notar también, como importantes puntos de interés, que se pone el acento en las cuestiones de participación en un grupo delictivo (art. 5) y se acompaña de un énfasis en materias de tanta trascendencia para adquirir un correcto enfoque paliativo del fenómeno como lo sería el necesario tratamiento del blanqueo de capitales (arts. 6 y 7), como elemento indispensable de la cultura de supresión de la prueba[294], y de la corrupción (arts. 8 y 9)[295], así como extender la responsabilidad penal y civil a las personas jurídicas (art. 10).

En lo que se refiere a la habilitación de reglas para el ejercicio de la actividad de investigación, el convenio se centra especialmente en materias de extremo interés como lo son la posibilidad de realizar investigaciones conjuntas (art. 9) y, particularmente, de manifestar la incuestionable necesidad de compartir ágilmente información en la escena internacional (art. 27.1a), recurriendo a la moderna tecnología (art. 27.3) e, incluso, realizando amplios estudios sobre su naturaleza y prospectiva.

El art. 29.1 incluye interesantes medidas en lo que se refiere a la implicación del estamento judicial y a la utilización de los recursos de la tecnología para combatir la DO trasnacional y, de forma expresa, lo referente al ámbito de la tecnovigilancia y la vigilancia de las telecomunicaciones.

De forma literal, por su interés, se extrae lo siguiente:

---

[293] La cuestión en favor de la flexibilidad conceptual sobre la gravedad para que alcance las *"formas nuevas y futuras de la delincuencia"* se aborda en el documento Conferencia de las Partes en la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional. *"Actividades de la Oficina de las Naciones Unidas contra la Droga y el Delito para hacer frente a las formas nuevas de delincuencia"*. (CTOC/COP/2010/3), pág. 3.

[294] Naturalmente, en la misma convención se recogen disposiciones para lograr recorrer el camino contrario al que siguieron los delincuentes, mediante las medidas de ámbito internacional para conseguir la localización, congelación y restitución de activos ilícitamente obtenidos.

[295] Posteriormente, con fecha de 31 de octubre de 2003, se promulgaría el ***Convenio de Naciones Unidas contra la Corrupción***. El fenómeno de la corrupción es, sin duda, uno de los mayores vectores de crecimiento de la DO. Tanto que su diseminación puede poner en cuestión la estabilidad y viabilidad de los estados.

Art. 29.1. Cada Estado Parte, en la medida necesaria, formulará, desarrollará o perfeccionará programas de capacitación específicamente concebidos para el personal de sus servicios encargados de hacer cumplir la ley, incluidos Fiscales, Jueces de instrucción y personal de aduanas, así como para el personal de otra índole encargado de la prevención, la detección y el control de los delitos comprendidos en la presente Convención. Esos programas podrán incluir adscripciones e intercambios de personal. En particular y en la medida en que lo permita el derecho interno, guardarán relación con:

…

g) El equipo y las técnicas modernos utilizados para hacer cumplir la ley, incluidas la vigilancia electrónica, la entrega vigilada y las operaciones encubiertas;

h) Los métodos utilizados para combatir la delincuencia organizada transnacional mediante computadoras, redes de telecomunicaciones u otras formas de la tecnología moderna;

Se hace evidente, por tanto, la decidida apuesta de la comunidad internacional por incorporar al Derecho Penal el uso de las herramientas tecnológicas que son, por su parte, normalmente utilizadas por el común de los ciudadanos en su vida diaria y malempleadas en la misma medida por los delincuentes para cometer sus crímenes. A este respecto, las Naciones Unidas afirmaron que:

"La revolución tecnológica, que ha cambiado radicalmente el mundo de las comunicaciones, el procesamiento de información, la salud y el transporte, ha borrado fronteras, modificado las corrientes migratorias y permitido que la información se comparta en todo el mundo con una rapidez inconcebible hace dos decenios. Esos cambios han surtido numerosos beneficios, pero también han hecho posible causar grandes daños. Un número cada vez menor de personas puede causar daños cada vez mayores, sin el apoyo de ningún Estado. Una nueva amenaza, la delincuencia organizada transnacional, socava el imperio de la ley a nivel nacional e internacional. Las tecnologías de la vida cotidiana pueden transformarse en instrumentos de agresión. No hemos comprendido aún la totalidad de los efectos de esos cambios, que anuncian, sin

embargo, un clima fundamentalmente diferente en materia de seguridad, con oportunidades sin precedentes de cooperación y con posibilidades nunca vistas de destrucción[296]*."*

Este es un mensaje cuasi apocalíptico que, en efecto, aparece reiteradamente en los documentos estudiados y, especialmente, en el que es objeto de análisis en este momento, como se puede comprobar, por ejemplo, tras la lectura del pfo. 18 (efectos secundarios devastadores sobre la economía mundial y las secuelas de pobreza generados por los ataques del 11 de septiembre de 2001 en EEUU) o del pfo. 23 (debilitamiento del Estado y los sistemas democráticos, favorecimiento de los conflictos civiles, etc.), hasta llegar a un acertado pronunciamiento sobre los obstáculos que a juicio del alto organismo internacional han impedido la adopción de medidas eficaces contra la DO transnacional y que serían, según el pfo. 167, *"…una cooperación insuficiente entre los Estados, la falta de coordinación entre los organismos internacionales y un incumplimiento inadecuado por parte de muchos Estados",* las razones contenidas en el pfo. 170 sobre el desfase entre la acción penal legítima y la capacidad de acción de la delincuencia *("La agilidad con que operan esas redes contrasta marcadamente con el laborioso intercambio de información*[297] *y la inadecuada cooperación entre los Estados en materia de investigaciones y enjuiciamientos penales")* o la existencia de fronteras para la cooperación jurídica, según el pfo. 173.

Naturalmente, por efecto de la quiebra actual del concepto de soberanía asociado a la globalización y las tecnologías del conocimiento que parece regir este evidente desfase, lo anteriormente afirmado por las Naciones Unidas es determinante para comprender por qué al exceder las acciones investigativas a los límites fronterizos de los estados actuales, se pierde prácticamente por completo la posibilidad de aplicar medidas dotadas del suficiente dinamismo y capacidad de acción que lleguen a ser

[296] Vid. Documento ONU *"Un mundo más seguro: la responsabilidad que compartimos". Documento del Quincuagésimo noveno período de sesiones. Tema 55 del programa. Seguimiento de los resultados de la Cumbre del Milenio. A/59/565.* Pfo. 16.

[297] En el caso de España, el "laborioso intercambio de información" se debe a la rémora del injustificado hipergarantismo. No se puede – y perdónese el casticismo – soplar y sorber al mismo tiempo. Si hay que ponerse a la altura del factor tecnológico y contrarrestar la parte negativa de la globalización, habrá que arbitrar medidas audaces para conseguir que el Estado de Derecho ejerza su legítimo derecho a la coerción en forma acorde con los tiempos, sin desmerecer con ello ninguno de los logros democráticos conseguidos.

equiparables a las que, incomprensiblemente, sí pueden utilizar los delincuentes en su favor[298].

Por ello, las Naciones Unidas hacen referencias expresas a propuestas provenientes del mundo académico[299], que van dirigidas a conseguir una evolución en el derecho procesal. Entre estas, pueden mencionarse los trabajos de SCHJØLBERG y GHERNAOUTI-HÉLIE bajo el sugerente título de *"A Global Protocol on Cybersecurity and Cybercrime"*[300], donde se propugnan medidas entre las que se destaca como referente legislativo internacional del ***Convenio sobre Cibercrimen del Consejo de Europa de 2001***[301], se identifican problemas tales como la posibilidad de acceder a la intervención de la *VoIP*[302] o la volatilidad de los DACE y su dificultad de aprehensión para ser usados en el proceso penal.

En este último sentido, GHERNAOUTHI-HÉLIE encuentra dificultades en determinar qué datos son relevantes para la investigación, cómo hacerles un seguimiento, cómo almacenarlos, cómo recuperarlos cuando han sido borrados, cómo probar cuál es el origen del mensaje, cómo relacionar la prueba digital con la persona responsable de los hechos delictivos, cómo custodiar la prueba digital para presentarla ante el juzgado[303], etc.

Estas incertidumbres ofrecen una genuina representación sobre cuáles son los problemas a los que se enfrenta el proceso penal actual motivados por la evolución de

[298] Sobre este efecto, y por si fuera poca la insistencia, las Naciones Unidas constatan *"…la falta de preparación de los organismos encargados de hacer cumplir la ley y el poder judicial estaban mal preparados y carecían de la capacidad necesaria para hacer frente a la evolución del delito cibernético y para reunir y utilizar pruebas obtenidas mediante tecnologías cibernéticas en la preparación de los procesos"* y la necesidad de operar adaptaciones en el derecho sustantivo y, especialmente, en el procesal, *"ya que La interceptación de las comunicaciones que utilizan la tecnología VoIP, la admisibilidad de las pruebas digitales en las causas penales, los procedimientos para investigar los casos en que se ha utilizado tecnología de cifrado o los medios de comunicación anónima son problemas que pese a ser urgentes, no se están abordando a nivel regional y solo en algunos casos se están tratando a nivel nacional"*, del Vid. *"Novedades recientes en el uso de la ciencia y la tecnología…op. cit.,* pfos. 37 y 39.

[299] Vid. *"Novedades recientes en el uso de la ciencia y la tecnología…op. cit.,* pfos. 37.

[300] Vid. Schjølberg, Stein y Ghernaouti-Hélie, Solange. *A Global Protocol on Cybersecurity and Cybercrime. An initiative for peace and security in cyberespace.* Oslo: E-dit, 2009.

[301] Por todos, en el art. 1 del subdocumento *"draft code on peace and security in cyberspace - a global protocol on cybersecurity and cybercrime",* contenido en el documento mencionado.

[302] En el art. 2 del *"draft code on peace…"* se afirma que la *"Voice over Internet Protocols (VoIP) and other new technologies may be a challenge for law enforcement in the future. It is important that law enforcement, government, the VoIP industry and ICT community consider ways to work together to ensure that law enforcement has the tools it needs to protect the public from criminal activity".*

[303] Lo que sería en la terminología el uso *"la conservación de la cadena de custodia de la prueba".*

las TIC y que son planteados diariamente por la PJE ante las autoridades judiciales para poder acceder a la prueba electrónica con eficiencia y plena sujeción a las garantías constitucionales más exigentes.

En el art. 15.2 del subdocumento "*A model law on cybercrime legislation"* se menciona la necesidad a estos efectos de establecer precisas salvaguardas, haciéndolas residir en el ámbito judicial o *"…en otra [autoridad] de supervisión independiente".* En el art. 20 se incluye una fórmula abierta para la captación en tiempo real de datos relacionados con las comunicaciones electrónicas o disponer su conservación porque sobre cualquier transacción electrónica se yuxtapone una comunicación de la misma naturaleza protegida por el derecho al secreto[304].

Como comentario a las meritorias propuestas contenidas en el protocolo mencionado en los párrafos precedentes, se ha de hacer notar que todo lo referido al intercambio de datos para la investigación en materia de cibercrimen, dada la evolución que se apuntó en el capítulo primero de este estudio, por la que se apreció una derivación del soporte de las comunicaciones electrónicas desde las operadoras de telefonía hacia el *Protocolo TCP/IP* (*VoIP*, fundamentalmente), se ha de referir necesariamente a datos asociados a comunicaciones amparadas por el secreto, según los diversos tratados internacionales y, consecuentemente, por su especialísima y estricta protección jurídica, de difícil encaje en la realidad jurídica de los estados de derecho donde han de causar efecto.

En los párrafos precedentes se ha tratado de explicar la posición de las Naciones Unidas sobre la imperiosa necesidad de evolucionar en el tratamiento de la DO como consecuencia de las nuevas posibilidades asociadas a la irrupción de la sociedad del conocimiento, es decir, que lo que se ha descrito no es sino únicamente el efecto potenciador o facilitador que ha tenido sobre aquella[305].

---

[304] Vid. González-Cuéllar Serrano, Nicolás. *Garantías constitucionales de la persecución penal en el entorno digital.* Prueba y proceso penal. ISBN 978-84-987-6007-1. Valencia: Tirant lo Blanch, 2008, pág. 168.

[305] Una clasificación distingue en *"dos categorías principales de actuación de los grupos delictivos: la utilización de la tecnología de la información por los grupos delictivos organizados tradicionales, y la comisión de delitos cibernéticos por grupos delictivos organizados"*. Vid. Choo, Kim-Kwang Raymond. *Organised crime groups in cyberspace: a typology*. Trends in Organized crime, Vol. 11, págs. 270-295, 2008, citado en *"Novedades recientes en el uso de la ciencia y la tecnología…op. cit.,* pfo. 27.

Pero esto no es todo respecto de su interés, puesto que las Naciones Unidas hacen suyos, junto a todo lo anterior, algunos aspectos inquietantes de la evolución del panorama criminal que evocan el concepto de delincuencia compleja en relación con el aprovechamiento de posibilidades criminales tecnológicas inéditas tan sólo hace unos años y que hacen extender la atención de la comunidad internacional hacia efectos ciertamente singulares[306].

El principal de estos sería el de la accesibilidad a lo criminal, entendida esta posibilidad como aquella que ha propiciado que, con grandes dosis de impunidad o anonimato, cualquiera pueda cometer un hecho criminal sin ni siquiera salir de su domicilio, con conocimientos técnicos mínimos o aprovechando cualquier espacio público para delinquir a través de la red[307].

Pero seguirían otros efectos desconcertantes, algunos ya citados a lo largo de este documento, como podría ser la migración de las comunicaciones electrónicas hacia la *VoIP*, es decir, fuera de la prestación de este tipo de servicios por las operadoras clásicas de telefonía, regidas mediante la LGT, en beneficio de las que ofrecen los prestadores de servicios de la sociedad de la información a través del *Protocolo TCP/IP* y, consecuentemente, dentro de la LSSI, con un marco jurídico-procesal sensiblemente diferente a las primeras a los efectos que interesan a este trabajo; el almacenamiento de archivos informáticos en ***cloud computing o nube***[308],

---

[306] Las Naciones Unidas, en referencia a la aplicación del Convenio de Ciberdelincuencia, dicen que *"en lo que respecta a la aplicación de la Convención contra la DO, deben tenerse en cuenta las siguientes características especiales de los grupos organizados que cometen delitos cibernéticos:*

a) Los grupos dedicados al delito cibernético suelen tener una estructura más flexible y abierta, que permite la incorporación de nuevos miembros por un período de tiempo limitado;

b) Los grupos que cometen delitos cibernéticos son con frecuencia mucho más pequeños que los grupos delictivos organizados tradicionales;

c) En muchos casos, los miembros de los grupos comunican entre sí exclusivamente en forma electrónica, sin tener nunca encuentros personales".

Vid. Pfo. a) en Choo, Kim-Kwang Raymond. *Organised crime groups…op. cit., p*ágs. 270-295; y, pfo. b), en Brenner, Susan W. *Organized crime? How cybercrime may affect the structure of criminal relationships.* North Carolina Journal of Law and Technology. 2002, pág. 27, ambos citados en *"Novedades recientes en el uso de la ciencia y la tecnología…op. cit.,* pfo. 29.

[307] Sería impensable que un ciudadano normalmente socializado, por ejemplo, allanase un domicilio para robar con fuerza unas películas de cine. Sin embargo, actualmente, los internautas se descargan millones de archivos sujetos a derechos de propiedad intelectual sin hacerse el menor reproche moral. O, sin siquiera ser consciente de ello, "sumar" la potencia computacional de su ordenador a otros miles o millones que hacen la función de una *botnet* para acabar con la prestación de un servicio público mediante un ciberataque de denegación de servicio.

[308] *Ibídem.*

nombre de resonancias límbicas al que difícilmente se le puede atribuir un espacio físico concreto o una jurisdicción a la que recurrir si legítimamente se ha de investigar en sus contenidos y atribuirlos a un determinado actor procesal[309,310]; la no presencia del autor en el lugar de los hechos, lo que incluye además la interposición de refugios seguros para las transacciones telemáticas[311]; el carácter instantáneo de las comunicaciones electrónicas de finalidad delictiva frente a las complejas maquinaciones en otro tipo de ámbitos clásicos, como en el narcotráfico, con grandes movimientos logísticos maliciosos para colocarlas en el mercado[312], etc.

Todo lo anterior merece una reflexión más profunda sobre la exactitud y validez de la categorización asumida por las Naciones Unidas, ya que la extensión del problema no se reduce, ni mucho menos, a considerar su afectación a la DO por alto que sea su alto nivel de tecnificación, sino a todo un nuevo universo de interacciones ilícitas de unos individuos frente a otros aprovechando las novedosas características

[309] Vid. *"Novedades recientes en el uso de la ciencia y la tecnología…op. cit.,* pfo. 5.

[310] El documento de la UE "*Combatiendo el cibercrimen y protegiendo la privacidad en la nube",* de octubre de 2012, elaborado por el Departamento de Derechos de los Ciudadanos y Asuntos Constitucionales (Dirección General de Política Interior), contiene una detallada descripción del grado de desconcierto que existe en la UE sobre la amenaza criminal que la nube pueda significar para los derechos de los ciudadanos, junto con la constatación del desbordamiento de la legislación para afrontarla. Junto con el reconocimiento de la inoperancia de la UE, con grave preocupación, los autores del documento no olvidan señalar los inenarrables "peligros" que puedan provenir de la intervención las FFSS: *"La falta de precisión jurídica alrededor del concepto de cibercrimen y el marco legal de las investigaciones basadas en la nube, así como las inadecuadas herramientas para salvaguardar la privacidad y la protección de los datos incrementan el potencial de malos usos y abusos de los agentes de la Ley y las agencias de policía. Los datos de los ciudadanos no están suficientemente protegidos al respecto. Este aspecto queda resaltado por las excepcionales medidas adoptadas en nombre de la seguridad y de la lucha contra el terrorismo. Lo sucedido en los Estados Unidos es particularmente significativo, tanto en lo referido a la Patriot Act, como en el caso de la US Foreign Intelligence Surveillance Amendment Act (FISAA) de 2008. En este caso, la cuestión del marco legal de procesado y transferencia de datos a terceros países es especialmente relevante"*.

[311] Nótese que el empleo "refugio seguro", que procedería de la traducción del *haven* inglés, y que en español se suele traducir impropiamente como "paraíso", trae reminiscencias de otro tipo de paraísos: los Fiscales. Es poco alentador observar que, si la comunidad ha fracasado estrepitosamente frente a estos – que tratan flujos económicos mensurables (tangibles) -, qué no sucederá con los informáticos, intangibles. Sobre esto, tanto la Asamblea General, en su resolución 55/63, como el Grupo de los Ocho, en los principios y el plan de acción para combatir la delincuencia de alta tecnología aprobados en la Reunión de Ministros de Justicia y del Interior del Grupo de los Ocho, celebrada en Washington, D.C., el 10 de diciembre de 1997, destacaron la necesidad de eliminar los refugios informáticos. Vid. "*Novedades recientes en el uso de la ciencia y la tecnología…op. cit.,* pfo. 15 y *Meeting of Justice and Interior Ministers of The Eight.* December 9-10, 1997. Communiqué. Washington, D.C.

[312] Un ejemplo sería el robo y difusión de información secreta por la red *Wikileaks*. Un grupo limitado de personas fue capaz de robar miles de copias de documentos secretos de los estados y darles una difusión mundial prácticamente instantánea a través de Internet, cuestionando el rol de los gobiernos. Para hacer esto tanto sólo hace unos hubiera sido necesario la penetración ilegal en decenas o centenares de archivos secretos y el robo o fotografiado de documentos, uno a uno.

del medio empleado para la expresión de su voluntad criminal y que carecerían de un encaje en clasificaciones criminales precedentes, evidenciando con ello la necesidad de una reacción de los poderes públicos a la altura de la perentoriedad impuesta por semejante situación, de la que no es ajena las posibilidades de supresión - también instantánea - de la prueba[313] y, obviamente, la necesidad de implicar a los proveedores de servicios de Internet (ISP) y al conjunto del sector privado[314], así como conseguir la concienciación social para lograr un correcta percepción de estos hechos en intrínseca naturaleza perturbadora.

Consecuentemente, y excepto en lo que se refiere a la necesidad de reaccionar, no puedo estar del todo de acuerdo con la clasificación de CHOO y BRENNER, porque con semejante descripción no podrían aplicarse las normas que establecen la consideración de grupo criminal a efectos jurídico-penales a fenómenos como *Anonymous*[315], *Lulzsec* o *Wikileaks* o, más domésticamente, a cualquiera de las vulneraciones menores que sólo son posibles gracias a las TIC y que merecen la oposición de mejores medidas de investigación procesal para tratarlas.

En el abordaje de todo ello las Naciones Unidas ven la quiebra de los instrumentos clásicos de investigación que fueron admitidos sin mayores problemas como válidos en el derecho procesal para obtener pruebas y la necesidad de que esta rama del Derecho evolucione sin perder los principios jurídicos que la animaron.

---

[313] *"La cooperación tempestiva y eficaz entre las autoridades de diferentes países es fundamental también porque en los casos de delitos cibernéticos las pruebas suelen suprimirse automáticamente y al cabo de poco tiempo. Los procedimientos oficiales prolongados pueden obstaculizar seriamente las investigaciones…Por consiguiente, el establecimiento de procedimientos para responder rápidamente a los incidentes y a las solicitudes de cooperación internacional se considera de importancia vital".* Vid. "*Novedades recientes en el uso de la ciencia y la tecnología…op. cit.,* pfos. 12 y 13.

[314] Vid. "*Novedades recientes en el uso de la ciencia y la tecnología…op. cit.,* pfos. 25 y 47.

[315] Para el Centro de Análisis y Prospectiva de la Guardia Civil, *"la amenaza además es asimétrica, no importa si se elimina una cabeza, hay más o surgen nuevas. Además su estilo es de guerrilla, mientras no pierdan van ganando. Es el conocido y estudiado fenómeno de guerra en red"* (Comentario a propósito de la presunta desarticulación de la "cúpula" de *Anonymous* en España el 10 de junio de 2011 en la Nota de Actualidad del CAP núm. 2). La anomia de Internet ha sido resuelta por estos flamantes grupos cibernéticos con la complicidad de sectores sociales poco advertidos de su peligro, convertidos por la debilidad de los sistemas políticos actuales en auténticos gendarmes de una ortodoxia que quieren imponer, no ya en la red, sino en la misma vida política y social de los ciudadanos en nombre de no se sabe bien qué superior posición moral, con que sin duda pretenden controlar o, al menos, condicionar la vida pública de las naciones.

Conceptos como la ***guerra cibernética***[316] asociados a la dependencia de la sociedad moderna de las TIC[317], exigen examinar el problema con ópticas más precisas.

Se puede decir que, en la percepción de cuáles son o pueden llegar a ser las amenazas que gravitan sobre la comunidad internacional, las Naciones Unidas operan una evolución conceptual en sus planteamiento que, quizá con más propiedad, se debiera denominar con el término de "*revolución conceptual*", pero de la cual se desconocen por completo sus exactos términos, pues parece que de esto se trata, al menos, cuando se constata una suerte de indefensión frente a sus facetas negativas que ni encuentra una definición precisa ni una aproximación jurídica sobre las que trabajar con buen pronóstico.

2. El Consejo de Europa

El instrumento jurídico esencial del Consejo de Europa es el ***Convenio sobre la Ciberdelincuencia***[318] (en adelante CCib), hecho en Budapest el 23 de noviembre de 2001 (ratificado por España el 20 de mayo de 2010). En lo que interesa a este estudio, el preámbulo fija su objeto *en "dotar de mayor eficacia las investigaciones y los procedimientos penales relativos a los delitos relacionados con los sistemas y datos informáticos, así como facilitar la obtención de pruebas electrónicas de los delitos"*, algo que difícilmente se consigue sin contar con una legislación procesal adecuada y con una Policía Judicial legalmente habilitada al efecto.

[316] Vid. *"El ciberdelito: guía…", op. cit.,* pág. 63.
[317] Vid. *"El ciberdelito: guía…", op. cit.,* pág. 70.
[318] Este convenio es una referencia para los posteriores desarrollos de la comunidad internacional como lo son los mencionados en el documento de la UIT sobre el que venimos trabajando. En los artículos 2 al 13, el Convenio de Ciberdelincuencia ya adelantó sus propias tipologías en materia de derecho penal sustantivo, y entre los arts. 14 y 22, las de Derecho Procesal. No obstante, y en referencia a este último aspecto, ha de anotarse que las utilísimas medidas de cooperación internacional que propician la rápida y efectiva congelación, conservación y cesión de datos informáticos lo son en tiempo real, es decir, a partir desde el momento en que gana eficiencia técnica una petición formal acogida al convenio, no imponiendo obligaciones respecto de la conservación de datos en la forma que exigen las directivas de UE que motivaron la transposición de la LCDCE, por lo que su capacidad real para la investigación de hechos ya pasados es prácticamente nula, por no haber impuesto similares obligaciones de conservación.

En este sentido, en el art. 16.1 se dice que *"cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para permitir a sus autoridades competentes ordenar o imponer de otra manera la conservación rápida de determinados datos electrónicos, incluidos los datos sobre el tráfico, almacenados por medio de un sistema informático"*, lo que aporta una definición bastante amplia o indeterminada del concepto *"dato electrónico*" como para salvar cualquier deficiencia de técnica legislativa que suponga una restricción injustificada de las categorías de datos a incluir en el texto de la Ley.

Otra de las importantes resoluciones es la contenida en el ***Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal*** (número 108 del consejo de Europa), hecho en Estrasburgo el 28 de enero de 1981, donde en su art. 9 se prevé la legal cesión de datos para la salvaguarda de los derechos de los ciudadanos puestos en peligro si tal cesión constituye *"…una medida necesaria en una sociedad democrática".* Sobre esta expresión, que sin duda contiene también un concepto jurídico indeterminado, gravita buena parte de la discusión que debe mantenerse sobre el principio de proporcionalidad cuando se ha de aplicar a las nuevas situaciones generadas por la evolución de las TIC. Por ello, el examen del término "necesidad", desde un punto de vista jurídico y de su relación con la limitación de los derechos fundamentales en una sociedad democrática, deviene central en este trabajo y será, a su debido tiempo, analizado en profundidad.

En el documento sobre las conclusiones del Consejo relativas a un ***Plan de Acción para establecer una estrategia común para combatir el Cibercrimen***, de 26 de abril de 2010, se reconocen los efectos de las tecnologías en el crimen y los retos que han de afrontarse para resolverlos, lo que aconseja incluso establecer plataformas de transmisión de alertas sobre uso delictivo de Internet, como la constituida en sede de EUROPOL. Se hace una mención especial a los ciberataques como amenaza de referencia en cuanto a las posibilidades de causar daño a unas sociedades que se han hecho plenamente dependientes de las TIC. Junto a estas observaciones, el documento incluye una serie de ambiciosas líneas de acción orientadas a resolver el reto. Como comentario a esta meritoria intención, ha de insistirse en que cualquier intento de

investigar en red pasa por la posibilidad de analizar las comunicaciones electrónicas en el marco del proceso penal[319].

3. La Unión Europea

El ***Tratado de Maastricht*** de 1992 supuso la creación de lo que se denominó la estructura de los ***tres pilares de la UE***[320], dado que sobre el pilar económico originario (Las Comunidades Europeas) que se fundara con los ***Tratados de Roma de 1957***, constitutivos de la Unión, se erigieron otros dos sucesivamente dedicados a la ***política exterior y de seguridad común*** (PESC) y a **los *asuntos de justicia e interior*** (JAI). Con posterioridad, el ***Tratado de Ámsterdam*** de 1997 (por el que se modificaron el Tratado de la Unión Europea, los tratados constitutivos de las comunidades europeas y determinados actos conexos) se creó un ***espacio de libertad, seguridad y justicia***[321] (ELSJ).

La Unión Europea, como entidad supranacional con la que se obligan los estados miembros, supone admitir por parte de estos una importante cesión de su soberanía nacional, tanto más sensible cuanto que sus exigencias llegasen a afectar a aspectos tan controvertidos como lo son la impartición de justicia o la regulación de los derechos fundamentales.

---

[319] Es una constante en los documentos estudiados el considerar la necesidad de contar con una capacitación técnica de los investigadores para intervenir los sofisticados instrumentos usados en la telemática y obtener la prueba electrónica válida, lo que sin duda es del máximo interés. Sin embargo, poco se repara en que, para que esto suceda, es necesario contar con la accesibilidad a los datos generados por su uso, en la que la habilitación legal de la PJE está en las antípodas de lo necesario para resolver los casos criminales. No puede reclamarse capacitación técnica sin proveer al mismo tiempo una habilitación procesal acorde con el medio sobre el que se desea intervenir.

[320] La estructura de los pilares ha quedado obsoleta tras la entrada en vigor del Tratado de Lisboa de 2007.

[321] En las modificaciones sustantivas del tratado incluidas en el art. 1 se establece la modificación del Título V mediante los arts. J.1 y ss en lo que se refiere a las disposiciones relativas a una política exterior y de seguridad común *"…de conformidad con los principios de la Carta de las Naciones Unidas, con los principios del Acta final de Helsinki y con los objetivos de la Carta de París"*, y del Título VI a través de los arts. K.1 y ss sobre las disposiciones relativas a la cooperación policial y judicial en materia penal, entre otras, mediante *"la aproximación, cuando proceda, de las normas de los Estados miembros en materia penal, de conformidad con lo dispuesto en la letra e) del artículo K.3 (la adopción progresiva de medidas que establezcan normas mínimas relativas a los elementos constitutivos de los delitos y a las penas en los ámbitos de la DO, el terrorismo y el tráfico ilícito de drogas)".*

A modo de ejemplo, puede verse como un avance de las libertades y una magnífica oportunidad para el desarrollo económico el establecimiento de un espacio europeo de libre circulación de mercancías y capitales y, en sentido contrario, como una invasión inaceptable de la soberanía nacional el reconocimiento mutuo de las resoluciones judiciales.

De este modo, en capítulos anteriores se ha presentado someramente la cuestión del vaciamiento del concepto de soberanía en favor de entidades superiores y de su subsiguiente afectación al de gobernanza, que deberá ser objeto de consensos alcanzados entre los países miembros plasmados en normas de común y obligado cumplimento, en la medida en que todas estas determinaciones, sin suponer una pérdida completa de la soberanía nacional, logren el ejercicio más eficaz de sus legítimas finalidades particulares, esto es, ser parte de su propia acción soberana.

En mi opinión, la estructura de la UE así descrita, y pese a sus incuestionables logros, se asentó en tres pilares que no gozaron de la misma solidez y resistencia porque, junto al poderoso pilar económico, se erigieron los otros dos dotados de una factura mucho más débil e inconsistente, lo que sin duda restó estabilidad y resistencia al conjunto de la Unión. Por ello, en la forma en que la Unión progrese, estos dos pilares deben ser consolidados para contribuir con idéntica fuerza que el primero al sostenimiento del edificio europeo[322]. Los esfuerzos de la UE se dirigen actualmente, no sin grandes dificultades, a compensar este desequilibrio mediante el establecimiento de instituciones y normas que doten de solidez a este tercer pilar que, aunque desaparecido a partir de la nueva organización establecida en el ***Tratado de Lisboa*** de 2007, permanece en su esencia como materia de necesario desarrollo para el futuro.

[322] En capítulos anteriores se ha resaltado la conexión existente – o más bien la difusa relación - entre el segundo y tercer pilar, entre otros, en materia del papel de las comunicaciones electrónicas y su afectación a la seguridad pública, pues buena parte de los problemas que son objeto de estudio exceden al propio proceso penal para incidir en cuestiones de seguridad mundial, como se ha visto al analizar los diferentes conceptos estratégicos comentados.

Es obra de este periodo, en cualquier caso, la creación de ***EUROJUST***[323], como organismo de cooperación judicial, y la potenciación de ***EUROPOL***[324] en materia de cooperación policial (que coordinan e integran sus esfuerzos mediante un acuerdo suscrito entre ambas instituciones, que entró en vigor el 1 de enero de 2010), así como un sinfín de normas tan trascendentales como *el* ***Acto del Consejo de 29 de mayo de 2000***, por el que se celebra, de conformidad con el artículo 34 del Tratado de la Unión Europea, el ***Convenio relativo a la asistencia judicial en materia penal entre los Estados miembros de la Unión Europea***, que han venido a suplir o suavizar los efectos negativos que el carácter transnacional de la delincuencia y su sofisticación causaban en aquellos espacios donde la soberanía nacional no podía alcanzar[325].

Junto a estas medidas, el Tratado de Ámsterdam modificó el TUE, entre otras cosas, mediante la introducción en su art. 1 del concepto de ***cooperación reforzada*** para facilitar la adopción de acuerdos entre varios de los estados miembros en aquellos casos en que deseasen "profundizar" en materia de cooperación policial y judicial mediante la facultad de invocar el uso mecanismos de mayor robustez que los disponibles bajo el régimen jurídico general de la Unión[326], siempre que tales facultades no supusiesen condicionar sus reglas de funcionamiento[327].

---

[323] EUROJUST fue creado por Decisión del Consejo 2002/187/JAI, de 28 de febrero de 2002, según el contenido del proyecto presentado en el consejo de Tampere en 1999. Esta norma fue enmendada por las posteriores decisiones del Consejo 2003/659/JAI, de 18 de junio, y 2009/426/JAI, de 16 de diciembre.

[324] La creación EUROPOL se estableció en el Tratado de la Unión Europea (TUE). Inició sus actividades como Unidad de drogas de EUROPOL (EDU) el 3 de enero de 1994. Con el paso del tiempo se fueron agregando otras áreas tácticas hasta el 1 de julio de 1999, fecha en que adoptó su estructura actual. Su regulación es mediante la Decisión del Consejo 2009/371/JAI, de 6 de abril.

[325] De muy importantes, y sin ánimo de exhaustividad, pueden calificarse las normas sobre reconocimiento mutuo de decisiones judiciales, los mecanismos de cooperación reforzada, los procedimientos de intercambio de inteligencia y datos, la orden europea de detención y entrega, la orden de investigación, de recogida de pruebas, los equipos conjuntos de investigación, la recuperación de activos, etc. Todos estos instrumentos han mostrado su eficacia frente a los delincuentes que ven cómo la perseguibilidad de sus actos no cesa en las fronteras nacionales y que, poco a poco, se gana en reactividad policial y judicial. La previsibilidad de la intervención penal es sin duda uno de los mejores elementos disuasorios de las expectativas de los criminales.

[326] El régimen de cooperación policial y judicial se estableció mediante la reforma del Título VI del TUE, recogiéndose las medidas de carácter obligatorio para el conjunto de los países miembros en los arts. K.1 al K.14, adelantándose en el art. K.12 la posibilidad de establecer un régimen de cooperación reforzada, que se desarrolló con el nuevo Título VI bis (Disposiciones para una cooperación reforzada) en los arts. K.15 al K.17.

[327] Aún con todos sus defectos, DEL MORAL valora positivamente los, en mi opinión, innegables logros de este régimen excepcional sin dejar de hacer notar que son fruto de acuerdos alcanzados inicialmente a extramuros de la propia UE, como sería el caso de los tratados de ***Prüm*** o la denominada ***Iniciativa Sueca***, sobre intercambio de datos e inteligencia policial. Otro importante instrumento, el ***Acuerdo de***

De forma particularmente interesante para cuanto se pretende poner de manifiesto en este trabajo y que será objeto de un estudio más detallado, se diseñaron instrumentos para el intercambio de datos e inteligencia entre los países signatarios[328], como los contenidos en el ***Tratado de Prüm***[329] o la ***Iniciativa Sueca***, luego incorporados al acervo europeo mediante sendas decisiones del Consejo[330], lo que confirma el interés de las medidas aludidas para el común de los miembros de la Unión Europea**.**

Desde un punto de vista policial y práctico, pese al efecto de pérdida en lo que se refiere tanto de la iniciativa como del mantenimiento de la capacidad de acción que supone el que una investigación de la PJE traspase las fronteras entre los países miembros de la UE, la experiencia a través de EUROJUST, mediante la resolución de los problemas procesales suscitados entre los países concernidos por una investigación judicial (por ejemplo, la resolución de conflictos de jurisdicción), y EUROPOL, implantando las necesarias medidas de coordinación policial y de intercambio de inteligencia[331], puede considerarse positiva.

No en vano, la Unión Europea congrega a diversos países cuyos estándares democráticos están firmemente reconocidos como condición sin la cual no podrían haber llegado a ser sus miembros. Esto permite que la concertación de las acciones jurisdiccionales en la escena europea sea razonablemente fácil de alcanzar y, en

---

Schengen, con un origen similar, fue firmado el 14 de junio de 1985. De la misma manera, desde la entrada en vigor del Tratado de Ámsterdam en 1999, el acervo de Schengen también está integrado en el de la Unión Europea en virtud de un protocolo anexo a dicho tratado. Vid. del Moral Torres, Anselmo. *Cooperación policial en la Unión Europea. Planteamiento de un Modelo Europeo de Inteligencia Criminal. Tesis Doctoral.* Madrid: UNED, 2010, págs. 79 y 278 y Urrea Corres, Mariola. *La cooperación reforzada en la Unión Europea: Concepto, naturaleza y régimen jurídico.* Colex, 2002.

[328] Los acuerdos internos entre los países miembros o los incorporados sucesivamente al acervo europeo, son complementados con una importante suma de instrumentos jurídicos de cooperación internacional de análoga eficacia suscritos con terceros países, entre los que merece destacarse los firmados con los EEUU, Noruega, Islandia o Suiza.

[329] *Convenio relativo a la profundización de la cooperación transfronteriza, en particular en materia de lucha contra el terrorismo, la delincuencia transfronteriza y la migración ilegal,* hecho en Prüm el 27 de mayo de 2005, ratificado por España el 18 de julio de 2006.

[330] Decisión 2008/615/JAI del Consejo, de 23 de junio de 2008, *sobre la profundización de la cooperación transfronteriza, en particular en materia de lucha contra el terrorismo y la delincuencia transfronteriza (Prüm) y* Decisión Marco 2006/960/JAI del Consejo, de 18 de diciembre de 2006, *sobre la simplificación del intercambio de información e inteligencia entre los servicios de seguridad de los Estados miembros de la Unión Europea* (Iniciativa Sueca). Sobre este último instrumento hay que decir que excluye a los datos obtenido por medios coercitivos, lo que impide frontalmente el intercambio de DACE conservados de acuerdo con al Directiva 2006/24/CE.

[331] Por ejemplo, a través de los AWF *o Analysis Working Files* (ficheros de análisis).

consecuencia, que la investigación policial pueda ejecutarse con suficiente solvencia bajo semejante amparo. Más aún, con este esquema pueden proyectarse acciones judiciales y policiales frente aquellos países terceros en representación de la acción legítima contra el crimen transnacional y que partirán de una Unión Europea que actúa con nombre propio.

La complejidad de la delincuencia transnacional y la irrupción de las TIC en el mundo del delito han supuesto un revulsivo sobre las formas clásicas de ordenación el proceso penal. Durante la fase de instrucción, queda obsoleta la figura tradicional del Juez como mero receptor en su sede de las aportaciones de la PJE e impartiendo las órdenes pertinentes o adoptando y comunicando resoluciones jurisdiccionales para cuya puesta en práctica precisase de su auxilio o el de terceros. La transferencia personal entre el Juez y la PJE, así como la relación con otros posibles operadores cuya participación pudiera ser relevante para la instrucción penal, quedaba relegada bajo este esquema a su más mínima expresión.

Sin embargo, el sistema de trabajo de EUROJUST, sin que ello inquiete a la independencia de las autoridades judiciales que concurren en representación de las causas que se hallan instruyendo en sus respectivos países, supone un avance sin precedentes para la eficacia de las acciones investigativas en la escena europea en la medida en que, en un mismo acto, se resuelven problemas de identificación de la jurisdicción[332], resolución de problemas de la misma naturaleza[333] y el ordenamiento de la actividad investigadora, tras tener un amplio conocimiento de unas necesidades, a veces dispares, que exceden al ámbito de instrucción penal de cada uno de los actores jurisdiccionales que participan en la investigación.

[332] Uno o varios miembros nacionales pueden dirigirse a sus respectivos países para determinar si existen causas que pudieran tener relación con los hechos materia del interés del caso que se pretende coordinar. A su aparición, EUROJUST propone coordinar la acción jurisdiccional incorporando al titular de la investigación de que se trate.

[333] En muchas ocasiones, concurren Jueces (o Fiscales) de un mismo estado miembro que tienen, por imperativo de las normas sobre competencia territorial, "fragmentos" que, aunque enjuiciables por separado, son parte de una misma maquinación criminal. Este sería el caso, por ejemplo, de una red que se dedicase a robos en domicilio en diversos países de la UE, lo que originaría tantos procesos penales como hechos hubieran sido conocidos en los diversos partidos judiciales. Es evidente que, una de las decisiones jurisdiccionales a proponer tendrían relación con la resolución de la cuestión de la competencia.

Es evidente que esta acción coordinadora integra y economiza los esfuerzos de todos los actores para el futuro enjuiciamiento[334] de los hechos delictivos que se investigan, es decir, logrando la inmediatez necesaria para lograr el más preciso conocimiento de la naturaleza de los hechos que un día serán objeto de juicio oral. El resultado final es la más eficaz reordenación de la instrucción en la dirección que el Juez haya estimado pertinente en uso de su independencia judicial y de acuerdo con el Derecho interno de su país, tras asistir a las reuniones de coordinación con otros titulares de la acción jurisdiccional, lo que sucederá exactamente bajo los mismos atributos que la Ley les otorga como tales.

Otro de los incuestionables avances del sistema de EUROJUST lo supone el hecho de que la pérdida de operatividad y capacidad de actuación de la PJE fuera de su ámbito territorial de competencia quede compensada por la capacidad de acción otorgada por la concertación a través de los miembros nacionales de los países representados ante el Colegio de EUROJUST.

Es necesario hacer notar que el éxito del proceso penal en estos casos tan complejos depende, en su expresión más práctica, real y ajena a los formalismos jurídicos, de la voluntad de las personas que se conciertan lealmente para llevar a cabo un trabajo con el que, excediendo a su propia posición profesional, logren remover todos los obstáculos que condicionen la viabilidad de la investigación.

Sensu contrario, nada *más fácil* y socorrido que refugiarse falazmente en la defensa de la soberanía nacional, en los ignotos impedimentos jurídicos del Derecho interno, el hipergarantismo, en los formalismos, la burocracia, la incompetencia funcionarial, la no disponibilidad de recursos materiales o personales, falta de tiempo o a las excusas técnicas para evitar hacer un trabajo cuya finalidad sea que impere la Ley. De ahí el indispensable valor que, según mi experiencia personal y profesional, ha adquirido EUROJUST en los años en que viene desarrollando su labor en la escena europea para concitar todos los esfuerzos en beneficio de la Justicia[335].

[334] La cuestión de "dónde se enjuiciará" es una de las que quedan resueltas en este tipo de reuniones de coordinación.

[335] Por ejemplo: En el Sumario 1/05 del Juzgado de Instrucción núm. 1 de Vinaroz (Castellón) consta una OEDE ante la República Checa que se emitió para que se detuviese a un presunto homicida huido de España y se registrase su domicilio. Tras su emisión formal surgió inesperadamente a la PJE la necesidad

El Tratado de Lisboa ha supuesto un esperanzador paso adelante para consolidar, mejorar y proyectar hacia el futuro todos estos avances para la lucha contra el terrorismo y la DO al introducir los siguientes avances:

- *La desaparición de los pilares comunitarios.*
- *Nuevos mecanismos relativos a los procedimientos de decisión*[336].
- *Un papel reforzado para el PE (Parlamento Europeo) y los Parlamentos Nacionales.*
- *La ampliación de la competencia del Tribunal de Justicia de las Comunidades Europeas.*
- *La naturaleza jurídica vinculante de la Carta de derechos fundamentales de la Unión.*
- *La atribución de personalidad jurídica a la UE.*
- *La posibilidad de crear una **Fiscalía Europea** y un **Comité Permanente de Seguridad Interior*** (En adelante, COSI)[337].

Especialmente interesantes son las disposiciones recogidas en el art. 69e, pfo. 1, sobre la creación de una Fiscalía Europea en EUROJUST que aunque en principio se dirija a la persecución de los delitos contra los intereses financieros de la UE, existe la posibilidad de extender sus acciones, de acuerdo con pfo. 4 del mismo artículo, a la persecución de la criminalidad grave que tenga una dimensión transfronteriza, todo ello por decisión unánime del Consejo alcanzada tras obtener el consentimiento del Parlamento Europeo y haber sido consultada la Comisión.

---

de observar también las acciones de la esposa del sospechoso previamente a que se practicase la prevenida detención que constaba en la OEDE, todo ello para comprobar su implicación en los hechos si realizaba en Madrid una determinada acción ante un notario (un vaciamiento patrimonial). La policía checa, escrupulosa con los pedimentos de la OEDE, quería ejecutarla cuanto antes ignorando los ruegos de los guardias civiles comisionados en Praga, quienes temían que su precipitación pusiese sobreaviso a la mujer. Finalmente, la diligente solicitud verbal del miembro nacional español ante EUROJUST a su colega checo fue bastante para, de un forma diplomática, vencer la resistencia de la policía checa, lo que permitió, no sólo observar los libres movimientos de la sospechosa, sino acreditar debidamente su participación en los hechos. La detención se practicó el 04/10/2006. Fuente: Entrevista con el Instructor de las diligencias policiales, perteneciente a la UCO de la Guardia Civil (OP. DESTINO).

[336] El proceso de codecisión agilizará la adopción de acuerdos referidos al ELSJ en el seno de la UE. A partir de 2014, la mayoría cualificada obedecerá al principio de doble mayoría (mayoría de los Estados miembros y de la población), que refleja la doble legitimidad de la Unión. La doble mayoría se alcanzará cuando los votos favorables representen, como mínimo, el 55% de los Estados miembros y el 65% de la población. Vid. del Moral Torres, Anselmo. *Cooperación policial en la Unión…op.cit*, pág. 83.

[337] Vid. Vieitez Pérez, Begoña. *El Tratado de Lisboa: Una aproximación al espacio de libertad, seguridad y justicia.* Madrid: Centro de Análisis y Prospectiva de la Guardia Civil, 2009.

En mi opinión, dada la gravedad actual de los fenómenos asociados al terrorismo y la DO transfronteriza o grave, sería necesario dotar a esta institución de los más altos poderes ejecutivos en la escena europea y el establecimiento de los tipos penales y medidas procesales de cualquier clase admisible en la Ley que permitieran su más eficaz actuación en el conjunto de la UE ante los tribunales de justicia y, en representación de esta, frente a países terceros, todo ello mediante la cesión plena de la jurisdicción e imposición y ejecución de penas y medidas de todo tipo, incluida la exigencia de responsabilidades civiles.

El COSI se constituyó, por su parte, mediante Decisión del Consejo de 27 de noviembre de 2009 como órgano de coordinación operacional entre autoridades de los estados miembros con competencia en la seguridad interior (art. 2)[338], pero sin capacidad para conducir operaciones concretas de acuerdo con el art. 4, lo que seguirá siendo competencia de los estados miembros, ni participar tampoco en el proceso legislativo.

En mi opinión, según parece, el COSI no viene revestido de una clara facultad operativa más allá que la de procurar los consensos entre las acciones que cada país decida emprender, algo que con mucha más eficiencia viene haciendo EUROJUST sin ser un organismo policial ya que, además, concita la resolutiva participación de quienes ejercen la acción jurisdiccional y representantes de cualquier institución que puedan ofrecer alguna aportación relevante para el buen fin de un investigación, como las aduanas, organismos de gestión tributaria, sanitarios, etc..

Hasta ahora se ha descrito de forma muy general el panorama evolutivo de la lucha contra la delincuencia en un ámbito jurídico supranacional ciertamente sofisticado como el que representa la Unión Europea, cuya producción normativa es de obligatoria implementación en el Derecho interno de sus países miembros. Esta circunstancia hace previsible el imperio del Derecho comunitario en cada uno de ellos y que la respuesta unitaria alcance todas sus finalidades.

[338] *"El COSI se encargará de que exista una estricta cooperación entre las agencias de la UE y los órganos implicados en la seguridad interior de la Unión (Europol, Frontex, Eurojust, Cepol y Sitcen)"*. Vid. *"Estrategia de Seguridad Interior de la Unión Europea "Hacia un modelo europeo de seguridad interior""*, de 26 de marzo de 2010.

Sin embargo, si las necesidades de seguridad eran ya imperiosas cuando se estimó la necesidad de sumar el pilar de la libertad, seguridad y justicia a la construcción de un espacio europeo formado por 500 millones de habitantes de 27 países distintos, por los indeseables efectos de la evolución de las TIC en la delincuencia que inmediatamente se hicieron tan visibles como desconcertantes, se está produciendo en el seno de la UE una auténtica revolución para tratar de ofrecer una respuesta a un problema que, merced a esta nueva circunstancia, se torna extraordinariamente complejo[339], especialmente por la aparición del factor de relación global propiciado por las comunicaciones electrónicas, sea cual fuere su expresión (telefonía móvil, Internet, etc.), y su subsiguiente afectación a los derechos fundamentales en caso de que se hubieren de intervenir en el marco de un proceso penal con vocación de exceder a los espacios de clásicos de soberanía[340].

Con todo ello, la UE pretende establecer desde el año 2003 una ***Estrategia de Seguridad Interior***[341] buscando todas las sinergias posibles en un proceso dotado de

[339] Por ejemplo, en lo que se refiere al delito cibernético: la Directiva 2000/31/EC del Parlamento Europeo y el Consejo *sobre ciertos aspectos jurídicos de los servicios en la sociedad de la información, en particular el comercio electrónico, en el mercado interno*; la DM 2000/413/JHA del Consejo de la Unión Europea *sobre la lucha contra el fraude y la falsificación de medios de pago distintos del efectivo*; la DM 2004/68/JHA del Consejo de la Unión Europea *sobre la lucha contra la explotación sexual de los niños y la pornografía infantil*; la DM 2005/222/JHA del Consejo de la Unión Europea *sobre los ataques contra los sistemas de información*, que puede ser objeto de reforma mediante la Propuesta de Directiva del Parlamento Europeo y del Consejo, de 30 de mayo de 2011; Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones *sobre la protección de infraestructuras críticas de Información «logros y próximas etapas: hacia la ciberseguridad global»* (COM(2011) 163 final), de 31 de marzo de 2011, como reflejo de los retos de la ciberdelincuencia; la Directiva 2006/24/EC del Parlamento Europeo y del Consejo de la Unión Europea *sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modificó la directiva 2002/58/EC*; y la DM 2008/919/JHA del Consejo de la Unión *Europea por la que se modificó la DM 2002/475/JHA sobre la lucha contra el terrorismo*.

[340] Los documentos que tratan el problema en la UE son muy numerosos. Por ejemplo, en la Comunicación de la Comisión al PE y al Consejo sobre *"Un espacio de libertad, seguridad y justicia al servicio de los ciudadanos – Mayor libertad en un ambiente seguro"* (COM (2009) 262 final) se señala la amenaza transfronteriza que supone el cibercrimen para los derechos y libertades de los ciudadanos de la Unión junto con el problema del incremento del intercambio de datos entre los ciudadanos y su pérdida de control, lo que supone una afectación a su privacidad (nótese las connotaciones que este hecho tiene para la investigación penal). En igual medida, a efectos de seguridad, el documento propone un *"modelo europeo controlado de intercambio de inteligencia"* y la intensificación de la cooperación policial y judicial, entre otras muchas medidas.

[341] Vid. *"Estrategia de Seguridad Interior de la Unión Europea "Hacia un modelo europeo de seguridad interior""*, de 26 de marzo de 2010. Este modelo está basado *"en los principios y los valores de la Unión: el respeto de los derechos humanos y las libertades fundamentales, el Estado de Derecho, la democracia, el diálogo, la tolerancia, la transparencia y la solidaridad."* También, Vid. Comunicación de la Comisión al

una vocación integradora[342]. Esta estrategia está orientada, según su revisión de 2010, a la finalidad de *"proteger los derechos y libertades; mejorar la cooperación y la solidaridad entre los Estados miembros; atender a las causas de la inseguridad y no sólo los efectos; priorizar la prevención y la anticipación; implicar a todos los sectores, que de una forma u otra, desempeñen una función en la protección pública (político, económico, social, etc.); comunicando las políticas de seguridad a los ciudadanos; y, por último, reconocer la interdependencia entre la seguridad interna y externa en la construcción de un enfoque de "seguridad global" en relación con terceros países"*[343].

En el documento de seguridad interior, y es ocioso ya mencionarlas, se relacionan todas y cada de las amenazas que se ciernen sobre la sociedad globalizada y tecnificada actual provenientes del terrorismo y la DO o grave. Como instrumentos de respuesta se proponen los siguientes:

- *"Análisis de situación y de escenarios futuros: anticipación a la amenaza.*
- *Respuesta adecuada: planificación, programación y gestión de las consecuencias.*
- *Efectividad sobre el terreno: el trabajo de agencias, instituciones y órganos: EUROPOL, EUROJUST, FRONTEX, etc.*
- *Herramientas basadas en el reconocimiento mutuo, para compartir información y para facilitar investigaciones y operaciones conjuntas.*
- *Mecanismos de evaluación para valorar la eficacia de [las] acciones".*

Consejo y al Parlamento Europeo sobre el *"Desarrollo de un concepto estratégico para hacer frente a la DO"* COM(2005) 232 final, de 2 de junio de 2005.

[342] Bajo los siguientes aspectos: *"Dimensión horizontal: …con la participación de las autoridades policiales y de gestión de fronteras, con el apoyo de la cooperación judicial, de los organismos de protección civil y también de los sectores político, económico, financiero, social y privado, incluidas las organizaciones no gubernamentales. Dimensión vertical: …la cooperación internacional, las políticas y las iniciativas de seguridad de la UE, la cooperación regional entre los Estados miembros y las propias políticas nacionales, regionales y locales de los Estados miembros… Dimensión externa: en su relación con terceros países".* Vid. *"Estrategia de Seguridad Interior de la Unión Europea "Hacia un modelo europeo de seguridad interior"",* de 26 de marzo de 2010.

[343] Entre los principios más importantes que animan la estrategia de seguridad se destacan la *"seguridad, libertad y justicia [que] son políticas que se refuerzan mutuamente, respetando los derechos fundamentales, la protección internacional, el Estado de Derecho y la intimidad"* y la confianza mutua como un elemento clave. Vid. Proyecto de Estrategia de Seguridad Interior de la Unión Europea: *"Hacia un modelo europeo de seguridad",* de 15 de febrero de 2010. Esta estrategia fue aprobada por el Consejo Europeo de los días 25 y 26 de marzo de 2010.

En lo que se refiere a la materia de más directo interés de este trabajo, el ***modelo europeo de seguridad***[344] pone el acento en los procedimientos de intercambio de inteligencia, para lo que sería necesario avanzar en el concepto de confianza mutua entre las autoridades de los países miembros. Bajo el principio de respeto al derecho a la intimidad, se puntualiza que *"este modelo de intercambio de información siempre debe respetar plenamente el derecho a la intimidad y la protección de datos personales. Si un mayor nivel de seguridad significa un aumento en el intercambio de datos*[345]*, es importante que este aumento se trate adecuadamente, sea proporcionado y respete la reglamentación en materia de protección de datos"*.

La Unión Europea ha ido materializando sus acciones para el logro de la seguridad a través de sucesivos programas, planificados para ser ejecutados en periodos de cinco años. El primero de ellos fue el ***Programa de Tampere*** (2000-2005), refrendado por el Consejo Europeo los días 15 y 16 de octubre de 1999, que fue el primer programa plurianual que fijó las prioridades de un espacio de libertad, seguridad y justicia[346]. Le sucedió el ***Programa de La Haya*** (2005-2010), que se firmó en mayo de 2005[347].

En la actualidad está en vigor el ***Programa de Estocolmo***[348], firmado en diciembre de 2009 para ser ejecutado en el periodo 2010 a 2015 y que merece algún mayor detenimiento en su análisis ya que, pese a la aparente reiteración de los

---

[344] El marco jurídico general de la lucha contra la DO en la UE puede consultarse en http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_organised_crime/index_es.htm.

[345] Nótese cómo el documento se hace eco de la evolución de las TIC en cuanto a que la necesidad de tratamiento de datos aumentará si se desea mejorar la seguridad de los europeos. Es evidente que el uso masivo de las TIC genera de forma instantánea el tráfico de millones de datos relacionados con las comunicaciones electrónicas con la consabida afectación al derecho a la intimidad y al secreto.

[346] Entre las principales líneas de acción hay destacar la voluntad de conseguir un marco para la consecución del reconocimiento mutuo de las resoluciones judiciales y el planteamiento de la lucha contra la DO, poniendo el acento en el capítulo de la cooperación (La creación de EUROJUST o CEPOL nacen de este programa, entre otros avances). La Comisión evaluó los resultados de los últimos cinco años de aplicación en su Comunicación de 2 de junio de 2004 en el documento *"Espacio de Libertad, Seguridad y Justicia: balance del programa de Tampere y futuras Orientaciones*", COM (2004) 401 final.

[347] El programa intensificó la atención sobre la protección de los derechos fundamentales e insistió en el intercambio de datos como factor esencial de la eficacia policial en la escena europea, tratando de equilibrar los conceptos de privacidad y seguridad. Vid. *"Diez prioridades para los próximos cinco años. Una asociación para la renovación europea en el ámbito de la libertad, la seguridad y la justicia"*, COM(2005) 184 final, de 10 de mayo de 2005.

[348] Programa de Estocolmo – Una Europa abierta y segura que sirva y proteja al ciudadano, de 3 de marzo de 2010.

objetivos estratégicos de seguridad a lograr, a día de hoy, como indica DEL MORAL, *"…la realidad es que si observamos la fecha de comienzo del primer programa , es decir, Tampere en 1999 y [si] se observa lo que se ha conseguido en diez años, podemos decir que no hay parangón en materia de cooperación policial entre Estados con respecto a otras zonas geopolíticas"*[349].

En otras palabras, que la evolución de la DO trasnacional en el ámbito mundial, recibe en los países que no son miembros de la UE una respuesta prácticamente limitada al círculo donde su soberanía puede alcanzar, y en los que pertenecen al ámbito regional de los países miembros de la UE, una reacción cual si se tratase de un estado soberano único, dotado de un régimen jurídico-penal común y de unos recursos compartidos y adecuados al reto o, al menos, de haber alcanzado un nivel de eficacia similar y, lo que resulta esperanzador, aún con todas las dificultades, con una razonable expectativa de evolución hacia unas mayores cotas de eficiencia futura.

Los puntos concretos de innovación contenidos en el Programa de Estocolmo, que señalan los progresos intermedios para el ELSJ, son:

- *"Establecer en la Unión un régimen completo y reforzado de protección de datos.*
- *Suprimir totalmente los procedimientos intermedios (exequátur) para la ejecución de las resoluciones judiciales de un Estado miembro en otro.*
- *Crear un programa de intercambio para la policía y reforzar el existente para las profesiones jurídicas (Erasmus de policías y profesiones jurídicas).*
- *Reforzar las garantías procesales en los procedimientos penales.*
- *Elaborar una estrategia de seguridad interior para la Unión.*
- *Crear una arquitectura de los sistemas de información que permita reforzar los intercambios de información entre los servicios policiales europeos.*
- *Reforzar la evaluación de las políticas europeas en materia judicial, y apoyar los esfuerzos de los Estados Miembros para la mejora de la calidad de sus sistemas judiciales.*

[349] Vid. del Moral Torres, Anselmo. *Cooperación policial en la Unión…op.cit*, pág. 115.

- *Establecer una política de inmigración flexible, en consonancia con las necesidades del mercado de trabajo, favoreciendo la inserción de los inmigrantes y luchando contra la inmigración ilegal.*
- *Reforzar la solidaridad entre los Estados Miembros para la acogida de los refugiados y solicitantes de asilo.*
- *Reforzar el esfuerzo de investigación en materia de técnica de seguridad".*

En ejecución del programa, se estableció un ***Plan de Acción***[350] en el que se ponderan los principales avances para el ELSJ, comenzando por las novedades contenidas en el Tratado de Lisboa sobre el papel del Parlamento Europeo como colegislador, las mejoras en el sistema de codecisión y mayorías y los procedimientos de control jurisdiccional[351].

En el Plan de Acción se contemplan aspectos de interés crucial para el logro de los objetivos relacionados con la lucha contra la DO, basados en el respeto a los derechos fundamentales y, especialmente, en la preservación de la intimidad y la protección de datos[352], tales como:

- *"Informes sobre la aplicación de la Directiva marco 2006/783/JAI relativa al reconocimiento mutuo de resoluciones de decomiso.*
- *Informe sobre la aplicación de la Decisión marco 2002/584/JAI sobre la orden de detención europea, y su seguimiento adecuado.*

[350] Vid. Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. *"Garantizar el espacio de libertad, seguridad y justicia para los ciudadanos europeos. Plan de acción por el que se aplica el programa de Estocolmo".* COM(2010) 171 final.

[351] Textualmente, se afirma que: *"En primer lugar, el papel cada vez más importante del Parlamento Europeo como colegislador en la mayoría de las materias y la mayor implicación de los parlamentos nacionales harán que la UE sea más responsable de sus acciones en interés del ciudadano, y reforzarán la legitimidad democrática de la Unión. En segundo lugar, la introducción de la decisión por mayoría cualificada en el Consejo para la mayoría de las materias racionalizará el proceso de toma de decisiones. Por último, el control jurisdiccional mejorará porque el Tribunal de Justicia de las Comunidades Europeas asumirá la supervisión jurisdiccional de todos los aspectos relacionados con la seguridad, la justicia y la libertad, mientras que la Carta de los derechos fundamentales de la UE se convierte en jurídicamente vinculante"*.

[352] Es de particular interés, en materia de protección de datos en el ámbito de la cooperación policial, *"el establecimiento de una agenda estratégica para el intercambio de información [para lo que se] exige tener una visión general de las recopilaciones de datos existentes, los sistemas de tratamiento e intercambio de datos, así como una evaluación de su utilidad, eficiencia, eficacia, proporcionalidad y respeto del derecho a la intimidad. También debería sentar las bases del desarrollo coherente de todos los sistemas de información existentes y futuros".*

- *Propuesta legislativa sobre un régimen global de obtención de pruebas en materia penal sobre la base del principio de reconocimiento mutuo y relativo a todos los tipos de pruebas.*
- *Propuesta legislativa para la introducción de normas comunes para la obtención de pruebas en materia penal con objeto de garantizar su admisibilidad.*
- *Propuesta de Reglamento por el que se confieren a Eurojust las facultades necesarias para iniciar las investigaciones, se aumenta la eficacia de la estructura interna de Eurojust*[353] *y se prevé la participación del Parlamento Europeo y los parlamentos nacionales en la evaluación de las actividades de Eurojust".*

Del anterior listado, que anticipa la verdadera dirección de los esfuerzos de la UE, se pueden deducir algunas de las claves que habrán de orientar el desarrollo futuro del ELSJ, pues se hace patente que la línea estratégica principal consiste en lograr un espacio policial y judicial único, donde las fronteras internas de la UE no supongan un obstáculo para alcanzar plenamente todos y cada uno de los objetivos de la justicia penal y que esta, además, se pueda proyectar a países terceros desde una solvente plataforma de unión entre naciones basada en el respeto a los derechos humanos.

Los conceptos básicos que configuran esta pretensión, fundada evidentemente en el principio de confianza mutua entre los países miembros, se pueden fácilmente entrever en los instrumentos jurídicos que se van implementando y cuyos signos son la admisibilidad y validez de los medios de prueba en cualquiera de los países miembros, la previsibilidad de la respuesta de la Ley y su eficacia en lograr el resarcimiento de las víctimas y la anulación de la capacidad criminal (materialización de decomisos y OEDE).

De manera especialmente sugestiva, se ofrece la posibilidad contemplada en el Tratado de Lisboa de habilitar a EUROJUST para que pueda iniciar investigaciones penales, incluso más allá de los ilícitos relacionados con la protección de los intereses financieros de la UE, haciendo posible además que cada Juez o fiscal pueda ordenar las

[353] Sobre el papel de las instituciones, vid. *Comunicación de la Comisión al Consejo y al Parlamento Europeo sobre el papel de Eurojust y la Red Judicial Europea en el marco de la lucha contra la DO y contra el terrorismo en la Unión Europea* COM(2007) 644 final, de 23 de octubre de 2007.

investigaciones en cualquier punto del territorio europeo mediante la emisión de la proyectada ***Orden Europea de Investigación*** (OEI)[354], con plena capacidad ejecutiva y sin necesidad, por tanto, de la emisión de una ***Comisión Rogatoria Internacional*** (En adelante, CRI) cuya prosperidad hubiera de depender de la voluntad del Juez o fiscal requerido de admitirla, tal y como sucede en la actualidad.

Pero el logro de tan ambiciosos objetivos no puede verificarse sin la dotación previa de un marco jurídico adecuado que lo propicie, comenzando por resolver, desde un punto de vista práctico, cuestiones tales como la recogida, tratamiento e intercambio de datos e inteligencia de forma útil a las finalidades de la prevención del delito (policía de seguridad) y de la investigación criminal (policía judicial) o, dentro de esta misma función, las diferentes figuras procesales que pueden invocarse dentro del proceso penal de cada uno de los países miembros.

Las disparidades que se observan en esta materia son sencillamente infinitas, como tantas veces la UE ha anotado cuando ha proclamado la necesidad de aproximar y armonizar las legislaciones nacionales. Las acciones recogidas en el plan, consecuentemente, se orientan a paliar este efecto con vocación de, mediado el tiempo, lograr alcanzar un estatus jurídico común tal que permita la consecución de sus objetivos de unidad más ambiciosos.

En efecto, si se examinan las acciones específicas contenidas en el plan, se puede contemplar esta voluntad de aproximar las legislaciones mediante:

- La búsqueda de fórmulas jurídicamente aceptables en relación con la protección de los derechos fundamentales y relacionadas con su recogida y cesión para usos internos y en cooperación con países terceros, tales como los registros de nombres de pasajeros, la evaluación y revisión de la Directiva 2006/24/CE sobre conservación de datos, la eficacia en la aplicación de los convenios de *Prüm* o la *Iniciativa Sueca*, el modelo de intercambio de información, la rastreabilidad de los usuarios de los servicios de comunicación de prepago, etc.

[354] Vid. Propuesta de Directiva del Parlamento Europeo y del Consejo *sobre la Orden Europea de Investigación en asuntos criminales*, de 3 de junio de 2010.

- El uso de los recursos tecnológicos para la investigación penal, particularmente en lo que se refiere a los diversos instrumentos de gestión de la información[355], para proveerles del sustrato material con que hacer eficaz el intercambio de datos e inteligencia, como puede ser la ejecución de medidas relativas al ***Sistema de Información Europeo de Antecedentes Penales*** (ECRIS), la viabilidad del ***Sistema Europeo de Índice de Ficheros Policiales*** (EPRIS) o las posibles medidas para promover el intercambio de información entre los Estados miembros, incluido Europol, sobre los desplazamientos de delincuentes violentos en relación con acontecimientos importantes.
- Las medidas de mejora de la cooperación policial y aduanera en la UE, incluidas reflexiones sobre los ***agentes encubiertos***, los ***Centros de Cooperación Policial y Aduanera***, el enfoque de la UE respecto de las funciones policiales basadas en la inteligencia y las acciones comunes para mejorar la cooperación policial operativa.
- Medidas relativas a una política de seguridad de la información y de la red reforzada y de alto nivel, incluidas iniciativas legislativas como la relativa a la ***Agencia Europea de Seguridad de las Redes y de la Información*** (ENISA), así como otras medidas que permitan reacciones más rápidas en caso de ciberataque o, también, propuestas legislativas para establecer las normas de competencia jurisdiccional relativas a la ciberdelincuencia, a escala europea e internacional.
- La consecuención de acuerdos de cooperación con países terceros.

En lo que se refiere a los ***ataques a los sistemas de información y la protección de las estructuras críticas***, la aproximación del derecho penal en un conjunto de normas mínimas se recoge en la Decisión marco 2005/222/JAI del Consejo, de 24 de febrero de 2005, que será objeto de sustitución caso de prosperar la Propuesta de Directiva del Parlamento Europeo y del Consejo relativa a los ataques contra los sistemas de información, de 30 de mayo de 2011.

[355] Vid. Comunicación de la Comisión al Consejo y al Parlamento Europeo. *Panorama general de la gestión de la información en el espacio de libertad, seguridad y justicia*. COM(2010)385 final, de 20 de julio de 2010.

En efecto, en el documento sobre la protección de las infraestructuras críticas[356], las amenazas que ciernen – y que no pueden ser abordadas sino en el escenario mundial - son clasificadas por la UE del siguiente modo:

- *"fines de **explotación**, como es el caso de las «amenazas persistentes avanzadas» (ataques a infraestructuras gubernamentales y del sector público), de espionaje económico y político (p. ej., GhostNet, sobre una red de espionaje), los robos de identidad, o los recientes ataques contra el sistema de comercio de derechos de emisión o contra los sistemas de TI de los Estados;*
- *fines de **perturbación**, como la denegación de servicio distribuido o el «spam» generado vía botnets[357] (p. ej., la red Conficker, con más de 7 millones de máquinas, o la red Mariposa, basada en España, con una red de 12,7 millones de máquinas), Stuxnet[358], o el corte de los medios de comunicación;*
- *fines de **destrucción**; esta es una posibilidad que todavía no se ha presentado pero, vista la omnipresencia creciente de las TIC en las infraestructuras críticas (p. ej., en las redes inteligentes y los sistemas de distribución de agua), no cabe descartarla en los próximos años"*[359].

A continuación, se describe una compleja estructura institucional desde la que planificar (incluyendo los ejercicios de simulación y la evaluación de los sistemas de respuesta coordinada) y prevenir, anular o paliar los efectos de los posibles fallos de las infraestructuras de comunicaciones o impedir los ataques a los sistemas

[356] Vid. *Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones sobre la protección de infraestructuras críticas de Información «logros y próximas etapas: hacia la ciberseguridad global» COM(2011) 163 final.*

[357] En la propuesta de Directiva se recoge la necesidad de tratar el riesgo de gran lesividad que suponen los nuevos *modus operandi* propiciados por las TIC, como sería el caso de "*la utilización de las redes infectadas (botnets) se caracteriza por que el acto delictivo conlleva fases posteriores, cada una de las cuales puede representar un peligro para el interés público. A este respecto, la [propuesta de] Directiva tiene por objeto, entre otros, establecer sanciones penales para la fase de creación de la red infectada, es decir, cuando se establece un control remoto sobre un número significativo de ordenadores infectándolos mediante programas nocivos a través de ataques informáticos dirigidos. En una fase posterior, los ordenadores infectados, que constituyen la red infectada, pueden activarse sin el conocimiento de los usuarios con el fin de realizar ataques informáticos a gran escala, que en circunstancias normales pueden causar daños graves".*

[358] Al virus *Stuxnet* le siguieron otros como el *duqu* o el *flame,* con capacidades devastadoras sobre los sistemas telemáticos que quedasen infectados.

[359] Véase el informe *«Global Risks 2011»*, del Foro Económico Mundial.

cibernéticos de los que la sociedad se ha hecho dependiente, trascendiendo de lo estrictamente policial para alcanzar de lleno al interés de la defensa[360].

Se hace notorio en lo que interesa a este trabajo que, tanto en lo que se discute en la UE sobre la delincuencia trasnacional organizada o grave, en un sentido genérico, como cuando desciende al análisis de los llamativos fenómenos relacionados con las TIC, que de lo que se está hablando es, entre otras muchas cosas, de diseñar una respuesta que afronte eficazmente el uso malicioso de las comunicaciones electrónicas para perturbar la libertad de los ciudadanos.

Por ello, junto con una estricta normativa de protección de los derechos fundamentales y, especialmente, de la protección de datos personales, la UE ha ido estructurándose para diluir de una manera real las fronteras interiores y los obstáculos que impiden una eficaz cooperación entre los estados miembros, todo ello con una clara vocación de conseguir un espacio único europeo en materia de cooperación policial y judicial. En este espacio único, consecuentemente, debe poderse acceder a la legal limitación de los derechos fundamentales en materia de acceso a los DACE de una manera adecuada y proporcional a las exigencias del marco tecnológico y funcional en que se desarrollan, dotándose los poderes públicos de los necesarios instrumentos procesales que lo permitan.

---

[360] *"…participará, en el marco de sus competencias, en foros tales como el G8, la OCDE, la OTAN (especialmente a través del nuevo concepto estratégico adoptado en noviembre de 2010 y de las actividades del centro de excelencia cooperativo en materia de ciberdefensa), la UIT (en el contexto de la creación de capacidad en el ámbito de la ciberseguridad), la OSCE (a través de su Foro de Cooperación en materia de Seguridad), la ASEAN, Meridian, etc. […] en el marco de la Directiva 2008/114/CE del Consejo sobre la identificación y designación de infraestructuras críticas europeas y la evaluación de la necesidad de mejorar su protección".* Algunos puntos de interés son muy llamativos, como es el caso de la seguridad de la nube (*"cloud computing"),* cuyas posibles vulnerabilidades deben ser tratadas, por tratarse de un elemento estratégico que configura un desarrollo social integral sin precedentes propiciado por las TIC y que debe permanecer ajeno al interés de los delincuentes. Este desarrollo, no exento de problemas procesales, es una reconocida preocupación para el TC, pues en la STC 173/2011, de 7 de noviembre, sobre la volatilidad de las pruebas contenidas en un ordenador intervenido por la PJE, dice que *"…tampoco aparece como irrazonable intentar evitar la eventualidad de que mediante una conexión a distancia desde otra ubicación se procediese al borrado de los ficheros ilícitos de ese ordenador o que pudiera tener en la "nube" de Internet"*. Un registro de un ordenador, como es de ver, afectará tanto al propio dispositivo como a las conexiones que, bajo el dominio del usuario, se puedan acceder y que sean del eventual interés del proceso penal.

III. CAPÍTULO TERCERO: PROPORCIONALIDAD E INTERVENCIÓN DE LAS COMUNICACIONES ELECTRÓNICAS

Este capítulo fue concebido en un primer momento como una mirada jurídica a la concepción actual del principio de proporcionalidad, según las diferentes fuentes de la doctrina y la jurisprudencia, de forma que aportase al estudio un amplio panorama desde el que enfocar el problema de la limitación del derecho fundamental al secreto de las comunicaciones y la afectación concomitante al marco constitucional de protección de datos de carácter personal asociado al desarrollo de las TIC, así como de su universal penetración en la sociedad contemporánea e, incluso, presentarlo con alguna vocación de explorar su evolución de un modo prospectivo.

Sin embargo, la humilde contribución que por mi parte podía hacerse, limitada a mostrar de forma sucinta una descripción de ese panorama, no adquiriría su verdadero valor si no se ponía en inmediata relación con los problemas que desde el mundo de la investigación criminal se intuyen y que afectan a la percepción jurídica y práctica de este trascendental principio con el que operan actualmente muchos países del entorno democrático de España.

Consideré por ello pobre limitarme a ofrecer una visión comprensiva de lo aportado por los insignes juristas que han reflexionado con autoridad y enjundia sobre el cada vez más invocado principio de proporcionalidad, sobre todo cuando se ha recurrido a su esencia jurídica para alcanzar resoluciones de estricta justicia que no gozasen de un acomodo preciso en el derecho positivo, dado el desbordamiento jurídico que han producido en los últimos tiempos las realidades tecnológicas.

El sesgo policial, del que honestamente no puedo sustraerme, invita al esfuerzo de tratar de encajar esta realidad social de las TIC en el mundo del Derecho, sobre todo, porque lo que se desea desde la Policía Judicial es alcanzar el mayor nivel de adhesión y participación activa a la cabal protección de los derechos fundamentales y que, al tiempo de hacerlo, puedan también ser limitados de una forma segura y aceptable para el Estado de Derecho, siempre bajo la dependencia funcional de Jueces y Fiscales.

Con este espíritu, la estructura de este capítulo, sin renunciar a sus contenidos jurídicos más significativos, pretende interrelacionar una realidad tecnológica y social muy sugerente con un panorama jurídico de referencia donde no todo casa como debe, quizá hasta el punto de haber creado importantes lagunas de impunidad donde

el Derecho, o no alcanza, o lo hace deficientemente, en tanto que el garantismo exacerbado, o el hipergarantismo, se sitúan en la mejor posición para ganar sus más trascendentales batallas en perjuicio de la tutela judicial efectiva, la seguridad pública y los derechos de los ciudadanos y, por qué no decirlo, de la propia solvencia del Estado de Derecho en su conjunto.

A. El principio de proporcionalidad

En este apartado se introduce el principio de proporcionalidad en sus aspectos básicos, junto con algunas consideraciones de orden práctico y policial que permitirán posteriormente sostener algunas de las propuestas que son objeto del este estudio.

1. Nociones elementales sobre el principio de proporcionalidad

Los derechos fundamentales no son derechos absolutos[361] aún en el caso en que las potestades para su limitación por parte del Estado no se especifiquen expresamente en los diferentes preceptos constitucionales que los proclaman. No obstante lo anterior, sí existe una expresa reserva para la injerencia del Estado en los derechos contenidos en el art. 18.3 CE, que centran el interés de este estudio en materia del secreto de las comunicaciones entre las personas[362], ya que únicamente puede ser acordada mediante una resolución judicial *"…de forma razonada y previa ponderación de la proporcionalidad, razonabilidad y necesidad de la medida…"*[363,364].

[361] En la STC 173/2011, de 7 de noviembre, se dice *"a esto se refiere nuestra doctrina cuando alude al carácter no ilimitado o absoluto de los derechos fundamentales, de forma que el derecho a la intimidad personal, como cualquier otro derecho, puede verse sometido a restricciones (SSTC 98/2000, de 10 de abril, FJ 5; 156/2001, de 2 de julio, FJ 4; y 70/2009, de 23 de marzo, FJ 3)".*

[362] Según LANZAROTE, el art. 18.3 CE se inspira en el art. 10 de la Ley Fundamental de Bonn de 23 de mayo de 1949, aclarando *"…que se refiere exclusivamente a las comunicaciones privadas, quedando fuera del mismo las que se hacen por medio de la radio, imprenta, televisión u otro procedimiento destinado a la difusión de pensamiento a un número indeterminado de personas. Ello se deduce así de la relación que las comunicaciones aludidas en el artículo 18 tiene con el derecho a la intimidad, y que las otras comunicaciones no privadas y los derechos fundamentales relativos a las mismas aparecen específicamente regulados en el artículo 20 CE"*. Vid. Lanzarote Martínez, Pablo. *Intervención de las comunicaciones,* en Rives Seva, Antonio Pablo, y otros. *La Prueba en el proceso penal. Doctrina de la Sala Segunda del Tribunal Supremo.* 4ª Edición. Pamplona: Thomsom - Aranzadi, 2008, pág. 709.

[363] Como indica MARCHAL, *"ciertamente, la Constitución, en sus arts. 15 y 18.1, no prevé expresamente la posibilidad de un sacrificio legítimo de los derechos a la integridad física y a la intimidad (a diferencia, por ejemplo, de lo que ocurre con los derechos a la inviolabilidad del domicilio o al secreto de las comunicaciones (art. 18.2 y 3 CE), mas ello no significa que sean derechos absolutos, pues pueden ceder ante razones justificadas de interés general convenientemente previstas por la Ley, entre las que, sin duda, se encuentra la actuación del ius puniendi (STC 37/1989)"*. Vid. Marchal Escalona, Nicolás. *Policía Judicial y limitación de derechos fundamentales en el proceso penal.* Tesis Doctoral. Madrid: Universidad Nacional de Educación a Distancia, 2010, pág. 318.

[364] STS de 1 de marzo de 1996, resolviendo el Rec. 797/95, y 15 de marzo de 1996 (RJ 1996/1953).

La base jurídica de Derecho Internacional para la limitación de este precepto constitucional se halla en el art. 12 de la *Declaración de los Derechos Humanos de 10 de diciembre de 1948*, en el art. 17 del *Pacto Internacional por los Derechos Civiles y Políticos,* hecho en Nueva York el 19 de diciembre de 1966, y en el art. 8 del *Convenio Europeo para la protección de los Derechos Humanos y de las Libertades Fundamentales,* hecho en Roma el 4 de noviembre de 1950. En el derecho comunitario europeo hay que referirse a la *Carta de los Derechos Fundamentales de la Unión*, hallando su referencia en el art. II-67 de la Parte II del *Tratado por el que se establece una Constitución para Europa* del año 2004[365].

Para que el Estado de Derecho pueda injerirse legítimamente en los derechos fundamentales, el Tribunal Constitucional ha ido configurando progresivamente un *corpus* jurisprudencial en torno al principio ***de proporcionalidad***, considerando que la irreprochabilidad constitucional de la resolución judicial que arbitre medidas limitativas del derecho al secreto de las comunicaciones *"ha de expresar la finalidad de la misma (la actividad delictiva que se investiga) y las razones por las que la escucha de las conversaciones se presenta como un medio idóneo y necesario de investigación. Se requiere por ello que la resolución judicial exprese los indicios existentes de que se ha cometido un delito, sin que resulte en consecuencia justificable desde la perspectiva constitucional no ya, como se ha señalado, que la intervención telefónica constituya el instrumento inicial de indagación, sino que se proceda a la misma por la mera sospecha de que el delito se ha cometido. El secreto de las comunicaciones no puede ser desvelado para satisfacer sin base objetiva que surjan en la mente de los encargados de la investigación penal, por más legítima que sea esta aspiración, pues de otro modo se desvanecería la garantía constitucional"* [366].

Del anterior fragmento se extraen con nitidez los presupuestos constitutivos del principio de proporcionalidad que, con algún detalle, se van a tratar en este capítulo; un principio cuyo concepto jurídico puede definirse como:

[365] Vid. Lanzarote Martínez, Pablo. *Intervención de las…op. cit.*, pág. 709.
[366] Entre otras, véanse las SSTS 49/1999 de 5 de abril (RTC 1999, 49), 126/2000 de 16 de mayo (RTC 2000, 126), 123/2002 de 20 de mayo (RTC 2002, 123), 165/2005 de 20 de junio (RTC 2005, 165), 150/2006 de 22 de mayo (RTC 2006, 150) y 253/2006 de 11 de septiembre (RTC 2006, 253). Vid. Lanzarote Martínez, Pablo. *Intervención de las…op. cit.*, pág. 785 y ss.

> *"El principio constitucional en virtud del cual la intervención pública ha de ser «susceptible» de alcanzar la finalidad perseguida, «necesaria» o imprescindible al no haber otra medida menos restrictiva de la esfera de libertad de los ciudadanos (es decir, por ser el medio más suave y moderado de entre todos los posibles —ley del mínimo intervencionismo—) y «proporcional» en sentido estricto, es decir, «ponderada» o equilibrada por derivarse de aquélla más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto, en particular sobre los derechos y libertades. En suma, pues, la acción estatal —en cualquiera de sus formas de expresión posibles (acto administrativo, norma, resolución judicial) — debe ser útil, necesaria y proporcionada. A su vez, cada uno de los subprincipios que lo integran (utilidad, necesidad y proporcionalidad strictu sensu) requiere un juicio o análisis diverso en su aplicación: el medio ha de ser idóneo en relación con el fin; necesario —el más moderado— respecto de todos los medios útiles y proporcionada la ecuación costes-beneficios"*[367].

La noción de la proporción, como concepto jurídico orientado a la determinación de una respuesta justa ante la comisión de un ilícito, relacionada con la idea de justicia material, no es nueva en la Historia del Derecho, pues aparece ya en textos tan antiguos como lo es la *Carta Magna de Juan Sin Tierra de 1215*[368] y en la doctrina y textos jurídicos a lo largo de los tiempos[369].

Se trata además de un principio jurídico estrechamente vinculado con el ***derecho de policía***[370] en el ámbito administrativo, lo que también resulta predicable

[367] Vid. Barnés Vázquez, Javier. *El principio de proporcionalidad.* Cuadernos de Derecho Público, núm. 5, 1998, pág. 23.
[368] Vid. Marchal Escalona, Nicolás. *Policía Judicial…op.cit.,* pág. 36.
[369] Según aporta SIEIRA, "*Beccaria, en su obra "De los delitos y las penas", sostuvo que la pena proporcional a la culpabilidad era la única pena útil; y por su parte la Declaración de Derechos del Hombre y del Ciudadano de 1789 proclamaba que la ley no debía establecer otras penas que las estrictamente necesarias".* Vid. Sieira Mucientes, Sara. *El principio de proporcionalidad como juicio de necesidad y la debida intensidad de control en su aplicación al Legislador.* La Reforma del Tribunal Constitucional: actas del V Congreso de la Asociación de Constitucionalistas de España. Valencia, 2007, pág. 2.
[370] Sobre la prohibición de exceso para la autoridad gubernativa, vid. Ruiz Ruiz, Ramón y de la Torre Martínez, Lourdes. *Algunas aplicaciones e implicaciones del principio de proporcionalidad*. Revista Telemática de Filosofía del Derecho, nº 14, 2011, págs. 27-44 D.L. M-32727-1998 ISSN 1575-7382, pág. 30 y vid. Fernández Nieto, J. Principio *de proporcionalidad y derechos fundamentales: una perspectiva desde el derecho común europeo*. Madrid: Dykinson, 2008, pág. 281.

para el ejercicio de la función de policía judicial en todos aquellos aspectos que rigen su actuación[371]. Por ello, la solicitud de la PJE para injerirse en los derechos fundamentales de las personas en el curso de una investigación en sede penal y, particularmente, cuando se trate de proponer la limitación de los que gozan de la alta protección otorgada por el art. 18.3 CE, deberá cimentarse en todas aquellas razones de orden fáctico y técnico – la razonabilidad, en suma - que le permitan justificar su más estricta adecuación al principio de proporcionalidad. A la Autoridad Judicial le corresponderá, en los mismos términos, disponerlas con el alcance, extensión y limitaciones que estime procedentes, especialmente en la consideración de que la mayoría de las veces se tratará de ***casos difíciles***[372]**,** para los que el control de la proporcionalidad de tales medidas deberá conjurar cualquier asomo de duda que pueda oponerse a su pertinencia.

Pero, una vez anotadas las sucintas referencias de los párrafos anteriores, debe hacerse constar que el contenido jurídico de este importante principio con el que opera el derecho interno adquirió una mayor precisión tras la irrupción en los ámbitos jurídicos de lo que se denominó el ***test alemán***[373], basado en la aplicación de la Ley con adecuación a los ***requisitos de necesidad, idoneidad y proporcionalidad en sentido estricto***[374], o subprincipios conformadores de la proporcionalidad, como criterios

[371] MARCHAL indica a este respecto que *"no hay que olvidar que el principal campo del principio de proporcionalidad en el ámbito administrativo se encuentra en el Derecho de Policía, destacándose por la doctrina dos aplicaciones de este principio: a) una relación razonable, adecuada y no desproporcionada entre el fin perseguido por la actuación policial y los medios que se utilizan para lograr dicho fin; y, b) que en existiendo varias formas de actuar se debe optar por el medio que restrinja en menor medida los derechos de los particulares y permita conseguir el fin perseguido".* Vid. Marchal Escalona, Nicolás. 2010. *Policía Judicial…op.cit.,* pág. *32.* En el texto el autor se apoya en Aguado Correa, Teresa. *El principio de proporcionalidad en el derecho penal.* Madrid: EDERSA, 1999, pág. 82. Vid. González-Cuéllar Serrano, Nicolás. *Proporcionalidad…op.cit.*, pág. 29.

[372] Para BERNAL PULIDO *"…el principio de proporcionalidad es el criterio imprescindible para fundamentar con la mayor racionalidad posible las decisiones de control de la constitucionalidad de los límites de los derechos fundamentales en los casos difíciles (que son la mayoría), es decir, en los que no aparece a primera vista (tomando como referencia la semántica de la Constitución) si el límite del derecho es o no inconstitucional". Vid.* Bernal Pulido, Carlos. *El principio de proporcionalidad y los derechos fundamentales.* Madrid: 2006, págs. 251-486, citado por Sieira Mucientes, Sara. *El principio de proporcionalidad como juicio…op. cit.,* pág. 852.

[373] Como señalan RUIZ y DE LA TORRE, carente de una acogida explícita en los textos positivos recientes. Vid. Ruiz Ruiz, Ramón y de la Torre Martínez, Lourdes. *Algunas aplicaciones…op.cit.*, pág. 28.

[374] Aunque el principio proporcionalidad ha sido regularmente invocado en la jurisprudencia española, el test alemán como tal fue adoptado a mediados de los años noventa del pasado siglo a partir de la STC 66/1995. El profesor GONZÁLEZ BEILFUSS afirma que *"aunque la influencia germánica no ha sido reconocida explícitamente por parte del Tribunal Constitucional español, la incorporación literal de los requisitos de la Geeignetheit, Erforderlichkeit y Verhältnismässigkeit im engeren Sinne, que vienen siendo*

hermenéuticos orientados a la apreciación de la estricta justicia en que se han de fundamentar las resoluciones adoptadas por las personas u órganos legitimados al efecto.

Es, por tanto, en el derecho alemán de nuestro tiempo - con efectos inspiradores sobre el Derecho Constitucional Español[375] - cuando toma carta de naturaleza y donde goza además de rango constitucional "…*(lo que hace extender su ámbito de aplicación incluso hasta el Derecho Privado), alcanzando al derecho procesal penal a partir de la II Guerra Mundial, en el sentido de que las normas procesales penales debían ser limitadas desde fuera de ellas mismas, a través de los principios generales y de los valores constitucionales"*[376].

Sin embargo, aunque el principio de proporcionalidad no tiene una referencia expresa en la Constitución Española de 1978, su sustento normativo, comenzando por la proclamación de la libertad en el art. 1.1 CE[377] como valor superior del ordenamiento jurídico, de la interdicción o proscripción de la arbitrariedad contenida en el art. 9.3 CE[378,379] y de la dignidad[380], en el art. 10.1 CE, confirma un incuestionable

---

utilizados desde hace décadas por la doctrina y jurisprudencia alemanas, la ponen claramente de manifiesto". Vid. González Beilfuss, Markus. *Últimas tendencias en la interpretación del principio de proporcionalidad por parte del Tribunal Constitucional Español*. Cuadernos Aranzadi del Tribunal Constitucional núm. 11, 2003, págs. 2 y 8. Vid. Barnés Vázquez, Javier. *Introducción al principio de proporcionalidad en el Derecho comparado y comunitario.* Revista de Administración Pública núm. 135, págs. 485 y ss*,* 1994. Vid. Pedraz Penalva, Ernesto y Ortega Benito, Victoria. *El principio de proporcionalidad y su configuración en la jurisprudencia dle Tribunal Constitucional y literatura espacializada alemanas.* El Poder Judicial núm. 17, 1990, págs. 69-89

[375] Según SIEIRA, *"en el derecho constitucional alemán se introduce a partir de la Ley fundamental de Bonn de 1949, en cuyo parágrafo 19.2 se alude a los límites de la intervención legislativa en los derechos fundamentales, que debe en todo caso respetar el contenido esencial de éstos, precepto que ha inspirado directamente el contenido del art. 53.2 de la CE de 1978".* Vid. Sieira Mucientes, Sara. *El principio de proporcionalidad como juicio…op. cit.,* pág. 2.

[376] Vid. González-Cuéllar Serrano, Nicolás. *Proporcionalidad…op.cit.,* pág. 24 y 25, citado por Marchal Escalona, Nicolás. 2010. *Policía Judicial…op.cit.,* pág. 36.

[377] Vid. Cobo del Rosal, Manuel y Vives Antón, Tomás Salvador. *Derecho Penal. Parte General.* Valencia, 1987, pág. 63.

[378] Art. 9.3 CE: *"La Constitución garantiza el principio de legalidad, la jerarquía normativa, la publicidad de las normas, la irretroactividad de las disposiciones sancionadoras no favorables o restrictivas de Derechos individuales, la seguridad jurídica, la responsabilidad y la interdicción de la arbitrariedad de los poderes públicos".*

[379] En sus comentarios sobre el art. 9.3 CE, PECES-BARBA hace algunas puntualizaciones de sumo interés que refuerzan la vertiente de claros límites constitucionales del principio de proporcionalidad como herramienta hermenéutica del Derecho, adaptable y en constante vigencia siempre que se ajuste a tales límites, ya que *"son principios que se refieren a aspectos o parcelas del ordenamiento que sirven para interpretar las normas de esas parcelas del ordenamiento. Son expresiones, en ellas, de un sistema jurídico que se identifica por tener como hecho fundante básico un Estado Social y democrático de Derecho y como contenido material a desarrollar los valores superiores. Es la llamada moral interna del*

enraizamiento en su espíritu, especialmente si se sigue la teoría de ALEXY de que "*lo "desproporcionado", por definición, daña el contenido esencial de los derechos (teoría relativa del contenido esencial)*"[381,382].

En este sentido, aunque GONZÁLEZ-CUÉLLAR disiente en que la constitucionalidad del principio se funde en los arts. 1, 9.3 y 10 CE, coincide con los demás autores consultados en que donde verdaderamente se debe asentar es en los artículos que proclaman los derechos fundamentales y las libertades públicas[383].

---

derecho […] de donde se deduce que no todos los principios constitucionalmente relevantes se hallan expresamente mencionados en un determinado precepto […] prohibición expresa de arbitrariedad de los poderes públicos […] recibe[n] su savia normativa del vigor constitucional en la protección de los derechos fundamentales". Vid. Peces-Barba Martínez, Gregorio. *Los valores superiores.* Madrid, 1986, citado por Vid. González-Cuéllar Serrano, Nicolás. *Proporcionalidad…op.cit.*, pág. 55. En este mismo sentido, Vid. Marchal Escalona, Nicolás. 2010. *Policía Judicial…op.cit.,* pág. 41.

[380] En materia del secreto de las comunicaciones, la estrecha relación entre la intimidad y la dignidad se reconoce en la STS de 20 de febrero de 1999 (RJ 1999, 512) del Rec. 298/98. En la jurisprudencia del TC, con gran vigor, se resume en la STC 173/2011, de 7 de noviembre de 2011, donde se afirma que *"según hemos venido manifestando, el derecho a la intimidad personal, en cuanto derivación de la dignidad de la persona (art. 10.1 CE), implica la existencia de un ámbito propio y reservado frente a la acción y el conocimiento de los demás, necesario, según las pautas de nuestra cultura, para mantener una calidad mínima de la vida humana (SSTC 207/1996, de 16 de diciembre, FJ 3; 186/2000, de 10 de julio, FJ 5; 196/2004, de 15 de noviembre, FJ 2; 206/2007, de 24 de septiembre, FJ 4; y 159/2009, de 29 de junio, FJ 3)".*

[381] Vid. Alexy, Robert. *Teoría de los derechos fundamentales.* Madrid: Centro de Estudios Constitucionales, 1993, pág. 286 y ss, citado por Sieira Mucientes, Sara. *El principio de proporcionalidad…op.cit.,* pág. 849.

[382] Así lo reconoce el TC, entre otras, mediante las SSTC 62/1982, FJ 5º; 66/1985, FJ 1º; 19/1988, FJ 8º; 113/1989, FJ 3º; 85/1992, FJ4º; 215/1994, FJ 4º; 50/1995, FJ 7º, 55/1996, FJ 3º; 136/1999, FJ 22º; 202/1999, FJ 6º, según la recopilación efectuada por Sieira Mucientes, Sara. *El principio de proporcionalidad…op.cit.,* pág. 849.

[383] Esta idea la expresa GONZÁLEZ-CUÉLLAR con el siguiente texto en referencia a los artículos donde se asienta la constitucionalidad del principio de proporcionalidad: *"…[el] art. 14 al 29 ó 30.2 [CE] como medio de defensa de los ciudadanos, frente a las injerencias desproporcionadas que afecten a sus derechos fundamentales, lo que permitiría la interposición de un recurso de amparo ante el TC, según los arts. 53.2 CE y 41 LOTC…la importancia práctica de la protección constitucional del principio de proporcionalidad no se encuentra en su posible apoyo los arts. 1, 9.3 y 10 CE, sino en la exigencia de su respeto impuesta por los preceptos constitucionales que garantizan los derechos fundamentales y las libertades públicas y que permiten la interposición del recurso de amparo en su defensa…En virtud de lo establecido en los arts. 1, 9.3 y 10 CE, reclaman la utilización de criterios muy estrictos en el enjuiciamiento de las medidas restrictivas que puedan afectar a su contenido, e imponen a los poderes públicos una gran mesura en su limitación. La ausencia de los presupuestos o requisitos de proporcionalidad en la regulación o adopción de injerencias estatales vulneraría el precepto constitucional que tutele el derecho fundamental o la libertad pública restringida".* Vid. González-Cuéllar Serrano, Nicolás. *Proporcionalidad…op.cit.*, pág. 53.

Por ello, siguiendo a MARCHAL y LÓPEZ GONZÁLEZ, el principio de proporcionalidad operaría como un principio general del Derecho, bajo los presupuestos indicados por este último autor[384]:

- *"El principio de proporcionalidad como portador de una serie de valores materiales básicos de nuestro Ordenamiento jurídico: Libertad y dignidad.*
- *El principio de proporcionalidad posee un fundamento institucional para los fines que nuestro Ordenamiento jurídico atribuye a la Administración ex art. 103.1 y 106.1 CE.*
- *Sirve de mecanismo básico del principio de legalidad, en el proceso regular de producción normativa y de aplicación del Derecho.*
- *Como medida de las potestades representa un límite sustancial a la actividad de la Administración.*
- *Cumple la triple función informadora, interpretativa e integradora del Derecho en relación con la actividad de la Administración".*

En la configuración del principio de proporcionalidad se deben contemplar también las obligaciones que para España nacen de los tratados internacionales suscritos sobre determinados derechos y que la vinculan *ex* art. 10.2 CE, lo que es reconocido por el propio Tribunal Constitucional en su jurisprudencia[385].

De igual modo, el principio de proporcionalidad *"se constituye en un ejemplo claro de Derecho público europeo emergente"* cuyo asentamiento se halla, de un lado, en los arts. 8 y 11 CEDH, en cuanto a que *"las injerencias en las libertades que consagra [el CEDH] sólo son admisibles en cuanto constituyen medidas necesarias en una sociedad democrática para los objetivos que se precisan"* y, de otro, en la jurisprudencia del TEDH, proclamando que *"los Estados miembros tienen un margen de libertad para elegir las medidas y restricciones que juzguen necesarias, reservándose, no obstante, este Tribunal [el TEDH] la potestad de comprobar si en cada caso se*

[384] Vid. López González, José. *El principio general de proporcionalidad en Derecho Administrativo.* Sevilla: Instituto García Oviedo, 1988, pág.42.
[385] SSTC 50/1995, FJ 7º y 157/1997, FJ 2º. Vid. Sieira Mucientes, Sara. *El principio de proporcionalidad…op.cit.,* pág. 849.

respetan las exigencias derivadas de la proporcionalidad", doctrina que ha aplicado en numerosas ocasiones con efectos sobre el derecho interno[386].

En al ámbito de la UE, se puede encontrar también una referencia expresa en el Tratado de Lisboa (en su art. 3 ter y en el "*Protocolo para la aplicación del principio de subsidiariedad y proporcionalidad"), y* en el art. 49 de la Carta de Derechos Fundamentales de la Unión Europea[387].

2. Proporcionalidad e intimidad y secreto de las comunicaciones

La doctrina es prácticamente unánime en considerar el derecho al secreto de las comunicaciones como uno de los bienes jurídicos merecedores de la mayor cota de protección dentro del ordenamiento constitucional español y que excede, en su concepción, al propio derecho genérico a la intimidad recogido en el art. 18 CE, por más que aquel quede expresamente contenido en uno de sus apartados.

Visto así, en el continente que representa este trascendental artículo se tutela un derecho que brilla con especial intensidad sobre los demás: el derecho al secreto de las comunicaciones.

Así lo expresa GIMENO – a quien seguiré profusamente en la materia - diciendo que

> *"Aun cuando dicho derecho [el del secreto de las comunicaciones] claramente se relacione con el derecho fundamental a la «intimidad» (y de aquí que no en vano sea el mismo art. 18 CE el que, en su primer párrafo, proteja*

[386] Entre otras, véanse las SSTEDH de 7 de diciembre de 1976 (TEDH 1976, 6) - *Caso Handyside* -, de 26 de abril 1979 - *Caso del Sunday Times* -, de 24 de marzo de 1988 (TEDH 1988, 2) - *Caso Olsson* -, de 20 de junio de 1988 - *Caso Schonenberber y Durmaz* - y de 21 de junio de 1988 (TEDH 1988, 3) - *Caso Berrehab* -. Vid. Lanzarote Martínez, Pablo. *Intervención de las…op. cit.*, pág. 803 y ss.

[387] Así lo señalan RUIZ y DEL LA TORRE, con interesantes referencias a BARNES y HÄBERLE. Vid. Ruiz Ruiz, Ramón y de la Torre Martínez, Lourdes. *Algunas aplicaciones…op.cit.*, págs. 32 y 33. También, vid. Barnés Vázquez, Javier. *Introducción al principio de proporcionalidad…op.cit.,* y Häberle, Peter. *Derecho Constitucional común europeo*. Revista de Estudios Políticos, núm. 79, 1993, págs. 7 y ss.

también este derecho fundamental), no se identifica absolutamente con él, sino que posee un contenido mucho más amplio"[388].

De acuerdo con esta consideración, en todo este estudio subyace el apoyo a la idea expresada pero, siempre, con la pretensión de, sin distorsionarla, ofrecer una nueva visión sobre el contenido del derecho al secreto de las comunicaciones – siempre vigente -, considerándolo perfectible en su interpretación jurídica si se ha de poner en relación con la realidad imperante en nuestra sociedad actual y el desarrollo de las TIC que, si bien de un lado exige un absoluto respeto a las expresiones más sensibles de la intimidad que proclama, de otro, está urgido de una mayor comprensión del significado actual del concepto de comunicación y, consecuentemente, de una actualización del derecho de injerencia, de forma que, preservando con decisión los valores democráticos que propugna el respeto a la intimidad, se alcancen a precisar con idéntico espíritu democrático también sus más exactos límites[389].

En este sentido, urge precisar con especial determinación cuándo se produce una efectiva limitación del derecho al secreto de las comunicaciones – y por tanto merecedora de la más radical protección - y cuándo, en realidad, con la actividad investigativa simplemente se están limitando otros aspectos de la intimidad, como los que afectarían únicamente al derecho a la protección de datos o a la autodeterminación informativa que, aunque estén en este caso relacionados con el ejercicio del derecho al secreto de las comunicaciones – en tiempo real o diferido - y

[388] Para esta afirmación, GIMENO se apoya en la siguiente jurisprudencia: SSTC 114/1984 de 29 noviembre, 34/1996 de 11 marzo, 127/1996 de 9 julio, 58/1998 de 16 marzo, 123/2002 de 20 mayo, 70/2002 de 3 abril, 56/2003 de 24 marzo), donde se extiende la protección más allá del contenido material de la intervención, cuestión esta que se sitúa en la raíz de los problemas objeto de estudio. Vid. Gimeno Sendra, Vicente. *La intervención de las comunicaciones,* en Marchal Escalona, Nicolás (Director). *Manual de lucha…op. cit.,* pág. 570.

[389] Con un pronunciamiento de extraordinaria obviedad, la STC 173/2011, de 7 de noviembre, dice que *"se deduce que el legislador ha de habilitar las potestades o instrumentos jurídicos que sean adecuados para que, dentro del respeto debido a los principios y valores constitucionales, las fuerzas y cuerpos de seguridad del Estado cumplan con esta función de averiguación del delito".* En la en la STC 70/2002, de 3 de abril, FJ 10, se refiere a las obligaciones respecto de la recogida de vestigios de la PJE como"*una habilitación legal específica que faculta a la policía para recoger los efectos, instrumentos y pruebas del delito y ponerlos a disposición judicial y para practicar las diligencias necesarias para la averiguación del delito y el descubrimiento del delincuente".* Mal se puede trasladar a la práctica este espíritu si la disociación entre la realidad criminal y la leyes procesales se hace cada vez más extensa e insalvable.

aún siendo también acreedores de una alta protección constitucional se verifique esta, decididamente, de una forma sensiblemente menos intensa[390].

En consecuencia, la apreciación de la proporcionalidad relativa a la legítima instauración de determinadas medidas limitativas del derecho constitucional a la intimidad debe estar sujeta a criterios de graduación ajustados, con la mayor precisión posible, a la trascendencia que en cada caso racionalmente se evidencie.

Sin embargo, la anterior tarea se antoja hercúlea si se asumen como inmutables – sagradas, podría decirse - las dominantes posiciones doctrinales y jurisprudenciales que inundan con aparente radicalidad el contenido jurídico-formal del derecho al secreto de las comunicaciones.

Abundando en esta cuestión, GIMENO, cuando identifica el bien jurídico protegido por el secreto de las comunicaciones, dice que es *"el derecho de los titulares a mantener el carácter reservado de una información privada o, lo que es lo mismo, a que ningún tercero pueda intervenir en el proceso de comunicación y conocer de la idea, pensamiento o noticia transmitida por el medio"*[391], con lo que parece centrar la idea de la protección, precisamente, en la preservación del secreto sobre el ***contenido material*** de la comunicación en sus aspectos más genuinamente humanos, esto es, en sus ***ideas, pensamientos y noticias***.

En efecto, el concepto de ***intimidad***, cuya protección constitucional se proclama en el art. 18 CE, está directa y estrechamente vinculado con *lo humano*. Su contenido semántico se encuentra en la segunda acepción del diccionario, donde se dice que la intimidad es la *"zona espiritual íntima y reservada de una persona o de un*

[390] No obstante, debe tomarse en consideración la transcendencia de la limitación de estos derechos. En este sentido, para OLIVER, la protección de datos "*constituye el derecho fundamental característico de esa faceta del mundo social que comúnmente llamamos Sociedad de la Información"*. Vid. Oliver Lalana, D. *El derecho fundamental «virtual» a la protección de datos. Tecnología transparente y normas privadas*, *Diario La Ley*, núm. 5592, 22 de julio de 2002. Oliver Lalana, D. *El derecho fundamental «virtual» a la protección de datos. Tecnología transparente y normas privadas*, *Diario La Ley*, núm. 5592, 22 de julio de 2002, pág. 1.

[391] Vid. Gimeno Sendra, Vicente. *La intervención de las comunicaciones,* en Marchal Escalona, Nicolás (Director). *Manual de lucha…op. cit.,* pág. 570.

grupo, especialmente de una familia" y que ***íntimo*** es, según su primera acepción, *"lo más interior o interno"*[392].

La lógica que se deduce de los párrafos precedentes es que la vigorosa protección constitucional se instituye sobre las comunicaciones íntimas de las personas, que deberán ser secretas *salvo resolución judicial* y no sobre otra cosa.

Las diferencias entre ***intimidad*** y ***secreto***[393] **–** que deben quedar a estos efectos perfectamente sentadas -, según la doctrina, son razonablemente nítidas.

En efecto, a propósito del análisis del art. 197 CP, la Sala Segunda del Tribunal Supremo (STS 534/2011 de 10 de junio), hizo las siguientes afirmaciones:

> *"En la STS 666/2006, de 19 de junio, se dice que "la idea de secreto en el art. 197,1º Cpenal resulta conceptualmente indisociable de la de intimidad" que es, a su vez, "ese ámbito propio y reservado frente a la acción y el conocimiento de los demás" (SSTC 73/1982 y 57/1994, entre muchas). En este sentido, se ha dicho, y es universalmente aceptado, que el de intimidad es un concepto psicológico que remite a ese "mundo propio" en el que cada quien desarrolla su "vida interior". Por tanto, un reducto que está más allá de la privacidad y que conecta con los estratos más profundos de la personalidad, de la que es primera manifestación…*
>
> *…En efecto, pues el de intimidad es un concepto, ético-psíquico y, por eso, cabe decir, material o sustantivo; mientras el de secreto es un artificio jurídicoformal, puesto constitucionalmente al servicio de una diversidad de bienes jurídicos, y aquí, concretamente, de la primera, para tratar de preservarla o asegurarla cuando, por salir de su espacio original y entrar en el de la comunicación, resulta más vulnerable y debe ser más intensamente protegida. En este sentido y, en rigor, el término "secretos" yuxtapuesto al de "intimidad" en el art. 197,1º Cpenal, podría decirse que no añade nada a la segunda, o nada realmente significativo en el plano de los contenidos".*

[392] Su tutela, además de lo proveído en sede penal, se garantiza a través de la Ley Orgánica 1/1982, de 5 de mayo, *de Protección Civil del Derecho al Honor, a la Intimidad Personal y Familiar y a la Propia Imagen*.

[393] También, vid. Gimeno Sendra, Vicente. *La intervención de las comunicaciones,* en Marchal Escalona, Nicolás (Director). *Manual de lucha…op. cit.,* pág. 570.

La STS comentada, centrada en el acceso de un profesor a los correos electrónicos de sus compañeros para sustraerles sus documentos académicos, contiene además algunos pronunciamientos de un extraordinario interés, ya que reflejan, con enjundiosos razonamientos, la necesidad que tiene el Derecho de precisar el alcance y grados del sacrificio que determinadas conductas puedan conllevar, lo que, a su vez, exige la correcta identificación del bien jurídico protegido puesto en peligro, que no implicará necesariamente un ataque a la intimidad o al secreto (una revelación que sería eventualmente punible desde el art. 197 CP) sino, como en esta concreta ocasión se evidenció, únicamente a la privacidad en relación con un acceso ilícito a algunos archivos protegidos por determinados derechos de propiedad intelectual[394].

Consecuentemente, y haciendo una interpretación extensiva de esta posición jurisprudencial, será necesario, en todos los casos, identificar con precisión el bien jurídico efectivamente atacado.

La doctrina contenida en esta sentencia, por tanto, permitiría discernir análogas categorías y grados cuando se tratase de analizar la injerencia en los contenidos material y formal de una comunicación, cuyo objetivo no correspondiese a una comunicación personal o íntima (es decir, un ataque orientado a *"la finalidad de ("para") franquear el umbral de la intimidad de otro",* como se dice en la STS), ni su

[394] Dice la sentencia: *"En el supuesto de esta causa, lo que resulta de los hechos es que el acusado, valiéndose de algún medio técnico, "accedió a los correos electrónicos" de algunos colegas, profesores universitarios, que la sala de instancia califica de "buzones [...] institucionales", que no se utilizaban de forma personal. No se dice en la sentencia, pero a tenor de alguna información que consta en los recursos y también en la causa, no cabe excluir que, no obstante, aquellos pudieran ser también objeto de algún uso de este último carácter. Pero nunca el propio del medio y tampoco el prioritario. Una circunstancia que no puede dejar de ser valorada.*
De este modo, al tratarse de los correos profesionales de quienes lo eran de una dedicación académica; y teniendo en cuenta que, a tenor de lo que consta en la sentencia, tal resultó ser la vertiente objeto del interés del acusado, lo realmente perseguido por este fue obtener información de actuaciones propias del trabajo universitario, es decir, de la actividad de aquellos como docentes o investigadores, de sus programas, lecciones, etc. Materias, por tanto, privadas y no íntimas en sentido propio, y que, en consecuencia, podrían tener ubicación en el marco de la propiedad intelectual, pero no en el que es objeto de tutela por el art. 197,1º Cpenal.
Siendo así, si en el curso del desarrollo de la conducta ilegítima que se enjuicia, el acusado pudo haber invadido, ocasionalmente, esa otra esfera, por razón de la calidad más personal que profesional de algún mensaje; pero incluso en este caso, su acción quedaría fuera de las previsiones del precepto".
Más adelante se incluye un estudio fenomenológico sobre la diversidad de casos que apoyarían la idea expresada y que son reflejo de los profundos cambios sociales en el uso de las TIC que motivan las propuestas que se dirán.

finalidad fuera la de vulnerar secreto alguno, todo ello por tratarse de un uso de las comunicaciones del todo ajeno a su propósito primario, esto es, a facilitar la comunicación entre personas y que consistiesen, en realidad, en cualquiera de los usos distintos que se describen en este estudio[395].

Pero en lo que realmente interesa, una vez discernido lo intimo (*concepto ético-psíquico, material*) de lo secreto (*artificio jurídico-formal*)[396], es aprehender la trascendencia de uno u otro concepto en relación con la cuestión de la proporcionalidad en la limitación del derecho al secreto de la comunicaciones, pues todo indica que, tanto el TC como el TEDH, han elaborado su doctrina dotando de un contenido formal a la cuestión del secreto[397], haciendo que lo que se proteja, más que el contenido material transmitido – el mensaje -, sea el canal por el que se transmite (del que se pretende excluir a terceros de su conocimiento), es decir, las redes públicas de comunicaciones y los dispositivos que permiten accederlas.

Este punto de vista de la jurisprudencia es sugerente de la estrecha vinculación que se establece entre lo íntimo y lo secreto, relación que se rompe, desasistida de razón, si se inunda de radicalidad el concepto de "lo secreto" y se convierte su instauración formal en una finalidad en sí misma, ajena a la realidad material a la que debe favorecer.

Por ello, el secreto, bajo determinadas circunstancias de naturaleza material – y, desde luego, las TIC proporcionan algunos argumentos al efecto -, debe ser objeto de una profunda ponderación de modo que se aplique con firmeza allí donde el espíritu del art. 18 CE lo haga preciso y revisable donde se compruebe, con idéntico

[395] En este sentido, concluye finalmente el tribunal sentenciador, en relación con el eventual propósito del actor de atacar la intimidad de otro, que: *"En efecto, pues, como se explica en la sentencia de esta sala 237/2007, de 21 de marzo, el art. 197,1º Cpenal requiere un tipo de dolo que, además de incorporar el conocimiento de los elementos del tipo objetivo, integre el especial elemento subjetivo consistente en que la acción haya sido ejecutada con la finalidad de ("para") franquear el umbral de la intimidad de otro. Por lo que, si en el caso que se examina -en el que, a tenor de los hechos, lo deliberadamente invadido fue una cierta privacidad propia de los afectados como profesionales de la enseñanza- se hubiera producido alguna lesión de su intimidad, esta, en cuanto no cubierta directamente por ese "para", sería imputable, a lo sumo, a un dolo eventual y, por eso, no podría resultar penalmente relevante a los efectos del precepto aquí tomado en consideración".*

[396] También, vid. Rodríguez Lainz, José Luis. *El principio de proporcionalidad…op. cit.*

[397] *"El concepto de secreto en el art. 18.3 tiene un carácter formal, en el sentido de que se predica de lo comunicado, sea cual sea su contenido y pertenezca o no el objeto de la comunicación misma al ámbito de lo personal, lo íntimo o lo reservado"* (SSTC 114/1984, de 29 de noviembre, FJ 7 y 34/1996, de 11 de marzo, FJ 4). Esta doctrina se vuelve a reiterar en la más reciente STC 70/2002, de 3 de abril, FJ 9.

rigor, su desvinculación de lo íntimo. Todo ello permitiría, sin duda, una aplicación bien ponderada del principio de proporcionalidad, dotándolo de la necesaria perspectiva que permita su más exigente adecuación a las realidades comunicativas sobre las que se haya de intervenir.

En línea con la doctrina comentada, la alta protección constitucional otorgada por el art. 18.3 a las comunicaciones personales afecta a las que se produzcan mediante el uso de los *"servicios especialmente concebidos para la comunicación entre personas distantes"*[398] (categoría en la que se englobarían sin duda las comunicaciones electrónicas), por lo que la garantía sobre el secreto de las comunicaciones se extendería, según VEGAS "*…a aquellas en que estén presentes los tres elementos examinados, esto es:*

1) *Que la transmisión del mensaje se lleve a cabo por medio de un servicio interpuesto entre el emisor y el receptor cuyo funcionamiento escapa al control de estos sujetos.*
2) *Que se trate de comunicaciones cerradas, esto es, dirigidas a una o varias personas determinadas de forma que el emisor del mensaje pueda controlar el sujeto o sujetos que lo recibirán.*
3) *Que la comunicación se canalice a través de servicios especialmente concebidos para la transmisión de mensajes entre personas distantes"*[399].

Según las razonamientos expuestos, sería sobre el segundo punto de los enumerados por el autor comentado donde podría encontrar su encaje la idea expresada en los párrafos anteriores, pues la casuística propiciada por las TIC excede con mucho al contenido descrito en este concreto requerimiento, en el que se describe un entorno cerrado donde los interlocutores autorizados, en número limitado, interactúan de un modo controlado transmitiéndose contenidos de naturaleza íntima.

[398] Extráigase de esta definición de VEGAS su clara precisión de que la comunicación se produce "entre personas" y que estás se hallan "distantes" entre sí. Este autor, para sostener la restricción del ámbito de aplicación del art. 18.3 CE se apoya indirectamente en la STC 281/2006, FJ 3º y, con cierta inestabilidad, en la STS de 9 de diciembre de 2008 sobre el Recurso 848/2008. Para este mismo autor, estarían igualmente excluidas de la protección del art. 18.3 CE *"…todas [las comunicaciones] las que se realicen mediante el empleo de cualquier otra herramienta informática o de red no concebida específicamente para la transmisión de mensajes".* Vid. Vegas Torres, Jaime. *Obtención de pruebas en ordenadores personales y derechos fundamentales en el ámbito de la empresa.* Madrid: Universidad Rey Juan Carlos. Cátedra de investigación financiera y forense KPMG-URJC, 2011, pág. 41 y ss.

[399] Vid. Vegas Torres, Jaime. *Obtención de pruebas…op. cit.,* pág. 43.

3. Estructuración del principio de proporcionalidad

Hechas las consideraciones incluidas en los apartados precedentes – con expresa referencia a la consolidada posición del TC sobre la proporcionalidad de las medidas limitativas de derechos - y habiendo definido el principio de proporcionalidad, la claridad expositiva y la estructuración conceptual que acompañan a las aportaciones de GONZÁLEZ-CUÉLLAR sobre la materia, aconsejan comenzar este apartado con una remisión literal a su formulación teórica básica y que servirá, a la vez, de introducción a los apartados siguientes, en los que se profundizará en su contenido jurídico:

> *"Los presupuestos para la admisibilidad de las injerencias, desde la perspectiva de la proporcionalidad, son la legalidad y la justificación teleológica. Dentro de los requisitos pueden distinguirse aquellos que son extrínsecos a las medidas, como el requisito subjetivo de judicialidad y el formal de motivación, de los que podrían denominarse intrínsecos, constituidos por los subprincipios de idoneidad (adecuación de la medida a sus fines), necesidad (intervención mínima) y proporcionalidad (ponderación de intereses y "concretización") en sentido estricto"*[400].

En efecto, la consideración de unos presupuestos (***legalidad y justificación teleológica***) y la distinción entre requisitos intrínsecos (***necesidad, idoneidad y proporcionalidad en sentido estricto***) y extrínsecos (***judicialidad y motivación***) facilitan la percepción conceptual y la reflexión sobre el contenido y alcance de este trascendental principio con el que operará la PJE, en lo que le corresponda, en el ejercicio práctico de la limitación de los derechos fundamentales[401].

[400] Vid. González-Cuéllar Serrano, Nicolás. *Proporcionalidad…op.cit.*, págs. 17, 25 y 69.

[401] El TS resume los requisitos para una intervención telefónica en la STS de 28 de noviembre de 2001 (RJ 2002, 1985). En sentencias posteriores los confirma: SSTS de 28 de febrero de 2007 (JUR 2007, 98400), de 15 de marzo de 2007 (RJ 2007, 2126), 17 y 25 de abril de 2007 (RJ 2007, 3265 y 3327), de 23 y 29 de mayo de 2007 (RJ 2007, 5099 y 3597) y 18 de junio de 2007 (RJ 2007, 4916). El enunciado de estos requisitos es el siguiente: *Habilitación judicial, motivación, excepcionalidad, subsidiariedad y huida del automatismo, imprescindibilidad o necesidad, proporcionalidad, duración razonable de la medida, prórrogas, transcripción bajo fe judicial y naturaleza de la prueba.* Vid. Lanzarote Martínez, Pablo. *Intervención de las…op. cit.*, pág. 792 y ss.

B. Presupuestos del principio de proporcionalidad

Los presupuestos del principio de proporcionalidad son los de legalidad y justificación teleológica, como elementos que anteceden en la valoración de la proporcionalidad de una medida limitativa de derechos fundamentales.

Por ello, cuando se identifica la necesidad de intervenir en un determinado ámbito de la vida social que conlleve la instauración de medidas de esta naturaleza debe, en primera instancia, ponderarse su adecuación a la Ley en razón de las finalidades que se pretendan alcanzar. Se trata, consecuentemente, de conceptos intensamente vinculados entre sí y que carecerían de sentido si no se pusiesen en relación como modo de enfocar la intervención del Derecho en la vida pública.

La vía para asentar este proceso en el devenir democrático de la sociedad no es otra que la de legislar la forma en que esto se producirá, vinculando a los poderes públicos de forma que, sin renunciar al justo margen de discrecionalidad inherente a la valoración de la proporcionalidad que les debe acompañar en sus decisiones, cuenten con el respaldo de una sólida y eficaz apoyatura en el derecho positivo.

Sobre estos presupuestos, en referencia a las formas de limitación del secreto de las comunicaciones y con carácter previo, se identifican dos grandes áreas de interés que comprometen la viabilidad del Estado para ejercer su legítimo derecho de injerencia:

En primer lugar, pese a la espectacular evolución de las TIC en materia de comunicaciones electrónicas, caracterizada por una gran diversificación en las formas de establecerlas y en su universal, masiva y fácil accesibilidad por los ciudadanos, no se constata una variación sustancial en las finalidades esenciales del derecho de injerencia en el secreto de las comunicaciones personales, esto es, sigue interesando al proceso penal el acceso a su contenido material y formal en la misma medida en que, a la aparición de la telefonía fija, se consideró ajustado a Derecho y proporcional el que el Estado se garantizase tal posibilidad.

En segundo lugar, la legislación procesal que ampara la intervención de las comunicaciones resultó defectuosa desde su misma fecha de concepción (reforma de la LCRIM operada mediante una ley orgánica de 1988[402]), época en que el mercado de las telecomunicaciones estaba limitado únicamente a la telefonía fija, lejos aún de emerger la telefonía móvil y de imaginar siquiera las comunicaciones a través de Internet, adoleciendo el art. 579 LCRIM de la adecuada calidad jurídica exigible a un Estado Democrático hasta el punto de merecer la reprobación del TEDH. Además, ante los nuevos retos de las TIC, especialmente por la irrupción de la telefonía móvil e Internet, deviene completamente obsoleta para asumir solventemente sus especiales características mediante su aplicación analógica. De esta constatación, surge la necesidad de legislar mejor.

1. Presupuesto formal de legalidad

El ***presupuesto formal de legalidad***[403], como principio fundamental del Derecho Público, asegura que toda medida limitativa de derechos debe estar prevista en la Ley. El CEDH así lo formula también al reclamar *"que las medidas limitativas estén "previstas en la ley", tiendan "a fines legítimos" y sean "necesarias en una sociedad democrática""*[404], con lo que, en el primer concepto hace una referencia directa al principio de legalidad y, en el segundo y tercer conceptos, describe respectiva y someramente los principios de justificación teleológica y de proporcionalidad propiamente dichos.

---

[402] *Ibídem*.

[403] Es jurisprudencia constante del TEDH que las medidas limitativas de los derechos tutelados por el CEDH se encuentren previstas por la ley y sean necesarias en una sociedad democrática para alcanzar ciertos fines legítimos previstos. En este sentido, vid. STEDH *Caso Handsyde* 07/12/76, STEDH *Caso The Sunday Times* 26/04/79 y STEDH *Caso Barthold* 25/03/85, entre otras.

[404] Como indica GONZÁLEZ-CUÉLLAR, *"así, los arts. 5, 8, 9, 10 y 11 CEDH garantizan los derechos a la libertad y seguridad, al respecto de la vida privada y familiar, del domicilio y de la correspondencia, a la libertad de pensamiento, conciencia y religión y a la libertad de expresión, reunión y asociación, establecen listas taxativamente limitadas de finalidades que justifican su restricción, si bien se hallan contenidos en conceptos indeterminados muy generales"*. Vid. González-Cuéllar Serrano, Nicolás. *Proporcionalidad…op.cit.*, pág. 99 y ss.

Las garantías que nacen del principio de legalidad[405], basadas en la exigencia de una *lex previa, scripta et stricta*[406], tienen su manifestación más práctica y cotidiana en la verificación de los requisitos de certeza y seguridad jurídica puestos al alcance de los ciudadanos para que sepan cómo adecuar su conducta a la legalidad y en qué medida les cabe esperar que sean restringidos sus derechos fundamentales en caso de incurrir en ilícitos.

Este último aspecto es de una extraordinaria importancia a la hora de resolver sobre la procedencia de una determinada medida limitativa de derechos, haciendo consciente a la PJE del papel que juega en todo momento para garantizar la claridad y transparencia de sus procedimientos técnicos y de su idoneidad para alcanzar las finalidades perseguidas y, especialmente, cuando su instauración deba ser objeto de un mandato judicial, de forma que todo este proceso no arroje dudas sobre su previsibilidad y procedencia.

---

[405] Sobre el principio de legalidad, GONZÁLEZ-CUÉLLAR afirma que *"la doctrina penalista distingue dentro del principio de legalidad cuatro garantías y manifiesta una triple exigencia respecto a la norma que las cumpla. Las garantías son:*

- *Garantía criminal: nullum crimen sine lege.*
- *Garantía penal: nulla poena sine lege*
- *Garantía de ejecución.*
- *Garantía jurisdiccional o procesal"*.

Vid. González-Cuéllar Serrano, Nicolás. *Proporcionalidad…op.cit.*, pág. 71 y ss.

[406] Sobre la *lex stricta* – especialmente importante para valorar la adecuación al principio de legalidad de una determinada medida limitativa de derechos fundamentales -, MIR dice que *"contiene un "mandato de determinación", como aspecto material del principio de legalidad que trata de evitar la burla del significado de seguridad y de garantía de dicho principio, burla que tendría lugar si al ley se limitase a utilizar cláusulas generales absolutamente indeterminadas"*. Por ello, es extraordinariamente importante el conjurar la indeterminación de los preceptos jurídicos en el derecho positivo y, máxime, cuando lo que esté en juego sean derechos fundamentales. Vid Mir Puig, Santiago. *Introducción a las bases del Derecho Penal. Derecho Penal. Parte General.* Barcelona, 1976, citado por González-Cuéllar Serrano, Nicolás. *Proporcionalidad…op.cit.*, pág. 78. En cuanto a la posición relativa del ciudadano frente a la posibilidad de recibir el reproche de la Ley dice GONZÁLEZ-CUÉLLAR, según la misma referencia bibliográfica enterior, que *"el CEDH, cuando utiliza la expresión "previstas por la ley", se refiere, según el TEDH, a la ley "accesible y previsible", de manera que el ciudadano pueda acomodar a ella su conducta; y pueda ser capaz, en su caso recabando asesoramientos autorizados, de prever, en la razonable medida que permitan las circunstancias, las consecuencias que pueda producir una acto determinado".* La cuestión es si, a falta de una ley de calidad, puede el delincuente acomodar su conducta a la elusión de la Ley. Por ejemplo, los delincuentes saben perfectamente que la Ley obliga a las operadoras a facilitar que sus teléfonos sean intervenidos y también que la ley no alcanza a obligar de igual forma a los ISP que facilitan comunicaciones de *VoIP*. He aquí una de las grandes contradicciones del Estado de Derecho, ya que las comunicaciones por uno u otro procedimiento son en lo esencial idénticas a efectos procesales y penales. Sobre la cuestión de la previsibilidad de la Ley contenida en el CEDH, vid. Lanzarote Martínez, Pablo. *Intervención de las…op. cit.*, pág. 767.

En el caso de la intervención de las comunicaciones electrónicas, es del perfecto dominio público la potestad genérica del Estado de injerirse en su contenido , que, por lo demás, aparece con regularidad en las resoluciones judiciales más comunes, por más que la evolución de las TIC pueda proporcionar eventuales territorios de difícil acceso técnico para el completo cumplimiento de los fines indicados o se haya generado la falsa creencia entre algunos ciudadanos de que existen medios técnicos para sustraerse de su capacidad de observación y actuar impunemente.

La controversia en la materia, por tanto, no se residenciará en la falta de legitimidad del Estado para ejercitar su derecho de injerencia sino, más bien, y por mor de la tecnología, en el ámbito donde el Derecho pueda alcanzar toda su eficacia y en la idoneidad de los instrumentos técnicos de los que haya de servirse para garantizarlo, dadas las presumibles dudas sobre su proporcionalidad que puedan suscitarse.

En el capítulo de las soluciones, deben cobrar un mayor protagonismo la adecuada acción jurisdiccional, las habilitaciones y garantías jurídicas sobre la actuación de la PJE y la instauración de los medios de salvaguarda tecnológica que puedan sumarse a las anteriores medidas.

El principio de legalidad tiene, con toda evidencia, importantes connotaciones con el concepto de ***seguridad jurídica***[407], que LARENZ define como *"la certidumbre de que se puede contar con reglas de Derecho, con su igual aplicación, y en determinados supuestos creados o calificados por el Derecho – por ejemplo, el registro, un documento, una sentencia firme, un acto administrativo inimpugnable – con los derechos adquiridos y su protección por los Tribunales"*.

En este mismo sentido, la STC 227/88, de 29 de noviembre, proclama que la seguridad jurídica es la *"suma de certeza y legalidad, jerarquía y publicidad normativa, irretroactividad de la no favorable e interdicción de la arbitrariedad sin perjuicio del valor que por sí mismo tiene aquel principio"*. En suma, es la certeza de que la Ley alcanzará inexorablemente todas sus finalidades.

[407] Vid. Larenz, Karl. *Derecho justo. Fundamento de ética jurídica*. Cívitas, Madrid, 1985, pág. 46.

La proscripción de la arbitrariedad modula las facultades discrecionales del actor jurisdiccional. En efecto, la función valorativa o estimativa, es decir, la *"apreciación en conciencia"* o de *"recta inteligencia"* contenida en el art. 741 LCRIM enerva y a la vez limita el prudente arbitrio judicial, que deberá ajustarse a *"las reglas de la lógica, del criterio racional y de la sana crítica, respetando también los principios o máximas de experiencia y los conocimientos científicos que responden a reglas inamovibles del saber…"*[408].

Pues bien, si se llevan todas estas ideas sobre el principio de legalidad y, dentro de este, al principio de tipicidad procesal *"nulla coactio sine lege"*, y se yuxtaponen críticamente sobre el sustrato jurídico que ampara en España la limitación del derecho fundamental al secreto de las comunicaciones, se anotarán graves deficiencias, generadoras de una inaceptable inseguridad jurídica y que son reiterada y unánimemente denunciadas por la doctrina y la jurisprudencia[409].

GIMENO, a este respecto, hace la siguiente observación:

> *"…la regulación que el nuevo art. 579 de la LECrim efectúa de este acto instructorio resulta ser muy insuficiente (STS 513/2010, de 2 de Junio), por el considerable número de lagunas que contiene en materias, tales como la ausencia de regulación de las comunicaciones telemáticas a través de «Internet»*[410] *y de los datos externos de los correos electrónicos, la falta de*

[408] STS de 13 de febrero de 1999 (RJ 1999, 502). Ver también, entre otras, las SSTS de 12 de noviembre de 1996 (RJ 1996, 8198), 25 de noviembre de 1996 (RJ 1996, 8000), 11 de marzo de 1997 (RJ 1997, 1710), Causa Especial 840/96, caso *Mesa Nacional de Herri Batasuna*, y 15 de diciembre de 2006 (RJ 2007, 429, sobre el Rec. 2239//05.

[409] Bien es cierto que, sobre esta situación, que el autor describe como de práctica anomia, concede que ha ido siendo colmada por el TC (con ciertos vaivenes en la valoración de la prueba), el TEDH (muy centrado en la cuestión de la *previsión legal* de las medidas limitativas de derechos fundamentales) y el TS, como puede verse en la STS de 16 de mayo de 2003 (RJ 2003, 4385). Véanse también las SSTS 12 marzo 2004 (RJ 2004, 3404) y 22 enero 2003 (RJ 2003, 1992).
Sobre las insuficiencias procesales en materia de intervención de las comunicaciones, véase la STC 49/1999, de 5 de abril (RTC 1999/ 49) y el reiterado reclamo de una solución mediante la STS de 22 de enero de 2003 (RJ 2003, 1992) diciendo que *"…la referencia a las normas esenciales de procedimiento establecidas por la Ley, nos lleva a llamar la atención sobre la necesidad, largamente requerida por la doctrina, de una regulación específica y detallada de las escuchas telefónicas que, garantizando los derechos constitucionales y sobre todo la intimidad y el derecho defensa, nos dé unas pautas legales a las que debe ajustarse esta diligencia".* Sobre tan denunciada *mora legislatoris,* véase la STS de 29 de mayo de 2007 (2007, 3597).

[410] Sobre la inaplicabilidad del art. 33 LGT y la LCDCE a las comunicaciones a través de Internet, idénticas en su finalidad a las que se hacen a través de la telefonía fija o móvil, vid. Vallés Causada, Luis.

determinación de los supuestos que justifican la intervención telefónica, la duración de la medida, el objeto y procedimiento de intervención y de transcripción en acta del contenido de los soportes magnéticos, la custodia y destrucción de los soportes magnéticos o telemáticos, el valor probatorio de la prueba inconstitucionalmente obtenida, etc., que provocó la condena del Estado español por la STEDH de 18 de febrero de 2003, Prado Bugallo c. España (si bien la posterior Decisión inadmisoria del TEDH, de 25 de Septiembre de 2006 –caso Abdulkadir Cobán v. España- parece rectificar dicha jurisprudencia)"[411,412].

Las razonadas críticas de GIMENO sobre la eficiencia de la normativa procesal que regula la intervención de las comunicaciones en el art. 579 LCRIM pueden todavía ampliarse, sobre todo si se pone la realidad de las TIC en relación con la propia CE (art. 18.3) y con los cuerpos legislativos complementarios, como la LGT, la LSSI, la LCDCE y las demás normas de desarrollo:

En primer lugar, sorprendentemente, la Ley no cuenta con una definición sobre lo que ha de entenderse desde un punto de vista jurídico por *comunicación*, por lo que ha de estarse a lo que la doctrina y la jurisprudencia hayan ido precisando. Esta cuestión no es baladí pues, por más que se otorgue actualmente una tutela estricta, universal e indistinta a cualquier tipo de comunicación, sean cuales fueren sus circunstancias[413], debiera quedar claro en el derecho positivo el rango de protección con que hubieran de tutelarse aquellas otras cuyos actores no fuesen sólo personas - o que ningún corresponsal en realidad lo fuese - y que, consecuentemente, debieran situarse fuera del escalafón más alto de la protección constitucional del art. 18.3.

Problemas procesales para la obtención de inteligencia sobre comunicaciones de telefonía móvil por la Policía Judicial. Madrid: UNED, 2009.

411 *Ibídem.* Vid. Gimeno Sendra, Vicente. *La intervención de las comunicaciones,* en Marchal Escalona, Nicolás (Director). *Manual de lucha…op. cit.,* pág. 579.

412 También vid. Lanzarote Martínez, Pablo. *Intervención de las…op. cit.*, pág. 767.

413 La amplísima definición del punto 32 del Anexo II de la LGT anota que por telecomunicaciones ha de entenderse *"toda transmisión, emisión o recepción de signos, señales, escritos, imágenes, sonidos o informaciones de cualquier naturaleza por hilo, radioelectricidad, medios ópticos u otros sistemas electromagnéticos".* Sin embargo, en la realidad de los años en que se legisló el art. 579 LCRIM, el teléfono fijo sólo servía, a efectos de la intervención legal que se pretendía regular, para transmitir la voz humana. Nada más. Los *smartphones* y los ordenadores corrientes de hoy día transmiten, además de la voz, una sorprendente variedad de *signos y señales* muy socorridos y útiles para el moderno *iter criminis.*

Este sería el caso, en mi opinión, de las comunicaciones de máquina a máquina, de máquina a persona o de persona a máquina[414], tan comunes en los usos técnicos o sociales de los medios de comunicación actuales y, desde luego, de tan clara utilidad para el éxito de determinadas conspiraciones criminales ya que, en estos casos, la comunicación deviene un elemento técnico mediato e instrumental para la consecución de fines por completo ajenos a la interacción humana.

En segundo lugar, tampoco consta en el derecho positivo, en idéntica situación, una ponderación sobre cómo debiera ser la protección cuando las comunicaciones sean en canal abierto, lo que es extraordinariamente frecuente, por ejemplo, en la interacción comunicativa a través de Internet[415,416].

En tercer lugar, con toda lógica, nada se previene sobre el uso de los medios de comunicación telemática segura entre los operadores jurídicos y demás participantes en los procesos propios de la intervención de las comunicaciones[417].

---

[414] Sobre la complejidad de este asunto, sobre el que se volverá más adelante, vid. González-Cuéllar Serrano, Nicolás. *Garantías constitucionales…op. cit.,* pág. 167 y ss.

[415] Adelantando alguna opinión al respecto, el acceso de la PJE al contenido de las comunicaciones abiertas no supondría una injerencia en la intimidad de quien, con perfecto conocimiento de sus actos, se dirige a un auditorio indeterminado para comunicar un contenido material de cualquier naturaleza. Esto sería coherente con la doctrina jurisprudencial, nacida del Fundamento 3º de la Sentencia del Tribunal Constitucional núm. 56/2003, de 24 de marzo, donde se dice *que "no hay secreto para aquel a quien la comunicación se dirige"* ya que, en nuestro caso, la comunicación estaría dirigida de una forma abierta a una pluralidad de personas quienes, sin restricción alguna, podrían accederla libremente en la red y, consecuentemente, ponerla la PJE a disposición del proceso penal. En este mismo sentido se pronuncian las SSTS, de 9 de mayo de 2008 y de 28 de mayo de 2008. Vid. Velasco Núñez, Eloy. *Delitos cometidos a través de Internet…op. cit.,* pág. 221 y ss.

[416] En la STC 173/2011, de 7 de noviembre de 2011, se recoge como antecedente la afirmación de la Sentencia de la Sección Primera de la Audiencia Provincial de Sevilla de 7 de mayo de 2008, dictada en procedimiento abreviado núm. 254-2007, donde se declara que *"difícilmente puede invocarse el derecho a la intimidad cuando los propios actos del acusado indican paladinamente que no tenía intención ni voluntad alguna de preservar para su esfera íntima, exclusiva y personal ninguno de los ficheros que conservaba en su ordenador, pues a ellos tenía acceso cualquier persona que se conectara en Internet a la misma red de intercambio"*.

[417] Algo que ya funciona en la práctica ya que, aunque la implantación actual no alcanza al total de las compañías de telecomunicaciones, el sistema GAITA, gestionado por la PJE para comunicarse con las operadoras (del que permanece ajeno la Administración de Justicia), cuenta con un módulo de comunicación WMS (*warrant management system* o sistema de gestión de mandatos) para transmitir los mandatos judiciales bajo protocolo de codificación PGP. Lamentablemente, hasta tanto se solvente, "la parte de la Justicia" ha de cumplimentarse mediante escaneado del documento original en papel firmado por el Juez de Garantías, que se adjunta por fin en formato electrónico al mensaje de GAITA, lo que reproduce todas las tachas de eficiencia puestas de manifiesto y, especialmente, la inaceptable dilación que todo este proceso ocasiona. Adicionalmente, pueden plantearse cuestiones de seguridad, veracidad y autenticidad, ya que el documento judicial original es recibido en la operadora con posterioridad a los efectos que por su carácter imperativo se instauren, todo ello mediante el envío precedente de una copia no autenticada del mandato judicial por el procedimiento telemático descrito.

En cuarto lugar, no existe tampoco un régimen jurídico específico y completo, con diferenciación del que se establece para el acceso al contenido material, pero que se refiera al tratamiento de los DACE de la intervención y, mucho menos, ponderando la intensidad de su protección jurídica de acuerdo con su capacidad identificativa o el sacrificio del derecho a la intimidad que cada categoría de datos suponga – esté relacionada o no con personas identificadas o identificables *ex* art. 3.a LOPD -, su mayor o menor vinculación con el acto de comunicación que lo está generando o, alternativamente, la valoración del dato cuando se haya obtenido en un tiempo diferido al de la comunicación a la que perteneció o, simplemente, se trate de un dato técnico que no tenga relación con comunicación alguna[418].

En quinto lugar, en lo que se refiere a los DACE conservados, el ámbito subjetivo de aplicación de la LCDCE queda restringido *ex* art. 2 al muy limitado sector de *"…los operadores que presten servicios de comunicaciones electrónicas disponibles al público o exploten redes públicas de comunicaciones, en los términos establecidos en la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones*", teniendo la consideración de *operador*, según la disposición adicional segunda de la LGT, la "*persona física o jurídica que explota redes públicas de comunicaciones electrónicas o presta servicios de comunicaciones electrónicas disponibles al público y ha notificado a la Comisión del Mercado de las Telecomunicaciones el inicio de su actividad".* Es decir, con absoluta exclusión de los prestadores de servicios de la sociedad de la información regulados por la LSSI, no sólo en materia de DACE, sino de acceso por el Estado al propio contenido material de las comunicaciones telemáticas y a los servicios subyacentes. Por si fuera poco, fracasa ostensiblemente el art. 33.10 LGT sobre la puesta a disposición del Estado de los protocolos de codificación en materia de comunicaciones por vía telemática.

Una extraña mezcla de telemática y rudimento documental a partes iguales, puede concluirse. Una virtud de este sistema es el transmisión digital de datos, lo que reduce errores al introducirlos en los sistemas informáticos de las operadoras. Un defecto es que no es extensivo a los mandamientos sobre los DACE conservados por la LCDCE, cuyo contenido se sigue introduciendo a mano, con los siguientes efectos de pérdidas de tiempo, limitación en el número de objetivos y posibilidad de introducir errores en la transcripción.

[418] Estas observaciones sobre los DACE se hacen, por otra parte, por más que en tiempos recientes se haya legislado parcialmente en materia de conservación en la LCDCE, esto es, a través de una ley ordinaria (con aparente desatención del art. 81.1 CE, si de lo que se está hablando es de regular un derecho fundamental), asunto que habrá de tratarse en el capítulo siguiente con mayor detenimiento.

En sexto lugar, no existen previsiones para el tratamiento de la urgencia ni condiciones en las que ampararse para la posible realización de pericias de inteligencia sobre el contenido de las comunicaciones electrónicas y, particularmente, sobre los DACE de suerte que, bajo determinadas circunstancias favorables, se pudiese obtener inteligencia de su análisis.

En séptimo lugar, no se establecen disposiciones jurídicas por las que se pueda facultar a los agentes para determinadas tareas de geolocalización, como pueda ser la apertura de medios de GPS de los dispositivos de comunicaciones, el análisis del ***espectro radioeléctrico***[419], la generación externa de datos de localización, los análisis de datos de cobertura de red, de intervención en los sistemas de antenas o celdas y, particularmente, los que se hayan de activar con perentoriedad en situaciones de urgencia vital o riesgo catastrófico.

En octavo lugar, no se arbitra un régimen de acceso a las comunicaciones entre los operadores jurídicos que, a lo largo del proceso penal, les habilite en relación con el acceso al contenido de la intervención de las comunicaciones.

En noveno lugar, no se atribuyen funciones u obligaciones a las operadoras del mercado de las telecomunicaciones ni a los prestadores de servicios de la sociedad de la información y que, en cualquier caso, podrían jugar un papel decisivo en materia de práctica de pericias o de prestación de auxilios jurisdiccionales.

En décimo lugar, no se establecen normas sobre la gestión de la evidencia legal o de las transcripciones ni de las facultades que la PJE tenga al respecto.

En decimoprimer lugar, nada se dice de los sistemas orientados a garantizar la autenticidad, veracidad, seguridad e integridad de los contenidos intervenidos, uso de la firma electrónica, procedimientos de contradicción, verificación o auditoría, regulación del secreto, ni tampoco del destino de los soportes o de la evidencia digital durante el proceso, el uso procesal de las copias, las obligaciones de destrucción a verificar en el momento procesal que se indique, las normas de cadena de custodia, las

[419] Según el pto. 12 de la LGT, el espectro radioeléctrico lo componen *"las ondas radioeléctricas en las frecuencias comprendidas entre 9 KHz y 3000 GHz; las ondas radioeléctricas son ondas electromagnéticas propagadas por el espacio sin guía artificial"*.

medidas de seguridad sobre la compañía que facilite servicios de comunicaciones electrónicas, etc.

En decimosegundo lugar, no se establecen ni se explican detalladamente las funciones jurisdiccionales y, particularmente, en qué consiste el control jurisdiccional[420,421] y de qué normas y medios puede disponer para alcanzar sus finalidades constitucionales.

En decimotercer lugar, nada se dice en la Ley sobre los medios de salvaguarda tecnológica, de certificación de medios técnicos, del registro lógico de los eventos telemáticos que compongan el acceso legal a las comunicaciones, etc.

En decimocuarto lugar, no existen previsiones jurídicas para la intervención de las comunicaciones orales directas que tenga en cuenta sus especiales características y, particularmente, los condicionantes de tiempo, lugar, presencia de interlocutores, idoneidad de los medios técnicos de grabación, etc.

La insuficiencia o mera ausencia de previsión legal, ocasiona un importante grado de inseguridad e indeterminación jurídicas, así como riesgos para los agentes de la PJE encargados de llevar a cabo las intervenciones. Por ello, estas incertidumbres debieran resolverse por el legislador restando tan indeseable margen de indefinición e introduciendo en el derecho positivo las necesarias reformas *de lege ferenda* que fuesen de estricta justicia admitir, algo que, evidentemente, está reclamando con urgencia el mundo de las TIC en la sociedad actual y, particularmente, en su afectación a la debida tutela del derecho al secreto de las comunicaciones, con plena y segura diferenciación de lo que afecte al derecho a la protección de datos personales o a otros aspectos de la intimidad.

---

[420] Como acertadamente observa NOYA. Vid. Noya Ferreiro, María Lourdes. *La intervención de las comunicaciones orales directas en el proceso penal.* Valencia: Tirant lo Blanch, 2000, pág. 262 y ss.

[421] La doctrina ha ido definiendo el control judicial como una actividad dinámica a desarrollar durante toda la vida de la medida limitativa de derechos y sin sujeción a protocolos que puedan constreñirla, tal y como se proclama, entre otras, en las SSTS de 11 de octubre de 1994 RJ 194, 8170) y 8 de septiembre de 2003 (RJ 2004, 2103).

La ausencia de control judicial puede conllevar además una vulneración de los derechos fundamentales – ya que, en el ámbito objeto de estudio, forma parte del contenido esencial del derecho al secreto de las comunicaciones - y, en consecuencia, conllevar una anulación de las pruebas que por mediación de la medida limitativa se hayan llevado al proceso penal, según se indica en la STS de 25 de enero de 1997 (RJ 1997, 1091) y la STC 49/1996 de 26 de marzo (RTC 1996, 49), entre otras. Vid. Lanzarote Martínez, Pablo. *Intervención de las…op. cit.*, pág. 811 y ss.

Por lo anterior, en mi opinión, es necesario que los poderes públicos lleven a cabo un profundo análisis fenomenológico que asumiese la naturaleza de las TIC, su uso criminal y las necesidades de revisar la Ley en cuanto a la limitación del derecho fundamental al secreto de las comunicaciones, con perfecta diferenciación de los ámbitos del Derecho afectados en cada caso.

El resultado del anterior proceso debe adecuarse con sentido estricto, pero abierto y práctico, al espíritu de los preceptos constitucionales mencionados, no posponiéndose por más tiempo la reforma que ha de practicarse, no ya en el art. 579 LCRIM, sino en el conjunto de las obsoletas leyes procesales españolas de forma que, junto con la valoración y toma en consideración de las propuestas enumeradas en este apartado, se sopesase especialmente la posibilidad de establecer en la Ley las causas de urgencia cuyo tratamiento pudiera ser objeto de un control posterior de jurisdiccionalidad, conjurando así la inseguridad jurídica actual y el grado de discrecionalidad con que se aplican hoy muchas de las normas procesales. Así, deberían establecerse las precisas condiciones en que esto debiera llevarse a cabo, tanto por la Autoridad Judicial, como por la PJE o, en general, por cualquier operador jurídico que se viese compelido a actuar en mérito a tan excepcionales circunstancias (de lo que no están exentos las FFSS, la propia PJE y los servicios de emergencia de cualquier clase).

2. El presupuesto material de justificación teleológica

Desde un punto de vista práctico policial, no resulta novedosa la necesidad de que la PJE acceda al contenido las comunicaciones como medio de satisfacer las legítimas finalidades de la investigación criminal en el marco del proceso penal.

Históricamente, la legal intervención de las comunicaciones tiene su origen en la limitación del secreto de la correspondencia postal, ya en el Siglo XIX, sin que los avances tecnológicos en la forma de hacerlo hayan ocasionado, en absoluto, variaciones sustanciales en las finalidades del Estado de Derecho, esto es, injerirse en el contenido de lo comunicado, tal y como sucediera con la aparición en la sociedad de

la telefonía fija. Con toda lógica, la promulgación del art. 18.3 CE no vino en lo esencial a innovar nada, sino a proteger una nueva forma de comunicarse en privado, enumerándola junto a las demás formas[422].

Por ello, la novedosa utilización de la telefonía para satisfacer las finalidades criminales, provocó la reacción del Estado democrático, que acabó disponiendo la forma técnica y jurídica de injerirse subrepticiamente en las comunicaciones telefónicas, todo ello mediante la interposición de determinados artificios que derivaban el contenido material de la comunicación a unos agentes facultados al efecto por una Autoridad Judicial – la PJE - para que lo escuchasen e interpretasen y, además, lo grabasen, con la finalidad última de aportarlo todo como prueba al proceso penal o para orientar el curso de las propias investigaciones.

Igualmente, los exiguos datos de tráfico que se asociaban a las comunicaciones intervenidas suscitaron también el interés del Estado, pues se evidenció también la necesidad de desvelar las relaciones de los investigados con terceros criminales que pudieran aparecer en escena lo que, a su vez, podía llegar a motivar la ordenación de nuevas intervenciones telefónicas.

En lo esencial, la diferencia material entre esta forma entonces novedosa de comunicarse no era sustancialmente distinta de la que se efectuaba por carta, al menos a lo que se refiere al peso o trascendencia para los derechos fundamentales referido a la limitación del secreto de las comunicaciones.

En efecto, en cuanto a su finalidad, la injerencia en el secreto de las comunicaciones electrónicas no ha variado tampoco con la evolución actual de las TIC, por ser idéntica a la que existía en los no tan lejanos tiempos en que la telefonía fija era la única disponible.

Al contrario, el derecho de injerencia del Estado y su necesidad de obtener cuantos datos fuera posible sobre las comunicaciones, sigue intacto y, ciertamente, mostrando una necesidad creciente de intervención, dada la versatilidad y profusión de su uso criminal. Es necesario por ello, ahora más que nunca, intervenir las comunicaciones de acuerdo con el principio de proporcionalidad, dadas las inmensas

[422] Vid. Vegas Torres, Jaime. *Obtención de pruebas…op. cit.,* pág. 41.

posibilidades de eficiencia y expectativa de impunidad que ofrecen las TIC a los delincuentes en la escena internacional.

En cuanto a la penetración social, eso sí, ha variado espectacularmente la panoplia de servicios añadidos que se asocian a las TIC, impensables en la época de la telefonía fija, como por ejemplo, la geolocalización de los terminales, el acceso a Internet y sus servicios subyacentes, la automatización de los procesos telemáticos, el uso de los ISP u otros servicios extraterritoriales para la conformación de los mensajes o las técnicas de *spoofing* o ***hacking***[423], generando además una serie de DACE cuyo interés llega a exceder al del propio contenido material de la comunicación.

Pero lo que no ha variado es, lamentablemente, el enfoque jurídico que merecen semejantes cambios, anquilosado en visiones procesales claramente obsoletas, cuya reacción se limita a buscar solemne refugio en el hipergarantismo y a mostrarse incapaz de asumir que, siendo la finalidad esencial la misma, los instrumentos jurídicos hayan de responder con normalidad a lo que es normal desde hace años entre los ciudadanos.

El escenario de las TIC ensancha y diversifica las relaciones humanas en sus aspectos más sociales, tanto para lo lícito como para lo ilícito. Si el Estado fue capaz de intervenir en el mundo físico de una manera solvente e integrar las tecnologías de telefonía fija cual si fueren un aspecto más de dicho mundo, ha de hallar también la manera de cumplir sus finalidades en el mundo virtual, lo que sin duda incluye la comprensión e interiorización de los cambios tecnológicos y su afectación al derecho al secreto de las comunicaciones. De lo contario, la brecha abierta entre el mundo del delito y la representación de los derechos de los ciudadanos por el Estado será cada vez mayor.

En su virtud, el ***presupuesto material de justificación teleológica***[424] supone que la limitación de los derechos fundamentales deba tener unos fines legítimos, es

[423] Técnica por la que el *"hacker",* como experto informático, vulnera la seguridad de un equipo informático para acceder ilegalmente a sus contenidos o, simplemente, modificarlo, destruirlo o causarle cualquier clase de daño.

[424] En el razonamiento de GONZÁLEZ-CUÉLLAR, a quien se sigue en este apartado, el presupuesto de justificación teleológica es de naturaleza material *"porque introduce en el enjuiciamiento de la admisibilidad de las intromisiones del Estado en la esfera de los derechos de los ciudadanos los valores que trata de salvaguardar la actuación de los poderes públicos y que precisa gozar de la fuerza*

decir, que la decisión de los poderes públicos de ejercitar su capacidad ablativa sea el legítimo resultado de sopesar si debe prevalecer el interés público o el de terceros sobre la preservación de los derechos fundamentales de determinadas personas a las que se aplicará una eventual medida limitativa. Se hace evidente en este presupuesto su conexión con el requisito extrínseco formal de motivación, toda vez que la resolución por la que se limite un derecho fundamental exige una plena identificación y justificación de su finalidad, lo que a su vez demanda, incuestionablemente, una razonada exposición material de su contenido.

La doctrina del TC puede resumirse, a través de su sentencia 173/2011, de 7 de noviembre, del siguiente modo:

> *"Por lo que se refiere a la concurrencia de un fin constitucionalmente legítimo que puede permitir la injerencia en el derecho a la intimidad, este Tribunal ha venido sosteniendo que reviste esta naturaleza "el interés público propio de la investigación de un delito, y, más en concreto, la determinación de hechos relevantes para el proceso penal" (SSTC 25/2005, de 14 de febrero, FJ 6 y 206/2007, de 24 de septiembre, FJ 6). En efecto, "la persecución y castigo del delito constituye un bien digno de protección constitucional, a través del cual se defienden otros como la paz social y la seguridad ciudadana, bienes igualmente reconocidos en los arts. 10.1 y 104.1 CE" [SSTC 127/2000, de 16 de mayo, FJ 3 a) y 292/2000, de 30 de noviembre, FJ 9]".*

Vuelve a suscitarse críticamente, por otra parte, la cuestión de la ***indeterminación jurídica*** sobre los fines que justifican el ponderado sacrificio de determinados derechos en beneficio de otros de mayor enjundia, cuando lo que se pretenda sea, con pocas probabilidades de éxito, establecer un catálogo tasado y preciso de las finalidades legítimas sobre las que habría de decantarse el Estado de Derecho[425], aspecto este que ha de relacionarse en buena medida con el impreciso

---

constitucional suficiente para enfrentarse a los valores representados por los derechos fundamentales restringidos". Vid. González-Cuéllar Serrano, Nicolás. *Proporcionalidad…op.cit.*, pág. 69.

[425] Sobre esta cuestión reflexiona GONZÁLEZ-CUÉLLAR al valorar la validez de las finalidades admisibles, diciendo que *"así, los arts. 5, 8, 9, 10 y 11 CEDH garantizan los derechos a la libertad y seguridad, al respecto de la vida privada y familiar, del domicilio y de la correspondencia, a la libertad de pensamiento, conciencia y religión y a la libertad de expresión, reunión y asociación, establecen listas taxativamente limitadas de finalidades que justifican su restricción, si bien se hallan contenidos en*

margen de discrecionalidad[426,427] subyacente en las resoluciones valorativas de la proporcionalidad que, en poco o en nada, pueden sujetarse a prescripciones.

En este mismo sentido, existen algunas posiciones doctrinales que niegan *"la suficiente legitimidad [a los Tribunales] para llevar a cabo las valoraciones y las apreciaciones que le exige la aplicación del principio de proporcionalidad y puesto que como la aplicación de este principio no puede orientarse por criterios jurídicos completamente certeros, por lo que el intérprete se ve compelido a llevar a cabo valoraciones subjetivas, cada aplicación del principio constituye una intervención ilegítima del Alto Tribunal en la competencia legislativa para configurar la Constitución […] y reduce la esfera de actuación que corresponde al legislador en el proceso de articulación de los intereses sociales y de configuración de la vida política"*[428]. Criterios subjetivos aplicados con un gran margen de discrecionalidad jurisdiccional, podría añadirse en suma[429,430].

---

conceptos indeterminados muy generales". Vid. González-Cuéllar Serrano, Nicolás. *Proporcionalidad…op.cit.*, págs. 99 y 100.

[426] MARCHAL lo expresa afirmando que *"aunque la norma procesal establezca las líneas generales de actuación otorgando cierta discrecionalidad al órgano actuante, es la proporcionalidad la que determina la solución justa de entre las posibles"*. Afirma también este autor que *"la potestad puede ser reglada, en cuyo caso la Administración se limita a la aplicación automática de normas. La dificultad surge en las llamadas potestades discrecionales, en las que la Administración debe completar por ella misma algunas determinaciones del contenido de ésta"*. Vid. Marchal Escalona, Nicolás. 2010. *Policía Judicial…op.cit.,* págs. 38 y 32, respectivamente, y López González, José. *El principio general…op. cit.*, pág. 99. RUIZ y DE LA TORRE, por su parte, consideran que el principio de proporcionalidad opera como una reducción de la discrecionalidad del Juez. Vid. Ruiz Ruiz, Ramón y de la Torre Martínez, Lourdes. *Algunas aplicaciones…op.cit.,* pág. 38.

[427] Respecto la ponderación del ejercicio de las facultades judiciales discrecionales, como método racional de resolver el conflicto entre principios, es muy interesante la lectura de Ruiz Ruiz, Ramón. *La ponderación en la resolución de colisiones de derechos fundamentales. Especial referencia a la jurisprudencia constitucional española.* Revista Telemática de Filosofía del Derecho, nº 10, 2006/2007, ISSN 1575-7382, págs. 53-77. En la pág. 75, este autor se suma en sus conclusiones a la opinión de PRIETO SANCHÍS con la siguiente cita literal: *"la rematerialización de la Constitución a través de los principios supone un desplazamiento de la discrecionalidad desde la esfera legislativa a la judicial: bien es verdad que no se trata ya de la misma discrecionalidad, y la diferencias es esencial: la del legislador ha sido siempre una discrecionalidad inmotivada, mientras que la del juez pretende venir domeñada por una depurada argumentación racional".* Vid. Prieto Sanchís, L. *Tribunal Constitucional y positivismo jurídico*. Doxa, nº 23, 2000, pág. 173.

[428] Vid. Ruiz Ruiz, Ramón y de la Torre Martínez, Lourdes. *Algunas aplicaciones…op.cit.,* pág.40.

[429] Sobre esto, razona PRIETO que *"la aplicación de los principios y de la técnica de la ponderación comporta importantes riesgos de subjetividad valorativa por parte del órgano jurisdiccional correspondiente (desde luego, mucho más que la aplicación de reglas)"*. Vid. Prieto Sanchís, L. *Tribunal Constitucional…op. cit.*, pág. 179.

[430] Sobre la cuestión de la proporcionalidad de las resoluciones judiciales, vid. Vidal Fueyo, Camino. *El principio de proporcionalidad como parámetro de constitucionalidad de la actividad del Juez.* Instituto de

Pero, en relación con las tesis centradas en la aplicabilidad del principio de proporcionalidad a la limitación de los derechos fundamentales, a una mínima ***legitimidad constitucional de sus fines***[431], como presupuesto básico de su admisibilidad en el Estado de Derecho, debe añadirse además su ***relevancia social***[432]. Sobre esta importante cuestión, GONZÁLEZ-CUÉLLAR reflexiona del siguiente modo:

> "*Los fines, para que doten de suficiente vigor a los medios puestos a su servicio para la restricción de derechos fundamentales, han de ser socialmente relevantes. Esta exigencia no aparece expresamente enunciada en la CE, ni en los tratados internacionales, pero ha sido reclamada por la jurisprudencia del TEDH. Las normas del CEDH reclaman que las medidas limitativas estén "previstas en la ley", tiendan "a fines legítimos" y sean "necesarias en una sociedad democrática". En el marco de esta última expresión, el Tribunal ha aislado una exigencia que no hace referencia a las medidas en sí mismas consideradas (es decir, su carácter instrumental), sino al propio fin que las justifica: se trata de una "necesidad social imperiosa" que demande su adopción".*

El autor, en referencia a diversos pronunciamientos del TEDH[433], advierte sobre el margen de discrecionalidad que el Tribunal otorga a los países adheridos al CEDH, a los efectos de valorar la ***necesidad social imperiosa***, incorporando este concepto jurídico – también indeterminado - de una forma separada y precedente a la valoración de la proporcionalidad en sí misma y propone para nuestro país *"como exigencia mínima de constitucionalidad, si el fin no se encuentra explícitamente previsto en la Constitución, el de la "relevancia""*[434].

Investigaciones Jurídicas de la UNAM. Anuario de Derecho Constitucional Latinoamericano, Núm. 20052, Sección de Previa, 2005.

[431] Vid. STC 11/1981, de 8 de abril.

[432] *"Es necesario acercarse a la valoración social del fin para dotarle de la fuerza necesaria para limitar los derechos fundamentales, los cuales contienen una grandísima carga valorativa justificativa de su reforzada protección constitucional"*. Vid. González-Cuéllar Serrano, Nicolás. *Proporcionalidad…op.cit.*, pág. 101 y ss. En la STC 173/2011, de 7 de noviembre, se refleja también la relevancia del interés público y el "*impacto considerable en la opinión pública"*.

[433] Vid. STEDH, de 28 de octubre de 1988, Caso Norris, STEDH, de 21 de febrero de 1975, Caso Golder, y STEDH Caso Barthold, de 25 de marzo de 1985.

[434] Nótese nuevamente la carga de indeterminación asociada al término *relevancia*. Vid. González-Cuéllar Serrano, Nicolás. *Proporcionalidad…op.cit.*, pág. 105.

Consecuentemente, la valoración de la necesidad social imperiosa[435], en las condiciones indicadas, deviene un ejercicio de valoración específico y diferenciado del control de proporcionalidad propiamente dicho, útil a la estricta justicia que cabe esperarse de todo este proceso.

C. Requisitos intrínsecos del principio de proporcionalidad

El principio de proporcionalidad o de prohibición de exceso, según la denominación ampliamente admitida en la doctrina, opera bajo los siguientes requisitos:

1. Idoneidad

La idoneidad se constituye en una prueba orientada a ponderar la adecuación de la medida al fin perseguido, esto es, a determinar *"si la medida enjuiciada supera el oportuno juicio de adecuación o, en otras palabras, si la relación medio-fin resulta adecuada e idónea"*[436]. Se trata, por tanto, de comprobar su grado de utilidad o su inutilidad para alcanzar las finalidades propuestas con independencia, en su caso, de que existiesen otras posibles alternativas que pudieran operar incluso con mayor eficacia.

Para GONZÁLEZ-CUÉLLAR, "*las notas esenciales de la idoneidad son:*

1. *Constitucionalidad. Se apoya en el carácter constitucional del principio de prohibición de exceso, con que se garantiza la defensa de los derechos fundamentales.*
2. *Carácter empírico del principio. Se apoya en el esquema medio-fin.*

[435] Como ejemplo, vid. STEDH, de 30 de junio de 2009, Caso *Batasuna*.
[436] Vid. Perelló Doménech, Isabel. *El principio de proporcionalidad y la jurisprudencia constitucional.* Jueces para la democracia, ISSN 1133-0627, Nº 28, 1997, págs. 69-75, pág. 70.

3. *Flexibilidad. Una medida es idónea si con su ayuda la satisfacción del fin deseado se acerca o facilita. No es necesaria una eficacia absoluta de la medida.*
4. *Aplicabilidad tanto desde una perspectiva objetiva como subjetiva"* [437].

Para NOYA, *"el grado de eficacia que ha de exigirse a la medida debe valorarse en relación con el caso concreto, en base a los siguientes tres requisitos:*

1. *La medida debe ser por su naturaleza la más apta para la consecución del fin previsto.*
2. *Su duración debe estar en estrecha relación con su finalidad.*
3. *El sujeto al que se dirija la medida ha de estar debidamente individualizado"*[438].

Para MARCHAL, "*una medida es idónea si con ella se consigue alcanzar el objetivo perseguido sin que el medio empleado sea excesivo"* [439]. Es sobre esta cuestión – que el medio no sea excesivo -, donde se plantean los aspectos de actualidad más interesantes y controvertidos en relación con el modo de limitar el secreto de las comunicaciones de una forma útil y, a la vez, admisible para el proceso penal. Es decir, aceptado el qué (injerirse el Estado de Derecho en las comunicaciones personales protegidas por el art. 18.3 CE), determinar el cómo (las técnicas y procedimientos que el Juez de Garantías puede autorizar para lograr los fines de las intervención de las comunicaciones).

Sin embargo, el estado actual de las TIC ofrece a quien desea comunicarse una amplia variedad de servicios cuyo sustrato técnico es el mismo que el de la transmisión de voz y que motivó la extraordinaria y justificada sensibilidad social y política sobre la necesidad de su más alta protección. Sin embargo, este sustrato técnico no es siempre utilizado para la transmisión de voz o texto sino también para facilitar otro tipo de prestaciones que no siempre merecerán un grado análogo de protección constitucional sino que, antes bien, deberá ponderarse su intensidad con arreglo al grado de sacrificio del derecho que haya de quedar limitado.

[437] Vid. González-Cuéllar Serrano, Nicolás. *Proporcionalidad…op.cit.*, pág. 154 y ss.
[438] Vid. Noya Ferreiro, María Lourdes. *La intervención…op. cit.,* pág. 151.
[439] Marchal Escalona, Nicolás. *Policía Judicial…op.cit.,* pág. 53.

Por consiguiente, desde un punto de vista jurídico-procesal, no puede tener el mismo tratamiento el acceso a un dato de localización geográfica de una ***BTS***[440] que da cobertura, en un momento dado, a un teléfono móvil fuera del acto de comunicación[441] que, en el otro extremo, la instalación legal de ***software de control remoto*** en un dispositivo electrónico para acceder a todos sus contenidos y contrarrestar la inoperancia del art. 33 LGT sobre el acceso a las comunicaciones electrónicas vía Internet, salvar los protocolos restringidos de codificación y, además, aventurar una solución a los problemas operativos y prácticos de limitación territorial de la Ley (correo electrónico, *VoIP*, documentos, fotografías, consultas web, listados de contactos, etc.).

Si en 1988, año en que se redactó el art. 579 LCRIM, toda la expectativa del legislador fue – pobremente y sin llegar a imaginar lo que estaba a punto de sobrevenir con la telefonía móvil e Internet – alcanzar a regular las intervenciones telefónicas de línea fija, donde la máxima aspiración era acceder a los contenidos de voz y, todo lo más, a los datos de contratación y de tráfico de llamadas, en la actualidad emergen necesidades como las descritas en este estudio y que exigen, no sólo una legislación eficaz, sino también medidas regulatorias en aspectos tales como la validación de los procedimientos policiales y la certificación de los instrumentos técnicos que emplee la PJE, todo ello puesto en relación con su idoneidad y proporcionalidad para alcanzar el fin perseguido y, de una forma admisible en Derecho, acceder y acercar la fuente de prueba al proceso penal con absoluta garantía sobre la autenticidad e integridad de su contenido[442].

---

[440] *Base Transreceiver Station*, o estación de recepción y transmisión de comunicaciones. Indica la posición geográfica de una antena de telefonía móvil a la que el terminal se ha registrado en el *transcurso de una comunicación, a veces desde distancias de decenas de kilómetros del terminal.*

[441] Este tipo de datos no informan ni del contenido material porque, sencillamente, no ha producido ninguno, ni de la posición del móvil y, mucho menos, de la persona que eventualmente pueda portarlo si es que acaso es su propietario.

[442] Sostiene VELASCO, respecto de los problemas de intervención que necesiten de la instalación de *troyanos,* que *"las cautelas técnicas incluso que garanticen la procedencia, inalterabilidad y autenticidad del contenido de lo seleccionado entre lo intervenido, su no descontextualización, el correcto almacenamiento y custodia de lo monitorizado (incluso con una especie de esquema histórico de incidencias y transformaciones de lo espiado), el control periódico judicial del resultado de lo encontrado y la proporcionalidad de sus prorrogas temporales con custodia judicial de lo hallado, y finalmente la «traducción» a soporte que permita una sencilla comprensión (a través de la vista y el oído) del contenido incriminatorio seleccionado intervenido, para su correcta valoración contradictoria en el acto del juicio oral.*

En el mundo físico, una vigilancia policial común sobre los movimientos de un objetivo y el testimonio posterior de los agentes de la PJ están perfectamente asumidos por el derecho procesal y listos para ser sometidos a la fase de contradicción y valoración de las pruebas en el acto del juicio oral. Sin embargo, e insistiendo en su carácter menos intrusivo[443], si lo que se pretendiera fuera, siguiendo el ejemplo anterior, simplemente tener una referencia técnica de la relación espacio-temporal de una BTS fuera del acto de comunicación de un determinado móvil al que da cobertura[444], se deberá acudir al mandato judicial por mor de la mera utilidad que semejante instrumento pueda tener en el futuro para establecer una comunicación electrónica, sea personal o no.

Si se analiza el cumplimiento de esta finalidad desde el punto de vista del sacrificio del derecho a la intimidad, en el mundo físico, con toda probabilidad, para alcanzar el conocimiento que se pretende, se adquirirán otros completamente innecesarios que supondrán una profunda penetración en aspectos íntimos del desarrollo personal del sujeto investigado. Por el contrario, si lo que está justificado, por ejemplo, es tener una referencia mínima de si entra o sale de una determinada zona geográfica a la que se desplaza o desde la que se desplaza para cometer delitos, esto es, una noticia notoriamente menos intrusiva sobre sus movimientos que la que supondría una vigilancia directa sobre las persona, el derecho procesal actuará inexorablemente para exigir un mandato judicial al efecto. Es impensable además que, por recoger la bandera del hipergarantismo, la operadora ceda este dato sin exigencia de un mandato judicial.

En definitiva, la cotidianeidad del uso de las nuevas tecnologías en nuestra vida privada conllevará cambios y adaptaciones en nuestra legalidad que descartarán protecciones innecesarias pero que también definirá hasta dónde y cómo se debe perseguir el delito, para poder compaginar el disfrute de la libertad con la seguridad precisa y esperada de nuestros sistemas democráticos". Vid. Velasco Núñez, Eloy. *ADSL y troyanos: Intervención de sus datos y telecomunicaciones en la investigación penal*. La Ley Penal núm. 82: La Ley, 2011.

[443] *"Ciertamente [con el uso de determinados medios técnicos] se pueden eludir otras formas más intrusivas de investigación y, además, hace posibles investigaciones que, de otro modo, serían poco menos que imposibles".* Vid. Pérez Gil, Julio. *El nuevo papel de la telefónia móivl en el proceso penal: ubicación y perfiles de desplazamiento,* en *El Proceso Penal en la Sociedad de la Información. Las nuevas tecnologías para investigar y probar el delito.* Coordinador: Pérez Gil, Julio. VVAA. Ed. La Ley. 2012, págs. 173-218, pág. 182.

[444] Este dato no es de obligada conservación de acuerdo con al LCDCE. Su obtención y cesión depende de la presumible disposición al efecto de la operadora a la que se le reclame en tiempo real. Adviértase, por tanto, la connotación negativa que todo esto tiene para la intervención en un caso de urgencia vital.

En el otro extremo, puede invocarse la introducción de soluciones técnicas ciertamente intrusivas, pero cuyo uso, en línea con lo propugnado en los párrafos anteriores, una vez certificada su idoneidad técnica, pueda ser admisible en la Ley[445].

Sería, por ejemplo, el caso de la introducción de *software de control remoto* en determinados dispositivos de comunicación electrónica para solventar el problema de la imposibilidad de imponer el art. 33 LGT a quienes generan ***paquetes de datos***[446] codificados para ser enviados vía Internet o extender su alcance al espacio jurídico extraterritorial. En este caso – sin duda constitutivo de un inapropiado parche jurídico y técnico – la falta de alternativas debe operar como una causa de justificación para que, con las debidas garantías, el Estado de Derecho no se vea en la tesitura de renunciar a una fuente de prueba que pueda contribuir a la demostración de los hechos.

Y, entre medias, toda una galaxia de nuevas formas delictivas basadas en la utilización de las comunicaciones electrónicas, hasta tal punto que las convierten en una finalidad delictiva en sí mismas, muy difícil de prever, por lo demás, por el legislador de 1988.

Los ejemplos de este enfoque son extraordinariamente variados, como el uso de las tarjetas SIM para lograr el vaciamiento patrimonial de empresas de prestación de servicios de tarificación adicional, para actuar como detonadores de cargas explosivas, como balizas para localizar víctimas o, más simplemente – o con gran complejidad – para obtener datos y claves de acceso mediante *phising* o *pharming* o para organizar cómodamente desde casa una red internacional para poner a disposición pública redes para ciberataques de DoS.

---

[445] Vid. Velasco Núñez, Eloy. *Delitos cometidos a través de Internet…op. cit.,* pág. 131 y ss.

[446] La digitalización del audio analógico (por ejemplo, la voz del ser humano), como parte de las aportación técnicas de la física de la electrónica, es un proceso de conversión del sonido a una secuencia de dígitos, esto es, de ceros y unos, a través del sistema binario, lo que recibe también la denominación de *muestreo* o *sampling*. El sonido así convertido, quedaría a la vista como una sucesión aparentemente arbitraria e ininteligible de ceros y unos que, para su comprensión, necesitaría de un descodificador que lo interpretase como tal sonido. Lógicamente, lo que circula por red pública de comunicaciones electrónicas no es el sonido, sino el código binario que lo representa o, en su caso, de los caracteres de texto, una imagen, etc. Puede suceder también que la información digitalizada se fragmente en paquetes de datos al distribuirse a través de la red y de diversos servidores instrumentales para, finalmente, recomponerse únicamente en el ordenador o dispositivo de comunicaciones del destinatario. Evidentemente, si la descodificación del mensaje completo de ceros y unos es de por sí compleja, lo será aún más el descifrado de paquetes fragmentarios de datos.

La investigación de estos casos difíciles de delincuencia compleja exigirá, a veces, la adquisición en la escena internacional de ***inteligencia de datos sobre las comunicaciones electrónicas*** (en adelante, IDACE) sobre millones de actos de comunicación y cobertura, tanto en tiempo real como diferido, necesidad cuya mera invocación sugiere un choque frontal e insalvable con lo aportado respectivamente por la mayoría de los autores estudiados respecto del uso de medios excesivos y de la individualización de los sujetos a los que se dirigen, lo que no tiene acogida por el momento en el Derecho español.

Lo anterior evidencia, por otra parte, que el derecho procesal vigente flaquea a la hora de interpretar la necesidad del Estado de Derecho para dotarse de unos instrumentos jurídicos para intervenir en unos casos en que, como mínimo, es dudoso que presupongan una limitación de los derechos del art. 18.3 CE, como se va a sostener.

Consecuentemente, la idoneidad de tales instrumentos técnicos y de los correspondientes procedimientos policiales al uso deben revisarse, especialmente, a luz de su afectación o no al derecho al secreto de las comunicaciones.

Es también evidente que esta revisión, de prosperar, no debe en ningún caso suponer un demérito del Derecho ni del conjunto de las garantías constitucionales de que gozan los españoles sino que, antes bien, su ejercicio debe responder a estrictos medios de salvaguarda que, llegado el caso, permitan un fehaciente control posterior de jurisdiccionalidad, basado en el uso de canales que aseguren la autenticidad e integridad de la prueba, tales como los que propugna la Ley 59/2003, de 19 de diciembre, *de firma electrónica*[447,448], la Orden ITC/110/2009 y las demás normas de análoga finalidad.

Debe admitirse también que la apreciación de la idoneidad de una determinada medida tiene un incuestionable componente técnico para cuya libre valoración debe

[447] Sobre la seguridad de las transacciones efectuadas mediante la firma electrónica, es muy ilustrativa la lectura de Davara Rodríguez, Miguel Angel. *La seguridad en las transacciones electrónicas: La firma electrónica.* Madrid: Universidad Pontifica de Comillas ICAI-ICADE, 2005.

[448] Sobre la firma electrónica y su utilidad es muy interesante la lectura de Davara Rodríguez, Miguel Angel. *Manual de derecho…op. cit*, pág. 470 y ss.

contarse, en mi opinión, con el prudente asesoramiento de la PJE y de los demás expertos que sean peritos en la materia.

Sobre el concepto jurídico del subprincipio de idoneidad y su afectación a la labor de la PJE versarán buena parte de las propuestas que a lo largo de este estudio se plantearán.

2. Necesidad

El juicio de necesidad conlleva ponderar *"…si la intervención pública es indispensable, por no existir un instrumento más moderado para su consecución… [por lo que] habrá de optarse por aquel que implique une menor restricción en la esfera jurídica de los afectados"*[449]. Consecuentemente, debe interpretarse este subprincipio como la cabal ponderación de todos medios existentes que resulten idóneos para el logro del legítimo fin perseguido de forma que, escogiendo aquel cuya aplicación suponga la alternativa menos gravosa para los derechos fundamentales de los sujetos, se *"garantice de modo satisfactorio el objeto que justifique el límite"*[450]. Es decir que, salvada la cuestión de la idoneidad del medio empleado, debe optarse por una medida que alcance un mínimo aceptable de eficiencia (se trata de un subprincipio comparativo entre todas las alternativas existentes[451]) y cuyo coste en derechos sea también el menor posible.

Desde el punto de vista policial, los aspectos más interesantes del subprincipio de necesidad vienen de la mano del emergente y a la vez exigente escenario de intervención donde, tanto la concertación criminal, como el uso criminal de las comunicaciones electrónicas como una finalidad en sí mismas, exigen, en unas

[449] Perelló Doménech, Isabel. *El principio de proporcionalidad…op.cit.*, pág. 70.
[450] Perelló Doménech, Isabel. *El principio de proporcionalidad…op.cit.*, pág. 70.
[451] Para GONZÁLEZ-CUÉLLAR, *"el principio de necesidad tiende a la optimización del grado de eficacia de los derechos individuales frente a las limitaciones que pudieran imponer en su ejercicio los poderes públicos. Obliga a los órganos del Estado a comparar las medidas restrictivas aplicables que sean suficientemente aptas para la satisfacción del fin perseguido y a elegir, finalmente, aquella que sea menos lesiva para los derechos de los ciudadanos"*. Vid. González-Cuéllar Serrano, Nicolás. *Proporcionalidad…op.cit.*, pág. 189 y ss.

ocasiones, la penetración en aspectos sensibles de su secreto y, en otras, el acceso a meros datos técnicos con nula o escasa afectación al derecho a la intimidad.

Sin embargo, la misma aparición de las TIC, vistas como factor modificador de la conducta criminal, permiten a su vez la diversificación de las formas de injerirse con diferente intensidad en la intimidad de los investigados. Es decir, que el imperativo de hallar el medio menos gravoso o más moderado de adquirir la prueba para el proceso penal, encuentra su acomodo en la posibilidad de servirse de unas TIC que facilitan el recurso a medios técnicos mínimamente invasivos, idea esta que puede sustentarse en los ejemplos que se exponen en este trabajo.

Otro interesante aspecto a analizar es la relación del subprincipio de necesidad con la idea de la urgencia[452], pues las TIC permiten el análisis de los actos de comunicación y de cobertura de red relacionados con las emergencias de todo tipo, de cara a una reacción rápida y oportuna, tanto de la PJE como de las FFSS, que evite las situaciones de riesgo personal o catastrófico, de tan desgraciada actualidad y que no están siempre relacionadas con hechos delictivos.

Para el abordaje de la problemática reflejada en apartados anteriores, no todo es rigidez, al reconocérsele al Estado una cierta capacidad alternativa de maniobra para afrontar formas novedosas de limitar los derechos fundamentales en la forma en que esté previsto en la Ley[453], debido a que el interés elemental del Estado es, precisamente, la tutela integral de los derechos de todos los ciudadanos, que no deben perderse de vista cuando de forma tan estricta y a veces inflexible se cuidan los de los justiciables.

Por ello, y pese a que no pueda adoptarse una medida si no está específicamente contemplada en la legislación - y esto aún en el caso de que sea menos gravosa -, siguiendo a GONZÁLEZ-CUÉLLAR, debe hacerse una referencia a que:

---

[452] *Ibídem.*

[453] Para GONZÁLEZ-CUÉLLAR es del interés del Estado*:*

1. *Exigir el respeto por los derechos fundamentales de los ciudadanos es un interés del Estado aún cuando se trate de adoptar medidas restrictivas.*
2. *Interés en la tutela de otros bienes constitucionalmente protegibles.*
3. *Interés en el correcto desarrollo del proceso y en el adecuado funcionamiento de las instituciones procesales".*

Vid. González-Cuéllar Serrano, Nicolás. *Proporcionalidad…op.cit.*, pág. 245.

"A pesar de la falta de regulación de medidas alternativas en nuestra Ley procesal y sin perjuicio del deseable desarrollo legislativo de alternativas menos gravosas en relación con todas las injerencias practicables durante el proceso que sean sustituibles por medidas suficientemente idóneas, puede defenderse en España la posibilidad de que los Jueces apliquen medidas alternativas a las legalmente previstas siempre que sean observadas las siguientes condiciones dirigidas a evitar la arbitrariedad judicial (siempre que la interpretación de las normas sea en el sentido más favorable para la efectividad de los DF):

1. *Idoneidad y menor lesividad de la medida alternativa.*
2. *Cobertura legal suficiente de la limitación de los derechos que le medida restrinja. El principio de legalidad exige que toda restricción de DF se encuentre regulada por la Ley, aunque ahora se trata de admitir medidas que no están contempladas en la Ley, pero cuya aplicación es exigencia del principio de intervención mínima…Como la medida que ha de ser sustituida en la aplicación del principio de necesidad sí se encuentra, por definición, regulada por la Ley, pues de otro modo el examen de su proporcionalidad carecería de sentido por ausencia del presupuesto constituido por el principio de legalidad, la restricción del derecho limitado por la medida alternativa dispone de cobertura legal, ya que la Ley autoriza la limitación en un volumen mayor que el finalmente ocasionado por el medio sustitutivo menos gravoso. Por tanto, la relativización del principio de legalidad que de esta manera se produce es tan sólo parcial, de carácter cuantitativo y en interés del ciudadano, quien ve limitados sus derechos en un grado menor que el previsto por la ley con carácter general.*
3. *Existencia de una infraestructura necesaria para su aplicación (condición de carácter instrumental)"*[454].

Del enjundioso contenido de este pronunciamiento doctrinal, merece destacarse lo afirmado en el punto tercero, poniéndolo en relación con lo aportado

[454] Vid. González-Cuéllar Serrano, Nicolás. *Proporcionalidad…op.cit.*, pág. 200 y ss.

sobre la necesidad de implementar las necesarias salvaguardas tecnológicas en las que deben apoyarse todos los actores del proceso penal.

Por ello, en tanto no se promulgue la ansiada reforma de la legislación procesal, el principio de proporcionalidad debe operar como un seguro instrumento que comprenda, interiorice y aporte seguridad jurídica a la necesidad del Estado de llevar la justicia a aquellos escenarios que exijan una renovada interpretación de su derecho a injerirse en las comunicaciones, deslindado, en primer lugar su más exacta naturaleza con perfecta diferenciación, cuando proceda, de los demás derechos puestos en juego.

3. Proporcionalidad en sentido estricto

Para GONZÁLEZ-CUÉLLAR "*el principio de proporcionalidad en sentido estricto pretende determinar, mediante la utilización de las técnicas del contrapeso de bienes o valores y la ponderación de intereses según las circunstancias del caso concreto, si el sacrificio de los intereses individuales que comporta la injerencia guarda una relación razonable o proporcionada con la importancia del interés estatal que se trata de salvaguardar…Sus notas son:*

1. *Es un principio valorativo, pues presupone el estudio de la relación empírica medida-finalidad.*
2. *Supone la ponderación de los valores e intereses involucrados, esto es, una ponderación entre fines y medios.*
3. *Tiene un contenido material"*[455].

Sobre el carácter valorativo de este subprincipio coinciden muchos de los autores consultados, que ponen el acento en la ponderación de los *"diferentes intereses contrapuestos y las circunstancias concurrentes en cada caso"*, lo que sugiere, por otro lado, el valor de individualización que contiene respecto de la configuración

[455] Vid. González-Cuéllar Serrano, Nicolás. *Proporcionalidad…op.cit.*, pág. 225 y ss.

jurídica original – esto es, caso a caso - aplicada al diseño material de la específica medida sometida a control de proporcionalidad[456].

En igual forma, la valoración de la gravedad de una conducta compatible con la adopción de una medida limitativa de derechos considerada proporcional, deviene un elemento esencial de la resolución judicial a que se refiere el art. 18.3 CE. Sin embargo, esta actividad debe tener en cuenta, no sólo este importante aspecto sino, además, la transcendencia social[457] de los hechos que se investigan y, en mi opinión, la naturaleza del ámbito de intervención – modificado por el uso de las TIC – cuando no existan medios alternativos para adquirir la prueba.

Dadas las circunstancias expresadas a lo largo de todo este trabajo – que afectan claramente al ámbito de intervención y a la trascendencia social de lo que en él ocurre -, la estricta valoración de la gravedad, como elemento esencial y único, puede llegar a ceder en importancia jurídica ante otras necesidades bien justificadas de intervención[458].

Así, en la STC 104/2006, de 3 de abril (RTC 2006,104), se apreció la proporcionalidad de una medida limitativa del derecho al secreto de las comunicaciones sin considerar estrictamente la gravedad penológica objetiva del ilícito investigado (por tratarse de un delito contra la propiedad intelectual de los recogidos en el art. 270 CP) porque *"más allá de la pena señalada al delito investigado, resultan evidentes la enorme trascendencia y repercusión social de las conductas objeto de investigación, por tratarse de cuestión íntimamente relacionada con el uso y abuso de las nuevas tecnologías, y el grave perjuicio que son susceptibles de generar"*[459].

Por ello, en lo que centra el interés de la apreciación jurisdiccional de la proporcionalidad en estricto, sin tomar en consideración las referencias cuantitativas penológicas, el TC en su sentencia dice:

---

[456] Por todos, vid. Perelló Doménech, Isabel. *El principio de proporcionalidad…op.cit.*, pág. 70.
[457] Véanse las SSTSS de 25 de junio de 1993 (RJ 1993, 5244) y 23 de noviembre de 1998 (RJ 1998, 9198).
[458] La jurisprudencia así parece reconocerlo. Por ejemplo, en la STS de 7 de diciembre de 2004 (RJ 2005, 1328), se estimó la proporcionalidad de una intervención telefónica de un funcionario que vendía datos personales, conducta que suponía una alteración del funcionamiento de los órganos públicos. Vid. Lanzarote Martínez, Pablo. *Intervención de las…op. cit.*, pág. 806.
[459] Nótese que la STC se basa, entre otras cosas, en el potencial lesivo para el patrimonio que las conductas podían suponer *("…grave perjuicio económico son susceptibles de generar")* y no en el concreto peligro que habían efectivamente supuesto.

> *"En definitiva, en el juicio de proporcionalidad de la interceptación de las comunicaciones telefónicas, además de la gravedad de la pena, del bien jurídico protegido y de la comisión del delito por organizaciones criminales, también puede ponderarse la incidencia del uso de las tecnologías de la información, pues su abuso facilita la perpetración del delito y dificulta su persecución"*[460].

Es decir, que el TC incluye en sus pronunciamiento elementos ajenos a la gravedad – sin pretender con ello ignorarla -, para otorgar un valor determinante en el juicio de proporcionalidad a la versatilidad de las TIC y su idoneidad para los propósitos criminales, así como las dificultades que representa para lograr la tutela judicial efectiva. Tras esta posición no es difícil vislumbrar la presencia de todas y cada una de las características criminológicas que se vienen poniendo de manifiesto y la perentoria necesidad de un abordaje jurídico-procesal adecuado.

Puede concluirse, por tanto, que los aspectos más importantes del subprincipio de proporcionalidad en estricto guardan relación con el concepto de ***gravedad***[461,462] – que ha devenido insuficiente para valorarlos -, al desbordarse las percepciones que lo ataban a aspectos relacionados con la mera retribución penológica cuantitativa por el concreto delito cometido, establecida en los límites objetivos señalados en los arts. 13 y 33 CP – haciendo necesario también apreciar la ***trascendencia social de las conductas***[463], la ***importancia del bien jurídico protegido*** y el ***ámbito de intervención***[464,465,466], conceptos estos de apariencia autónoma pero que, dentro de la

---

[460] Vid. Lanzarote Martínez, Pablo. *Intervención de las…op. cit.*, pág. 806.

[461] Sobre esta cuestión y su problemática interpretación en relación con el art. 1.1 LCDCE, por todos, vid. Pérez Gil, Julio. *El nuevo papel de la telefónia móvil…op. cit.*, pág. 199.

[462] RODRÍGUEZ LAINZ excepciona del régimen general del art. 1.1 LCDCE respecto de la gravedad, el acceso por la PJE de propia autoridad a los datos relacionados con el registro de tarjetas prepagadas, ya que "*la disp. adic. única, apartado 4 LCDCE [respecto de las categorías incluidas en el apdo. 1] sí permite, sin embargo, la superación del límite de la gravedad del delito, al hablar solamente del concepto de delito, con tal que los principios de necesidad y proporcionalidad se respeten en el supuesto concreto. El dato identificador del adquirente, en concreto nombre y apellidos o denominación social, nacionalidad y número de identificación del documento de identidad exhibido, al menos en tanto en cuanto se conserve en tal concepto, será accesible para la investigación de cualesquiera delitos*". Vid. Rodríguez Lainz, José Luis. *Peculiaridades de la intervención judicial de comunicaciones electrónicas.* Diario La Ley, 2009.

[463] Vid. *Special Eurobarometer 371, Wave EB75.4 TNS Opinion & Social de la Comisión Europea.*

[464] Sobre la necesidad de tomar en consideración el ámbito en que se producen los delitos, GONZÁLEZ LÓPEZ afirma que *"partiendo de este umbral, atendida, al igual que sucede con la intervención, la idoneidad del acceso a este tipo de datos en relación con los delitos en cuya comisión se emplean las comunicaciones electrónicas (amenazas por tales medios, difusión de contenidos ilícitos por la Red, estafas informáticas, etc.), entendemos admisible que, tomando como referencia la regulación común al acceso a los datos de carácter personal, se establecieran previsiones específicas respecto de los delitos*

casuística del uso criminal de las TIC, tienen sugerentes puntos de encuentro, no exigiéndose en todos los casos de una forma estricta la apreciación de la gravedad en razón de la pena asociada al ilícito, sino en su ponderación conjunta, precisamente, con los otros aspectos mencionados[467], tomando en consideración la realidad social y su preocupación por las formas comisivas, que exige afrontar la aparición de nuevos *modus operandi* con independencia de la gravedad intrínseca de los hechos y por no existir otra alternativa en algunos casos que la de actuar en el mismo escenario en el que se producen[468,469].

---

en que las comunicaciones aparecen como medio de comisión. Esta circunstancia (la particular eficacia de la medida referida a los datos de tráfico) debería ser tenida en cuenta por el Juez al analizar el caso concreto y determinar si la medida se ajusta en éste a las exigencias del subprincipio del que nos estamos ocupando". Vid. González López, Juan José. *Los datos de tráfico…op.cit.,* pág. 379.

[465] VELASCO, en sendos párrafos dice al respecto que *"la constante necesidad de aplicar medidas restrictivas de algunos de los derechos fundamentales recogidos en el art. 18 CE, en delitos de leve penalidad, es otra característica de la investigación de este tipo de delitos que debe vincularse más a la esfera de utilización sobre la que recaen las nuevas tecnologías que a consideraciones innecesarias sobre la gravedad penológica",* así como que *"el Tribunal Constitucional aleja la caracterización de la "gravedad" necesaria para injerir derechos fundamentales en este tipo de investigaciones de meras consideraciones matemáticas como las consignadas a otros efectos en el art. 33 CP y las residencia en la afección a la relevancia jurídica penal de los hechos, su bien jurídico protegido y la trascendencia social afectados".* Vid. Velasco Núñez, Eloy. *Delitos cometidos a través de Internet…op. cit.,* pág. 73.

[466] En la STC 173/2011, de 7 de noviembre, frente a hechos de suficiente gravedad por sí mismos, el TC no deja de considerar la circunstancia coadyuvante del *iter criminis* relacionada con el uso de las TIC, al afirmar que "*hemos de valorar, además, que la investigación se circunscribía de manera específica a un delito de distribución de pornografía infantil, lo que resulta relevante, no sólo por la modalidad delictiva y la dificultad de su persecución penal al utilizarse para su comisión las nuevas tecnologías e Internet, sino fundamentalmente en atención a la gravedad que estos hechos implican, derivada ésta de la pena que llevan aparejados por referirse a víctimas especialmente vulnerables".*

[467] Sobre esto, GONZÁLEZ LÓPEZ observa algunas insuficiencias, ya que *"…tanto el TC como el TS han acudido principalmente a la gravedad de la pena que tiene aparejada el delito para valorar la proporcionalidad de la medida, un criterio que además es el seguido por el Derecho comparado y por el TEDH. Sin embargo, junto a éste, se ha acudido a nuevos fundamentos de la legitimación, como son el bien jurídico protegido y la relevancia social de los hechos (SSTC 166/1999, de 27 de septiembre, FJ 3; 167/2002, de 11 de diciembre, FJ 4), que constituyen conceptos difusos, escasamente garantes desde la perspectiva de la seguridad jurídica y con un marcado carácter subjetivo".* El autor se apoya en la siguiente nota al pie: *"En virtud de ello, se apunta en Montero Aroca, Juan, y otros. Derecho jurisdiccional III. Valencia: Tirant lo blanch, 2007,* pág. *170, que el tipo de procedimiento es indiferente para la proporcionalidad, ya que no se atiende al criterio exclusivo de la gravedad de la pena. En Gimeno Sendra, V., Derecho…, op.cit.,* pág. *408, se mencionan como ejemplos de tales delitos los que afectan al buen funcionamiento y al crédito de la Administración del Estado, los relativos a la corrupción política y los de carácter económico".* Vid. González López, Juan José. *Los datos de tráfico…op.cit.,* pág. 277.

[468] Algunos ejemplos, además de algunas de las expresiones fenomenológicas muy comunes de la casuística actual, lo constituirían aquellos en que la afectación alcanza a aspectos poco relevantes en cuanto a su gravedad intrínseca, como lo sería el uso inespecífico de una *botnet* para distribuir *spam*, usurpar una imagen de marca, para apropiarse de determinados datos, amenazar levemente a través de la red, "tutelar" en la *web* a los enfermos de anorexia para que sepan cómo evitar el tratamiento, etc., que, por su propia naturaleza tecnológica, no podrían ser estudiados sin liberar los DACE cuyo estudio permitiese su esclarecimiento.

Además, como señalan algunos autores, el enfoque cuantitativo de la pena, como límite objetivo de la gravedad, estaría sujeto a circunstancias de naturaleza coyuntural como los que se deducen de las sucesivas reformas de la normativa penal[470,471].

Sobre todo esto, en capítulos anteriores se analizó la cuestión de la necesidad de intervención de la PJE en un espacio que se podría denominar virtual, lugar inmaterial donde los ciudadanos han transferido, en tiempos relativamente recientes, partes importantes de las actividades que antes desarrollaban en la vida física y cuya investigación, cuando trascienden a lo criminal, debe basarse en el análisis de los innumerables actos de comunicación[472] que dotan a la maquinación delictiva del imprescindible sustrato técnico.

---

[469] Por recurrir al ejemplo del P2P, una sola película sujeta a derechos de propiedad intelectual puede descargarse simultáneamente por miles de personas, reconstruyéndola mediante un artificio técnico que la extrae, no de un único servidor, sino a base de unificar fragmentos proveídos desde centenares de servidores ubicados en decenas de países. Se debe hacer constar también que, para perseguir este delito, que no se considera grave, además de las limitaciones impuestas por el art. 270 CP y el contenido de la Circular 1/2006 de la Fiscalía General del Estado, se necesitaría un legislación procesal suficiente para intervenir en todos esos países mediante el uso de la tecnología aunque, todo ello, finalmente, será para perseguir a un infractor que se ha apropiado de algo cuyo valor no excede los veinte euros.

[470] Sostiene RODRÍGUEZ LAINZ sobre la referencia penológica que *"la evolución normativa del precepto perdería toda su lógica interna con la publicación de la LO 15/2003, de 25 de noviembre, para la que el delito grave pasaría a ser nada más y nada menos que el castigado con penas entre otras superiores a cinco años de prisión; y ello simplemente por una reconocida razón didáctica, sin más pretensión: diferenciar los delitos cuyo enjuiciamiento corresponde a las Audiencias Provinciales frente a los que competen a los Juzgados de lo Penal. Con la última gran reforma del Código Penal, la operada por la Ley Orgánica 5/2010, de 22 de junio, cualquier intento de buscar una razón de fondo a la diferenciación entre el delito grave y el menos grave ha perdido todo su interés".* MAEZTU, al comentar la cuestión del aumento de la penalidad, sugiere la idea de que responde a criterios de organización de la justicia. Vid. Maeztu Lacalle, David. *La identificación del titular del una dirección IP. Problemática en aplicación de la Ley 25/2007, de conservación de datos* en *El Proceso Penal en la Sociedad de la Información. Las nuevas tecnologías para investigar y probar el delito.* Coordinador: Pérez Gil, Julio. VVAA. Ed. La Ley. 2012, págs. 241-266, pág. 260. También, vid. Rodríguez Lainz, José Luis. *El principio de proporcionalidad…op. cit.*

[471] Tampoco parece adecuada la referencia a listados de delitos, como recomendó la Comisión Europea, en referencia a la lista de delitos contemplada en la orden de detención europea (Decisión Marco 2002/584/JAI del Consejo, de 13 de junio de 2002, *relativa a la orden de detención europea y a los procedimientos de entrega entre Estados miembros*). En mi opinión, este recurso obligaría a prescindir de otros criterios, como el del ámbito de intervención de las TIC o la transcendencia social de los hechos.

[472] Por ejemplo, mediante injerencias leves en el derecho a la intimidad, la PJE podía acreditar en el espacio físico la compra de productos o servicios (adquirir un billete de avión para acudir a una cita de narcotraficantes, publicar textos (citas con lenguaje convenido mediante anuncios en periódicos en papel), suplantar la identidad (falsificación de documentos) o escenificar un engaño (intentar una estafa). Sin embargo, todos estos actos en espacio virtual supondrían un acto de comunicación respaldado radicalmente por el derecho al secreto de las comunicaciones – cuya limitación supondría una injerencia grave en la intimidad - como lo serían, siguiendo con el ejemplo, visitar una *web* de viajes desde un ordenador personal o un *smartphone* y activar sucesivamente varios servicios subyacentes (accesos telemáticos secundarios a varias compañías aéreas y cuentas bancarias para efectuar los pagos

Puede decirse que, en estos casos, la prosperidad del *iter criminis* depende de la calidad de las comunicaciones electrónicas que se empleen para alcanzar plenamente todas sus ilícitas finalidades y ello con independencia de que consistan o no en intercambios de contenidos íntimos.

Incuestionablemente, de no contarse con un derecho positivo que lo ampare, todo lo anterior hace extremadamente dificultosa o imposible la apreciación de la proporcionalidad en sentido estricto o que su valoración devenga tan controvertida que sólo pueda estimarse sobre fragmentos mínimos del escenario de intervención, ya que, por mor de precisarse el acceso a las comunicaciones electrónicas o a sus DACE, solo serían accesibles de considerarse la posible existencia de un delito grave que lo justifique.

La calificación de grave, normalmente, estará ausente de muchas de estas tipologías, según el concepto clásico de la retribución penológica cuantitativa. La consecuencia inmediata que cabe esperarse será el veto a la intervención mediante la invocación de las medidas limitativas previstas en el art. 18.3 CE, con la consiguiente omisión de una intervención de los poderes públicos que podría ser objetivamente necesaria como única vía para tutelar los derechos lesionados.

Pero la terca realidad criminal de las TIC es otra, ya que muchas de las maquinaciones, a cuya eficaz resolución el Estado de Derecho debiera aspirar, no puede hacerlo al estar constreñidas sus facultades por la rigidez del concepto de gravedad penológica, ayudado por una incomprensión de la naturaleza material y jurídica del espacio en que tienen lugar.

RODRÍGUEZ LAINZ, razonando sobre las tensiones generadas por la entrada en vigor de la nueva e intrusiva LCDCE y su ámbito objetivo de aplicación limitado a los delitos graves, confirma que, efectivamente, la tutela judicial varía dependiendo de el hecho de que los sucesos delictivos idénticos se produzcan en el espacio físico o en el virtual.

---

por el servicio contratado), publicar una amenaza velada en un "tablón virtual" de anuncios públicos de una red social, simular una identidad en red (para lograr el acceso carnal a un menor) o urdir una trama de *phising* o *pharming* para vaciar de su patrimonio o datos personales a un número indeterminado de víctimas.

Con mención expresa a delitos no graves, como a algún caso de injurias, pequeñas estafas o calumnias, de la aportación de este autor puede deducirse que, efectivamente, los mismos hechos tendrían una tutela judicial efectiva y sin problemas de verificarse en el espacio físico pero que, caso de producirse por vía telemática, no podrían recibir una protección igual por no poderse acceder a las bases de DACE debido a la prohibición contenida en el art. 1.1 LCDCE[473,474].

Consecuentemente, el Estado de Derecho debe asumir la necesidad de intervenir en el espacio virtual de una forma análoga a como lo hace en el espacio físico, aceptando sus realidades y tomando en consideración que, al hacerlo, no exista un compromiso inaceptable sobre el derecho al secreto de las comunicaciones cuando, en realidad, solo suponga una injerencia leve en el derecho a la intimidad[475], cuestión está que, por otro lado, resultará siempre difícil discernir.

La injerencia en los DACE puede, por lo demás, considerarse menor, ya que como sostiene GONZÁLEZ LÓPEZ, apoyándose en las notas que en el siguiente texto se incluyen, *"…Las particularidades que supone la intervención de los datos de tráfico en relación con el principio de proporcionalidad en sentido estricto radican en la menor*

[473] En palabras de RODRÍGUEZ LAINZ, *"frente a un tener al alcance de la mano tan apetecible pero inaccesible fruto, como si se tratara del castigo divino impuesto a Tántalo"*. O, en mi opinión, si quiere verse desde el otro extremo, que el que calumnia, injuria o estafa en red goza en la práctica de un plus de impunidad garantizado por la rigidez de esta ley, al no tener muchos de su tipos penales – por lo demás muy comunes en red - fijada una retribución como la prevista en los arts. 13 y 33 CP.
El autor no parece encontrar suficiente fundamento en la tutela judicial efectiva como para romper la barrera de la gravedad, al sostener que *"…la norma [la LCDCE] marcaba un tope concreto: el concepto de delito grave. Concepto que debía operar como frontera, criterio de exclusión, que habría de dejar fuera de tan colosal fuente de información heurística cualquier intento, más allá de tal barrera, de utilización de la información contenida en dichas bases de datos para cualesquiera fines investigadores que pudieran pretender justificar en términos de justicia material su acceso y utilización; y ello por muy loable que fuera el empeño de, haciendo uso de tales herramientas a disposición judicial, pretender atender al principio de garantía de la tutela judicial efectiva como fundamento final de la decisión"*. Vid. Rodríguez Lainz, José Luis. *Hacia un nuevo entendimiento del concepto de gravedad del delito en la Ley de Conservación de Datos relativos a las Comunicaciones Electrónicas*. Diario La Ley, 143/2012, Nº 7789, Sección Doctrina, 2 Feb. 2012, Año XXXIII, Editorial LA LEY.

[474] También, vid. Martín Pallín, José Antonio. 2008. *El equilibrio entre la conservación…op. cit.,* pág. 154 y ss.

[475] RODRÍGUEZ LAINZ señala en este sentido que *"la STS 780/2007, de 3 de octubre, que tras distinguir con claridad la naturaleza de contenido de comunicación y dato de carácter personal de los datos de tráfico en función del momento y la fuente de su obtención, sienta, ya aparentemente con carácter consolidado, la doctrina de que el recabo del listado de llamadas requiere de «...un nivel de exigencia y control mucho más bajo que el de una intervención de las conversaciones porque la injerencia es mucho menor sin que exista vulneración al derecho fundamental al secreto de las comunicaciones»".* Vid. Rodríguez Lainz, José Luis. *El principio de proporcionalidad…op. cit*.

exigencia que se plantea al realizar la ponderación característica de este principio[476]*. Así, la menor gravedad de la injerencia que supone esta modalidad de intervención puede utilizarse como argumento para permitir la práctica de la misma respecto de infracciones que no hubieran legitimado una invasión en el contenido de las comunicaciones. Asimismo se ha acudido por la doctrina a esta característica para mantener la posibilidad de su empleo respecto de "infracciones criminales que no son tenidas por el legislador como precisamente graves, pero que pueden incidir profundamente en la libertad, intimidad, salud o sosiego de los ciudadanos, en especial en lo referente a modalidades criminales tales como las amenazas, coacciones, injurias, vejaciones...", admitiendo su aplicación incluso a supuestos de faltas*[477,478]*.*

Posición, sin duda, de una inestimable importancia para comprender las razones que obligan a ponderar, con cierta amplitud de miras, el alcance real que en términos de sacrificio del derecho fundamental pueda suponer la intervención de los DACE[479,480].

D. Requisitos extrínsecos del principio de proporcionalidad

1. Judicialidad

La ***reserva de judicialidad*** contenida en la CE sobre la capacidad del Estado de limitar los derechos fundamentales, aunque no es universal para todos ellos, alcanza

[476] Así se constata en la STC 123/2002, de 20 de mayo (FJ 6), cuando sostiene que "*no puede desconocerse la menor intensidad de la injerencia en el citado derecho fundamental*".
[477] Rodríguez Lainz, J.L. I*ntervención…*, *op.cit.*, p.235 y *ss.*
[478] Vid. González López, Juan José. *Los datos de tráfico…op.cit.,* pág. 277 y ss.
[479] Nótese que el autor citado hace estas referencias en fecha anterior a la promulgación de la LCDCE.
[480] Un buen ejemplo de la evolución jurisprudencial positiva, en el sentido de valorar la proporcionalidad en relación con el grado de injerencia que pueda suponer, bajo determinadas circunstancias, no en el secreto de las comunicaciones sino, en realidad, en otros aspectos del derecho a la intimidad, lo supone el cambio de línea doctrinal de la STS 130/2007 a la ya consolidada desde la promulgación de la 249/2008, en que de suponerse una grave limitación de estos derechos por el uso del *IMSI Catcher* (obtención del IMSI y el IMEI mediante una análisis del espacio radioeléctrico), se pasó a considerar su utilización por la PJE no suponía sino tan sólo una leve injerencia en el derecho a la intimidad, situando su empleo a efectos jurídicos a extramuros de la limitación de los derechos específicamente contenidos en el art. 18.3 CE.

de manera inequívoca al núcleo esencial de los más sensibles[481,482]. Su materialización representa una de las aportaciones más valiosas a la seguridad jurídica y, en definitiva, a la protección de los derechos fundamentales en un país democrático[483].

Sin embargo, pueden introducirse algunos elementos de discusión sobre este particular que, lejos de ensombrecer el papel superior que en la tutela de los derechos vinculados al secreto de las comunicaciones se reserva a los Jueces, contribuyen y hacen más eficaz y segura esta trascendental función de garantía constitucional.

Se trata, de un lado, de la instauración de las necesarias salvaguardas, tanto jurídicas como materiales, que complementen su acción como elemento de aseguramiento de la veracidad, autenticidad e integridad de la prueba y, de otro, de la consideración del tiempo en que ha de producirse el control jurisdiccional de una medida limitativa del secreto de las comunicaciones, a considerarse en determinados y muy precisos casos – que debieran estar bien tasados -, esto es, de las excepciones a la obligación de contar con una resolución judicial previa a la injerencia en el derecho fundamental afectado.

La discusión en este punto no es sencilla, pues la Constitución, la jurisprudencia y la doctrina son claras y contundentes respecto de la reserva exclusiva de judicialidad contenida en el art. 18.3 CE, pero sí invita a alguna reflexión, al menos, teórica y práctica, sobre algunos aspectos de interés.

---

[481] Para GONZÁLEZ-CUÉLLAR, *"la CE impone el requisito extrínseco subjetivo de judicialidad para la limitación de los derechos fundamentales en los arts. 17.2, 17.4, 18.2, 18.3, 20.5 y 22.4, por ser los órganos judiciales los constitucionalmente previstos para garantizar de forma inmediata de estos derechos, quedando sometido a su juicio la decisión sobre la proporcionalidad de las medidas limitativas".* Vid. González-Cuéllar Serrano, Nicolás. *Proporcionalidad…op.cit.*, pág. 109.

[482] Para MARCHAL, *"la necesaria intervención del poder judicial al limitar derechos fundamentales se encuentra, en primer lugar, en que la actividad jurisdiccional está vinculada necesariamente al derecho, cuyo interés, como ya quedó expuesto, es la garantía de los derechos e intereses lesionados. En un segundo orden, la actividad jurisdiccional ejerce una actividad de cierre del sistema de garantías mediante la adecuación al caso concreto y la corrección de las desviaciones que se produzcan en su aplicación. Pero, en tercer lugar, será el carácter de la imperatividad, de la posibilidad de que un poder real, operativo e independiente, con capacidad de imponerse a los demás poderes del Estado cuando la situación lo exija, la que configurarán a la autoridad judicial como garantía de las garantías al decidir conforme al derecho y solo a derecho".* Vid. Marchal Escalona, Nicolás. *Policía Judicial…op.cit.,* pág. 49.

[483] Por todas, véase la STS de 22 de febrero de 2007 (RJ 2007, 841), donde se proclama la exclusividad judicial, la realización en el marco de una investigación criminal, la ponderación de la proporcionalidad de la medida, su excepcionalidad, la perfecta fijación de su ámbito subjetivo, su motivación (lo que es extensivo a la disposición de las prórrogas) y la permanente actividad de control judicial durante toda la vida de la medida.

Una de estas cuestiones es la de las ***salvaguardas***, dentro del marco general de las garantías constitucionales en las que la PJE pudiera y debiera operar con una mayor seguridad jurídica, siempre bajo el amparo del actor jurisdiccional.

Visto desde su perspectiva material, el concepto de salvaguarda (o salvaguardia), en sintonía con la acepción cuarta del diccionario, respondería a la suma de *custodias, amparos o garantías* a los que el Estado de Derecho podría recurrir, a los efectos que interesan y a la luz del art. 24 CE, para asegurar la tutela judicial efectiva y el derecho a la defensa de los ciudadanos, de forma que los instrumentos de prueba, sea cual fuere su naturaleza, material o inmaterial, e independientemente del operador jurídico que los invocase, proporcionarán al juzgador la irrefutable certeza sobre su idoneidad para erigirse en el sustrato material que asegure la veracidad, integridad y autenticidad de los hallazgos que por su mediación se certifiquen, de forma que se sometan en el acto de juicio oral a su debida contradicción y valoración como prueba, esto es, en definitiva, a fundamentar su validez objetiva para cumplir con las finalidades el proceso penal.

La progresiva implementación de salvaguardas tecnológicas en materia de las TIC[484], no obstante, ha suscitado desde siempre en la doctrina y la jurisprudencia una irracional reserva, de la que no queda exenta de su tanto de culpa la pretendida, pero inexistente, pulsión de la PJE de controlar la vida de los ciudadanos (cual si del Gran Hermano redivivo se tratase[485]), como tan inoportunamente sucedió con la polémica

[484] *Ibídem*.

[485] La polémica, con rasgos de leyenda urbana o de *thriller* propio de una novela de John Le Carré, en la que no faltó su uso como munición en la contienda política (poniéndose en cuestión irresponsablemente la solvencia del Estado de Derecho), llegó a su paroxismo en épocas coetáneas a la de la promulgación de las diversas SSTS que validaron la solvencia del SITEL en torno al año 2009. Como botón de muestra, alguna de las perlas de BERMEJO: *"El SITEL es un avanzado sistema informático desarrollado por la multinacional Ericsson, que permite la interceptación sin límite, de todas las telecomunicaciones que tengan lugar en España…el gran problema que se plantea con la norma que regula SITEL (La Ley 25/2007 de conservación de los datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones), es que los Agentes facultados pueden a acceder a una serie de datos que afectan directamente a la intimidad personal, sin ninguna autorización judicial previa".* Sin más comentarios, vid. Díaz Bermejo, Guillermo. *SITEL. La gran oreja del Gobierno no tiene suficientes garantías jurídicas.* Noticias Jurídicas, octubre de 2009 (Disponible en: http://noticias.juridicas.com/articulos/20-Derecho%20Informatico/200910-4939479023902378.html). También, vid. Ortíz Pradillo, Juan Carlos. *Hacking legal al servicio de la investigación criminal: nuevos instrumentos para la investigación y prueba de la delincuencia informática.* Proyecto de Investigación I+D DER2008-03378. *Problemas procesales de la ciberdelincuencia y de la ciberresponsabilidad*, págs. 67-92.

del SITEL, ya felizmente saldada para fortuna del Estado de Derecho[486,487], y que puede tomarse como ejemplo, en lo negativo, de la afirmación contenida en este párrafo[488].

Sin embargo, para la aceptabilidad de un adecuado sistema de salvaguardas destinado a la limitación de los derechos fundamentales en una sociedad democrática, el CEDH no exige siquiera la participación de una Autoridad Judicial para la injerencia en el protegido por el art. 8 CEDH respecto de la intervención de las comunicaciones[489], apreciación que sirve de argumento para, sin mayores pretensiones, justificar y comprender, desde un punto de vista meramente descriptivo, hasta qué punto su seguridad jurídica puede descansar en un conjunto diverso de factores que, bien normativizados, sumen las garantías aportadas por el hecho de la intervención de la propia PJE, de los operadores jurídicos y, también, de los elementos y contrastes tecnológicos y certificaciones que aseguren la total objetividad de la prueba en cuanto a su validez, autenticidad, veracidad e integridad.

Todas estas posibilidades en modo alguno vacían las funciones jurisdiccionales claramente instituidas en la CE, sino que, antes bien, las enriquecen y las hacen, no sólo más seguras y objetivas, sino que las llenan de nuevas posibilidades para la calidad del proceso de contradicción en el juicio oral.

Pero el legislador constitucional español fue contundente en la redacción del art. 18.3 CE *in fine (“…salvo resolución judicial”)*, con lo que despejó todas las dudas al respecto, cortando al mismo tiempo en seco cualquier propuesta que, siendo legítima

---

[486] *Ibídem*. Vid. (SSTS 19, 23 de Marzo, 6 de Junio, 5 de Noviembre, 30 de Diciembre de 2009 y 15 de julio de 2010.

[487] Pero si, pese los pronunciamientos del TS y de la AEPD, quiere recibirse una nueva dosis de hipergarantismo sobre el incomprendido SITEL, vid. Fernández Rodríguez, J.J. *La intervención de las comunicaciones digitales: a propósito del sistema SITEL.* AAVV. *Cuestiones de inteligencia en la sociedad contemporánea*. Seminario de Estudios de Seguridad y Defensa USC-CESEDEN. Centro Nacional de Inteligencia. Ministerio de Defensa, 2011, págs. 61-76.

[488] En un capítulo posterior y con una finalidad ilustrativa sobre la cuestión del SITEL, se incluirá un detallado análisis del voto particular contenido en la STS 1215/2009, que resolvió el Recurso de Casación 404/09.

[489] GONZÁLEZ-CUÉLLAR sostiene que *“la jurisprudencia del TEDH no considera imprescindible la previa autorización judicial para la autorización de comunicaciones telefónicas, e incluso ni siquiera entiende ilegítima la supresión del control judicial posterior. Aun considerándolo deseable, por ofrecer la intervención judicial garantías de independencia, imparcialidad y regularidad en el procedimiento, admite el Tribunal de Estrasburgo que la exclusión del control no transgrede los límites del CEDH si se compensa con otras salvaguardas legales (en este caso órganos de control parlamentario en la RFA, p.e.), privándose con ello el Poder Judicial no sólo de la primera palabra, sino también de la última”. Ibídem*. Vid. González-Cuéllar Serrano, Nicolás. *Proporcionalidad…op.cit.*, pág. 111. Vid. STEDH, DE 6 de septiembre de 1978, Caso *Klass*.

y aceptable en otros espacios de nuestro entorno democrático[490], difícilmente tendrían cabida en el español. Por ello, las escuálidas propuestas que se desgranarán en este estudio quedarán necesariamente ceñidas a aspectos exiguos o menores de la limitación del derecho fundamental al secreto de las comunicaciones.

Sobre el ***carácter previo***[491] de que debe gozar la resolución judicial para la limitación del derecho fundamental al secreto de las comunicaciones - cuestión de la que ya se ha hablado algo en párrafos anteriores -, GONZÁLEZ-CUÉLLAR se pronuncia de una manera específica diciendo que:

> *"No se reclama desde esta exigencia de judicialidad la intervención de los órganos de la Jurisdicción en un momento cualquiera tras la adopción de la medida con el objeto de controlar su legalidad. Ciertos derechos constitucionales sólo pueden ser restringidos con autorización del órgano judicial, intervención que ha de ser necesariamente previa a la limitación de ciertos derechos o producirse de modo inmediato tras la restricción de otros".*

Aunque el autor estudiado admite el control posterior de jurisdiccionalidad para los arts. 17.2, 17.4 y 18.2 CE, deja meridianamente clara la exclusión de esta posibilidad en lo referido al art. 18.3 CE, con la única salvedad de lo dispuesto en el art. 55.2 CE[492,493], en relación con las investigaciones relacionadas con las ***bandas armadas*** *o los* ***elementos terroristas***. Salvedad que se materializó mediante la introducción en la LCRIM, tras la promulgación en 1988 de una ley orgánica, del hoy vigente art. 579, en cuyo párrafo 4º se contiene el siguiente precepto:

> *Art. 579.4 LCRIM: "En caso de urgencia, cuando las investigaciones se realicen para la averiguación de delitos relacionados con la actuación de*

[490] GIMENO hace notar al efecto, por ejemplo, *"las escuchas administrativas"* de algunos países de nuestro entrono. Vid. Gimeno Sendra, Vicente. *La intervención de las comunicaciones,* en Marchal Escalona, Nicolás (Director). *Manual de lucha…op. cit.,* pág. 570. También, vid. González-Cuéllar Serrano, Nicolás. *Proporcionalidad…op.cit.*, pág. 111.

[491] Según el diccionario, previo es *"lo anticipado, que va delante o que sucede primero"*.

[492] Art. 55.2 CE: *"Una Ley Orgánica podrá determinar la forma y los casos en los que, de forma individual y con la necesaria intervención judicial y el adecuado control parlamentario, los derechos reconocidos en los artículos 17, apartado 2, y 18, apartados 2 y 3, pueden ser suspendidos para personas determinadas, en relación con las investigaciones correspondientes a la actuación de bandas armadas o elementos terroristas"*.

[493] *"…la garantía que nuestra Constitución articular en trono a los derechos consagrados en los arts. 17, 18.2 y 3, 20.5 y 22.4 sitúa nuestro ordenamiento jurídico entre los más garantistas en este terreno".* Vid. González-Cuéllar Serrano, Nicolás. *Proporcionalidad…op.cit.*, pág. 109 y ss.

bandas armadas, elementos terroristas o rebeldes, la medida prevista en el número 3 de este artículo podrá ordenarla el Ministro del Interior o, en su defecto, el Director de la Seguridad del Estado, comunicándolo inmediatamente por escrito motivado al Juez competente, quien, también de forma motivada, revocará o confirmará tal resolución en un plazo máximo de setenta y dos horas desde que fue ordenada la observación". (Redactado según LO 4/1988, de 25 de mayo).

Anotaré por mi parte que los elementos esenciales que se extraen de la redacción de este artículo son:

- La urgencia o necesidad imperiosa de resolver sobre cuestiones perentorias atinentes a una determinada investigación de la PJE.
- La lógica reserva a hechos de extrema gravedad relacionados con determinados fenómenos criminales que, en la época de la redacción del precepto constitucional del art. 55.2, se consideraron justificados en relación con la carga de amenaza a la sociedad española (las investigaciones relacionadas con las bandas armadas y el terrorismo).
- El señalamiento de las autoridades administrativas del más alto nivel que quedaban legitimadas para limitar el derecho al secreto de las comunicaciones
- La obligación para las autoridades anteriores de disponer la medida mediante escrito motivado.
- La disposición de un control posterior de jurisdiccionalidad sobre la concreta medida adoptada y el establecimiento de un determinado plazo de validación judicial para que surtir los debidos efectos en el proceso penal, lo que evidencia la asunción de una serie de inaceptables riesgos jurídicos para quien actuase invocando esta disposición legal.

Sobre la excepción contenida en el art. 579.4 LCRIM, es también interesante hacer notar que cuando el legislador la introdujo en 1988, añadió *ex novo* una categoría a las contempladas en el art. 55.2 del texto constitucional, extendiendo el

catálogo de las amenazas a la seguridad del Estado a los ***rebeldes***[494] y acreedoras, por tanto, de las medidas limitativas de derechos fundamentales cuyo control de jurisdiccionalidad podía ser posterior a su instauración material.

Todo esto sugiere que, de respetarse la reserva de ley orgánica establecida en el art. 81.1 CE[495] para la regulación de todas aquellas materias que pudieran afectar a un derecho fundamental, el precepto constitucional del 55.2 bien podría flexibilizarse ponderadamente en el sentido de adaptarse a las gravísimas amenazas emergentes que la defensa de la seguridad pública requiriese, materia en la que debieran incluirse, en mi opinión, tanto determinadas expresiones de la moderna delincuencia compleja de las que desestabilizan al Estado de Derecho[496], condicionando incluso su propia supervivencia, como para intervenir en aquellas situaciones de urgencia vital en que, sin ser materia de bandas armadas, terrorismo[497] o actuación de *elementos rebeldes*, fuese preciso obtenerse directamente del prestador de servicios de la sociedad de la información o de la operadora de redes de comunicaciones electrónicas los DACE[498] necesarios para resolverlas.

A estos fines, una ley orgánica debiera precisar de *lege ferenda* los más exactos límites para el ejercicio de tan excepcionales facultades o, en su caso, de su mera

[494] Que son quienes, de acuerdo con el art. 472 CP "…*se alzaren violenta y públicamente para cualquiera de los fines"* que se contemplan en el mismo artículo, categoría completamente distinta a las contenidas respectivamente en los conceptos de "banda armada" o "elemento terrorista", como es de ver.

[495] Art. 81.1 CE: *"Son Leyes orgánicas las relativas al desarrollo de los derechos fundamentales y de las libertades públicas, las que aprueben los Estatutos de Autonomía y el régimen electoral general y las demás previstas en la Constitución".*

[496] *Ibídem*.

[497] La sociedad actual, y desde luego el legislador constitucional de 1978, hacen residir toda la carga de la amenaza en el terrorismo. Pero este fenómeno es, con seguridad, ajeno a una sociedad a la que ataca "desde fuera". Sin embargo determinadas e inquietantes formas delictivas organizadas o complejas pueden poner en duda la gobernanza de la sociedad, atacándola "desde dentro". En este sentido, en el *Special Eurobarometer 371, Wave EB75.4 TNS Opinion & Social* de la Comisión Europea, de noviembre de 2011, no se advierte una diferencia clara entre una u otra preocupación en la percepción de los ciudadanos europeos (25 %, terrorismo, 23 %, criminalidad organizada, extendiéndose también su preocupación por la corrupción a un 18 % de los consultados). En la ficha española, destaca una preocupación lógicamente mayor por el terrorismo (ETA, yihadismo) pero también por los riesgos emergentes relacionados con la corrupción, la delincuencia organizada y la delincuencia informática, con una confianza en su afrontamiento por el Estado poco alentadora (Pregunta QC5b). Por su parte, la *Séptima edición de los riesgos globales del 2012* del Foro Económico Mundial refleja una apreciación similar, poniendo un especial acento a los riesgos tecnológicos asociados a los ciberataques. A veces, parece que se fuerza el lenguaje para aportar artificialmente carga de amenaza al fenómeno al que ha de referirse utilizando eufemismos como "terrorismo mafioso" o "terrorismo empresarial", lo que ayuda en poco a enfocar el problema racionalmente. Por ello, en mi opinión, si están justificadas determinadas medidas para el terrorismo, podrían estarlo también para la delincuencia organizada.

[498] Básicamente los regulados en la LCDCE que centran el interés de este estudio.

remisión al régimen general de protección de datos, materia de la que se tratará en capítulos posteriores.

Por otra parte, dicho sea a título de mero comentario ilustrativo, las facultades que fueron otorgadas mediante el art. 579.4 LCRIM al ***Ministro del Interior*** *o al* ***Director de la Seguridad del Estado***[499] (hoy día Secretario de Estado de Seguridad) jamás fueron ejercidas en el ámbito de la lucha contra el terrorismo, hasta donde me ha sido posible indagar. Las razones son tan obvias que ilustran hasta qué punto, por un lado, el legislador se vio legitimado para recurrir a formas audaces para dotar de instrumentos legales a la PJE y como, por otro, esta o su cadena de mando orgánico no los utilizó nunca por sentirse, a todas luces, jurídicamente insegura y para evitar incurrir en alguna causa de nulidad que comprometiese el eventual éxito de una investigación, cuya prueba se hubiera obtenido, en parte, por la invocación del contenido de este articulo (sin olvidar el racional temor de los agentes a adquirir alguna responsabilidad penal).

A lo anterior se debe sumar, en mi opinión, la cuestión de su innecesaridad porque, a su alumbramiento en 1988, ningún beneficio aportaba al tratamiento de la urgencia en la investigación respecto de las habilitaciones anteriores y que no pudiese ser resuelta con mayor inmediatez, celeridad y mayores garantías jurídicas por un Juez de Instrucción (ya que tal necesidad estaba supeditada únicamente a lograr la debida diligencia en la instauración excepcional de determinadas medidas limitativas de derechos fundamentales relacionadas normalmente con la telefonía fija, pues a la promulgación de la ley en aquel año no existían ni la telefonía celular ni las comunicaciones a través de Internet), a lo que ningún valor añadido podían aportar, nada más y nada menos, que el Ministro del Interior o el Secretario de Estado de Seguridad quienes, bajo ningún concepto reúnen el perfil de disponibilidad que no presentaran por sí mismas las diversas autoridades judiciales a los mismos efectos.

Pero ahí queda, por lo demás, un precedente legislativo que, en mi opinión, se podría invocar[500] para resolver ciertas cuestiones mediante una profunda revisión de la

[499] Adviértase que se trata de altos cargos de la Administración del Estado y, en ningún caso, miembros de la Policía Judicial.

[500] No obstante, es unánime la doctrina al considerar cerrada la lista de categorías contenida en el art. 579.4 LCRIM. Por todos, valga el comentario de GIMENO diciendo que *"la especialidad de este régimen,*

normativa jurídica actualmente vigente, que debiera utilizarse para responder decididamente ante necesidades planteadas en situaciones de urgencia vital o riesgo catastrófico, para cuyo abordaje la PJE está claramente necesitada de nuevas habilitaciones legales, como sería el caso de la disposición diligente de los DACE.

El efecto sobre la función policial del carácter previo del mandato judicial es, en cualquier caso, absoluto, incluido lo referido a la inexistencia de casos de aplicación práctica, por innecesaria y arriesgada jurídicamente, de las facultades establecidas en el art. 579.4 LCRIM por las autoridades administrativas – que no de la Policía Judicial – del Ministerio del Interior.

Otra de las cuestiones controvertidas, más allá de cuanto pueda decirse del deseable uso seguro de la telemática en la Administración de Justicia, es la que se deduce de la excesiva ***burocratización*** que lastra el procedimiento penal español, pues quedando garantizada la seguridad jurídica que debe ser inherente a cualquier procedimiento legal por razón de su expresión documental fehaciente, la obtención de un mandamiento judicial previo a la práctica de determinados actos procesales supone una importante rémora en aquellos casos en que razones de urgencia y eficacia aconsejarían legislar un más eficiente procedimiento de control jurisdiccional, más diligente en cuanto a su concepción y más efectivo en cuanto a sus posibilidades de acceder a la inteligencia criminal[501].

---

ello no obstante, se agota con lo dicho, sin que pueda justificarse laxitud alguna en el control judicial de estas intervenciones, tal como tuvo ocasión de recordar el TC en una lejana decisión (STC 26 de marzo de 1996)". Vid. Gimeno Sendra, Vicente. *La intervención de las comunicaciones,* en Marchal Escalona, Nicolás (Director). *Manual de lucha…op. cit.,* pág.572.

[501] Algunas observaciones sobre este particular serían las siguientes:

- La solicitud de mandamiento judicial se hace mediante un documento escrito en el que el Instructor policial desgrana las razones de idoneidad, necesidad y proporcionalidad de la medida que solicita, con referencia a razones fundadas de orden fáctico e indiciario que haya podido recoger durante las investigaciones preliminares, lo que conlleva la correspondiente carga burocrática.
- El anterior documento debe presentarse físicamente ante la autoridad que debe concederlo, modificarlo o denegarlo, lo que conlleva un traslado del Instructor policial a la sede judicial. Los procedimientos telemáticos de intercambio de documentos con firma electrónica, plenamente disponibles en otros ámbitos de la sociedad y sus administraciones públicas, tan sólo asoman hoy en la de Justicia tímida e insuficientemente.
- Su atención y diligenciamiento está sujeto a la disponibilidad personal del Juez y del Fiscal, así como del cuerpo funcionarial del juzgado que se halle en funciones de guardia.
- Su concesión está condicionada también al grado de conocimiento actualizado y suficiente que el Juez y el Fiscal tengan sobre asunto en cuestión, especialmente cuando se trate de

La experiencia señala además que los plazos que median entre la solicitud y la ejecución de los mandamientos judiciales pueden ser incluso de semanas, ajenos por completo a la dinámica normal de cualquier investigación por simple que ésta sea. En el caso de los secuestros y desapariciones de personas, por ejemplo, en que la urgencia de actuar se torna en ocasiones angustiosa, las unidades especializadas de la PJE estiman que su plazo medio de entrada en efectividad es de unas inaceptables cuatro horas desde que se instaura la necesidad de la obtención de la IDACE, lo que incluye las demoras que puedan sumar las operadoras en su aportación de datos. Es evidente que este periodo de "ceguera de datos" es inasumible si lo que se desea es salvar la vida de una persona o conseguir que recupere su libertad o conserve su integridad.

Es conveniente también contemplar aquellos casos en que pueda invocarse el ***estado de necesidad***[502]**,** en los que existiría legitimidad para ocasionar daños a

investigaciones complejas. La respuesta judicial vendrá a su vez determinada por la calidad del juicio de proporcionalidad que en su virtud pueda realizar.

- El procedimiento de formación del auto judicial, acordando de forma motivada la medida, es también escrito y debe ejecutarse en ocasiones a su presencia o con la delegación en el funcionario judicial que designe. Vuelven, por tanto, a reproducirse condicionamientos de disponibilidad personal.
- Una vez librado, debe enviarse por la PJE por canal seguro a la operadora de telecomunicaciones tras cumplimentar un proceso burocrático por vía telemática. Una vez hechas las comprobaciones pertinentes, la operadora cederá los datos a la PJE.
- Los mandamientos judiciales no pueden contener fórmulas abiertas que permitan el análisis inteligente de fuentes de datos, esto es, limitan la habilitación del agente de la Policía Judicial para la obtención de datos muy concretos, pero nunca informaciones que puedan ser elaboradas, precisamente, mediante el análisis técnico de dichas fuentes y, mucho menos, utilizando para ello herramientas informáticas específicas. La obtención de estos mismos resultados, que conllevaría poco esfuerzo de contarse con la habilitación adecuada y mínima injerencia en la intimidad de los investigados, exigiría de sucesivos mandamientos que se harían, a la postre, incompatibles por completo con la dinámica que demandaría la propia investigación.
- Puede ser que las razones de urgencia policial no sean siempre tenidas en cuenta, sino tan sólo las meramente jurídicas.

[502] Junto al estado de necesidad, GONZÁLEZ-CUÉLLAR contempla también otro concepto jurídico – para rechazarlo -, cuyo contenido se trasluce ubicado en algún extremo del relativo a la necesidad social imperiosa, y que consistiría en el trasvase al proceso penal del ***estado de necesidad justificante*** ante determinadas situaciones para las que el Derecho no tuviese una previsión concreta, de tal forma *"que condujera incluso a la posibilidad de adopción, por parte de órganos jurisdiccionales o administrativos, de medidas legalmente inadmisibles cuando concurrieran importantes intereses del Estado […] para compensar así las carencias de las normas que habilitan a los poderes públicos para restringir los derechos fundamentales en la persecución de fines legítimos".* En la discusión doctrinal a la que me adhiero sobre esta cuestión, no precisamente pacífica, el autor se decanta por considerar inaceptable el peligro que este planteamiento supondría para la efectiva imposición de los debidos límites a las restricciones y porque podría propiciar que *"el Estado [enmascarase] con argumentos pseudojurídicos actuaciones arbitrarias".* Sobre esta posición, Vid. González-Cuéllar Serrano, Nicolás. *Proporcionalidad…op.cit.*, pág. 70 y ss.

determinados bienes jurídicos en beneficio de otros de inequívoca y superior necesidad de protección en situaciones de clara y plenamente justificadas. La idea de la excepcionalidad, asociada con toda evidencia a la aplicación del estado de necesidad, debe tener, en cualquier caso, una muy estricta apoyatura en el principio de legalidad[503].

Sobre esta misma idea de la excepcionalidad de determinadas medidas limitativas de derechos, para cuya resolución pueda invocarse el estado de necesidad, cuando además vengan revestidas de un carácter perentorio, debieran, con idéntica sujeción al principio de legalidad, ser instauradas *ex officio* por la PJE en aquellos casos tasados en una norma por la que cupiera demandársele una conducta reactiva urgente y proporcionada, siempre sometida, en cualquier caso, a un exigente control posterior de jurisdiccionalidad que confirme, modifique o revoque su procedencia[504].

Naturalmente, y salvo lo dispuesto en el art. 11.1 LOPJ sobre la nulidad de la prueba ilegítimamente obtenida, estas dos últimas circunstancias no deben conllevar automáticamente la adquisición de una responsabilidad penal o disciplinaria por parte de la PJE actuante en aquellos casos en que, aunque no pueda tenerse la medida por ajustada, se hubiere adoptado de un modo justificable, apreciadas la buena fe y la debida diligencia profesional de los agentes intervinientes.

La noción del aval del Juez evoca de nuevo la cuestión del momento del ejercicio de las facultades jurisdiccionales que le están reservadas, pues su materialización en tiempo diferido no le resta capacidad de control sobre aquellas

[503] A este respecto, QUERALT afirma que *"los derechos y libertades fundamentales son absolutamente vinculantes para todos los agentes públicos; su lesión, aún de la mano de pretendidas satisfacciones del orden público o del interés general, sólo puede venir de la Ley, y nunca del criterio del funcionario actuante, salvo supuestos excepcionalísimos del estado de necesidad en los que se trate de salvar otro derecho fundamental de un tercero que se encuentre en concreto más protegido"* Vid. Queralt, Joan Josep. *Introducción a la Policía Judicial…op. cit.,* pág. 48.

[504] En esta línea, para GARCÍA DE PAZ *"es admisible que en casos excepcionales por razones de urgencia la ley prevea que algunas puedan ser adoptadas por la autoridad policial siempre que se requiera su confirmación judicial en breve plazo…Lo que sí consideraríamos inadmisible es que la intervención policial autónoma pudiera mantenerse en el tiempo sin el aval del Juez".* Vid. Sánchez García de Paz, Isabel. *Problemas de legitimidad de una respuesta excepcional frente a las organizaciones criminales* en Cancio Meliá, Manuel y Pozuelo Pérez, Laura. *Política criminal en vanguardia. Inmigración clandestina, terrorismo, criminalidad organizada.* Cizur Menor (Navarra): Aranzadi S.A., 2008, págs. 451-494, págs. 481 y ss.

situaciones en que, debido a su excepcionalidad, ello esté perfectamente justificado y previsto en la Ley.

Esta forma peculiar de ejercer el control de jurisdiccionalidad aporta además una gran carga de seguridad jurídica a la actuación perentoria de la PJE y, simultáneamente, con toda lógica, una importante capacidad de tutela del interés público allí donde no es materialmente posible la actuación directa y oportuna del actor jurisdiccional[505].

Las facultades y deberes genéricos de la PJE, plasmados en el cuerpo legislativo que la rige, propician y facilitan el cumplimiento de las funciones jurisdiccionales posteriores en estos casos excepcionales ya que, *ex* art. 549.1.a) LOPJ, tiene la ineludible obligación de dar cuenta de forma inmediata a la Autoridad Judicial y Fiscal de los hechos en los que intervenga. Por tanto, mediada la necesaria seguridad jurídica nacida de un cuerpo legislativo adecuado, no sólo se propicia que el ciudadano sepa a qué atenerse cuando incumpla la Ley, sino que además esta se aplicará de la forma más proporcionada posible y, siempre, sometida a las más estrictas garantías relativas al derecho a la tutela judicial y a la defensa que vienen consagradas en el art. 24 CE.

En definitiva, en referencia a la aplicabilidad del estado de necesidad a la limitación de derechos fundamentales, lo que se constata en la realidad diaria es la existencia de determinadas y graves situaciones cuya perentoria resolución no puede atenerse al más que deseable régimen de tutela jurisdiccional previa sino, por esta misma razón, a su atención directa y urgente por quien esté en situación de hacerla – en este caso la PJE[506] – y, posteriormente, ser objeto del más estricto control de jurisdiccionalidad.

---

[505] Un buen ejemplo de lo anterior lo representaría la necesidad de actuar la PJE reactivamente para resolver un secuestro y evitar con gran diligencia y celeridad los males que suelen estar asociados a la pérdida de la libertad del sujeto pasivo, como lo serían las lesiones, los ataques a su libertad sexual, las pérdidas patrimoniales o incluso la de la propia vida. En estos casos es necesario, entre otras cosas, la cesión inmediata de los DACE de todos los actores de los hechos (víctimas, familiares, sospechosos, intermediarios, negociadores, etc.), como lo serían, sin ánimo de exhaustividad, los datos de cobertura de los medios de telefonía móvil (cuya conservación no es obligatoria actualmente de acuerdo con la LCDCE) o de los *logs* de determinadas comunicaciones telemáticas (por ejemplo, los de inserción de contenidos en una determinada red social que puedan orientar al investigador sobre la animosidad de determinados actores contra la víctima).

[506] MARCHAL, con una referencia expresa a la dependencia funcional de la Autoridad Judicial, indica que hay limitaciones de derechos fundamentales de "…*urgencia, porque hay diligencias que no pueden*

En este sentido, en materia de secreto de las comunicaciones, el art. 18.3 CE tiene una inequívoca reserva de judicialidad bajo la declaración *in fine "…salvo resolución judicial"*, sobre la que los autores estudiados coinciden unánimemente en su instauración temporal previa a la limitación de tan sensible derecho fundamental.

Pero, como antecedente a tener en cuenta, es bien cierto también que, además de lo dicho en el párrafo anterior, el legislador constitucional dejó abierta la posibilidad *ex* art. 55.2 CE de derivar determinados casos de gravísima trascendencia social a un control posterior de jurisdiccionalidad (bandas armadas y terrorismo), algo que, por lo demás, el legislador posterior interpretó con gran insuficiencia en 1988 con la nueva redacción dada al art. 579.4 LCRIM[507], generando al mismo tiempo una gran inseguridad jurídica e incertidumbre.

2. Motivación

El enraizamiento constitucional del ***requisito extrínseco formal de motivación*** queda consagrado en el art. 120.3 CE[508] *"…que exige la motivación de las sentencias judiciales como trasunto de ese valor superior que es la Justicia reclamada en el artículo 1 CE; pero, además de en dicho precepto, la motivación también está ínsita en los derechos del proceso; y, más concretamente, en el derecho a obtener una*

esperar a que se produzca el mandamiento judicial para su ejecución, ya que perdería en no pocas ocasiones su esencia y razón de ser". Vid. Marchal Escalona, Nicolás. 2010. *Policía Judicial…op.cit.,* pág. 34.

[507] GONZÁLEZ-CUÉLLAR dice que *"con ello no ha quedado zanjada la discusión sobre la colisión de las limitaciones del art. 18.3 CE con el principio de legalidad, dada la absoluta indeterminación de la norma, los graves problemas interpretativos que provoca y su incongruencia con otros principios de la LCRIM"*. Con mención expresa a la STEDH del Caso *Malone*, recuerda este autor que *"si no se determinan con suficiente claridad las facultades discrecionales concedidas a los poderes públicos para la restricción del derecho a la intimidad mediante la interceptación de las comunicaciones, ello impide considerar que las medidas se encuentran "previstas en la Ley"*. Vid. González-Cuéllar Serrano, Nicolás. *Proporcionalidad…op.cit.*, pág. 93.

[508] Art. 120.3 CE: *"Las sentencias serán siempre motivadas y se pronunciarán en audiencia pública"*. Nótese, por tanto, que se refiere a *las sentencias*, aunque esto, como se verá, es extensivo a las demás resoluciones judiciales. En este sentido, por todos, vid. González-Cuéllar Serrano, Nicolás. *Proporcionalidad…op.cit.*, pág. 143. También, vid. SSTC 14/1991, de 28 de enero, y 173/1987, de 3 de noviembre.

resolución de fondo fundada en derecho sobre el asunto[509]*[…] Por otra parte, la carga de la prueba de la motivación corre a cargo del órgano que limita el derecho, ya que aquél debe aportar "motivos pertinentes y suficientes" que justifiquen la aplicación de las injerencias en el ámbito de los derechos que el CEDH tutela"*[510,511].

Otros preceptos jurídicos derivados del texto constitucional y que dan sustento a la obligación de motivar las resoluciones judiciales "*se hallan en los arts. 141, 508.2, 550, 558 y 579.2, 3 y 4*[512] *LCRIM y 292.2 LOPJ"*[513].

Sobre la materialización del requisito formal de motivación, *"la expresión "resolución" del art. 18.3 CE, a diferencia del término mandamiento, dejó clara la obligación de plasmar por escrito la motivación de efectuar una limitación de un derecho fundamental*[514]. En la STC de 18 de enero de 1990 se dice que *"la motivación de las resoluciones limitativas de derechos fundamentales es un requisito de proporcionalidad". Si no hay fundamentación, la medida puede tacharse de desproporcionada…la falta de motivación constituye un síntoma de exceso (contrario al principio de prohibición del exceso)"*[515]. Por ello, el elocuente contenido semántico del

[509] Aclara MARCHAL que en esta línea se entiende *"que el respeto de esta regla impone la motivación de la resolución judicial que excepcione o restrinja el derecho, pues sólo tal fundamentación permitirá que se aprecie, en primer lugar, por el afectado y que se pueda controlar, después, la razón que justificó, a juicio del órgano judicial, el sacrificio del derecho fundamental (STC 37/89)".* Vid. Marchal Escalona, Nicolás. *Policía Judicial…op.cit.,* pág. 52 y ss.

[510] El autor refiere las SSTEDH de 26 de Abril de 1.979 (caso *The Sunday Times*) y de 25 de Marzo de 1.985 (caso *Barthold*).

[511] Vid. Marchal Escalona, Nicolás. *Policía Judicial…op.cit.,* pág. 52 y ss.

[512] Sobre la limitación del derecho al secreto de las comunicaciones, el art. 579.2 LCRIM dice que *"asimismo, el Juez podrá acordar, en resolución motivada, la intervención de las comunicaciones telefónicas del procesado, si hubiere indicios de obtener por estos medios el descubrimiento o la comprobación de algún hecho o circunstancia importante de la causa"*, lo que es extensivo a la justificación de las prórrogas. En el párrafo cuarto se incluyen idénticas obligaciones de motivación de las resoluciones de las autoridades administrativas que en el mismo se indican.

[513] El precepto del art. 292.2 LOPJ tiene su concordancia actual en el art. 248 LOPJ. Vid. González-Cuéllar Serrano, Nicolás. *Proporcionalidad…op.cit.*, pág. 141.

[514] Vid. González-Cuéllar Serrano, Nicolás. *Proporcionalidad…op.cit.*, pág. 146. Nótese también, siguiendo a NOYA, que en la Constitución no se dice nada sobre cómo debe ser la resolución a la que se refiere el art. 18.3, es decir, que el legislador no adoptó la fórmula alternativa "…salvo resolución judicial *motivada*", sin duda jurídicamente más enjundiosa. Como la misma autora indica, no obstante, la doctrina y la jurisprudencia son mayoritarias a favor de la obligación de motivar tales resoluciones limitativas del derecho contenido en el mencionado artículo. Vid. Noya Ferreiro, María Lourdes. *La intervención…op. cit.,* pág. 164.

[515] Vid. González-Cuéllar Serrano, Nicolás. *Proporcionalidad…op.cit.*, pág. 146. Según la STS de 12 de diciembre de 1994 (RJ 1994, 10076) *"la absoluta falta de motivación de la resolución judicial habilitante de la invasión del espacio protegido de la intimidad personal supone una vulneración del derecho constitucional al derecho al secreto de las comuniaciones telefónicas proclamado en el art. 18.3 de la*

término se ve desbordado por la propia trascendencia del principio de proporcionalidad.

El Tribunal Supremo definió, por su parte, la motivación diciendo que *"significa la exteriorización razonada de los criterios en los que se apoya la decisión judicial. Es decir, [que] la exigencia de motivación se satisface cuando, implícita o explícitamente, se puede conocer el razonamiento, esto es, el conjunto de reflexiones que condujeron al Juez a tomar la decisión que tomó, incluidos los supuestos de conceptos jurídicos indeterminados"*[516,517]. Y, puede añadirse, no sólo una mera relación de razonamientos jurídicos sino, también, de la existencia de unos hechos de naturaleza criminal[518].

La modelación hecha de este requisito por el Tribunal Constitucional asocia el deber de motivación de las resoluciones judiciales con el derecho constitucional a la tutela judicial efectiva recogido en el art. 24 CE[519]. Sin embargo, a este tipo de resoluciones, el TC *"no traslada la doctrina sentada sobre la motivación de las sentencias, sino que la motivación se conforma con "la expresión de la ponderación efectiva hecha por el Juez en relación con los valores o bienes jurídicos en juego en cada caso, haciendo efectiva la exigencia de proporcionalidad inherente a la justicia""*[520].

Sobre el deber de motivación de las resoluciones judiciales y de su auto habilitante[521], cabe señalar dos importantes aspectos relacionados con sus finalidades:

Constitución". Vid. Lanzarote Martínez, Pablo. *Intervención de las…op. cit.*, pág. 795. Evidentemente, una situación de facto así descrita permitiría invocar las previsiones del art. 11.1 LOPJ.

[516] ATS de 18 de junio de 1992 (RA 6102), citado por Noya Ferreiro, María Lourdes. *La intervención…op. cit.,* pág. 166. El derecho del justiciable a conocer y comprender las razones por los que se le limitó un derecho se reconocen en las SSTS de 31 de octubre de 1998 (RJ 1998, 8728), 4 de febrero de 1997 (RJ 1997, 1275), 11 de abril de 1997 (RJ 1997, 2802) y 26 de mayo de 1997 (RJ 1997, 4133). Vid. Lanzarote Martínez, Pablo. *Intervención de las…op. cit.*, pág. 794 y ss.

[517] En relación con lo que viene aportándose a este trabajo, resulta del máximo interés sobre esta definición la cuestión de que en la motivación se incluyan los necesarios pronunciamientos jurisdiccionales sobre aquellos conceptos jurídicos indeterminados, cuya precisión deba ser materia de la prudente interpretación judicial.

[518] STS de 11 de abril de 1997 (RJ 1997, 2802).

[519] STC 61/1983 de 11 de julio (RTC 1983, 61). La ausencia de motivación de la resolución judicial como causa de nulidad se recoge en la STC 85/1994 de 14 de marzo (RTC 1994, 85).

[520] STC 123/1997 de 1 de julio (RTC 197,123). Otras sentencias que reiteran la doctrina sobre la limitación del derecho al secreto de las comunicaciones son las SSTC 150/2006 de 22 de mayo (RTC 2006, 150) o la 253/2006 de11 de septiembre (RTC 2006/ 253).

[521] Sobre el requisito formal de motivación en materia de protección del secreto de las comunicaciones, véanse las SSTS de 2 de febrero de 2004 (RJ 2004, 2187), 20 de enero de 2005 (RJ 2005, 1444) 22 de julio

- *"Posibilitar la impugnación de las resoluciones de los órganos jurisdiccionales cuando no sean acordes con los posicionamientos de las partes.*
- *Evitar la inseguridad jurídica que se produciría como consecuencia de una arbitrariedad judicial"*[522].

Se hace obvio, de acuerdo con estas finalidades, el papel que la PJE ha de jugar a la hora de solicitar y ejecutar los mandatos judiciales sobre determinadas medidas limitativas de derechos fundamentales, procurando que la calidad de la prueba obtenida mediante el uso de la tecnología (con instrumentos técnicos provistos de las necesarias salvaguardas y certificaciones sobre su veracidad, autenticidad e integridad) y los procedimientos técnicos policiales (metodología adecuada y transparencia en la exposición de los indicios) la haga idónea para el proceso de contradicción e irrefutable en su apreciación objetiva por parte del tribunal.

Debe tenderse, en este sentido, a que los debates procesales se centren en la valoración de la prueba y nunca en el instrumento o los procedimientos con los que se obtuvo, siempre, naturalmente, que gocen de todas las garantías exigibles. Es también obvio que actuar de esta forma, con el beneficio añadido que supone hacerlo bajo la leal inmediatez a Jueces y Fiscales, contribuye a reducir los espacios de inseguridad jurídica – tan extensos en materia de limitación del derecho al secreto de las comunicaciones o a la protección datos - y a facilitar solventemente la necesaria interdicción de la arbitrariedad.

Por ello, el intenso proceso intelectivo que debe preceder a la formación de una resolución judicial motivada debe venir respaldado, a su vez, por una similar obligación de la PJE de justificar rigurosamente sus solicitudes en el estricto marco de

---

de 2005 (RJ 2005, 5635) y 8 de mayo de 2006. La ausencia de esta obligación formal como causa de nulidad, se contempla en la STS de 13 de abril de 2005 (RJ 2005, 5182).

[522] Vid. Noya Ferreiro, María Lourdes. *La intervención…op. cit.,* pág. 166 y ss.

Por otro lado, según la STC 55/87, de 13 de mayo, *"el requisito de motivación tiene una doble consideración:*

1. *Permitir el control de la actividad jurisdiccional.*
2. *Lograr el convencimiento de las partes y los ciudadanos acerca de su corrección y justicia, mostrando una aplicación del Derecho vigente libre de arbitrariedades".*

las atribuciones que le son propias[523]. Obrar de otra forma propiciaría, por lo demás, un inaceptable quebranto del precepto constitucional contenido en el art. 24 CE sobre la tutela judicial efectiva, el derecho a la defensa y a un proceso con todas las garantías.

En este sentido, aunque no se trate de jurisprudencia pacífica, la STS de 23 de enero de 1995 (RJ 1995, 157), como indica LANZAROTE, *"previene de la utilización de resoluciones impresas intercambiables y polivalentes que puedan abarcar toda la infinita variedad de supuestos que presenta la realidad, si bien admite (con referencia textual al pronunciamiento jurisprudencial) que "en casos muy específicos, la petición policial, si está suficientemente razonada y justificada, puede servir de antecedente fáctico a la resolución motivada del Juez de Instrucción""* y la STS de 4 de marzo de 1996 (RJ 1996, 2405) admite que en el marco del derecho al secreto de las comunicaciones, la ***motivación por remisión al oficio policial*** sea perfectamente admisible, lo que da una idea de la extraordinaria consideración que con ello el TS otorga a la PJE[524].

En otras sentencias, el TS reconoce *"que los autos de autorización de intervenciones telefónicas pueden ser integrados con el contenido de los respectivos oficios policiales…de forma que es lícita la motivación por referencia a los mismos, ya que el órgano jurisdiccional por sí mismo carece de la información pertinente y no sería lógico que abriese una investigación paralela al objeto de comprobar los datos suministrados por la policía judicial",* lo que representa todo un alentador comentario sobre la merecida confianza que la Justicia ha de depositar en una PJE cabalmente

[523] En muchos de los pronunciamientos traídos a este trabajo, se trasluce una intención de considerar a la PJE como una mera ejecutora de las resoluciones judiciales. Parece en ocasiones, que su labor deba reducirse a la puesta en práctica de determinados automatismos ordenados expresamente por un Juez "que es quien de verdad investiga". No es así en la práctica, ni podría serlo. La PJE tiene unas capacidades inmensas en todos los aspectos y, en razón de ello, debe imbricársele de un modo jurídicamente seguro en el proceso penal. Y sí, la PJE investiga.

[524] Otras SSTS que confirman esta doctrina son las de 7 de abril de 1997 (RJ 1997,2702), 20 de febrero de 1998 (RJ1998, 1466) y 31 de octubre de 1998 (RJ 1998, 8728). En la STS de 14 de junio de 1995 (RJ 1995, 5345) se afirma *"que no es necesario explicitar lo obvio".* Vid. Lanzarote Martínez, Pablo. *Intervención de las…op. cit.*, pág. 798.

originada en el art. 126 CE y, desde luego, en su capacitación técnica y en su valiosa posición dentro del proceso penal[525].

El autor citado, tras recordar que la línea jurisprudencial mayoritaria admite los formularios impresos, transcribe también el siguiente extracto de la STS de 20 de febrero de 1999 (1999, 512), por el que se recomienda *"que se añadan razonamientos ad hoc, con objeto de individualizar cada una de las resoluciones adoptadas, aunque la ausencia de fundamentación fáctica puede convalidarse por remisión al contenido del oficio de la policía judicial, en el que se contienen los detalles y antecedentes por los que se solicita la decisión judicial"*[526].

De estas posiciones jurisprudenciales cabe deducirse el singular papel que se reserva a la PJE en su contribución al más exacto cumplimiento del requisito de motivación que deben contener las resoluciones judiciales, lo que resulta especialmente sugerente de cara a la actuación en casos de urgencia vital donde, la suma de las razones de orden fáctico que aconsejarían una determinada medida para la limitación de un derecho fundamental, se contendrán íntegra y exclusivamente en la comunicación policial, bien sea por escrito o mediante cualquier otro medio de constancia, lo que no debe excluir en casos extremos la voz (comparecencia física o mediante uso de un medio de comunicación seguro).

En este sentido, la idea de una resolución enjundiosa y acaso prolija en los demás casos, donde se analicen los aspectos fácticos y jurídicos que permitan adoptar una específica limitación de un derecho fundamental, de acuerdo con el principio de proporcionalidad, goza de algunas excepciones, ya que una ***motivación escueta*** no es incompatible con la más estricta observancia del citado principio en determinadas ocasiones[527]. Esta circunstancia es, desde luego, de un gran valor para la apreciación

[525] Por todas, véaNse la STS de 9 de abril de 2007 (RJ 2007, 2258) y la STC 123/1997 de 1 de julio (RTC 1997, 123). Vid. Lanzarote Martínez, Pablo. *Intervención de las…op. cit.*, pág. 799 y ss.

[526] Vid. Lanzarote Martínez, Pablo. *Intervención de las…op. cit.*, pág. 796.

[527] GONZÁLEZ-CUÉLLAR lo expresa diciendo que La STC 58/97, de 13 de mayo, sostiene que *"una motivación escueta y concisa no deja por ello de ser tal motivación". La STC 100/87, de 12 de junio, "no exige del Juez o Tribunal una exhaustiva descripción del proceso intelectual que le ha llevado a resolver en un determinado sentido, ni le impone una determinada extensión, intensidad o alcance en el razonamiento empleado"…el alcance de la motivación puede llegar a variar un criterio jurisprudencial, siempre que esté los suficientemente razonado".* Vid. González-Cuéllar Serrano, Nicolás. *Proporcionalidad…op.cit.*, pág. 147. Por su parte, NOYA aporta la STC 184/1988, de 13 de octubre, y

de la proporcionalidad de determinadas medidas que hubieran de aplicarse de un modo perentorio.

Semejante visión es, además, sugerente de la necesidad de integrar a todos los operadores jurídicos en un sistema telemático que facilite la ágil toma y puesta en la práctica de las decisiones judiciales que demanda la casuística actual, acortando sus tiempos de implementación y su eficacia, y proporcionando al mismo tiempo a la PJE la más que deseable tutela judicial previa a la acción limitativa que por su mediación se haya de ejecutar, de la que en modo alguno pretende sustraerse.

En determinadas ocasiones, debiera bastar la orden imperativa judicial por canal seguro a la operadora de telefonía o al prestador de servicios de la sociedad de la información para que se ejecutase una determinada medida limitativa, eso sí, con cumplimiento posterior del deber formal de motivación, perfeccionándose con todo detenimiento por parte de la Autoridad Judicial que así se hubiera determinado. Esta idea, sin duda controvertida, es apoyada por JIMÉNEZ CAMPO, quien en palabras de NOYA, dice que:

> *"el autor [JIMÉNEZ CAMPO] defiende la idea de que en casos excepcionales y por motivos de urgencia el Juez pueda autorizar a la policía a realizar una medida de intervención de las comunicaciones*[528]*, procediendo después a dar la forma debida a ese acto si bien reconoce que este tipo de actuaciones debería estar prevista legalmente y no dejarse al arbitrio de la autoridad judicial"*[529]*.*

Comparto plenamente esta sugerente idea, sobre la que puede comentarse lo siguiente:

- Facilita el imprescindible respaldo formal de la Autoridad Judicial a la PJE con precedencia a la ejecución de una medida limitativa del secreto de las comunicaciones o al de protección de datos en casos de urgencia, lo que es,

---

diversas SSTS que muestran el carácter pacífico de esta visión jurisprudencial. Vid. nota la pie 211 en Noya Ferreiro, María Lourdes. *La intervención…op. cit.,* pág. 177.

[528] NOYA aclara que el autor se refiere a *órdenes verbales.*

[529] En este pronunciamiento se encuentra nuevamente la necesidad de contar con una ley previa a la que el Juez de Garantías deba ajustarse. Vid. Jiménez Campo, Javier. *La garantía constitucional del secreto de las comunicaciones.* REDC, núm. 20, 1987, pág. 67, citado por Noya Ferreiro, María Lourdes. *La intervención…op. cit.,* pág. 176.

siempre, del máximo interés por razones de seguridad jurídica y para que la prueba, una vez obtenida, goce de la suficiente validez para servir a los legítimos fines del proceso penal[530].

- Refuerza la idea de que el ámbito de discrecionalidad en la adopción de la medida – el margen judicial de apreciación - pueda reducirse y precisarse en el caso de que este tipo de facultades jurisdiccionales estén perfectamente previstas en una Ley precedente. Esta Ley debería establecer con exactitud qué facultades puede invocar por sí la PJE sin necesidad de un mandato judicial, según los diferentes grados de intromisión en el derecho a la intimidad proclamados en el art. 18 CE.
- La diligencia y sentido de la oportunidad con que podría intervenir la Autoridad Judicial haría por completo innecesaria cualquier iniciativa de la PJE en los ámbitos más sensibles del derecho al secreto de las comunicaciones, incluida la extemporánea invocación de las facultades reconocidas al Ministro del Interior o el Secretario de Estado de Seguridad recogidas en el art. 579.4 LCRIM.
- Refuerza la idea de contar el Juez con el apoyo de la tecnología para facilitar la adopción material de esta medida y comunicarla mediante un canal seguro que ponga en relación a los operadores jurídicos involucrados en su ejecución, incluida la PJE, con las operadoras de telefonía o los proveedores de servicios de la sociedad de la información a efectos de cumplimento y posterior control de jurisdiccionalidad. En este sentido, una orden verbal como la pretendida sería absolutamente ineficaz, pues cabe esperar la resistencia de los cedentes de la señal a cumplir una orden verbal no apoyada en un soporte material (sello del juzgado y firma del Juez) o inmaterial (firma electrónica)[531].

[530] Aunque es ocioso repetirlo, ninguna de las propuestas de este trabajo se dirigen a sustraerse del control judicial más estricto, que debe ser siempre precedente en el tiempo cuando inequívocamente se trate de limitar el derecho fundamental al secreto de las comunicaciones y, posterior, aunque no por ello menos exigente, en los demás casos. Resta definir cómo ha de realizarse, lo que será tratado más adelante.

[531] ¿Cómo se daría semejante orden? ¿Mediante llamada telefónica del Juez? ¿Utilizando a la PJE como transmisor? ¿Mediante personación de un funcionario judicial ante la operadora? Ninguno de estos procedimientos es realista. De contar con la adecuada previsión en la Ley, la solución pasa por el uso de un canal telemático seguro.

- Reconoce la necesidad de efectuarse un control posterior de judicialidad que, dadas las circunstancias de la urgencia, deberá estar reforzado en su calidad. Ello exige una determinación jurídica de el concepto de control de judicialidad[532], de forma en que ha de ejecutarse y del papel de auxilio que juegan los operadores jurídicos en su materialización.

Una orden de esta naturaleza debe incluir en su contenido[533], previamente establecido en la Ley, la identificación del órgano judicial emisor, el contenido material de la orden (con exclusión del relato fáctico de los hechos por evidentes razones de reserva), su carácter inmediatamente ejecutivo por motivos de urgencia, las facultades del agente comisionado, referencia al auto motivado que se formará y los demás que al Autoridad Judicial considere pertinentes, requisitos que se deberían cumplimentar de forma sencilla y transmisible mediante medios telemáticos de comunicación.

E. La indeterminación del principio de proporcionalidad

Para algunos de los autores estudiados, al tiempo de reconocer la enjundia jurídica y los avances alcanzados durante los años de evolución en los que la jurisprudencia lo ha ido conformando, el principio[534] de proporcionalidad debe seguir siendo considerado como un ***concepto jurídico indeterminado***[535], tal y como lo

[532] *Ibídem*.

[533] PEDRAZ afirma, sobre la necesidad de contar con instrumentos jurídicos adecuados, que *"la necesaria reforma [procesal] total cubrirá las gravísimas deficiencias observables en la práctica de diligencias lesivas de derechos fundamentales, so pretexto más o menos justificado de su urgencia y necesidad o ante lagunas normativas que dificultan incluso el control ex post de su acomodo a las exigencias de nuestra Carta Magna. Hasta ahora la jurisprudencia constitucional y ordinaria ha venido asumiendo un papel subsanador de las deficiencias e insuficiencias legislativas, temporalmente justificable, pero no como coartada legislativa y por ende política en hipótesis de soluciones, en un momento determinado, socialmente discutidas y susceptibles de ser utilizadas para justificar una pasividad política difícilmente legitimadora. Esa temporalidad que permite a los Tribunales asumir el papel de legisladores resulta ya excesivamente dilatada"*. Vid. Pedraz Penalva, Ernesto. 2008. *Notas sobre policía…op. cit.,* pág. 109.

[534] El primer término que lo describe, "principio", que el diccionario define como *"base, origen, razón fundamental sobre la cual se procede discurriendo en cualquier materia",* sugiere, como sinonimia, el concepto de "idea rectora", que resultaría en este caso ajeno e incluso antitético al de "regla" o "norma" que encorsetarían o limitarían de forma indeseable, llegado el caso, el contenido jurídico extraído del principio de proporcionalidad.

[535] Tal y como se reconoció en la STC 62/82, al poner de manifiesto algunas de sus posibles consecuencias indesables, al afirmar que *"el principio de proporcionalidad, por tratarse de un concepto*

sostiene el profesor GONZÁLEZ BEILFUSS quien, tras analizar su desarrollo dogmático, ya bien entrada la primera década de los dos mil, considera que *"la principal novedad de los últimos años radica, en cambio, en el intento del Tribunal Constitucional español de formalizar este principio, es decir, de llenarlo de contenido mediante diversos criterios que permitan disminuir, en la medida de lo posible, su indeterminación"*[536,537].

De esta carga de indeterminación se desprenden el *quantum* de ineficiencia de la labor ablativa del Estado y los riesgos jurídicos que emergen de semejante circunstancia.

Sobre el carácter relativo del principio de proporcionalidad, de él no se desprenden prohibiciones abstractas o absolutas, ya que *"no [se] proscribe para siempre el empleo de un instrumento cualquiera, ni la persecución de un determinado objetivo, aisladamente considerados, por lo que puede calificarse de principio relacional, en el sentido de que compara dos magnitudes: los medios a la luz del fin"*[538].

En la tensión entre ambas magnitudes – medios y fin - gira una discusión, con vocación de extenderse *ad infinitum,* sobre la virtualidad jurídica de determinadas propuestas relativas a una determinada forma de limitar los derechos fundamentales, lo que adquiere una de sus más notorias expresiones cuando de lo que se habla es de las TIC y de su relación con el derecho a la intimidad como generadoras de insospechadas necesidades de manifestarse el derecho ablativo del Estado. Una tensión que, por otra parte, no resuelve una eventual y supuesta colisión entre diversos principios sobre los que hay que anotar la incertidumbre y aún la

---

jurídico indeterminado, presenta un margen de apreciación peligroso desde el punto de vista de la seguridad jurídica y de la igualdad en la aplicación de la ley (derivado de la idoneidad subjetiva de las medidas), por eso, frente a la construcción positiva del mismo (si una medida es o no proporcionada), nuestro TC ha optado como criterio de control el negativo, esto es, si la medida enjuiciada es desproporcionada o no para la defensa del bien que da origen a la restricción".

[536] Vid. González Beilfuss, Markus. *Últimas tendencias…op.cit.,* pág. 1. Vid. González-Cuéllar Serrano, Nicolás. *Proporcionalidad y derechos fundamentales en el proceso penal.* Madrid: Colex, 1990, pág. 315. Vid. Marchal Escalona, Nicolás. 2010. *Policía Judicial…op.cit.,* pág. 37.

[537] Como indica GONZÁLEZ-CUÉLLAR, los conceptos jurídicos indeterminados *"…presenta[n] tres zonas diferenciadas: el núcleo del concepto o zona de certeza positiva (algo es a todas luces proporcionado); la zona de certeza negativa (es evidente la desproporción); y, por último, una zona de sombra o incertidumbre o "halo del concepto" (supuestos de solución difícil, que depende en última instancia del juicio que se haga del mismo)"*. Vid. González-Cuéllar Serrano, Nicolás. *Proporcionalidad…op.cit.*, pág. 315 y ss. 38.

[538] Vid. Ruiz Ruiz, Ramón y de la Torre Martínez, Lourdes. *Algunas aplicaciones…op.cit.,*29. Sobre la calificación de "principio relacional", vid. Fernández Nieto, J., *principio de proporcionalidad…op.cit.*, pág. 290.

contradicción sobre el resultado de tamaña colisión, según sean los casos objeto de valoración, de forma que el principio que se consideró precedente no ocasiona automáticamente la invalidación del que, por esa vez, se pretirió[539].

Se trata, por tanto, de una labor inacabada de la que se esperan nuevos frutos en cuanto a las perspectivas de contar con criterios jurídicos solventes con los que determinar la procedencia de las medidas limitativas de derechos fundamentales que puedan concebirse conforme evolucionen las TIC y en tanto no existan previsiones legales suficientes.

Consecuentemente, el principio de proporcionalidad debe ser considerado un ente vivo y abierto a una nueva hermenéutica, tan respetuosa con los derechos fundamentales y con el elevado grado de garantismo que se trasluce del espíritu del texto constitucional español, como adaptable y flexible para afrontar los retos que puedan surgir, hoy y en el futuro, en el seno de una nueva realidad propiciada por las TIC en la que la sociedad se desenvuelve dinámicamente con una soltura equiparable, o incluso superior, a la del mundo físico – llena de posibilidades para el desarrollo de las libertades -, pero en la que aparentemente, con su propia evolución, ha creado paralelamente un incomprensible espacio de impunidad donde el Derecho avanza con sensibles dificultades[540].

De una forma comprensiva sobre lo reflexionado hasta el momento sobre la idea de la proporcionalidad, se podría concluir añadiendo que la Justicia acciona apoyándose preferentemente en el principio de proporcionalidad para limitar el derecho fundamental al secreto de las comunicaciones, dotado de un sólido blindaje constitucional en su estricta concepción dentro del Estado de Derecho español, como consecuencia de las dificultades inherentes a su insuficiente e inestable remisión al

[539] Vid. Ruiz Ruiz, Ramón y de la Torre Martínez, Lourdes. *Algunas aplicaciones…op.cit.,* pág. 38.

[540] En la STC 119/2001, de 24 de mayo, sensible a estas tensiones, se afirma *que "estos derechos han adquirido también una dimensión positiva en relación con el libre desarrollo de la personalidad, orientada a la plena efectividad de estos derechos fundamentales. En efecto, habida cuenta de que nuestro texto constitucional no consagra derechos meramente teóricos o ilusorios, sino reales y efectivos ...se hace imprescindible asegurar su protección no sólo frente a las injerencias ya mencionadas, sino también frente a los riesgos que puedan surgir en una sociedad tecnológicamente avanzada. A esta nueva realidad ha sido sensible la jurisprudencia del Tribunal Europeo de Derechos Humanos, como se refleja en las Sentencias de 21 de febrero de 1990, caso Powell y Rayner contra Reino Unido; de 9 de diciembre de 1994, caso López Ostra contra Reino de España, y de 19 de febrero de 1998, caso Guerra y otros contra Italia" (FJ 5").*

derecho procesal (art. 579 LCRIM), según es opinión prácticamente unánime en la doctrina[541].

Además, ante la duda, no exenta de prejuicios y de defectos en la aprehensión de la forma en que actualmente se materializan las comunicaciones electrónicas –especialmente en los *casos difíciles* - y de las salvaguardas y evidencias electrónicas manejadas por la PJE en beneficio del proceso penal, esta inestabilidad, haciéndose tabla rasa, parece resolverse del lado del hipergarantismo ante la falta de interiorización de la evolución de las TIC. Esto puede deberse a no haber comprendido el Derecho la exacta dimensión de su afectación a la vida social actual, todo ello de forma que le permita discernir, en términos de estricta justicia, cuándo hay un real compromiso al secreto de las comunicaciones, y por tanto merecedor de la más alta tutela, y cuándo determinados hechos que se les relacionan no lo es de ninguna forma o cuándo merece un rango de protección menor[542].

Por ello, con cierta e injustificada radicalidad, se continúa manteniendo una reserva de judicialidad universal para cualquier materia que lejanamente pueda sugerir una limitación de este derecho, por insignificante que parezca. De esta forma, en el defectuoso derecho procesal, el *quantum* de indeterminación jurídica que contiene el principio de proporcionalidad, el grado de discrecionalidad con que el actor jurisdiccional puede interpretarlo, la convivencia en el proceso penal de resoluciones valorativas contradictorias sobre la apreciación de este principio y, en definitiva, la incertidumbre sobre su fortuna y sobre la seguridad jurídica asociada a su ejercicio hacen que, al menos desde el punto de vista policial, suponga en elemento

[541] Por todos, vid. Gimeno Sendra, Vicente. *La intervención de las comunicaciones,* en Marchal Escalona, Nicolás (Director). *Manual de lucha…op. cit.,* pág. 579.

[542] En la STC 173/2011, de 7 de noviembre, no sin cierta sensación de desconcierto, sobre el redimensionamiento de los espacios donde se puede manifestar el derecho fundamental a la intimidad, se reconoce que *"a tal fin conviene empezar recordando que este Tribunal ha reseñado, ya en su STC 110/1984, de 26 de noviembre, que "la inviolabilidad del domicilio y de la correspondencia, que son algunas de esas libertades tradicionales, tienen como finalidad principal el respeto a un ámbito de vida privada personal y familiar, que debe quedar excluido del conocimiento ajeno y de las intromisiones de los demás, salvo autorización del interesado. Lo ocurrido es que el avance de la tecnología actual y el desarrollo de los medios de comunicación de masas ha obligado a extender esa protección más allá del aseguramiento del domicilio como espacio físico en que normalmente se desenvuelve la intimidad y del respeto a la correspondencia, que es o puede ser medio de conocimiento de aspectos de la vida privada. De aquí el reconocimiento global de un derecho a la intimidad o a la vida privada que abarque las intromisiones que por cualquier medio puedan realizarse en ese ámbito reservado de vida" (FJ 3)".*

distorsionador de su eficiencia para alcanzar los legítimos fines del proceso penal, además de un riesgo jurídico inaceptable para el investigador.

Pero, a la hora de razonar sobre las cuestiones planteadas en los párrafos anteriores, el vetusto sistema de enjuiciamiento criminal de España parece seguir a día de hoy gravitando entre la injustificada desconfianza de los operadores jurídicos en la labor de la PJE y el providencialismo atribuido a la intervención del Juez, sin reparar en que puede construirse todo un sistema de salvaguardas, al uso de las propugnadas en el CEDH, que residencie las debidas garantías sobreponiéndolas a las que los actores procesales – Juez, Fiscal, Secretario Judicial, etc. - por sí mismos representen.

Entre medias, y como mejor expresión de semejantes extremos, se deja pendiente la irremediable y siempre urgente labor de actualización de un sistema de garantías que, si se venciese la secular resistencia de la sociedad española a la modernidad, podría basarse en buena medida, no sólo en la imprescindible participación de los actores jurídicos – y, decididamente, del judicial - sino en la introducción efectiva de las más sofisticadas salvaguardas y medios de control jurisdiccional que la misma tecnología proporciona, accionándolos sobre cualquier decisión de legítima disposición de los derechos fundamentales de aquellas personas cuyos actos sean del interés del proceso penal.

F. La proporcionalidad desde el punto de vista policial

En relación con la investigación tecnológica, las deficientes normas de derecho positivo procesal[543] son suplidas en la práctica mediante una interpretación jurisdiccional del principio de proporcionalidad, en los términos que se han explicado, unida al ejercicio de las facultades discrecionales de que disponen los Jueces para ordenar, cuando proceda, la limitación de los derechos fundamentales en la investigación de los *casos difíciles*[544] (que, en materia de uso criminal de las TIC, lo serán prácticamente todos).

Esta circunstancia presenta, en su indeterminación jurídica y desde un punto de vista policial y extrajurídico, dos efectos indeseables para la investigación criminal que conviene exponer con la mayor claridad posible:

- En primer lugar, cuando existe en todos los operadores jurídicos la previa convicción de que, de instaurarse una determinada medida de investigación, se producirá la limitación de un derecho fundamental con reserva de mandato judicial previo.
- En segundo lugar, cuando existe la convicción de la PJE de que la medida de investigación no limitará derecho fundamental alguno, motivo por el que se considera no se precisará de un mandato judicial previo.

El primer caso supone que el actor jurisdiccional haya de pronunciarse de una manera jurídicamente enjundiosa sobre la más exacta proporcionalidad de la medida limitativa de derechos fundamentales, cuyo asiento jurídico positivo es *a priori* inestable. Ello le exigirá un considerable esfuerzo intelectivo que tendrá su reflejo en la

[543] PÉREZ GIL, en materia de deficiencias procesales en la investigación en el entorno de las TIC, se suma a los muchos autores que así se pronuncian al afirmar que *"hoy por hoy nuestro ordenamiento jurídico en relación con las medidas de investigación penal en las que la tecnología ocupa un papel relevante no cumple, ni aun en la más benevolente de las interpretaciones posibles, las condiciones exigidas por el art. 8.2.º del Convenio Europeo de Derechos Humanos para las injerencias en la intimidad. Mientras la materia a regular hizo su entrada hace ya bastante tiempo en el siglo XXI, su plasmación en la norma procesal penal sigue instalada en pleno siglo XIX"*. Vid. Pérez Gil, Julio. *Investigación penal y nuevas…op.cit.,* pág. 220.

[544] Sobre los casos difíciles y los conceptos de principio y *regla* en su aplicación a la interpretación judicial, se hace muy interesante la lectura de las aportaciones de ROJAS AMANDI centradas en la obra del filósofo del derecho RONALD DWORKIN. Vid. Rojas Amandi, Víctor Manuel. *El concepto de derecho de Ronald Dworkin.* Revista de la Facultad de Derecho de México, núm. 246, Sección de Artículos. 2006.

necesidad de adquirir un profundo conocimiento de la situación fáctica, e incluso técnica (a veces haciéndose necesario adquirir conocimientos de todo clase ajenos a su formación específica), y de formular a continuación complejos razonamientos de orden jurídico que culminen, en su caso, con la autorización motivada de la medida de que se trate, de sus más exactas condiciones de cumplimiento y de las actuaciones para el control posterior de jurisdiccionalidad. El origen de esta actividad lo será, bien por la propia iniciativa judicial, bien a propuesta de cualquier otro operador jurídico debidamente legitimado a tales efectos, como sería el caso de la Fiscalía o de la PJE.

Sin embargo, la postura del actor jurisdiccional en un Estado de Derecho, vistos además del de proporcionalidad, los principios de independencia judicial y de libre valoración de la prueba, nunca se ajustará a patrones preestablecidos, con toda lógica, sino que responderá al ejercicio de su prudente arbitrio judicial.

En este sentido, bajo idénticas condiciones de hecho, podrían esperarse resoluciones distintas y aún contradictorias según las diferentes autoridades judiciales a las que se les plantease la procedencia de una determinada medida limitativa de derechos fundamentales. Esto podría ser resultado de las diferentes opiniones jurídicas personales que sobre tales medidas se hubiesen formado y que podrían ser reflejo, además, de la adhesión previa a una determinada línea doctrinal de las variadas que sobre el tema puedan existir y que estén, incluso, en franca confrontación.

Expuesto lo anterior, debe consecuentemente admitirse que la inseguridad jurídica y la incertidumbre sobre la fortuna de una medida solicitada por la PJE sea el signo característico de esta situación, por lo demás muy típica de las fases de investigación ante un Juzgado de Instrucción.

Y no sólo lo anterior, sino que en la dinámica del proceso penal, en instancias posteriores, lo que en las primeras se autorizó con la cabal ponderación del Juez de Instrucción, en las siguientes se deniegue ocasionado la anulación de importantes vías de prueba *ex* art. 11.1 LOPJ y que, como inmediata consecuencia, den finalmente al traste con toda una investigación penal y con las legítimas consecuencias jurídicas que sobre los justiciables debieran haber recaído de haber existido una mayor precisión y seguridad en el sistema jurídico.

Es evidente, por tanto, que la conducción de una investigación criminal por la PJE quedará, *a priori,* seriamente condicionada por la inestabilidad de la armadura jurídica a la que debiera acogerse con total seguridad, lo que en ocasiones obligará a renunciar a prevención al uso de determinadas formas de obtención de pruebas que, racionalmente, debieran ser admisibles en un proceso penal rodeado de las debidas garantías constitucionales pero que, muy por el contrario, motivan la adopción de precauciones de tal fuerza imperativa que aconsejan al Instructor el no invocarlas pese a ser técnicamente viables, disminuyendo o anulando la calidad final de la investigación.

En todo este itinerario, podrá incluso ponerse en duda el proceder de los agentes de la autoridad que las hayan solicitado o ejecutado, con resultado de una grave inseguridad jurídica, tanto sobre los medios de investigación, como por la posible responsabilidad disciplinaria o penal que hubieran podido contraer.

Como ejemplo de lo anterior, pueden mencionarse las novedosas técnicas de infección de los dispositivos electrónicos de comunicación de los investigados, realizadas bajo estricto control judicial en su proporcionalidad, mediante la instalación intrusiva de *software de control remoto* por la PJE, siempre y cuando no sea posible injerirse en las comunicaciones por un procedimiento técnico distinto menos intrusivo[545], posibilidad que, no sin grandes reservas, en sentido favorable ha sido estudiada por VELASCO[546] y HERNÁNDEZ GUERRERO[547].

Las anteriores y contradictorias posiciones, auguran inciertos resultados para el proceso penal pues, ante una primera y positiva valoración de la proporcionalidad de semejantes medidas limitativas de derechos por un Juez de Instrucción, puedan seguirles anulaciones en instancias superiores que no compartan sus fundamentos jurídicos, de tal forma que la prueba así obtenida quede finalmente anulada en todos sus efectos procesales.

---

[545] Normalmente, sorteando los protocolos de codificación no conocidos por los estados en los que operan determinadas compañías de servicios de la sociedad de la información en la escena internacional, donde no alcanzan las obligaciones del art. 33 LGT. Debe anotarse también el carácter de solución improvisada y extraordinariamente limitada que tiene el procedimiento de infección por software de control remoto, a falta de disponer el Estado de un instrumento tecnológico al uso, como lo sería para las demás intervenciones el SITEL.

[546] Vid. Velasco Núñez, Eloy. *Delitos cometidos a través de Internet…op. cit.,* pág. 131 y ss.

[547] Entrevista con el autor celebrada el 22 de noviembre de 2011.

Por ello, cabe preguntarse si, ante tamaña incertidumbre y a falta de derecho positivo que respalde su actuación, pueda la PJE fundar el progreso de sus investigaciones en la inestabilidad y falta de solidez en la práctica de determinados medios de prueba que, por otra parte, no dan lugar a ser sustituidos por otras alternativas. Esta inestabilidad conduce, directamente, a la prudente renuncia policial a acudir a tan controvertidas fuentes de prueba, aunque sean invitados a ello por una primera predisposición de la Autoridad Judicial en fase de instrucción.

La consecuencia constatable de esta situación, además de otras consideraciones que por el momento no se introducen, sería la creación de amplios espacios de impunidad, tanto por la imposibilidad de intervenir legalmente, como por la escasa o nula fiabilidad de las que pueden practicarse de forma alternativa con los recursos tecnológicos actuales.

En el segundo caso, de configuración aún más inestable si cabe, a falta también de precisión en el repertorio jurídico sobre la materia, juega un papel determinante el conflicto entre la necesidad de mantener el secreto sobre los recursos, técnicas y procedimientos policiales y la de preservar al mismo tiempo los derechos que amparan al justiciable, contenidos en el art. 24 CE en relación con la tutela judicial efectiva y el derecho a la defensa.

La línea que separa una cuestión de la otra no es siempre visible. No obstante, y contrariamente a lo que pueda pensarse, en estos casos, si por algún lado toma opción la PJE es por el del garantismo pues, ante la más mínima noción de que pudiera estar poniéndose en compromiso algún derecho fundamental, se recurre inmediatamente a la solicitud del correspondiente mandato judicial.

Esta previsión evita además que, en el futuro, importantes líneas de prueba queden inhábiles para el proceso penal, lo que explica que, en ocasiones, se hagan exageradas las precauciones. Tanto es así que, en casos como los que cuestionaron la afectación al secreto de las comunicaciones por el uso del IMSI *Catcher* para el análisis del espectro radioeléctrico orientado a la obtención del IMSI[548] y el IMEI[549] de los

[548] El IMSI es el acrónimo del inglés *International Mobile Subscriber Identity* (Identidad internacional del suscriptor del teléfono móvil), que se expresa mediante un código alfanumérico que identifica e individualiza una tarjeta de telefonía móvil. La tarjeta, cedida al usuario por un operador del mercado de

terminales de telefonía móvil, hoy negada mayoritariamente, y que será tratado con mayor profundidad más adelante[550], aún después de consolidarse una jurisprudencia constante en el sentido de negarse la vulneración de derechos fundamentales con la instauración de concretas medidas, alguna de estas técnicas siguen siendo objeto de solicitud de mandato judicial previo por la PJE, lo que conlleva el improcedente efecto colateral de exponer el medio de investigación al conocimiento de los delincuentes. Los actos de investigación, hasta donde sea posible y la Ley lo permita, deben quedar fuera del conocimiento de los investigados.

Las consecuencias de la STS 130/2007 supusieron la anulación de las condenas de dieciséis narcotraficantes y la indeseable exposición del procedimiento técnico al conocimiento del mundo delincuencial, suscitándose con todo ello una innecesaria controversia por más que sea fortuna del Estado de Derecho el que, con acierto o sin él, las discusiones jurídicas se resuelvan donde deben: en sede judicial.

Junto a lo anterior, deben hacerse constar los riesgos jurídicos que se cernieron sobre los agentes de la PJE, a quienes se les insinuó una posible responsabilidad penal de acuerdo con el art. 198 CP, afortunadamente sin consecuencias en esta ocasión.

Las lecciones aprendidas sobre el ejercicio de la función investigadora muestran que, cuando la PJE se ve en la necesidad de limitar derechos fundamentales en el ámbito de las TIC, la regla que debiera permitirlo adolece de la conveniente seguridad, entre otras cosas, al producirse un desequilibrio o inestabilidad entre la norma de derecho positivo existente, sea adecuada o no a la finalidad perseguida, y la intuición sobre cómo responderá el principio de proporcionalidad ante un problema novedoso, llegado el caso, cuando devenga este en el instrumento jurídico de referencia que configure una resolución judicial expresa.

En efecto, sobre los conceptos jurídicos de *principio* y *regla*, al menos en lo que interesa al ejercicio de la función de PJ, se puede sostener una interesante discusión,

---

las telecomunicaciones e insertada en su aparato, pone en relación el terminal móvil con un número de abonado (que el que se marca en el dial cuando se desea comunicar con él) y este, a su vez, con los datos personales del suscriptor del servicio.

[549] El IMEI es el acrónimo del inglés International *Mobile Equipment Identity*, (Identidad Internacional de Equipo Móvil) es un código pre-grabado en los teléfonos móviles GSM que identifica al propio aparato y que, como tal dato, se pone en relación con el IMSI al establecerse una comunicación.

[550] SSTS 130/2007, considerando la afectación al derecho fundamental, y las 249/2008 y sucesivas, negándolo mayoritariamente.

pues el primero sugiere una amplitud en las posibilidades hermenéuticas del principio de proporcionalidad, frente a una eventual y defectuosa positivización en una regla que contuviese una indeseable constricción de las facultades sobre las que se pretende legislar de forma admisible en una sociedad democrática.

Sumado a lo anterior, la indeterminación que existe detrás del concepto jurídico de ***interdicción de la arbitrariedad*** permite hacer una exégesis del término que cierra la expresión y que permita decidir, con espíritu democrático, cuál sería la diferencia entre lo que es arbitrario y, consecuentemente, inadmisible para el Estado de Derecho, y lo no arbitrario y, por ello, útil al proceso penal.

Si se traslada esta discusión al ámbito de la extraordinaria evolución de la sociedad tecnológica actual, no parece descabellado plantear la cuestión del abordaje eficaz de la limitación de los derechos fundamentales desde una perspectiva más abierta.

En la ya muy avanzada, pero inacabada, modelación por el Tribunal Constitucional del principio de proporcionalidad, surge una labor de comprensión de las formas en que la misma sociedad se desenvuelve y que el Derecho no puede eludir; una sociedad que marca de esta forma el paso a las nuevas formas con las que ha de protegerse, al mismo tiempo, de las desviaciones con las que el mal uso de la tecnología amenace la libertad de los ciudadanos.

Por ello, un adecuado conocimiento técnico y práctico entre los operadores jurídicos de lo que las TIC significan realmente para la sociedad actual, permitiría retirar de la conceptuación – o más bien, la presunción - de arbitrarias a determinadas y novedosas medidas de investigación que supondrían, en un caso, una aceptable limitación de los derechos fundamentales a adoptar con exclusividad por el estamento judicial y, en otro, más simplemente, admitir que no todo lo que hace la PJE para investigar un delito en el ámbito de las TIC, sin intervención previa judicial, supone automáticamente una intromisión intolerable en el ámbito de la intimidad de los sujetos investigados y una puesta en cuestión de las libertades y garantías constitucionales.

Sobre la necesaria positivización de las formas constitucionalmente aceptables con las que ha de llevarse a cabo la limitación de los derechos fundamentales, impelida por las experiencias poco alentadoras que vienen de la mano de la irrupción de las TIC en el mundo del Derecho, en detrimento de su materialización a través de una aplicación cada día más extensa del principio de proporcionalidad, pueden encontrarse algunas respuestas en lo que se ha denominado la ***doctrina del periodo transitorio***. Su esencia la expresa PÉREZ GIL con la siguiente aportación:

> *"Del legislador ha de ser exigible que mantenga una actitud vigilante y de diligente actualización. O dicho con palabras de una reciente sentencia del Tribunal Constitucional Federal alemán*[551]*: «A causa de los cambios tecnológicos derivados de la sociedad de la información, rápidos y peligrosos para la protección de los derechos fundamentales, el legislador tiene que observar con atención los desarrollos tecnológicos y, en caso de urgencia, intervenir mediante legislación complementaria corrigiéndola…». Pero en la medida en que en este preciso instante se hacen perceptibles afecciones a derechos fundamentales sin sustento legal claro, no parece que quede otro remedio que aplicar la doctrina del periodo transitorio (Übergangszeit), también acuñada por el Tribunal Constitucional Federal alemán: las medidas restrictivas de derechos fundamentales carentes de una regulación legal expresa sólo pueden ser aplicadas durante un lapso temporal transitorio, en tanto el legislador acomete la tarea de su elaboración, a la cual se verá compelido por decisiones jurisprudenciales en ese sentido"*[552]*.*

Sin embargo, la voluntariosa previsión contenida en la doctrina alemana del periodo transitorio de propiciar cuerpos jurídicos adaptados dinámicamente a las necesidades surgidas de la realidad social – y especialmente en el mundo de las TIC -, incluso "corrigiendo la ley con legislación complementaria", no está exenta de riesgos pues la producción de nuevo derecho positivo puede suponer, por exceso de

[551] El autor se refiere a la sentencia *BVerfGE de 12 de abril de 2005 – 2 BvR 581/1.*

[552] El autor anota que *"sobre la necesidad de un fundamento legal para adoptar medidas limitativas de los derechos fundamentales en la investigación penal (referida a la habilitación legislativa para la práctica de medidas de intervención corporal) vid. la reciente STC de 14 de febrero de 2005 (ponente García-Calvo), FJ 6, así como el voto particular de Casas Baamonde al que se adhiere Aragón Reyes".* Vid. Pérez Gil, Julio. *Investigación penal y nuevas…op.cit.,* págs. 222 y ss.

garantismo o falta de calidad técnica, no un avance del Estado de Derecho sino un absoluto despropósito, echándose a faltar, en este caso, algo menos de dinamismo y más de explorar y asumir los progresos en materia de apreciación de la proporcionalidad.

En efecto, y a modo de ejemplo, la introducción en el Derecho alemán de la infección por la Policía Judicial mediante la instalación subrepticia de *software de control remoto* en dispositivos técnicos de comunicaciones electrónicas de los investigados (troyanos)[553], con las correspondientes modificaciones impuestas por su Tribunal Constitucional[554,555], supuso su incomprensible y exclusiva reserva a los casos de terrorismo, como si este fuese el único y grave riesgo al que se somete la sociedad actual[556], y una excepcionalidad que no se corresponde con los imperativos de la realidad diaria y constatable de la delincuencia en el mundo de las TIC[557].

Esta incomprensible constricción cercena cualquier posibilidad de aplicación proporcional de la medida en casos tan graves como lo serían los propios de la delincuencia, organizada o grave, o donde el uso de la tecnología haya resultado determinante para el perfeccionamiento de un delito de los que, con la perspectiva actual, sería materia perfectamente previsible de una intervención judicial clásica de las comunicaciones[558].

Es decir, que se trata de una norma que, de haberse redactado correctamente, en mi opinión, debiera haber alcanzado por analogía a aquellos casos en que una

---

[553] Sobre este interesante y novedoso asunto, vid. Ortíz Pradillo, Juan Carlos. *Hacking legal…op. cit.*

[554] Vid. pfo. *§ 20k: Verdeckter Eingriff in informationstechnische Systeme* de la ley *Bundeskriminalamtgesetz (BKAG) "Gesetz über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten"*.

[555] También, vid. Velasco Núñez, Eloy. *ADSL y troyanos…op.cit.*

[556] *Ibídem*.

[557] En mi opinión, tanto o más peligro que en el terrorismo atribuyo a algunas de las amenazas criminales organizadas tales como las que se muestran capaces de dominar o comprometer la acción de gobierno o menoscabar la confianza en la función pública, generar estados fallidos, poner en peligro la salud de los ciudadanos, condicionar la libertad o la viabilidad de sus proyectos de vida, atacar la estabilidad del sistema económico, etc. Se ha otorgado a la palabra *terrorismo* un valor que encierra en sí misma, haciéndola a la vez operar como concepto excluyente de otros fenómenos, todo aquello de lo que la sociedad ha de precaverse, sin reparar en que, al descargar falazmente el contenido del mal en la palabra que mejor lo contiene, se desarbola al mundo jurídico de la posibilidad de afrontar con vigor otras amenazas de igual o superior peligro como las que se han citado. Tanto es así que, en un penoso esfuerzo de retorcer el lenguaje para lograr que alcance a expresiones de lo criminal, igualmente reprobables, se hable de "terrorismo mafioso", "terrorismo doméstico", "terrorismo empresarial", etc.

[558] Por ejemplo, la intervención de una línea telefónica fija privada.

intervención común de las comunicaciones hubiera sido plausible de no haberse usado por los investigados unos medios técnicos de codificación de los que están al alcance del público general, pero cuyo descifrado no haya sido facilitado al Estado al uso del art. 33.10 LGT, por cualquier razón de las aludidas, bien por alguna operadora de telefonía, bien por algún prestador de servicios de la sociedad de la información, si es que a estos últimos les alcanzasen tales obligaciones.

Por ello, desde un punto de vista fáctico, el resultado material final de la injerencia legal en las comunicaciones electrónicas mediante el uso de *software de control remoto* no diferiría en nada de la que se haría por cualquier otro medio certificado como el SITEL, dado además que se hace por una PJE revestida de todas las presunciones de adecuación técnica y jurídica y bajo la más estricta autorización y control jurisdiccional.

Vista así esta norma alemana, supondría la creación de un prometedor espacio de impunidad lleno de inmensas posibilidades para el progreso de una delincuencia que gozará de la seguridad de no ser perseguidos por ese medio debido a una defectuosa interiorización por el legislador de la naturaleza inocua de la medida. Los delincuentes saben ahora que pueden refugiarse a placer en el secreto de sus comunicaciones, si usan los medios indicados sin ser terroristas, con la seguridad de que el Estado no les perseguirá.

Como resumen de lo anterior, se extraen algunas conclusiones, no todas alentadoras:

- En primer lugar, desear que el Estado cuente, en un tiempo razonable, oportunamente y sin conceder espacio a la arbitrariedad, con leyes de calidad que permitan afrontar los nuevos retos propiciados por el uso socialmente difundido de las TIC en condiciones análogas a las del espacio físico.
- En segundo lugar, temer que esta supuesta norma, por su falta de calidad, constriña indeseablemente el marco en que ha de ejercerse una función, haciéndose peor el remedio que la enfermedad.
- En tercer lugar, desear que una eventual y nueva norma no suponga un encorsetamiento indeseable del principio de proporcionalidad, siempre

> presente cuando la norma – buena o mala - haya de aplicarse a realidades concretas, sino una ocasión de medir los exactos términos en que, bajo la ponderada aplicación de este principio, alcanzará la Justicia a los investigados sin menoscabo de sus derechos fundamentales.

Hay que anotar también que, desde un punto de vista práctico policial y extrajurídico, la viabilidad de los métodos para la limitación de los derechos fundamentales gira en torno al insuficiente derecho positivo disponible – de una pésima calidad técnica y cuya obsolescencia debiera ser urgentemente resuelta -, a la indeterminación de los conceptos jurídicos y principios que pueden ser invocados y a la previsiblemente contradictoria aplicación material del principio de proporcionalidad por las sucesivas autoridades judiciales que, el ejercicio de sus facultades discrecionales, toman parte del complejo proceso penal español.

En definitiva, como GONZÁLEZ-CUÉLLAR meridianamente explicó en relación con la indeterminación del principio de proporcionalidad, se crea "*una [tercera] zona de sombra o incertidumbre o "halo del concepto" (supuestos de solución difícil, que depende en última instancia del juicio que se haga del mismo)*"[559] y, añadiría, una zona cuyo halo es de tal amplitud que entorpece o hace impredecible la legítima injerencia del Estado en los derechos fundamentales y que se desborda de una forma particularmente intensa cuando el ámbito de injerencia es el de las TIC, condicionando y haciendo confusa al mismo tiempo la regular actuación de la PJE.

Sin embargo, también desde un punto de vista extrajurídico, los avances de la PJE provenientes de las TIC no siempre suscitan el entusiasmo de importantes sectores de la doctrina, que muestran sus temores por una eventual e indeseable minoración del papel del actor jurisdiccional que, en mi opinión, lejos de producirse, se reforzaría si las reformas procesales integran las propuestas contenidas en este estudio hasta donde sea jurídicamente posible.

Estas reservas las expresa PÉREZ GIL del siguiente modo:

> *"Uno de los riesgos provocados por la irrupción de nuevas tecnologías en el proceso penal es la posibilidad de facilitar el socavamiento del papel del Juez,*

[559] *Ibídem*.

convirtiéndolo en un instrumento de mera convalidación de lo fáctico[560] *[…] Tras la merma de sus funciones en beneficio de la actividad policial, la necesidad de conocimiento del Juez queda con ello diluida […] La requerida especialización para una investigación precisada de una tecnificación y grado de conocimiento exacerbado puede ser una de las vías para que la policía pueda verse liberada de controles por parte del instructor y el fiscal. La complejidad técnica en la investigación de determinados delitos o la urgencia para asegurar fuentes de prueba se han erigido en muchas ocasiones en la única motivación para delegar en la Policía Judicial funciones eminentemente ligadas a facultades judiciales instructoras*[561] *[…] Nos enfrentamos por ello con la no lejana amenaza advertida por PEDRAZ en otra sede de que «de un Juez decisor —imprescindible y activo protector de los derechos y libertades fundamentales— se llegara al simple homologador formal de decisiones administrativas de policía…»… La preconstitución probatoria que la tecnología lleva implícita puede erigirse con ello en fuente de debilitamiento del judicial, al convertirle en mero agente de convalidación de unas decisiones que le vienen ya tomadas […] el funcionamiento de la tecnología forense puede ser imposible de refutar por contar con zonas inaccesibles […] investigaciones y análisis forenses que requieran la utilización de programas de código cerrado (es decir, prácticamente todos) […] el imputado que se viera perjudicado por un dictamen forense realizado con software de código cerrado no estaría en disposición de poder realizar un contraanálisis plenamente eficaz, en tanto toparía con un área vedada a la refutación […] nos conduciría a reconocer la claudicación del derecho frente a la tecnología"*[562].

Lo que PÉREZ GIL describe representaría, en sus propias palabras, *"una claudicación del Derecho frente a la tecnología"* que, en mi opinión, caso de existir y no resolverse, debiera expresarse más bien como *una claudicación del Derecho frente a la*

[560] El autor hace una referencia a Etxeberría Guridi, José Francisco. *La protección de los datos de carácter personal en el ámbito de la investigación penal.* Madrid: Agencia de Protección de Datos, 1998, pág. 153.
[561] El autor se apoya en López Ortega, J. J. *La admisibilidad de los medios de investigación basados en registros informáticos,* en *Delincuencia informática. Problemas de responsabilidad*. Madrid: Consejo General del Poder Judicial, 2002, págs. 77-111.
[562] Vid. Pérez Gil, Julio. *Investigación penal y…op. cit.,* pág. 230 y ss.

sociedad, pues esta hace años que asume la tecnología con naturalidad en su devenir diario. Esto sucedería, en todo caso, si no fuese capaz de servirse de los medios del Estado para encontrar soluciones justas, por haberse llenado el mundo jurídico de prejuicios insalvables que bloquean los progresos sobre el comedido papel que debe reservarse a la tecnología en el proceso penal y, de forma asociada, desprendiéndose del injustificado temor a que la PJE la use, siempre e incondicionalmente, del lado de la Justicia.

En este sentido, uno de los caminos para evitar el progresivo *"socavamiento del papel del Juez"* o su pretendida sujeción a la tecnología es que sea parte activa de sus progresos – debe *"unirse al enemigo"*, si se me permite el comentario -, pues, a los efectos, ha de constituirse en un operador más de los recursos tecnológicos admisibles en el proceso penal[563].

La clave es, decididamente, apostar en la dirección de introducir las necesarias salvaguardas tecnológicas para solventar el problema de "*incurrir en la confianza acrítica en la profesionalidad de los agentes"* que lamentan MARCHENA y MAZA[564] y tornarla crítica, ya que, reservando el lugar que el carácter de objetiva pueda corresponderle a la prueba tecnológica, la fase de contradicción del juicio oral discurra libremente – críticamente - centrada únicamente en las aportaciones de los operadores jurídicos al proceso penal para someterlas con todas las garantías imaginables a la libre valoración judicial.

Siendo así, las aportaciones de la PJE serían materia de la más estricta y directa contradicción y posterior valoración, al estar desprovistas de la fuente de duda que los prejuicios comentados asociarían a sus aportaciones tecnológicas[565].

---

[563] Sobre las inmensas posibilidades de desarrollo de la Administración de Justicia en materia de tecnología, vid. Fundación Telefónica. *Las TIC en la justicia del futuro.* Madrid: Airel, 2009.

[564] Véase más adelante el estudio sobre las dudas planteadas por estos magistrados sobre el SITEL en su Voto Particular de 1 de febrero de 2010 al Recurso de Casación 404/2009.

[565] Evidentemente, los medios de certificación impuestos mediante Ley devienen un elemento estratégico para garantizar la prueba tecnológica. Algo que, de un modo práctico, podría definirse, en referencia a una determinada salvaguarda tecnológica, que esta "hace lo que dice que hace", liberando al Juez de extender su duda o su crítica sobre el propio procedimiento y dedicándose a la pura labor de contradicción y valoración de la prueba obtenida por su mediación. Las pruebas tecnológicas, en este sentido, ni condenan ni absuelven. Lógicamente, el proceso de certificación excluye la admisión de cualquier suerte *software* secreto o procedimiento oscuro o cerrado que pueda pretenderse. Luz y taquígrafos para este cometido.

Un testimonio, el informe de una vigilancia policial, una prueba pericial o una transcripción de una conversación telefónica pueden adquirir, en virtud de este proceso esencial de contradicción propio de un sistema democrático de justicia, su más exacta dimensión, tanto para afirmar los hechos, como para refutarlos o para acreditar, en definitiva, su más absoluta irrelevancia para el proceso penal, distinta, por otra parte, de la opinión que a estos efectos pudiera haberse formado el Instructor Policial que es también, a estos efectos, de la más absoluta irrelevancia para formar la opinión judicial.

Concluye el autor estudiado que *"la evidente inadecuación de la actual legislación española sobre investigación penal al grado de desarrollo tecnológico merece todo tipo de reproches. Pero escudarnos en una fatalidad que vendría constituida por una ley inaceptable no puede ser la solución, así como tampoco lo sería el delegar íntegramente la respuesta en los Jueces, obligándoles a interpretaciones creativas"*. Legíslese eficazmente entonces.

Finalmente, PÉREZ GIL dice que *"de ahí que presentar las transformaciones tecnológicas como desencadenantes en una inevitable relación causa-efecto de las reformas procesales penales podría ser, como mínimo, una simplificación del problema"*[566]. Sobre esto, sencillamente, es el Estado el que debe asumir con naturalidad todos y cada uno de los condicionantes que la evolución de la sociedad produzca y, si estos han de tener consecuencias sobre el Derecho, pues asúmanse con adecuación a los irrenunciables valores democráticos que la CE proclama.

Los problemas procesales de actualidad respecto de la limitación del derecho al secreto de las comunicaciones, por tanto, no deben quedarse en su mera enunciación, por lo que en este estudio se propugna como solución es la correcta interiorización por el legislador de la más exacta naturaleza de este Derecho, a la luz de la evolución de las TIC, de la introducción de nuevas salvaguardas tecnológicas para asegurar que las pruebas que se practiquen sean objetivas, seguras y auténticas, y de la necesidad que la PJE haga progresar sus investigaciones mediante medios y procedimientos contrastados, muchos de los cuales ya están a su alcance.

[566] Vid. Pérez Gil, Julio. *Investigación penal y…op. cit.,* pág. 234.

Lo contrario supondría renunciar a que el Derecho actuase en aspectos sensibles de la vida social, generando prósperos espacios de impunidad para los delincuentes, que serán progresivamente más amplios conforme evolucionen las TIC y aumenten los injustificados prejuicios de importantes sectores de la doctrina.

IV. CAPÍTULO CUARTO: ASPECTOS DE INTERÉS SOBRE LAS COMUNICACIONES ELECTRÓNICAS

A. La necesidad del Estado de injerirse en las comunicaciones electrónicas

Todos los estados democráticos tienen en sus legislaciones previsiones para la legítima limitación del derecho fundamental al secreto de las comunicaciones y a la protección de datos personales[567]. La cuestión, desde la óptica de las TIC, es comprobar el grado de eficiencia que puede alcanzarse en España en relación con dicha limitación, tanto desde un punto de vista jurídico como técnico o práctico policial.

1. El concepto de comunicación en sentido amplio

a) Conceptos elementales sobre comunicación

Hasta el momento, poco se ha precisado sobre el propio concepto de comunicación y se hace necesario ahora profundizar en él con algún detenimiento.

Según la acepción tercera del diccionario, por ***comunicación*** debe entenderse la *"transmisión de señales mediante un código común al emisor y al receptor"*, es decir, en el terreno práctico, el entendimiento mutuo que se alcanza entre dos o más interlocutores[568] cuando emplean entre sí un sistema común de transmitirse mensajes[569] inteligibles. Con este concepto quedan abarcados, sin distinción, todos aquellos métodos y procedimientos que permitan completar el proceso de la comunicación entre personas con independencia del lugar donde se hallen o del uso o no de un instrumento técnico de comunicación de cualquier clase.

---

[567] Vid. Morillas Cueva, Lorenzo, y otros. *La intervención de las comunicaciones electrónicas. Posibilidades técnicas y límites jurídicos.* Madrid, 2005.
[568] Según el diccionario *"cada una de las personas que toman parte en un diálogo"*.
[569] Según la acepción séptima del diccionario, *"conjunto de señales, signos o símbolos que son objeto de una comunicación"*.

El concepto jurídico aplicable vendría definido en el art. 2.d) de la Directiva 2002/58/CE, del Parlamento Europeo y el Consejo, de 12 de julio de 2002, *relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas* (Directiva sobre la privacidad y las comunicaciones electrónicas), donde se dice que es comunicación "*cualquier información intercambiada o conducida entre un número finito de interesados por medio de un servicio de comunicaciones electrónicas disponible para el público. No se incluye en la presente definición la información conducida, como parte de un servicio de radiodifusión al público, a través de una red de comunicaciones electrónicas, excepto en la medida en que la información pueda relacionarse con el abonado o usuario identificable que reciba la información".*

De esta definición merece resaltarse la constricción del concepto a que la comunicación se produzca *entre un número finito de interesados*[570], lo que es sugerente, *sensu contrario*, de la proscripción de su aplicabilidad cuando el emisor no precise o identifique quiénes son los destinatarios o receptores del mensaje.

Esta percepción se refuerza, además, en la lectura de la frase final, respecto de los servicios de radiodifusión, ya que los mensajes transmitidos por este medio no pueden relacionarse con un abonado o usuario identificable, en cuyo caso tampoco se podrán tener por comunicación.

b) Insuficiencia del concepto de telecomunicación

Cuando la comunicación se produzca a tal distancia entre los interlocutores que no les sea posible mantenerla por sus propios medios o, alternativamente, hayan de servirse de un instrumento de cualquier naturaleza para establecerla, se podrá hablar, según el diccionario, de la ***telecomunicación*****,** que es un *"sistema de comunicación*

[570] En este mismo sentido, el *Reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de usuarios*, aprobado por Real Decreto 424/2005, de 15 de abril, en su art. 64, define la "comunicación" en la materia que aquí interesa como *"cualquier información intercambiada o conducida entre un número finito de interesados por medio de un servicio de comunicaciones electrónicas disponible para el público".* Véase también la STS 130/2007.

telegráfica, telefónica o radiotelegráfica y demás análogos"[571], término que sugiere un ámbito - perfectamente identificable en razón del instrumento mediato de la comunicación -, que alcanzaría a todos aquellos sistemas de transmisión a distancia de contenidos, intercambiados entre dos o más comunicantes y cuyo soporte, material o inmaterial, consistiese en el uso de los dispositivos tecnológicos de comunicación[572] existentes o que pudieran existir en el futuro, esto es, se trataría de un concepto que excluiría las comunicaciones que no se sirvan de un "*concreto artilugio técnico o medio mecánico a través del cual se transmite la información*"[573].

Sin embargo, el concepto de *telecomunicación*, pese a su enraizamiento en la CE[574], en el contenido de la LGT[575] y en la legislación complementaria, aún sin perder vigencia jurídica por su práctica equivalencia al de *comunicaciones electrónicas*, deviene insuficiente a la luz de la evolución legislativa operada en tiempos recientes desde la Unión Europea[576] - que opta por este último –, ya que el de *comunicaciones*

[571] Es evidente que, a los efectos que interesan a este estudio, al venir referido a las *comunicaciones electrónicas,* se establece un plus de significado sobre su exclusivo ámbito de intervención, al distinguir de entre todos los medios posibles de comunicación aquellos que sean intermediados por un dispositivo tecnológico basado en la aplicación de la electrónica.

[572] GONZÁLEZ LÓPEZ delimita y precisa el ámbito de intervención asociado al concepto de telecomunicación, afirmando que *"debe señalarse que la combinación de estas características sirve de fundamento a la inclusión en el ámbito de las telecomunicaciones de las comunicaciones telegráficas, telefónicas y telemáticas, así como de la radio y la televisión, pero no de las orales directas ni de las postales"*. Vid. González López, Juan José. *Los datos de tráfico…op.cit.,* pág. 30.

[573] Vid García de Enterría, E. y de la Quadra Salcedo, T. (coordinadores). *Comentarios a la Ley General de Telecomunicaciones. Ley 11/1998, de 24 de abril*. Madrid: Civitas, 1999, pág.858.

[574] Art. 149.1.21º CE.

[575] En la LGT viene definido el concepto de telecomunicación en su Anexo II como *"toda transmisión, emisión o recepción de signos, señales, escritos, imágenes, sonidos o informaciones de cualquier naturaleza por hilo, radioelectricidad, medios ópticos u otros sistemas electromagnéticos"*.

[576] Tras identificar su origen en la Comunicación de 10 de noviembre de 1999 de la Comisión al Consejo, al Parlamento Europeo, al Comité Económico y Social y al Comité de las Regiones titulada "*Hacia un nuevo marco para la infraestructura de comunicaciones electrónicas y los servicios asociados. Revisión de 1999 del sector de las comunicaciones"*, GONZÁLEZ LÓPEZ enumera las siguientes:*"Directiva 2002/19/CE, del Parlamento Europeo y del Consejo, de 7 de marzo de 2002, relativa al acceso a las redes de comunicaciones electrónicas y recursos asociados, y a su interconexión; Directiva 2002/20/CE, del Parlamento Europeo y del Consejo, de 7 de marzo de 2002, relativa a la autorización de redes y servicios de comunicaciones electrónicas; Directiva 2002/21/CE, del Parlamento Europeo y del Consejo, de 7 de marzo de 2002, relativa a un marco regulador común de las redes y los servicios de comunicaciones electrónicas; Directiva 2002/22/CE, del Parlamento Europeo y del Consejo, de 7 de marzo de 2002, relativa al servicio universal y los derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas; Directiva 2002/58/CE, del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas; y Directiva 2002/77/CE, de la Comisión, de 16 de septiembre de 2002, relativa a la competencia en los mercados de redes y servicios de comunicaciones electrónicas"*. Vid. González López, Juan José. *Los datos de tráfico…op.cit.,* pág. 40. A este listado hay que añadir la Directiva 2006/24/CE, del Parlamento Europeo y del Consejo de 15 de marzo de 2006, *sobre la*

electrónicas sumaría al de *telecomunicaciones* un nuevo catálogo de servicios relacionado con las posibilidades de la ***interactividad***[577] propiciada por el uso de la ***telemática***[578], ausentes conceptualmente del término primigenio de *telecomunicación*[579]**.**

Los no ya tan novedosos efectos de la interactividad en el mundo de las comunicaciones electrónicas tienen su expresión en un sinnúmero de aplicaciones informáticas – *software*- de los más insospechados propósitos, accesibles desde servidores telemáticos ubicados en cualquier punto del globo, que, para alcanzar sus finalidades, deben salir a la red a través de las infraestructuras técnicas de telecomunicación reguladas, en el caso de España, mediante la LGT[580].

En el esquema planteado pueden identificarse dos elementos para la transmisión de mensajes:

Uno de ellos, perfectamente conocido y normalmente controlado y regulado de forma suficiente en cada uno de los espacios nacionales soberanos mediante las leyes que regulan las telecomunicaciones (lo que incluye la obligación de permitir el acceso a su intervención legal por parte del Estado), consiste en la puesta a disposición de los

---

conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE.

[577] Según la acepción segunda del diccionario: *"Dicho de un programa: Que permite una interacción, a modo de diálogo, entre el ordenador y el usuario"*. Es decir, que los programas de ordenador, incluidos los que se distribuyen de cualquier forma a través de Internet, permiten un diálogo con el usuario de modo que este último configura dinámicamente el uso que desea hacer de su ordenador, produciéndose un intercambio de información que le es útil a sus propósitos. Por ejemplo, si el usuario desea adquirir un billete de avión, "interactuará" vía Internet con otros ordenadores conectados a la red para elegir el proveedor, el destino, las fechas, gestionar el pago a través de un servicio de banca electrónica, imprimir los billetes, etc.

[578] Según el diccionario: *"Aplicación de las técnicas de la telecomunicación y de la informática a la transmisión a larga distancia de información computarizada"*, definición muy sugerente para las finalidades de este estudio al sumar las inmensas posibilidades técnicas de comunicación propias de ambos conceptos técnicos, de tan fácil acceso a la práctica totalidad de los ciudadanos.

[579] A favor de un concepto intregrador de las comunicaciones electrónicas, o *"convergencia de las comunicaciones"*, vid. Hernández Guerrero, Francisco. *La intervención de las comunicaciones electrónicas.* Estudios Jurídicos del Ministerio Fiscal, III-2001, pág. 347. Este autor sostiene que la convergencia se basa en "*el proceso tecnológico en cuya virtud las señales de comunicación se unifican como medio de transporte de contenidos que, al ser digitalizados, permiten un tratamiento técnico homogéneo*".

[580] Por ejemplo, un mensaje de voz o texto codificados por un servicio prestado por un ISP fuera del territorio español, cuya conformación se hace internamente para, luego de ser codificado, ser enviado a sus destinatarios a través de la red pública de comunicaciones electrónicas que interconectan los servicios de Internet.

usuarios de las infraestructuras de redes públicas de comunicaciones electrónicas por las que circulan sus mensajes[581].

Pero el otro – y de ahí la singularidad de lo que se pretende poner de manifiesto -, consiste en la conformación en sí misma del mensaje, que puede trascender a la intervención personal del comunicante y del dispositivo que use, por haber sido sometido, por su voluntad, a un tratamiento informático ofrecido por un ISP (lo que puede incluir la codificación de los contenidos), cuyos servidores telemáticos podrán estar además ubicados en cualquier parte del mundo y accesibles libre o restringidamente desde otro.

Una vez configurado técnicamente el mensaje en la forma descrita, se enviará a sus destinatarios también a través de las mismas redes públicas de comunicaciones electrónicas que sirven para el uso de la telefonía clásica, bien en tiempo real o en diferido, bien en paquetes de datos digitales fragmentados o completos[582].

Lo común a ambos elementos es que los mensajes conformados por los ISP acceden a Internet a través de las redes públicas de comunicaciones del mismo modo a como sucede con la telefonía clásica pero, de un lado, con la configuración telemática que se ha explicado – incluido lo de la posible codificación - y, de otro, excediendo frecuentemente el espacio soberano de las naciones por cuyas redes públicas de comunicaciones electrónicas circule simultánea o sucesivamente la información así tratada.

c)Insuficiencia del ámbito objetivo de la LCDCE

Consecuencia de lo explicado en el párrafo anterior, del mero acto de la circulación en red de cualquiera de las formas y contenidos materiales descritos, las comunicaciones electrónicas dejan un rastro lógico según los diversos DACE que sean

[581] Por ejemplo, para hacer una llamada telefónica de voz o enviar un mensaje de texto (SMS), según el concepto más clásico de esta función.
[582] Por ejemplo, mensajes a través de *Skype, Whatsapp, Viber, ooVoo, Line,* etc.

necesarios técnicamente para que se produzcan y que serán conservados parcialmente por imperativo del art. 3.1 LCDCE.

Paradójicamente - y he aquí la cuestión nuclear que ha de plantearse en este estudio -, es que, de la conservación de los DACE producidos por el mero tránsito de los mensajes a través de las redes públicas de comunicaciones electrónicas, se ocupa la LCDCE *ex* art. 3.1 con notable suficiencia. Sin embargo, esta Ley no obliga a los proveedores de servicios de la sociedad de la información o ISP en su faceta de mediadores para la creación de los mensajes telemáticos (con la correspondiente generación de DACE), en idéntica forma que a los operadores regulados por la LGT, salvo cuando coincidentemente actúen como operadores, es decir, en opinión de GONZÁLEZ LÓPEZ, *"[cuando] proporcionan conexión a Internet, pero no cuando actúan como proveedores de contenidos"*. Quedan incomprensiblemente fuera de las obligaciones de conservación de la LCDCE, por tanto, los ***logs***[583] de las transacciones telemáticas.

La cuestión de fondo que plantea GONZÁLEZ LÓPEZ sobre la materia evidencia, en mi opinión, las deficiencias de la LGT para incluir en su ámbito objetivo de aplicación a determinadas formas de configuración de la comunicación electrónica, que son las protagonizadas por los ISP, cuyas expresiones interesan también al proceso penal con idéntico interés que las contempladas en el art. 3.1 LCDCE.

Así, bajo el concepto amplio de comunicaciones electrónicas que este jurista concibe, afirma que:

> *"De la combinación de ambas previsiones [el autor se refiere a determinados aspectos de la LGT], así como de la inclusión de las comunicaciones telemáticas en el concepto de "comunicaciones electrónicas" se desprende que la aplicación de la normativa referente a las comunicaciones*

[583] Es un registro técnico de los eventos que forman parte de las transacciones telemáticas. De una forma rudimentaria, pueden describirse como un registro o bitácora de los sucesos digitales que las configuran en relación con el tiempo y huso horario de su materialización. Podrían explicarse también como los DACE que se generan cuando un usuario accede y utiliza los servicios de un ISP, desde que se conecta e interactúa hasta que se desconecta, habiendo generado en todo este proceso dos tráficos de datos: uno a través de la red pública de comunicaciones electrónicas como consecuencia de su acceso a Internet para interactuar con el ISP y el que se produce en sus servidores por el propio uso de sus prestaciones telemáticas. Es esta última actividad la que deja el "rastro" o *logs* a que me refiero y que están ausentes de las obligaciones de conservación de la LCDCE.

electrónicas es aplicable no sólo a los proveedores de comunicaciones electrónicas, sino también a los proveedores de servicios de Internet (incluidos los de acceso y las instituciones y personas con acceso directo a Internet sin necesidad de recurrir a un proveedor, cuando la información se envíe fuera de la Red privada, ya que el concepto de "operador" está referido a las redes públicas y servicios disponibles al público). Ahora bien, de acuerdo con lo establecido en el artículo 1.2 los servicios de la sociedad de la información sólo estarán incluidos en el ámbito de aplicación de la LGT cuando "consistan, en su totalidad o principalmente, en el transporte de señales a través de redes de comunicaciones electrónicas"". […] "En cuanto a los proveedores de servicios adicionales (como la elaboración de perfiles), en cuanto no impliquen transmisión o encaminamiento de señales en redes de telecomunicaciones, no les es aplicable la LGT. La consecuencia es, en definitiva, que los proveedores de servicios están incluidos en la citada Ley cuando proporcionan conexión a Internet, pero no cuando actúan como proveedores de contenidos. Por ello, aunque no estaría de más, a efectos clarificadores, una previsión semejante a la del artículo 33 LGT en la LSSICE, merced a la interpretación que del concepto de la expresión "servicio de comunicaciones electrónicas" prevista en el Anexo de la LGT debe hacerse, cabe entender que tales proveedores se hallan incluidos en el ámbito de aplicación de la LGT"[584].

Sin embargo, de este párrafo se colige que el autor considera suficientes las obligaciones deducidas de la LGT con respecto al tránsito de los mensajes conformados por los ISP, opinión respecto a la que he de oponer la mía.

En efecto, la anterior discusión evidencia la insuficiencia que se trata de poner de manifiesto en este estudio pues, en términos de las necesidades de la investigación criminal que motivaron la promulgación de la LCDCE, no basta con disponer de los registros históricos del mero paso por la red de los paquetes de datos asociados a una comunicación telemática, sino también de los *logs* que sirvieron para conformarla internamente en los ISP y que debieran ser objeto de conservación mediante la imposición *ex novo* de una obligación análoga a la contenida en el art. 3.1 LCDCE.

[584] Vid. González López, Juan José. *Los datos de tráfico…op.cit.,* pág. 224 y ss.

En apoyo de este punto de vista, dice RODRÍGUEZ LAINZ de forma clarividente que:

> *"La definición de los sujetos concernidos es más modesta, menos ambiciosa, que la que imponía el art. 12 de la LSSICE, pues a los operadores de redes y servicios se añadía el concepto de prestadores de servicios de alojamientos de datos, sometidos eso sí, a la obligación de conservación de datos referentes solamente a los que permitan identificar «...el origen de los datos alojados y el momento en que se inició la prestación del servicio». La exclusión de la norma impositiva de prestadores de servicios de alojamiento supone una importante restricción al campo natural propio de la investigación sobre la trazabilidad de comunicaciones. Buena parte de la actividad terrorista internacional se difunde mediante el alojamiento temporal de información, no sólo mediática o publicitaria de sus fines ilícitos, sino también sobre consignas u órdenes concretas que suelen enmascararse en su contenidos publicados en servidores o prestadores de servicio de alojamiento de datos; rota la posibilidad de acceder a tales fuentes de información, en concreto los relacionados con el origen de los datos alojados, resultará imposible acceder a información para descubrir a sus autores, como no sea incidiendo de forma específica, tras el recabo de la oportuna autorización judicial, sobre los accesos que realicen en el futuro sobre la fuente originaria de los datos almacenados, disminuyendo peligrosamente las posibilidades de éxito en la investigación"*[585].

[585] Opinión que suscribo, especialmente en la indeseable constricción que supone para las capacidades de investigación de la PJE en ámbitos de las comunicaciones electrónicas extraordinariamente socorridos por los delincuentes de toda condición. Vid. Rodríguez Lainz, José Luis. *El principio de proporcionalidad…op. cit*. Sin embargo, y en contra de la opinión de este autor y pese a haber detectado la raiz del problema, GONZÁLEZ LÓPEZ, reiterando en un trabajo posterior la opinión ya expuesta sobre la materia, esta vez con la LCDCE en vigor, insiste en que *"…tampoco podemos coincidir con el autor referido [Rodríguez Lainz, en la referencia indicada] cuando echa de menos la previsión de este deber respecto de los "prestadores de servicios de alojamiento de datos" (como hacía el artículo 12 LSSICE), ya que, conforme a la definición de "servicio de comunicaciones electrónicas" y al artículo 1.2 LGT, y a la interpretación que el GRUPO DEL ARTÍCULO 29 proporciona, los proveedores de servicios quedan incluidos en el ámbito de la Ley cuando sus servicios consistan total o principalmente en el transporte de señales a través de redes de comunicaciones electrónicas, que es, en definitiva, lo que interesa en relación con el objeto de la LCD, siendo la pretensión de extender el deber de almacenamiento a los contenidos (implicando al administrador) contraria a la exclusión del contenido material que la propia LCD hace".* En mi opinión, este autor considera suficiente el reflejo conservado por imperativo de la LCDCE del paso por la red de comunicaciones electrónicas del tráfico IP mediado por los ISP, pero no alcanza a valorar que el proceso penal queda huérfano de los *logs* conservados de las transacciones

Es decir que, en tanto estos últimos DACE no sean utilizados para el concreto propósito de la telecomunicación a través de las redes públicas de comunicaciones, sino para el funcionamiento telemático del servicio interactivo regulado por la LSSI, todo el tráfico interno de datos asociado a su prestación material quedará al margen de la regulación de la LCDCE y sin imposición de obligación análoga alguna de conservación[586].

d) Análisis de las anomalías en el ámbito objetivo de la LCDCE

La explicación de las anomalías presentadas en el apartado anterior se encuentra en el análisis del ámbito objetivo de aplicación de la LCDCE donde, en el número 2 de su articulado, se dice que *"son destinatarios de las obligaciones relativas a la conservación de datos impuestas en esta Ley los operadores que presten servicios de comunicaciones electrónicas disponibles al público o exploten redes públicas de comunicaciones, en los términos establecidos en la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones"*, limitando con ello la aplicación a un sector muy concreto: el de los *"operadores"*.

Esto se debe a que la LGT, en su Disposición Adicional Segunda, que a su vez remite al Anexo II, define los siguientes conceptos que aclaran el ámbito objetivo de la Ley en la forma excluyente de los ISP en que se viene describiendo:

- Por *"operador"* debe entenderse "*la persona física o jurídica que explota redes públicas de comunicaciones electrónicas o presta servicios de*

telemáticas finalizadas, es decir, del contenido formal de tales comunicaciones y no del material, cuya conservación de ningún modo se pretende. Vid. González López, Juan José. *Comentarios a la ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.* Revista General de Derecho procesal. 16 de octubre de 2008.

[586] SALOM anota y lamenta también esta omisión por ocasionar evidentes ineficiencias en el acceso a la información relevante para la investigación criminal. Vid. Salom Clotet, Juan. *Incidencias de la nueva regulación en la investigación de los delitos cometidos a través de medios informáticos*. [ed.] Agencia Española de Protección de Datos. *La protección de datos en la cooperación policial y judicial.* Madrid: Aranzadi S.A., 2008, págs. 133-152, pág. 148.

comunicaciones electrónicas[587] *disponibles al público y ha notificado a la Comisión del Mercado de las Telecomunicaciones el inicio de su actividad".*

- Por "*acceso"* se entiende *"la puesta a disposición de otro operador, en condiciones definidas y sobre una base exclusiva o no exclusiva, de recursos o servicios con fines de prestación de servicios de comunicaciones electrónicas. Este término abarca, entre otros aspectos, los siguientes: el acceso a elementos de redes y recursos asociados que pueden requerir la conexión de equipos por medios fijos y no fijos (en particular, esto incluye el acceso al bucle local y a recursos y servicios necesarios para facilitar servicios a través del bucle local); el acceso a infraestructuras físicas, como edificios, conductos y mástiles; el acceso a sistemas informáticos pertinentes, incluidos los sistemas de apoyo operativos; el acceso a la conversión del número de llamada o a sistemas con una funcionalidad equivalente; el acceso a redes fijas y móviles, en particular con fines de itinerancia; el acceso a sistemas de acceso condicional para servicios de televisión digital; el acceso a servicios de red privada virtual"*.

Se desprende de la lectura del art. 2 LCDCE, por tanto, que la Ley no alcanza a obligar también a los prestadores de servicios de la sociedad de la información o ISP regulados por la LSSI[588], generando con ello una vasta laguna de servicios relacionados con el concepto ampliado de las comunicaciones electrónicas fuera de regulación de la

[587] En el art. 2.c de la Directiva 2002/21/CE puede leerse la siguiente definición: "*Servicio de comunicaciones electrónicas: el prestado por lo general a cambio de una remuneración que consiste, en su totalidad o principalmente, en el transporte de señales a través de redes de comunicaciones electrónicas, con inclusión de los servicios de telecomunicaciones y servicios de transmisión en las redes utilizadas para la radiodifusión, pero no de los servicios que suministren contenidos transmitidos mediante redes y servicios de comunicaciones electrónicas o ejerzan control editorial sobre ellos; quedan excluidos asimismo los servicios de la sociedad de la información definidos en el artículo 1 de la Directiva 98/34/CE que no consistan, en su totalidad o principalmente, en el transporte de señales a través de redes de comunicaciones electrónicas".* En el art. 1.2 de la Directiva 98/34/CE del Parlamento Europeo y del Consejo, de 22 de junio de 1998, *por la que se establece un procedimiento de información en materia de las normas y reglamentaciones técnicas y de las reglas relativas a los servicios de la sociedad de la información*, se define "servicio" como *"todo servicio de la sociedad de la información, es decir, todo servicio prestado normalmente a cambio de una remuneración, a distancia, por vía electrónica y a petición individual de un destinatario de servicios".* Con estos dos conceptos se comprueba la exclusión del ámbito objetivo de la LCDCE la materia relativa a la prestación de este tipo de servicios.

[588] Sería tanto más preciso definirla como "Sociedad del Conocimiento" pues su verdadero y revolucionario valor hay que percibirlo mucho más allá de lo que tiene de mero servidor de datos o informaciones. Los datos llevan a las informaciones, éstas al conocimiento y, finalmente, a la obtención de pruebas válidas.

Ley y cuyo tratamiento es imprescindible para conseguir los objetivos marcados por la Unión Europea en materia de conservación de los DACE, que son relevantes para la investigación penal o para cumplir con los demás propósitos que se proponen en este estudio, como lo sería el acceder a la intervención de la *VoIP* o la resolución de los casos de urgencia vital o riesgo catastrófico[589,590].

Para solventar este problema hubiera sido más útil el haber incluido una mejor redacción que obligase indistintamente a los *"…operadores de telecomunicaciones y prestadores de servicios de las sociedad de la información…",* lo que traería al ámbito de la norma estudiada a todos los operadores o prestadores de servicios susceptibles de conservar datos de absoluta relevancia para las acertadas finalidades de la Ley y cuya definición puede encontrarse en la LSSI.

Sin ánimo de exhaustividad y a título ilustrativo, por no tener la condición de operadores según la LCDCE, sino de meros prestadores de servicios, quedarían excluidos de la obligación de conservar DACE servicios tan importantes como:

- Servicios de todo tipo que ofrecen a sus clientes un valor añadido tales como redes Wi-Fi[591] o cable, públicas o privadas, gratuitas o a título oneroso, como las que hay en los aeropuertos, cafés-Internet, hoteles, centros cívicos o culturales, ayuntamientos, iniciativas privadas de todo tipo, etc. Los prestadores de estos servicios, como máximo, se limitarán, en el mejor de los casos y sin obligación jurídica alguna, a anotar los datos personales del usuario a efectos de facturación[592,593], pero que no tendrán

[589] Para comprobar de un modo práctico tal ausencia del ámbito de aplicación de la Ley, baste consultar el Registro de Operadores de la Comisión del Mercado de las Telecomunicaciones para verificar el escaso número de los sujetos obligados que han incluido su denominación en tal registro. Como se puede ver, sólo se hallan incluidos los proveedores de acceso a Internet y telefonía, pero no a los prestadores de servicios. Ver en http://www.cmt.es/cmt_ptl_ext/SelectOption.do.

[590] Vid. Vallés Causada, Luis. *La conservación y cesión de datos sobre telecomunicaciones a la Policía Judicial a la luz de la Ley 25/2007.* Madrid: UNED, 2009.

[591] Redes inalámbricas de conexión a Internet.

[592] En muchas ocasiones estos datos no vendrán referidos a la eventual conexión a Internet sino al mero uso del servicio general de que se trate (alojamiento en hotel, estancia en aeropuerto, etc.), con lo que no se podrá vincular en modo alguno al sospechoso con un supuesto tráfico de datos objeto del interés de la investigación, con la consiguiente pérdida de capacidad probatoria.

[593] No deja de sorprender, por otra parte, que la ley conceda la conservación para los efectos comerciales de facturación y sea tan restrictiva para la defensa de la seguridad pública.

obligación alguna de conservar los datos de tráfico en la forma que la LCDCE obliga.

- Servicios de correo electrónico, como pueda ser el que facilitan los servicios de intranet de las corporaciones públicas o privadas.
- Canales de IRC o *Internet Relay Chat*, que son servicios que ponen en relación a las personas que tienen intereses comunes de diferente naturaleza (Los usuarios entran en "salas" donde publican sus propias comunicaciones o mantienen comunicaciones netamente privadas).
- Accesos a redes sociales como *Facebook, Tuenti* o *Twitter*.
- Mensajería instantánea: Servicios en los que la comunicación se hace en un entorno estrictamente privado, como *Whatsapp*.
- *VoIP* (*Voice over IP*) o voz sobre IP: Son servicios de telefonía facilitados sobre el *Protocolo TCP/IP*.
- Servicios de comercio y banca electrónica[594].

Algunos casos o *modus operandi* en que se usaron con fines delictivos algunos de los servicios anteriores son los siguientes:

- Los servicios de mensajería instantánea son utilizados habitualmente por todo tipo de pederastas que simulan perfiles personales inocuos para conseguir fotografías o videos de menores en posturas sexuales explícitas e incluso trabar citas personales con el objetivo de abusar sexualmente de estas personas.
- Los canales de IRC han sido profusamente utilizados en numerosas ocasiones para establecer contactos sobre actos xenófobos, intercambio de contenidos de pornografía infantil[595], concertación para cometer delitos, etc.

[594] En delincuencia económica es muy común identificar a los manipuladores de los testaferros que administran sociedades fraudulentas mediante la determinación del acceso a través del *Protocolo TCP/IP* a las cuentas bancarias que debieran ser manejadas por estos últimos, evidenciando así al verdadero delincuente, que no es otro que el que verdaderamente maneja las cuentas de una forma clandestina. Este tipo de datos no estaría contemplado como objeto de conservación con arreglo a la actual redacción de la LCDCE.

[595] Sobre los peligros que la tecnología puede representar para los menores, vid. Ruiz Rodríguez, Luis Ramón y González Agudelo, Gloria. *El factor tecnológico en la expansión del crimen organizado. ¿Menores en riesgo?* [aut. libro] Luz María Puente Aba, Mónica Zapico Barbeito y Luis Rodríguez Moro.

- Las direcciones de correo electrónico corporativo han sido utilizadas para el robo de información, *hacking*, *phishing*[596], *farming*[597], instalación de *malware* o *troyanos*[598], usurpación de identidad, robo de secretos industriales, robo de fondos de comercio, amenazas, coacciones, etc.

Por todo ello, la redacción de la Ley debía extender la obligación a los sujetos indicados (*"…y prestadores de servicios de la sociedad de la información"*) e incluir también una referencia a la obligatoria llevanza de un libro-registro[599] con la identidad de los usuarios que acceden a Internet, así como una referencia al momento temporal en que tal conexión se produce. De esta forma, la acción de la LCDCE se extendería no sólo a los servicios de los operadores contemplados en la LGT sino también a los prestadores de servicios descritos en la LSSI.

e) Necesidad de un concepto amplio de comunicaciones electrónicas

Sobre la cuestión del alcance de los conceptos que han de manejarse para interpretar adecuadamente el fenómeno comunicativo de la sociedad actual, siguiendo nuevamente a GONZÁLEZ LÓPEZ, la expresión ***comunicaciones electrónicas*** resulta, frente al de *telecomunicaciones*, más adecuada para describir, con las correspondientes consecuencias jurídicas, las incuestionables realidades mencionadas en los párrafos anteriores, al entenderse como:

Criminalidad orgnizada, terrorismo e inmigración. Retos contemporáneos de la política criminal. Granada: Comares S.L., 2008, págs. 1-40.

[596] Sistema informático por el que se engaña a un usuario para obtener sus claves y contraseñas.

[597] Simulación de una página *web* para engañar a sus usuarios y conseguir sus datos (Por ejemplo: página *web* de un banco o de un sistema de comercio electrónico al que el usuario accede creyendo que representa a la entidad de su confianza, cediendo luego toda clase de datos que serán finalmente usados por los criminales).

[598] Programas que se instalan ilegítimamente en un sistema informático que se desea controlar y/o manipular.

[599] La llevanza de estos libros-registro, en lo que se refiere a la LCDCE, no ha supuesto en la práctica el más mínimo avance en la seguridad jurídica en cuanto a la identidad de los que adquieren las tarjetas prepago. Muy por el contrario, algunos ciudadanos han hallado su negocio en la adquisición a su nombre de elevadas cantidades de tarjetas para luego cederlas en uso a buen precio a delincuentes anónimos.

> *"El resultado de combinar tres elementos: los servicios de comunicaciones electrónicas, las redes de comunicaciones electrónicas y los recursos y servicios asociados"*, elementos cuya definición respectiva puede hallarse en el art. 2, apdos. a), c) y e) de la Directiva 2002/21/CE, del Parlamento Europeo y del Consejo, de 7 de marzo de 2002, *relativa a un marco regulador común de las redes y los servicios de comunicaciones electrónicas (Directiva marco)*[600,601].

En lo que interesa en este momento, es necesario aclarar en palabras del autor comentado el concepto de los *"recursos asociados"*, ya que "*implican el fenómeno telecomunicativo de nuevo cuño que justifica la mayor amplitud del contenido de las comunicaciones electrónicas frente al concepto tradicional de telecomunicaciones"* y que representa el problema que se trata de desentrañar.

Esta faceta, ajena a las prestaciones originarias de la telefonía fija o móvil, configura un universo de servicios para los que el Derecho no está preparado suficientemente y que obliga a explorar y a proponer un concepto amplio de lo que son y representan las comunicaciones electrónicas.

---

[600] Como oportunamente señala GONZÁLEZ LÓPEZ, *"dicha Directiva tiene como ámbito de aplicación, según su artículo 1.1, el establecimiento de "un marco armonizado para la regulación de los servicios de comunicaciones electrónicas, las redes de comunicaciones electrónicas y los recursos y servicios asociados""*. Vid. González López, Juan José. *Los datos de tráfico…op.cit.,* pág. 40 y ss.

[601] En ella se encuentran algunas definiciones de interés sustancial:
Art. 2.a: "*Red de comunicaciones electrónicas: los sistemas de transmisión y, cuando proceda, los equipos de conmutación o encaminamiento y demás recursos que permitan el transporte de señales mediante cables, ondas hertzianas, medios ópticos u otros medios electromagnéticos con inclusión de las redes de satélites, redes terrestres fijas (de conmutación de circuitos y de paquetes, incluido Internet) y móviles, sistemas de tendido eléctrico, en la medida en que se utilicen para la transmisión de señales, redes utilizadas para la radiodifusión sonora y televisiva y redes de televisión por cable, con independencia del tipo de información transportada*".
Art. 2.c: "*Servicio de comunicaciones electrónicas: el prestado por lo general a cambio de una remuneración que consiste, en su totalidad o principalmente, en el transporte de señales a través de redes de comunicaciones electrónicas, con inclusión de los servicios de telecomunicaciones y servicios de transmisión en las redes utilizadas para la radiodifusión, pero no de los servicios que suministren contenidos transmitidos mediante redes y servicios de comunicaciones electrónicas o ejerzan control editorial sobre ellos; quedan excluidos asimismo los servicios de la sociedad de la información definidos en el artículo 1 de la Directiva 98/34/CE que no consistan, en su totalidad o principalmente, en el transporte de señales a través de redes de comunicaciones electrónicas".*
Art. 2.d: "*Red pública de comunicaciones: una red de comunicaciones electrónicas que se utiliza, en su totalidad o principalmente, para la prestación de servicios de comunicaciones electrónicas disponibles para el público".*

En consecuencia, para solucionar el problema descrito en los párrafos anteriores, el Derecho debe dejar resuelta "*la confluencia de la LGT, en lo tocante a los aspectos comunicativos de Internet, y la LSSICE, por lo que respecta a las obligaciones de los proveedores de servicios"*, en palabras de GONZÁLEZ LÓPEZ, ya que, por el momento, de esta necesidad jurídica se descuelga la parte de la LSSI, pese a contar con un precedente, ya incomprensiblemente derogado - que no mejorado -, que obligaba difusamente a conservar datos a los ISP en su art. 12[602].

En efecto, la promulgación de la LCDCE supuso, entre otras, la derogación del art. 12 de la Ley 34/2002, de 11 de julio, *de servicios de la sociedad de la información y de comercio electrónico* (LSSI)[603], que imponía determinadas obligaciones genéricas - aunque adoleciendo de acierto técnico-legislativo -, de conservación de datos a los sujetos obligados por la citada Ley, todo ello de un modo parecido en esencia a las impuestas a los sujetos obligados según las previsiones del art. 33 LGT[604].

No obstante, a diferencia de los que hoy se impone en el art. 1.1 LCDCE sobre la ineludible necesidad de contar con un mandato judicial para acceder a los DACE, el procedimiento de cesión durante el periodo de vigencia del extinto art. 12 LSSI[605], se hizo bajo el régimen general de protección de datos, es decir, sin exigirse una orden judicial previa[606].

---

[602] Vid. Fernández de Palma, Rosa. *Análisis de la Ley 25/2007, de 18 octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones,* en *La protección de datos en la cooperación policial y judicial.* Madrid: Aranzadi S.A., 2008, págs. 175-176.

[603] En la Disposición Derogatoria Única dejó sin vigor el imperativo contenido en el apdo. 3 del art. 12 LSSI contenía sobre el acceso y cesión de datos a la Policía Judicial, cuya redacción era como sigue: *"Los datos se conservarán para su utilización en el marco de una investigación criminal o para la salvaguardia de la seguridad pública y la defensa nacional, poniéndose a disposición de los Jueces o Tribunales o del Ministerio Fiscal que así los requieran. La comunicación de estos datos a las Fuerzas y Cuerpos de Seguridad se hará con sujeción a lo dispuesto en la normativa sobre protección de datos personales"*.

[604] Tras el revulsivo que supuso la entrada en vigor de la LCDCE, se desplazó la carga de conservación de DACE desde los ISP, cuyo art. 12 LSSI quedó vacío de contenido, a las operadoras regidas por la LGT. Con ello, el Derecho parece ignorar lo que, en palabras de la STS 236/2008, de 9 de mayo, queda descrito como un uso meramente instrumental del teléfono en la transmisión de contenidos telemáticos: *"En la telefonía convencional los números desde donde se efectúan o reciben las llamadas se hallan protegidos por el derecho al secreto de las comunicaciones (S.T.E.D.H.: caso Malone de 2-agosto-1984); sin embargo en las comunicaciones por Internet el teléfono es un mero instrumento de comunicación con la red"*, lo que sin duda viene a evidenciar un clamoroso vacío legislativo (Interesa el instrumento, sí, pero mucho más, la conformación material y formal del mensaje).

[605] GONZÁLEZ LÓPEZ cita este artículo y su posterior derogación por la LCDCE como medio de referirse a una misma necesidad de conservación. Vid. González López, Juan José. *Comentarios a la ley 25/2007…op. cit*.

[606] Vid. González-Cuéllar Serrano, Nicolás. *Garantías constitucionales…op. cit.,* pág. 172.

Todo lo anterior permite comprobar el interés del legislador por atender una necesidad que, con los vaivenes observados en el cuerpo jurídico reciente, ha quedado incomprensible y precariamente desatendida.

Sería muy deseable, por tanto, regresar a la imposición de las mismas obligaciones mediante un nuevo art. 12 LSSI aunque, eso sí, dotado de una redacción sensiblemente más eficaz que la fallida que en su día tuvo[607].

Este concepto amplio de las comunicaciones electrónicas no puede ignorar que, en la conformación del mensaje, se produce la intervención singular de un elemento que excede a la intervención de las propias personas y de los dispositivos e infraestructuras de transmisión y que no son otra cosa que los servicios telemáticos puestos a disposición de los usuarios por los proveedores de servicios de la sociedad de la información, intervención que, con toda lógica, interesa al proceso penal con análoga fuerza a la relativa a las redes e infraestructuras públicas de comunicaciones y a los correspondientes servicios de comunicaciones electrónicas.

Consecuente con lo anterior, el tratamiento jurídico-procesal de las comunicaciones electrónicas demanda regresar a un enfoque mixto que integre el uso de las redes públicas de comunicaciones junto con cualquier otro elemento que contribuya directa o indirectamente a la conformación del mensaje.

2. Relevancia del contenido material para el proceso penal

No es ocioso, yendo al interés general y directo de la intervención de las comunicaciones electrónicas para el proceso penal, que la CE de 1978 haya otorgado un valor supremo a la defensa y protección de la intimidad y el honor personal en el art. 18 CE, estableciendo en su apartado tercero un extraordinario blindaje al derecho al secreto de las comunicaciones, con una mayor fortaleza a la establecida en el propio

[607] Por ejemplo, el art. 12.3 LSSI establecía el tiempo máximo de conservación de datos pero no el mínimo, lo que supuso una magnífica ocasión a los ISP para incumplir el meritorio propósito del legislador de conservar los DACE en cuestión o, más sencillamente, no definir de qué datos se estaba hablando, ya que tampoco se enumeraban las categorías que debían ser objeto de conservación y eventual cesión.

art. 8 CEDH debido a la reserva de judicialidad otorgada por el ordenamiento interno, al considerarla una de las expresiones más valiosas y dignas de protección dentro del derecho genérico a la intimidad porque, ciertamente, la comunicación verbal que se desea mantener de forma privada entre personas supone una de las expresiones del ser humano de mayor profundidad y carácter de estricta intimidad, superior incluso a las que se producen en las comunicaciones escritas.

La comunicación verbal – como expresión más sensible del ***contenido material*** de una comunicación -, por su propia naturaleza, presenta una inconmensurable riqueza para el desarrollo vital y la interacción social de la persona, consecuencia de la voluntaria, pero reservada, apertura hacia otro de su ser íntimo. Su carácter dinámico, espontáneo e irrepetible, hace de cada acto de comunicación una de las más altas y creativas representaciones de los intereses y sentimientos humanos, en los que, además, participan personas diferentes que, por un momento[608], interactúan para lograr una transferencia de conocimientos útiles a su respectivo desarrollo personal y vital.

En esto, naturalmente, cabe de todo, desde la más íntima y cabal transferencia del pensamiento, los secretos o los sentimientos humanos, como lo sería una expresión de afecto, a la más abyecta intención de causar un mal en otro, como pueda ser el conseguir el acceso carnal a un menor. Entre medias, puede hallarse todo universo de transferencias de información personal que, aunque incluyan también las de carácter anodino, irrelevante o incluso las meramente técnicas o no personales, gozarán todas ellas indistintamente de la más alta protección constitucional pues, por el momento, la Ley no ha establecido diferencias, grados o excepciones en tan estricta consideración. Tanto ha sido así, que en materia de conservación de los DACE existe una constatable confusión entre el derecho a la protección de datos y al secreto a las comunicaciones, controversia se pretende arrojar alguna luz en este estudio[609,610].

[608] Debe constatarse la indeterminación de esta expresión, ya que es relativa, debido que hay comunicaciones secretas que no se inician y acaban dentro de un mismo lapso de tiempo, como por ejemplo la emisión y posterior lectura de un mensaje de correo electrónico que, vistas de esta forma, constituyen una misma unidad de comunicación.

[609] GONZÁLEZ LÓPEZ, sostiene que *"la LCD parte de una concepción claramente errónea de la delimitación del derecho al secreto de las comunicaciones, a partir de la cual llega a conclusiones adecuadas desde el punto de vista del derecho fundamental realmente afectado (el derecho a la*

En lo que se refiere al estricto interés del proceso penal, tan sólo una ínfima parte del contenido material de las comunicaciones interpersonales tendrá normalmente relevancia – no por ello se deja de valorar el factor colateral de obtención de inteligencia operativa - y, más difícilmente, valor probatorio[611].

Por ello, desde un punto de vista práctico, una intervención telefónica, por ejemplo, podrá no haber tenido durante el proceso penal significado como prueba, pero habrá podido ser extraordinariamente útil para el descubrimiento de determinados elementos del escenario criminal, sin los cuales no hubiera sido posible acceder con posterioridad a la evidencia legal[612,613].

La cuestión más polémica respecto al acceso a los contenidos materiales hay que residenciarla en que, junto con la aprehensión de la evidencia que resultará del directo y estricto interés del procedimiento penal, se adquiere un innecesario conocimiento de otros aspectos de la intimidad de las personas investigadas o de terceros con los que se relacione espontáneamente y que, inevitablemente, se alcanza por no poderse determinar en qué momento se producirán, ni existir forma alguna de

---

protección de los datos de carácter personal) pero que, precisamente debido a su inadecuada fundamentación dogmática, son susceptibles de desdibujar la protección debida a ambos derechos, de lo que hay sobradas muestras en la propia LCD". Vid. González López, Juan José. *Comentarios a la ley 25/2007…op. cit*.

[610] Sobre las dudas que generan algunos pronunciamientos del TC y, aún más, del TS, RODRÍGUEZ LAINZ dice que *"en la doctrina emanada por el Tribunal Supremo pudo apreciarse un cierto grado de desorientación a la hora de aplicar los postulados defendidos por nuestro Tribunal de garantías constitucionales, manteniéndose la cierta confusión que le ha caracterizado a la hora de discriminar, conforme a las directrices anticipadas por el Tribunal de Derechos Humanos y el Tribunal Constitucional, cuándo se afecta al derecho al secreto de las comunicaciones y cuándo al derecho a la protección de datos de carácter personal o simplemente a la intimidad"*. Vid. Rodríguez Lainz, José Luis. *El principio de proporcionalidad…op. cit.*

[611] La relevancia será directa, si representa una verdad contrastable; e indirecta, si conduce únicamente a la obtención de inteligencia útil para el proceso investigativo o propicia el aseguramiento de otro tipo de pruebas. En ambos casos, y en frase ciertamente excesiva, se estaría hablando de "la verdad que conduce a la Verdad", toda vez que hasta las más esclarecedoras manifestaciones deben ser objeto de comprobación o refutación en el proceso penal (contradicción), lo que exige una previa actividad policial al efecto (Como ejemplo extremo, se podría aportar que es relativamente común que las líneas policiales 902 de colaboración ciudadana reciban llamadas de individuos que se atribuyen a sí mismos la autoría de delitos para dar satisfacción a su deseo mórbido de notoriedad).

[612] Ejemplo: Un dato de localización que permite descubrir un domicilio que oculta droga y ponerlo en relación con los autores del delito si, en un momento preciso, alguien dice *"te doy una llamada perdida cuando esté al lado de tu casa"*. Es evidente que la mera posición geográfica de una BTS en sí misma no ofrece la más mínima evidencia legal sobre la comisión de un delito contra la salud pública, pero permite al investigador colegir sagazmente que algo interesante sucede en el entorno de su zona estimada de cobertura.

[613] Véanse las SSTS de 17 de noviembre de 1994 (RJ 1994, 9276) y de 24 de marzo de 1999 (RJ 1999, 2052)

que estos datos desaparezcan, al menos, de la memoria del gestor de la ITCE que intervino en su análisis[614].

La participación en la función de salvaguarda de los derechos fundamentales que debe otorgarse al gestor policial de la ITCE debería hacerse extensiva, en mi opinión, a su activa intervención – darle un valor añadido, podría decirse, como la primera barrera opuesta al franqueamiento de la intimidad de los justiciables - para preservar estas facetas, que corresponden única y exclusivamente a lo más interior y privado del ser humano, y que son por completo ajenas al interés del proceso penal.

Así, durante el posterior trabajo de análisis y transposición de los contenidos, estos fragmentos quedarán precautoriamente trabados, salvo acreditada necesidad procesal de someterlos a contradicción, en cualquier momento, por haber sido solicitado por cualquiera de las partes y sometido todo ello al debido control jurisdiccional, en tanto pueda confirmarse la procedencia de ordenar la interdicción definitiva de acceso a los contenidos retirados[615,616].

Dicho sea con todas las reservas, pudiera ser procedente que el agente gestor de la ITCE extendiese, bajo las anteriores apreciaciones y dada su posición precedente

[614] Estas partes no se transcriben en el cuerpo del atestado policial, pero se conservan íntegras en los soportes que forman la evidencia legal a disposición de los operadores jurídicos. La decisión inicial corresponde al Instructor Policial, lo que no deja de recoger los reparos por parte de la doctrina sobre la idoneidad de tales decisiones, como ya se ha hecho constar en este trabajo.

[615] No debemos olvidar, por otro lado, que la limitación del derecho alcanzará la mayor parte de las veces tan sólo a uno de los interlocutores, dejando expuesta la intimidad del otro u otros sin que exista la más mínima necesidad al efecto (Por ejemplo, las conversaciones de un sospechoso con su cónyuge, que es ajeno por su parte a los delitos que se le presuponen).

[616] Se plantea como garantía o salvaguarda el uso de programas de análisis de contenidos electrónicos mediante ***sistemas de búsqueda ciega***, que son los que permiten la extracción discriminada de lo que interesa al proceso penal mediante criterios impuestos en el mandato judicial e impiden lo demás (parametrización de consultas). Esta es una interesante cuestión que merece algún detenimiento mayor, por su carácter controvertido, ya que el uso de herramientas de acceso parcial o restringido a una comunicación o sus DACE puede plantear alguno de los siguientes problemas: a) Generar dudas sobre el uso sin autorización de la parte del contenido no accedido con la habilitación judicial; b) No aportar al proceso penal partes del contenido no habilitado que pudieran ser del interés de cualquiera de las partes, incluida la defensa; c) Necesidad e importancia de contar con la debida seguridad jurídica y tecnológica de la configuración específica de instrumento, tanto en lo referido al *hardware* como al *software*; d) Necesidad de contar con un sistema seguro de certificación del instrumento (por ejemplo, un sellado de audio); siendo útiles todas estas prevenciones para evitar los problemas de nulidad relacionados con el derecho a la tutela judicial efectiva, el derecho a la defensa y a un procedimiento con todas las garantías. No obstante, este sistema, en términos de obtención de la IDACE en un ámbito tan complejo como el de las TIC, debería considerarse, precisamente, por su evidente utilidad para la extracción de evidencias digitales de entre la ingente cantidad de datos que se producen en los complejos procesos criminales de la actualidad, esto es, de IDACE admisible en el proceso penal.

en el proceso penal, alguna suerte de certificado, señal o prevención sobre específicos fragmentos del contenido de una ITCE, con los que quedasen provisionalmente trabadas aquellas partes estrictamente atinentes a la intimidad de los investigados.

La intervención de los contenidos materiales presenta algunas otras peculiaridades que conviene conocer y estudiar:

En relación con su espontaneidad, sin duda dependerá del grado de concernimiento o sospecha que el sujeto investigado pueda tener, tanto sobre los propios hechos que se le atribuyan y sobre la posibilidad de que esté siendo objeto de una acción de ITCE, como por el dominio sostenido en el tiempo que pueda ejercer sobre tales perturbaciones, de tal modo que le aconseje, incluso, manipularlas para tratar de utilizarlas en su favor para generar falsas evidencias que acaben siendo incorporadas al proceso penal o, al menos, conseguir maliciosamente diseminar una inteligencia falsa que dificulte la persecución del delito.

Sobre este mismo concepto de espontaneidad, es decir, de la ausencia de reserva intelectual del interlocutor sobre el contenido de su locución, se pueden sumar algunas otras observaciones que enriquecen el valor de la ITCE, ya que el vehículo por el que la comunicación se establece, esto es, el habla, no es un instrumento mecánico que aporte datos de una manera fría y automática sino que, muy por el contrario, está continuamente sometido a matices que incrementan su valor para la comunicación humana.

En este sentido, una frase aparentemente anodina puede adquirir un extraordinario valor para la investigación si se ha pronunciado con cierto énfasis, lo que puede conducir al analista a fijar su atención en el contenido concreto con el objetivo de tratar de descifrar su real significado, especialmente si se analiza en contraste con los hallazgos provenientes de las mismas o diversas fuentes de prueba.

La subjetivación que supone la participación del analista en la interpretación de lo escuchado durante una intervención de las comunicaciones, de la que no resulta ajena una buena carga de capacidad intuitiva, evidencia en numerosas ocasiones el valor orientativo que tan singularísima actividad policial encierra.

Algo parecido sucede cuando lo que se expresa tiene la apariencia de ser parte de un lenguaje convenido previamente. En este punto es donde entran en juego dos aspectos interesantes: de un lado, la necesidad de contar con analistas de extraordinaria habilidad y experiencia, capaces de actuar intuitiva y sagazmente para extraer el verdadero significado de la comunicación y contribuir a la demostración en el acto de juicio oral de la veracidad de la versión que sostienen (normalmente con un contenido contradictorio e imposible de unificar atendiendo a las meras reglas de la semántica); y, de otro, la necesidad de que su participación sea en el marco general de la investigación, que deberán conocer profundamente, lo que será garantía de la perfecta integración de la ITCE y su permanente adecuación y adaptación a la propia dinámica de la investigación dentro del proceso penal[617].

Por último, con la aparición de la telefonía móvil y la popularización de una gran diversidad de dispositivos telemáticos y formas de conexión a las redes públicas, se evidenció – o, como mínimo, se magnificó – el problema de la identificación del usuario real del dispositivo de comunicaciones y, con ello, la necesidad de probar la vinculación entre el contenido, material y formal, de las comunicaciones y la persona contra quien se dirigiese el proceso penal.

El problema, clásico ya en telefonía fija y, más intensamente, en la móvil, responde a la pregunta de quién es la persona que protagoniza el acto de comunicación o de conexión que puede resultar relevante como prueba de cara al juicio oral, pregunta que debe resolverse mediante la obtención colateral de pruebas e indicios directos o indirectos, que son normalmente aportados al atestado mediada la debida diligencia policial[618].

Pero, el problema así planteado, se complica cuando se trata de las comunicaciones a través de Internet.

---

[617] En determinados países, como es el caso del Reino Unido, los servicios de interceptación de las comunicaciones trabajan, por imperativo de un Derecho Procesal excesivamente garantista en este punto, de espaldas a los servicios de investigación propiamente dichos, con lo que se pierde la fecunda riqueza del esquema español de conciliación de ambos aspectos investigativos.

[618] Algunos sistemas como el SAIVOX (base de datos digitalizada de voz) pueden contribuir a aportar la prueba adicional que relacione una voz dubitada con la identidad indubitada de su emisor. Esto evidencia la formación de la convicción judicial es resultado de un complejo proceso intelectivo que debe alimentarse con una suma suficiente de evidencias proporcionadas desde la actuación policial investigativa. Naturalmente, este sistema puede ser admisible para cuando el mensaje sea de voz y, completamente inútil, para cualquier otro tipo de mensajes.

Esto se debe a que, *a priori,* no existe seguridad material alguna sobre la identidad real de los suscriptores de los servicios de la sociedad de la información *ex* arts. 23 y 24 LSSI – el famoso anonimato de la red -, resultando inútil que, en la realidad práctica de Internet, se invoque al efecto la ***buena fe contractual***[619,620] entre las partes que acuerdan una prestación de servicios, ni existir norma alguna de derecho internacional que aporte la más mínima eficacia a este acto, dada la naturaleza extraterritorial de las transacciones telemáticas en el plano más tangible de su realidad.

Esto puede atribuirse a que el candidato a usuario de uno de estos servicios, cuando se halla inmerso en el proceso telemático de suscripción, puede ofrecer una identidad imaginaria cuyo único medio de contraste sería a través de la verificación de una cuenta de correo electrónico precedente, de las que facilita cualquier otro ISP, como parte del proceso de vinculación telemática, que es normalmente exigido por el prestador como requisito meramente técnico para facilitar a su nuevo cliente el acceso a sus servicios y que, por las mismas razones, puede sufrir un idéntico vicio de certeza que la que se pretende suscribir[621].

Por todo ello, la única forma de adverar la identidad real sería mediante la resolución de las IP de las transacciones telemáticas de los contenidos, allí donde alcanzase el imperio de la Ley, lo que en España se traduce en la solicitud y cumplimiento del correspondiente mandato judicial ante un operador de comunicaciones electrónicas.

Esta posibilidad, en el modo que se ha explicado en apartados anteriores, únicamente facilitaría el conocimiento de los datos de conducción técnica de la comunicación a través de la red pública de comunicaciones, siempre y cuando el usuario se hubiera servido de un acceso a la red a través de un teléfono fijo o móvil

---

[619] Que *"significa fundamentalmente rectitud y honradez en el trato y supone un criterio o manera de proceder a la cual las partes deben atenerse en el desenvolvimiento de las relaciones jurídicas y en la celebración, interpretación y ejecución de los negocios jurídicos*". Vid. Díez-Picazo y Ponce De León, Luis. *La doctrina de los actos propios: un estudio crítico sobre la jurisprudencia del Tribunal Supremo*. Barcelona: Bosch, 1963, pág. 137.

[620] En la Directiva 2002/58/CE se dice, en su considerando 13 *que "las tarjetas de prepago se consideran asimismo un contrato".*

[621] Eso cuando no haya usado, para dificultar el trazado de sus suscripciones, alguno de los múltiples servicios instrumentales de simulación, falseamiento o activación temporal sin dejar rastro de cuentas de correo electrónico, como http://10minutemail.com/ o http://www.fakemailgenerator.com/.

cuyos datos contractuales personales fuesen ciertos[622], cosa que puede fácilmente eludirse, en su caso, mediante el uso malicioso de una tarjeta prepago contratada con incumplimiento de la obligación de identificación impuesta por la LCDCE o utilizando una red de acceso público a Internet de las que no identifican a sus usuarios[623], como un cibercafé, la red wifi de una universidad, un punto de acceso público de un ayuntamiento, etc.

Pero, aunque he considerado pertinente incluir en el apartado anterior determinados conceptos generales sobre las comunicaciones electrónicas, el acceso al contenido material de las comunicaciones adquirirá una atención secundaria en el interés de este trabajo, quizá animado por la necesidad de incidir en el estudio de la IDACE como parte integrante, pero sensiblemente distinta, respecto de otras facetas de la ITCE, ya que las materias de interés van a ser todas aquellas informaciones que, estando relacionadas con las comunicaciones electrónicas, no supongan en sí mismas injerencia alguna en el contenido de las comunicaciones privadas, ni tampoco revelación de la identidad de los usuarios que las estén manteniendo.

3. La conformación técnica del mensaje y su valor para el proceso penal

a) Facetas del derecho a la intimidad relacionadas con las comunicaciones electrónicas

Con ser el acceso al contenido material de las comunicaciones personales un elemento de interés prioritario para la mayoría de las investigaciones que se conducen en sede penal, la legítima limitación del derecho vertebrado por el art. 18 CE alcanza

[622] La relación contractual de los usuarios con cualquiera de las operadoras que prestan sus servicios de comunicaciones públicas en España se establece tras verificarse la identidad de los contratantes, a través de su DNI, domicilio, cuenta bancaria, etc., lo que normalmente no ofrece la más mínima duda al recabarse estos datos para las finalidades policiales de la investigación.

[623] Bien por tener un acceso abierto, bien por conseguir las claves con identidad falsa o, más sencillamente, por compartirse las claves entre varios usuarios. Adviértase además, la ineficiencia del registro de tarjetas SIM prepagadas en el ámbito de la UE, donde no existen normas armonizadas al efecto ni forma, en ocasiones, de adverar la identidad reales del usuario efectivo.

también, aunque sea de una forma necesitada de una urgente precisión jurídica, a aspectos estrechamente relacionados con la comunicación de cualquier naturaleza, pero atinentes a aspectos de su mera conducción técnica.

La conducción técnica de las comunicaciones electrónicas suscita algunas cuestiones que la relacionarían directamente, más con el derecho a la intimidad en relación con la protección de datos personales (art. 18.1 CE), que con el propio derecho al secreto de las comunicaciones (art. 18.3 CE) o, todo lo más, con el derecho a la autodeterminación informativa (art. 18.4 CE[624]), especialmente en materia de DACE conservados que, obviamente, se corresponden a actos de comunicación ya finalizados. En algunos casos, además, estos DACE no tendrán relación alguna con actos de comunicación personal, por haber sido generados como consecuencia de la mera puesta a disposición de la red al usuario o de la prestación de otros servicios añadidos de los que facilita la tecnología propia de los dispositivos actuales de comunicación, como es el caso de los *smartphones*.

Todo ello genera alguna confusión sobre la más exacta naturaleza del ámbito del Derecho concernido cuando se trate de invocar su legítima limitación y que es necesario resolver ya que, en efecto, en materia del derecho a la intimidad reconocido en el art. 18 CE, se hace necesario, con carácter general, definir la intensidad de la injerencia según corresponda a la naturaleza del derecho sacrificado en cada caso.

b) Contenido formal de las comunicaciones electrónicas

Las comunicaciones no son sólo los sonidos, signos, señales o caracteres dotados de significado que se transmiten o intercambian entre personas, sobre todo en la era de la telefonía móvil y la telemática, sino también un proceso para cuya materialización es necesario el soporte de una conducción técnica, cuya producción de

[624] GONZÁLEZ-CUÉLLAR, con anterioridad a la transposición de la DCD, sin excluir la protección del derecho al secreto de las comunicaciones, afirmaba sobre *"los datos producidos en el entorno digital del individuo"* que *"su examen…pone de manifiesto su insuficiencia [de la legislación vigente] y la necesidad de situar el problema en toda su complejidad en el ámbito del art. 18.4 CE, conforme al cual la Ley debe garantizar la intimidad – junto con otros derechos – frente a la utilización de la informática"*. Vid. González-Cuéllar Serrano, Nicolás. *Garantías constitucionales…op. cit.,* pág. 152.

DACE de todo tipo – el ***contenido formal***[625] - se asocia específicamente a cada comunicación individualizándola.

Estos aspectos de conducción técnica pueden dividirse en tres grandes áreas: En primer lugar, el acceso y circulación a través de una red pública de comunicaciones de los paquetes de datos de que esté compuesto un determinado mensaje digital de cualquier clase; en segundo lugar, el propio proceso de configuración del mensaje en sí mediante el uso de un determinado *software* y, en tercer lugar, la asociación de los datos técnicos o DACE que los anteriores procesos generen en cualquier momento, sea en la red pública de comunicaciones electrónicas, sea en los proveedores de servicios de la sociedad de la información cuya capacidad telemática los pueda producir.

Sobre las diferenciaciones puestas de manifiesto en el párrafo anterior surgen, precisamente, los territorios difusos en los que se entremezclan los derechos a la protección de datos y al secreto de las comunicaciones que es preciso deslindar, ya que el derecho interno, a través principalmente de la LGT, regula perfectamente lo concerniente al uso material de las redes públicas de comunicaciones electrónicas *ex* art. 33, en lo que se refiere al ***derecho de injerencia del Estado***, pero adolece de medidas eficientes sobre el acceso al contenido material y formal (en esto último, tanto en tiempo real como en diferido) de los paquetes de datos que conforman el mensaje transmitido en los casos que son objeto de este estudio, bien en claro, bien bajo protocolos de codificación de los contenidos materiales.

Esto es así porque, más allá de las infraestructuras de comunicación, los medios de transmisión y el objeto mismo de esta última, es decir, del mensaje o la información que se transmite, en que se centran las obligaciones de que se ocupan el art. 579 LCRIM, 33 LGT y la LCDCE en su conjunto, lo cierto es que, en razón de la producción material del mensaje y de su configuración electrónica, la tecnología pone a disposición de los comunicantes tal diversidad de medios para alcanzar sus fines a través de los diferentes usos de la red Internet – los servicios de la sociedad de la información -, que es necesario extender de forma específica unas previsiones análogas para este tipo de servicios en cuanto a su propio sustrato técnico.

[625] Vid. González López, Juan José. *Los datos de tráfico…op.cit.,* pág. 62 y ss.

En esta idea inclusiva de Internet, siguiendo a GONZÁLEZ LÓPEZ, es necesario considerar que:

> *"Internet no es un "tipo" determinado de comunicación, sino un "sistema" que se apoya en infraestructuras de comunicación variables (cable, emisor de ondas radioeléctricas, etc.) para permitir distintas formas de comunicación*[626]*. Es por ello que Internet se muestra como un instrumento de comunicación polifacético. Gracias a su configuración, es susceptible de permitir tanto la realización de comunicaciones interpersonales como de comunicación de masas*[627]*. Debido a ello, en Internet se manifiesta con singular relevancia la diversidad de tratamiento regulador, por un lado de las comunicaciones electrónicas que implica y en que se apoya, y por otro de los contenidos de los servicios suministrados, así como la confluencia de la LGT, en lo tocante a los aspectos comunicativos de Internet, y la LSSICE, por lo que respecta a las obligaciones de los proveedores de servicios (muchos de los cuales proporcionan servicios precisos a fin de hacer posible la comunicación), en cuanto marco legislativo de referencia"*[628].

Sobre la naturaleza del mensaje en sí mismo hay algo más que añadir pues, con la aparición de Internet como *"un instrumento de comunicación polifacético"*, tal y como lo describe GONZÁLEZ LÓPEZ, se producen insospechadas aplicaciones prácticas sobre el contenido material del mensaje que, a diferencia de lo ocurrido con la telefonía fija o móvil, ya no se limitará a la transmisión de voz, esto es, a relacionar entre sí a un número limitado de aquellos hablantes en los que pensó el legislador constitucional en 1978, sino también a transmitir mensajes de contenido técnico o, si se prefiere, no humano, a otros dispositivos – o máquinas, tal y como fueron referidas en párrafos precedentes - pero que serían tan inútiles como ininteligibles para las

---

[626] En este sentido, vid. Llaneza González, P. *Internet y comunicaciones digitales*. Barcelona: Bosch, 2000, págs. 35 y *ss*. Acerca de Internet es especialmente interesante del Grupo del Artículo 29 el *"Documento de trabajo. Privacidad en Internet: Enfoque comunitario integrado de la protección de datos en línea"*, adoptado el 21 de noviembre de 2000. En dicho documento se define Internet como "*una red de ordenadores que se comunican entre sí utilizando el* protocolo *de control de transporte/*protocolo *de Internet (TCP/IP)*", pág. 9. Lo anterior, es citado por González López, Juan José. *Los datos de tráfico…op.cit.,* págs. 33 y 34.

[627] Fernández Esteban, M.L. *Nuevas tecnologías, Internet y derechos fundamentales.* Madrid: MacGraw-Hill, 1998, pág. 26, citado por González López, Juan José. *Los datos de tráfico…op.cit.,* págs. 33 y 34.

[628] Vid. González López, Juan José. *Los datos de tráfico…op.cit.,* págs. 33 y 34.

personas o que, sin mediar un acto de comunicación, se produzcan una serie de datos relacionados con los servicios añadidos presados por el aparato o por su inserción en el medio radioeléctrico a disposición de cualquiera de sus posibles usos.

En mi opinión, la equiparación jurídica de los mensajes humanos con los técnicos supone una interpretación tan radical como errónea del espíritu del texto constitucional, lo que será objeto de análisis más adelante, siempre en la idea de hallar un enfoque jurídico-procesal coherente con la realidad social que este hecho representa.

Pero, sea cual fuere la naturaleza del mensaje, toda actividad de comunicación que, intermediada por un dispositivo técnico, se sirva de una red pública de comunicaciones electrónicas para la transmisión de un mensaje, como es obvio, genera un registro material y lógico dotado de un alto valor para la investigación criminal, aún en el caso de que el dato considerado en sí mismo, con arreglo a los medios de que dispone la PJE, no tenga un significado inteligible[629], pues, aún siendo así, debidamente interpretado, el dato puede ser usado como evidencia legal ante los tribunales una vez se ponga en relación con determinadas personas, haciendo que la actividad de la PJE de recopilación de todo ello y su uso como inteligencia para hacer prosperar las investigaciones sea del máximo interés para el proceso penal[630].

En este sentido, cuando se emplee la expresión ***obtención por la Policía Judicial de inteligencia sobre comunicaciones electrónicas*** (es decir, la inteligencia genérica sobre el conjunto de los contenidos material y formal de las comunicaciones electrónicas o ITCE), aunque pueda deducirse que de lo que se habla es del acceso al

[629] El IMSI, por ejemplo, no contiene en sí mismo ninguna información que pueda colegirse de su mera configuración alfanumérica. Únicamente la tendrá si se pone en relación con otros datos, como pueden ser los que se obtienen tras requerir judicialmente a la operadora los del contrato que le esté asociado. Pero, antes de que esto suceda, puede determinarse, con mayor o menor eficiencia, cuál es la estructura de corresponsales en las comunicaciones concretas de cada uno de los códigos IMSI que se conozcan o la ubicación geográfica de la antena que les dio servicio, por ejemplo, para determinar qué código IMSI se corresponde al móvil una persona concreta o si estuvieron varios de ellos en una determinada área, todo ello objeto del interés del proceso penal, por contraste o descarte de otros no captados en sucesivos escenarios geográficos donde se ha usado el *IMSI Catcher* ante dicho objetivo.

[630] Sobre la estricta naturaleza formal de los DACE referidos a las comunicaciones por Internet, algunos autores plantean dificultades y dudas en determinados casos para distinguirlos de los de naturaleza material. Vid. Oliver Lalana, D. *Autorregulación, normas jurídicas y tecnologías de privacidad. El lado virtual del derecho a la protección de datos*, en VVAA, XVII Encuentros sobre Informática y Derecho 2002-2003, Universidad Pontificia Comillas. Madrid 2003, pág. 87 y Crump, C. *Data retention: Privacy, Anonymity, and Accountability Online*. Stanford Law Review, nº. 1, volume 56, october 2003.

contenido material de las comunicaciones que las personas establecen entre sí en canal cerrado, en realidad, se estará hablando de un campo extraordinariamente complejo y abierto, en que el acceso al contenido formal adquirirá también un altísimo valor para el proceso penal, imposible de disociar del interés que pueda concitar el material e incluso superarlo en no pocas ocasiones.

c)Aproximación a la inteligencia sobre el contenido formal de las comunicaciones electrónicas

Bajo el enfoque general de la ITCE expuesto en el párrafo anterior, hay que referirse de una forma específica a la ***inteligencia sobre los datos asociados a las comunicaciones electrónicas*** (para la que se viene usando el acrónimo IDACE), entendiendo como tales DACE – por el momento bajo un concepto general - los que se producen como consecuencia del mantenimiento de la propia comunicación o del ***registro técnico del dispositivo***, tanto en los sistemas del prestador de servicios de Internet, como del operador de servicios de comunicaciones electrónicas de cualquier clase y que se incorporan a la investigación mediante el estudio exhaustivo del soporte tecnológico en que se materializaron, haciendo que la inteligencia de las comunicaciones electrónicas, centrada en sus datos de naturaleza tecnológica (la IDACE y los obtenidos tras el análisis forense del dispositivo técnico utilizado[631]), adquiera cada vez una mayor relevancia para el esclarecimiento de los hechos y, consecuentemente, para el proceso penal.

Hechas las anteriores consideraciones, los aspectos de conducción técnica, cuyos datos son plenamente conocidos, tanto por las operadoras de comunicaciones electrónicas, como por los ISP, representan en los últimos tiempos un creciente y extraordinario valor para la investigación policial[632], a veces crítico, como sucede en los

[631] Véanse, por ejemplo, las posibilidades de análisis de los ficheros de localización que pueden extraerse mediante análisis forense de los terminales incautados. Vid. Pérez Gil, Julio. *El nuevo papel de la telefónia móvil…op. cit.*, pág. 184.

[632] El término "creciente" que se ha usado en este párrafo se explica por sí mismo, bastando para ello la mera observación de los productos que el mercado tecnológico, en continuo desarrollo, ofrece a los consumidores. Estos productos están dotados de una extraordinaria variedad e imaginativas prestaciones rápidamente aceptadas por usuarios, lo que, a su vez, conlleva el nacimiento de nuevas e

casos de urgencia vital o, de forma decididamente útil, bien como orientadores imprescindibles de la investigación criminal, bien como medio de prueba para el proceso penal[633].

4. Nociones sobre la intervención de Internet

a) Modalidades de intervención legal de las comunicaciones por Internet

Es necesario comenzar este apartado haciendo notar los siguientes e importantes aspectos relacionados con la materialización del derecho de injerencia del Estado a través de la intervención de Internet, como ejemplo vivo de la diversidad del uso de las TIC y de su relevancia para el proceso penal[634]:

---

insospechadas fuentes de datos de interés para la investigación policial. Un buen ejemplo de ello sería el de la geolocalización de teléfonos celulares, algo impensable tan sólo hace unos pocos años por la muy sencilla razón de que estos dispositivos no existían.

[633] Sobre el valor para el proceso penal, véanse entre otras, SSTS de 31 de octubre de 1994 (RJ 1994, 9076), 19 de octubre de 1996 (RJ 1996, 7834) y 22 de abril de 1998 (RJ 1998, 3811). Sobre la función dicotómica, como instrumento de investigación y medio de prueba, véanse las SSTS de 17 de noviembre de 1994 (RJ 1994, 9276) y de 24 de marzo de 1999 (RJ 1999, 2052).

[634] Sobre la relevancia del *"entorno digital del individuo"* GONZÁLEZ-CUÉLLAR sostiene que *"está compuesto por la información en forma electrónica, magnética o luminosa que, voluntaria o involuntariamente, de forma consciente o inconsciente, genera con su actividad, no importa dónde se encuentren los archivos informáticos que la contengan o los canales de comunicación a través de los cuales discurra. Ya sea durante un instante, ya sea transitoria o permanentemente, una buena parte de los actos de la persona dejan un rastro energético, en algún medio o lugar, susceptible de servir como fuente de conocimiento de la realidad".* Vid. González-Cuéllar Serrano, Nicolás. *Garantías constitucionales…op. cit.,* pág. 150. El texto citado refleja una nueva realidad en la red, donde el ciudadano, sin saber bien cuáles de sus datos circulan, no tiene el más mínimo control o dominio de su entorno digital. Sobre la inquietante pérdida de control de los datos por el ciudadano, ya se aportó le preocupación contenida en el documento de la UE *"Un espacio de libertad, seguridad y justicia al servicio de los ciudadanos – Mayor libertad en un ambiente seguro"* (COM (2009) 262 final)". Por su parte, VELASCO, respecto de la expectativa de protección de datos sobre el entorno digital abierto que supone Internet dice que *"[la LOPD] prevista para entornos informáticos cerrados, no alcanza a valer para entornos abiertos como Internet, a cuyas dimensiones no puede poner efectivo coto".* Vid. Velasco Núñez, Eloy. *Delitos cometidos a través de Internet…op. cit.,* pág. 138. También, vid. Ballesteros Moffa, Luis Ángel. *La privacidad electrónica.* Valencia: Tirant lo blanch, 2005. DEL CASTILLO anota, por su parte, la transparencia que para los datos de los ciudadanos supone la tecnología, haciéndolo con una llamativa referencia histórica al uso por los nazis de las tarjetas perforadas para localizar a las víctimas de su política racial criminal. Critica, en general, la inevitabilidad de la diseminación de los datos por efecto de la tecnología. Vid. del Castillo Vázquez, Isabel-Cecilia. *Protección de datos: Cuestiones constitucionales y administrativas.* Cízur Menor (Navarra): Thomson Civitas, 2007, págs. 64 y ss.

El primero hace referencia al término "intervención", según un concepto clásico, que se ordenaría judicialmente en un sentido análogo al de las comunicaciones de telefonía fija o móvil, esto es, mediante la adquisición por la PJE del tráfico de los contenidos inteligibles que circulan por Internet entre dos terminales telemáticos, - en canal cerrado y a través de la red pública de comunicaciones -, uno de los cuales es, al menos, objeto del interés judicial.

Llevando este concepto a las comunicaciones de Internet, esta modalidad básica se podría denominar como ***intervención pasiva de Internet***, lo que, explicándolo de una forma más sencilla, supondría la interposición entre los comunicantes, objeto del interés de la intervención legal, de un dispositivo técnico de grabación que capte el tráfico de comunicaciones sin aportar otra actuación que la indicada. Es decir que, de no mediar alguna suerte de codificación en la transmisión del mensaje[635], el dispositivo sea capaz de aportar al proceso penal su contenido material y formal mediante la simple grabación pasiva de lo que circule por la red pública de comunicaciones electrónicas entre los sujetos de la intervención.

El segundo, alternativo al anterior, consistiría en la inmisión por orden judicial en el dispositivo telemático objeto del interés procesal, con la finalidad de conocer los contenidos y sus DACE que se hallen preordenados para su transmisión inmediata por la red pública de comunicaciones, todo ello al no ser posible su intervención durante el proceso específico de la transmisión por circular previamente codificados[636].

A esta forma se le denominará ***intervención activa de Internet***, para lo cual será necesario utilizar un *software de control remoto*[637]. Este *software* deberá

[635] Nótese que, sobre lo aplicable a las comunicaciones electrónicas mediadas por los operadores regulados por la LGT, que tienen la obligación *ex* art. 33.10 de entregar los códigos al Estado para que pueda ejercer su derecho de injerencia, los ISP que conformen los mensajes que harán circular por la red Internet, no estarán sujetos a esta misma obligación. Consecuentemente, una intervención pasiva de Internet sólo será útil en tanto los contenidos mediados por los ISP no circulen codificados por la red pública de comunicaciones electrónicas.

[636] Sobre el problema del cifrado, GONZÁLEZ-CUÉLLAR, recogiendo la amenaza que supone para los intereses del Estado si es usado para finalidades criminales, dice que *"el Estado se plantea como una necesidad acuciante la invasión del entorno digital, hasta el punto de otorgar la consideración de armas de guerra a los sistemas de blindaje de la información eficaces".* Vid. González-Cuéllar Serrano, Nicolás. *Garantías constitucionales…op. cit.,* pág. 151. Citados por el autor, vid. González Navarro, B.A., *Criptología y libertades públicas,* en Internet y Derecho Penal, Madrid, 2001, págs. 147 y ss y Fernández Rodríguez, J.J. *Secreto e intervención de las comunicaciones en Internet.* Madrid, 2004, págs. 175 y ss.

[637] Este tecnología no deja de ser un parche ante la imposibilidad de imponer obligaciones de facilitar la intervención en forma análoga a como se hace *ex* art. 33 LGT con *"los operadores que exploten redes*

instalarse con autorización judicial de forma subrepticia en el dispositivo de comunicaciones del objetivo, de modo que sus prestaciones técnicas solventen los problemas de acceso legal a los contenidos que puedan ser objeto de codificación no regulada.

El tercero, que puede considerarse una variación del anterior y que ha de tratarse de un modo diferenciado, se centraría en el registro y adquisición de los contenidos almacenados en cualquiera de las memorias de un dispositivo telemático, sin que la intervención hubiese de producirse necesariamente sobre los concretos elementos preordenados para su inmediata o futura transmisión a través de la red pública de comunicaciones.

Este procedimiento se denominará indistintamente ***registro remoto*** o ***registro virtual***[638] de un dispositivo telemático y de los derechos de acceso a los repositorios telemáticos de contenidos privados del objetivo, como los que se hallen almacenados en los sistemas de almacenamiento en nube.

El cuarto, sería el constituido por la ***navegación web*** realizada privadamente por un usuario de Internet mediante el libre acceso y consulta de cuantos contenidos estén disponibles en la red, bien en abierto, bien de forma restringida, cuya naturaleza íntima no ofrece dudas[639,640]. Este punto de vista es coincidente con el expresado por

---

públicas de comunicaciones electrónicas o que presten servicios de comunicaciones electrónicas disponibles al público", tratándose, por lo demás, de un recurso excepcional, de complejo y controvertido uso, muy lejos de la versatilidad y accesibilidad que tiene el SITEL, lo que evidencia la insuficiencia del Estado de Derecho para ejercer su legítimo derecho de injerencia cuando el usuario decida recurrir a medios de codificación fuera de regulación de las leyes sobre la intervención de las comunicaciones.

[638] ORTÍZ PRADILLO, consciente al tiempo de la volatilidad de la evidencia digital, reclama una reforma legislativa de tono garantista y orientada al ámbito tecnológico en que se produce la investigación, de modo que supere la aplicación analógica de los arts. 545 LCRIM y ss ("de los libros y papeles") a la que se recurre para la materialización de los registros virtuales. Sin embargo, se muestra contrario a aceptar opiniones más abiertas como las sostenidas por VELASCO NÚÑEZ (*Ibídem. Vid.* Velasco Núñez, Eloy. *Delitos cometidos a través de Internet…op. cit.,* pág. 138). Vid. Ortíz Pradillo, Juan Carlos. *El registro "on line" de equipos informáticos como medida de investigación del terrorismo (online durchsuchung)* en Serrano-Piedecasas Fernández, José Ramón y Demetrio Crespo, Eduardo (Directores) y AAVV. *Terrorismo y Estado de Derecho*. Madrid: Iustel. Portal de Derecho, 2010, págs. 457-477.

[639] En la STC 173/2011, de 7 de noviembre, de forma absolutamente esclarecedora, se dice que *"es evidente que cuando su titular navega por Internet, participa en foros de conversación o redes sociales, descarga archivos o documentos, realiza operaciones de comercio electrónico, forma parte de grupos de noticias, entre otras posibilidades, está revelando datos acerca de su personalidad, que pueden afectar al núcleo más profundo de su intimidad por referirse a ideologías, creencias religiosas, aficiones personales, información sobre la salud, orientaciones sexuales, etc. Quizás, estos datos que se reflejan en un ordenador personal puedan tacharse de irrelevantes o livianos si se consideran aisladamente, pero si*

el Grupo del Artículo 29, que considera que este tipo de comunicación debería ser confidencial[641]. Sin embargo, y como admite este mismo autor, la navegación por Internet desborda el concepto clásico, propio a su vez de una visión elemental del de comunicación, del emisor y el receptor, ya que, evidentemente, no existe un receptor al que dirigir una comunicación[642].

La LCDCE, en cualquier caso, opta por esta visión al equiparar en su art. 1.3 las consultas *web* con el contenido material de una comunicación: *"Se excluye del ámbito de aplicación de esta Ley el contenido de las comunicaciones electrónicas, incluida la información consultada utilizando una red de comunicaciones electrónicas"*[643].

Esta posición es extensible a los registros del servidor generados mediante la oferta de un servicio de motor de búsqueda, ya que deben considerarse contenido y no dato de tráfico, entendido, en mi opinión, en tanto formen parte de las consultas *web* descritas en los párrafos anteriores y no como inteligencia de fuentes abiertas a que se refieren los siguientes[644].

---

se analizan en su conjunto, una vez convenientemente entremezclados, no cabe duda que configuran todos ellos un perfil altamente descriptivo de la personalidad de su titular, que es preciso proteger frente a la intromisión de terceros o de los poderes públicos, por cuanto atañen, en definitiva, a la misma peculiaridad o individualidad de la persona. A esto debe añadirse que el ordenador es un instrumento útil para la emisión o recepción de correos electrónicos, pudiendo quedar afectado en tal caso, no sólo el derecho al secreto de las comunicaciones del art. 18.3 CE (por cuanto es indudable que la utilización de este procedimiento supone un acto de comunicación), sino también el derecho a la intimidad personal (art. 18.1 CE), en la medida en que estos correos o email, escritos o ya leídos por su destinatario, quedan almacenados en la memoria del terminal informático utilizado. Por ello deviene necesario establecer una serie de garantías frente a los riesgos que existen para los derechos y libertades públicas, en particular la intimidad personal, a causa del uso indebido de la informática así como de las nuevas tecnologías de la información".

[640] GONZÁLEZ LÓPEZ sostiene que *"en el ámbito de la "navegación por Internet", por el contrario, por mucho que una determinada información esté disponible al público, existe un acto volitivo de solicitud de la misma en que se manifiesta la capacidad del usuario o abonado de elegir el momento y contenido de la información a que tendrá acceso".* Por ello, este autor, pese a que reconoce a renglón seguido que *"la conexión a Internet no es comunicación y, por tanto, no existe un destino de la misma, sino sólo el hecho de acceder a Internet*". Vid. González López, Juan José. *Los datos de tráfico…op.cit.,* pág. 65 y ss.

[641] Vid. Grupo del Artículo 29, el "*Documento de trabajo. Privacidad en Internet: Enfoque comunitario integrado de la protección de datos en línea*", adoptado el 21 de noviembre de 2000, págs. 55 y 56. Desde un punto de vista práctico policial, la navegación en Internet no es sino una parte de un todo no diferenciable dentro del conjunto de una intervención de las comunicaciones, accedido en sede policial mediante el uso de una sonda pasiva o activa, todo lo cual haya sido previamente ordenado por un Juez.

[642] Vid. González López, Juan José. *Los datos de tráfico…op.cit.,* pág. 64.

[643] Sobre esta cuestión, vid. Rodríguez Lainz, José Luis. *El principio de proporcionalidad…op. cit.*

[644] Dictamen del Grupo de Trabajo del Artículo 29 sobre cuestiones de protección de datos relacionadas con los motores de búsqueda, de 4 de abril de 2008. Algunos ejemplos serían los motores de *Google* o *Yahoo*.

b) La excepción de la inserción de contenidos en canal abierto

Un quinto y último aspecto, estaría representado por la ***inserción en canal abierto de contenidos en Internet,*** que quedarían a la libre disposición de un grupo indeterminado e ilimitado de usuarios[645,646] o, dicho en sentido contrario, que no se destinen de forma cerrada o restringida a un grupo identificado y limitado de interlocutores, en cuyo caso el nivel de protección sería el determinado por el art. 18.3 CE[647,648].

De esta última categoría, centrada en los incontables *terabytes* de información disponible en Internet, debe distinguirse lo que se podría denominar, siguiendo a GONZÁLEZ LÓPEZ, el ***ciber-patrullaje***[649,650], que sería una función genérica de la policía de seguridad orientada a la vigilancia, prevención y evitación de ilícitos cuya evidencia conste en la red, de la que se denominará ***análisis de fuentes abiertas***[651], que se correspondería a la función de la PJE dirigida a la búsqueda de informaciones que contribuyan al esclarecimiento de los hechos delictivos ya cometidos y que son objeto del interés del proceso penal[652,653].

---

[645] Y, debería añadirse, bajo la pérdida de control más absoluta por parte de su autor de todos los datos insertados en la red.

[646] En la STS 236/2008, de 9 de mayo, se reconoce que *"no se precisa de autorización judicial para conseguir lo que es público y [que es] el propio usuario de la red es quien lo ha introducido en la misma. La huella de la entrada […] queda registrada siempre y ello lo sabe el usuario"*.

[647] GONZÁLEZ LÓPEZ, de forma inclusiva, dice que *"el hecho de que los usuarios de ciertos servicios deban someterse a un proceso de registro no excluye el carácter de comunicación en canal abierto, cuando dicho registro no se acompaña de una verificación de la información personal"*. Vid. González López, Juan José. *Los datos de tráfico…op.cit.,* pág. 114.

[648] GONZÁLEZ-CUÉLLAR dice que *"…no afecta al derecho fundamental del art. 18.3 CE, la captación de datos difundidos públicamente por Internet". k* vid. González-Cuéllar Serrano, Nicolás. *Garantías constitucionales…op. cit.,* pág. 166.

[649] Anota GONZÁLEZ LÓPEZ que *"la posibilidad de que la percepción de la notitia criminis derive del ejercicio de funciones preventivas (como el control de espectáculos, labores de patrulla, etc.) es destacada en Martínez Pérez, R., Policía Judicial y Constitución, Aranzadi, Navarra 2001,* pág. *380. En este sentido, "a la actividad de patrullaje se le han atribuido dos objetivos: prevenir el delito, dificultando las posibilidades de cometer delitos y facilitando la detención de los autores, y crear un sentido de seguridad ciudadana". Rico, J. M. y Sala, L. Inseguridad ciudadana y policía, Tecnos, Madrid, 1988,* pág. *100"*. Vid. González López, Juan José. *Los datos de tráfico…op.cit.,* pág. 131.

[650] Vid. STS 236/2008, de 9 de mayo, FD 3º.

[651] Más adelante se tratará con más profundidad este asunto.

[652] Es de hacer notar que la investigación, en este caso, se dirige primariamente más desde el hecho a la persona que al contrario y que, al seguirse o trazarse indicios existentes en la red en abierto, pueden

Sobre esta importante fuente de información, el Parlamento Europeo ha enviado a la Comisión una declaración escrita en la que pide que la Directiva se amplíe a los motores de búsqueda *"para luchar rápidamente contra la pornografía infantil en línea y los abusos sexuales"*[654], lo que debe interpretarse como una invitación a la conservación de DACE relacionados con las transacciones telemáticas en línea con lo que se propugna en este estudio. Y no sólo eso, sino propiciando una cesión diligente de los datos en la escena internacional.

Sin embargo, como es notorio, el campo de la pornografía infantil, a pesar de su muy execrable existencia, no es el único motivo de interés para esta modalidad investigativa pues, con toda evidencia, existen innumerables bienes jurídicos a proteger con idéntico e incluso superior concernimiento público e idoneidad de los instrumentos jurídicos y tecnológicos, por lo que esta iniciativa debiera tener una aplicación horizontal o genérica en el ámbito de lo criminal.

Es también interesante la lectura de la STS 236/2008, de 9 de mayo, sobre el ***rastreador HISPALIS,*** utilizado por el GDT para relacionar los *hash* de los archivos previamente identificados como de contenido pornográfico infantil (conservados en un repositorio de datos *ad hoc*), con las IP de los usuarios criminalmente responsables de su distribución telemática vía *Peer to Peer* o *P2P*[655], por la que el tribunal sentenciador, pese a la oposición del Ministerio Fiscal, consideró que *"las claves identificativas (Internet Protocols: IPs) no concretan a la persona del usuario, sino sólo el ordenador que se ha usado*[656]*, lo que hace necesario para poder llegar a conocimiento del número*

---

aportarse como evidencia digital ante la Autoridad Judicial o Fiscal que entienda del caso y, eventualmente, motivar una posterior limitación del derecho al secreto de las comunicaciones.

[653] Sobre la naturaleza procesal de esta medida de investigación, distinta de la actividad de la Policía de Seguridad, de naturaleza netamente administrativa, por todos, vid. Queralt Jiménez, Joan Josep. *Oportunidad, necesidad y legalidad en la actuación policial.* Policía y sociedad. Madrid: s.n., 1990, págs. 162-165, pág. 161.

[654] Declaración escrita de conformidad con el artículo 123 del *Reglamento interno sobre la creación de un sistema europeo de alerta rápida contra los pederastas y los delincuentes sexuales*, 19.4.2010, 0029/2010.

[655] Por ejemplo, véase el intercambiador en red de archivos *eMule*.

[656] Yerra el tribunal, aunque de forma meramente anecdótica, al considerar que la IP, que sólo identifica una conexión genérica a Internet, tiene la facultad de identificar, entre otros posibles dispositivos conectados simultáneamente, también al ordenador en cuestión. Sin embargo, como tal dispositivo telemático, la identificación sólo podría determinarse mediante el acceso su dirección *MAC* si, a su vez, pudiese previamente estudiarse la del *router* que le dio servicio en el momento preciso que interese a la investigación (Además, sea esto dicho con todas las reservas sobre la seguridad de la identificación debidas a la fácil y arbitraria modificabilidad de las respectivas *MAC* por el usuario). Lo de los datos

de teléfono y titular del contrato[657] *(datos que pueden reputarse reservados) la autorización judicial, que es lo que se hizo en el caso que nos ocupa ante el Juzgado de Instrucción nº 7 de Sevilla que expidió el correspondiente mandamiento".* Por ello, concluye en lo que interesa a la exposición, que "*los rastreos policiales previos que se tildan de ilegales, sólo afectaban a datos públicos de Internet no protegidos por el art. 18-1º y 3º de la Constitución y en consecuencia las pruebas obtenidas y las derivadas no se hallaban afectas a vicio alguno".*

En mi opinión, fundada en todo lo planteado hasta el momento, nada obsta para que la accesibilidad de la PJE a los contenidos insertados en abierto en Internet sea plena y sin necesidad de previo mandato judicial, ya que, como sostiene VELASCO,

> *"Internet es una red pública internacional, y quien distribuye en ella sus contenidos – en ofrecimiento público, genérico, universal e indiscriminado – y utiliza sus herramientas, sabe que deja rastros de su entrada y uso que pueden ser analizados por los investigadores, de la misma manera que quien delinque en la calle sabe que se expone a que se encuentren pruebas de su autoría. Su búsqueda no es sino la inspección ocular en el mundo virtual que, si no afecta a áreas de privacidad ni a secretos comunicativos, se hace exactamente igual que en el mundo convencional […] Internet es un tablero o expositor de contenidos, que excluye la reserva y la privacidad"*[658].

Esta interesante opinión responde a la lógica de los tiempos, necesitada de una intervención policial parangonable a la ya perfectamente consolidada en el mundo físico, tanto en los aspectos de vigilancia y seguridad pública en la red, como en términos de la actividad indagatoria propias de la PJE[659].

---

individualizadores del ordenador y, naturalmente, la identidad del usuario, serían por tanto otro cantar, objeto como siempre de la sagacidad investigadora de la PJE. Es ocioso recordar, por otra parte, que entre los DACE conservados por la LCDCE no se encuentran los de las *MAC* mencionadas.

[657] Datos que, en principio, nada tienen que aportar a la investigación pues puede tratarse de un acceso público aprovechado anónimamente por el delincuente. La investigación, por tanto, habrá de completarse a través de otros derroteros totalmente distintos a los esperados en este caso.

[658] VELASCO se apoya, entre otras, en la STS, de 9 de mayo de 2008 (donde se niega siquiera la protección del art. 18.1 CE para los "datos públicos" relacionados con las inserciones de contenidos abiertos en Internet). Vid. Velasco Núñez, Eloy. *Delitos cometidos a través de Internet…op. cit.,* pág. 220 y ss.

[659] También vid. González-Cuéllar Serrano, Nicolás. *Garantías constitucionales…op. cit.,* pág. 166.

Sin embargo, la realidad del día a día policial, en tanto la información de fuentes abiertas no pueda extraerse de un modo directo y jurídicamente seguro de la red, acabará siendo objeto de la tabla rasa que supone el exceso de garantismo, sustentado en la indefectible postura dominante que la vinculará a la exigente protección del art. 18.3 CE, todo ello por haber existido previamente, o existir en tiempo real, determinados actos de comunicación yuxtapuestos como medio de materializar la inserción en la red.

Por lo anterior, cualquier intento de la PJE de obtener DACE de un ISP, por ejemplo, estará condenado al fracaso. Esta situación será tanto más tangible cuanto que la investigación se aleje del hecho y se acerque más a la persona que la haya originado donde, ciertamente, será difícil distinguir qué partes de sus comunicaciones serán de carácter íntimo y cuáles no, lo que, con toda evidencia, exigirá, sin ninguna duda, la anuencia de la Autoridad Judicial para la intervención legal de sus comunicaciones[660].

Existen también otros elementos distintivos de las categorías enunciadas respecto de la intervención clásica de las comunicaciones y que representan un grave problema, dado que, frente al inestable cuerpo jurídico-procesal que ampara con alguna suficiencia la intervención de las comunicaciones telefónicas, establecido en el art. 579 LCRIM y la copiosa jurisprudencia existente – que se aplica por analogía a la intervención pasiva de Internet, a la de los consultas *web* y a la inserción en canal abierto de contenidos en Internet (en tanto los ISP o el usuario no codifiquen sus contenidos) -, las previsiones que al efecto contiene el art. 33 LGT para las operadoras de telefonía, no tendrían el parangón que obligase de la misma forma a los ISP en lo referido a su puesta a disposición del Estado para el ejercicio de su derecho de injerencia, lo que perturba, tanto el tratamiento jurídico del problema, como la dotación de una solución tecnológica alternativa, ciertamente precarios.

Las razones de esto último son de una inquietante obviedad: Un Estado no puede imponer su Ley fuera de su territorio soberano o allí donde pueda llegar,

[660] Por ejemplo, averiguada una dirección IP de un pedófilo, la labor de identificación deberá ser solicitada del Juez de Instrucción, tal y como se deduce de la STS de 12 de noviembre de 2008. Vid. Velasco Núñez, Eloy. *Delitos cometidos a través de Internet…op. cit.,* pág. 223.

siempre precariamente, mediante la invocación, llena de incertidumbres e inseguridad jurídica, de determinadas facultades admitidas por el derecho internacional.

En este sentido, la provisión de servicios de Internet puede hacerse desde cualquier punto del mundo donde pueda instalarse un servidor telemático (incluidos los paraísos informáticos) e, incluso, distribuirse la información en paquetes de datos cohesionados digitalmente pero fragmentados, por el mismo medio, en una constelación ignota de servidores físicamente instalados en diversos países del mundo[661].

Tampoco puede obligarse a cada ISP, siguiendo los razonamientos planteados, a entregar sus protocolos de codificación en analogía a lo que impone el art. 33.10 LGT a las operadoras de telefonía dentro del territorio nacional[662].

Por todas las anteriores razones, la respuesta de los ISP queda al pairo de cuanto asuman, dentro del territorio nacional (o donde alcance en tiempo diferido la respuesta en la escena internacional mediante los imperativos jurídicos o de otra naturaleza que sean), respecto del deber genérico de colaborar con la Justicia que obliga a todo ciudadano *ex* arts. 118 CE y 17 LOPJ[663] y de que haya mediado también la

[661] Tal es la versatilidad de los servicios de almacenamiento en nube que podría hablarse, durante la investigación de algunos delitos, por ejemplo, no en la posesión o distribución de contenidos ilícitos, como lo podría ser una imagen o un video de pornografía infantil, sino de determinados de derechos de acceso adquiridos por los investigados sobre un mismo ejemplar ilícito puesto a disposición "en nube" en favor de un determinado número de usuarios que participarían de semejante actividad delictiva. La dificultad de análisis de esta fuente de prueba y su puesta a disposición del juzgador durante el acto de juicio oral es evidente. La pregunta sería ¿En qué parte de la nube está y cómo se obtiene la evidencia digital que, de una forma jurídica segura, sirva a la finalidad del proceso penal?

[662] En este último caso, orientado a superar los obstáculos ocasionados por el uso de las técnicas de codificación en el envío de los paquetes de datos, queda de manifiesto, nuevamente, la inoperancia del art. 33.10 LGT al no alcanzar a los ISP la obligación que sí tienen los operadores ya que, como en dicho precepto se indica, *"en el caso de que los sujetos obligados apliquen a las comunicaciones objeto de interceptación legal algún procedimiento de compresión, cifrado, digitalización o cualquier otro tipo de codificación, deberán entregar aquellas desprovistas de los efectos de tales procedimientos, siempre que sean reversibles"*. Como es sabido, los ISP no son *sujetos obligados* por la LGT.

[663] Artículo 118 CE:

Es obligado cumplir las sentencias y demás resoluciones firmes de los Jueces y Tribunales, así como prestar la colaboración requerida por éstos en el curso del proceso y en la ejecución de lo resuelto.

Artículo 17 LOPJ:

> *1. Todas las personas y entidades públicas y privadas están obligadas a prestar, en la forma que la Ley establezca, la colaboración requerida por los Jueces y Tribunales en el curso del proceso y en la ejecución de lo resuelto, con las excepciones que establezcan la Constitución y las Leyes, y sin perjuicio del resarcimiento de los gastos y del abono de las remuneraciones debidas que procedan conforme a la Ley.*

fortuna de no haberse invocado la ***excusa técnica***[664]***,*** tan socorrida como difícil de eludir.

Otro elemento, inédito en la época de la entrada en vigor del art. 579 LCRIM (y que dará una idea de las dificultades de su aplicación analógica para la intervención de las comunicaciones telemáticas), lo constituye lo que puede denominarse el ***doble secreto***, por el que, además del que de un modo formal protege genéricamente el derecho a la intimidad en las comunicaciones electrónicas, se añade el que introduce el internauta cuando acciona determinados servicios de Internet a través de su nombre de usuario y contraseña, circunstancia que, obviamente, añade un plus de protección a la navegación *web*[665].

Consecuente con todo lo anterior, e intentando que no se resienta el derecho de injerencia del Estado, ni se limiten los derechos fundamentales de forma inaceptable, la tecnología de la investigación criminal ha debido agudizar sus sentidos para poder ofrecer al proceso penal los indicios obtenidos por este medio con absoluta garantía de su autenticidad, veracidad e integridad pero, lamentablemente, con un

---

2. Las Administraciones Públicas, las Autoridades y funcionarios, las corporaciones y todas las entidades públicas y privadas, y los particulares, respetarán y, en su caso, cumplirán las sentencias y las demás resoluciones judiciales que hayan ganado firmeza o sean ejecutables de acuerdo con las Leyes.

[664] Concepto extrajurídico con el que me refiero, según la experiencia, a determinadas actitudes de los operadores ante la recepción de mandatos a poco que la Ley deje algún hueco, respondiendo que: "No tengo lo que me piden", "Es contrario a la Ley por más que lo mande el Juez y no lo haré", "No me obliga la Ley", "Ha habido una avería y se han perdido los datos", "Los datos (nimios) afectan a la intimidad" e, incluso, la muy peregrina justificación de "esto perjudicará a mi cliente" con la que ponen por delante el interés comercial al público incluso en los casos más sangrantes (Las sondas pasivas de Internet, por ejemplo, se instalan cerca del domicilio del investigado, lo que supone una importante limitación operativa, a veces insalvable, y la activación de importantes y costosos recursos de orden técnico y logístico. Suponen también una limitación de la capacidad o pérdida de calidad de los servicios prestados por la línea ADSL en tanto dura la intervención. Esto puede ser intuido por el investigado, lo que compromete la discreción y eficiencia de la medida y es por lo que, las operadoras, con gran sentido comercial, se quejan de que "se perjudica" a su cliente y a la imagen de la propia compañía. Sin embargo, estas intervenciones pueden hacerse en centralita sin los defectos que se han señalado, aunque sin imperativo legal, a lo que suelen negarse las operadoras que no quieren ver a agentes de la PJE en sus instalaciones y menos aún "manipulando" sus dispositivos).

[665] Puede servir el ejemplo de un usuario, cuyas comunicaciones telemáticas son objeto de intervención judicial y, en un momento dado, accede mediante su nombre de usuario y contraseña a su cuenta privada de banca electrónica, realizando determinadas operaciones en las que, incluso, utiliza elementos de seguridad añadidos como, por ejemplo, una tarjeta de coordenadas o un número de tarjeta de crédito para validarlas.
Es evidente el esfuerzo jurídico que ha de realizarse para establecer en estos casos la finalidad de la intervención de Internet, sus objetivos, sus límites, la motivación, etc. (Sobre la formación de la decisión judicial y las especiales medidas de control jurisdiccional, vid. Velasco Núñez, Eloy. ADSL y troyanos…*op.cit.*).

quantum de confianza de los operadores jurídicos más bien raquítico en lo referido a las dudas – muchas veces acríticas - sobre su proporcionalidad y seguridad.

c)Métodos e instrumentos para la intervención de Internet

Para las modalidades próximas a la forma tradicional de intervención de las comunicaciones, en que la aplicación analógica de la normativa parece consolidada, la PJE dispone de lo que se denominan ***sondas pasivas***, que se interponen, bien en un lugar próximo al domicilio del investigado, bien en la centralita de la operadora telefónica que le preste servicios de acceso a Internet[666]. Esta sonda deriva una copia a los ordenadores de la PJE del trasiego de los paquetes de datos inteligibles comunicados o recibidos por el ordenador investigado a través de la red pública de comunicaciones. Más recientemente, la evolución tecnológica de las prestaciones asociadas al SITEL permite su adaptación para este mismo fin en tanto no usen los ISP de determinados protocolos de codificación.

Es necesario añadir que, este tipo de sondas pasivas, como su propio nombre indica, en ningún caso sirven para acceder al contenido material o formal conservado en el ordenador, servidor, *smartphone,* servicio en nube o dispositivo de que se trate y que no haya sido enviado a través de la red.

Pero, para las demás categorías, y siguiendo a VELASCO NÚÑEZ, la sempiterna falta de derecho positivo sobre la intervención de Internet obliga a que se ordene judicialmente mediante *"la posibilidad de la aplicación analógica, que aquí se postula [en su propuesta sobre la instalación de "troyanos"] mientras tanto por remisión a las normas y jurisprudencia que permiten las intervenciones de otras telecomunicaciones electrónicas o magnéticas, sobre la base de la observación de los criterios habilitantes que el Tribunal Supremo y el Constitucional han ido pautando respecto de toda inmisión que afecte al derecho al secreto de las telecomunicaciones regulado en el art. 18. 3 CE, esto es, que se realice siempre bajo control y autorización motivada por la*

[666] Se está hablando, no de los ISP que facilitan al cliente los diversos servicios telemáticos de su interés o de alguno de estos en concreto, sino de la operadora de la red pública de comunicaciones electrónicas que le facilite la conexión al *Protocolo TCP/IP*, esto es, a Internet.

Autoridad judicial, y exclusivamente para los casos relevantes o graves, permitiendo los límites de la temporalidad y la garantía de la defensa"[667,668].

Pero esta opinión positiva de VELASCO sobre las sondas activas no es pacífica pues, otros juristas consultados, se muestran remisos a considerar la posibilidad de intervenir los contenidos obtenidos de la intrusión en el terminal telemático. Las razones las fundan en el hecho de que, en algunos casos, para la intervención de determinados tráficos a través de Internet o para el acceso al contenido conservado en el terminal informático, es necesario dar un paso adelante que permita eludir los protocolos de codificación de las comunicaciones[669] – al no existir obligación jurídica de su depósito a disposición del Estado - mediante la instalación de lo que ha venido en denominarse "troyanos" o ***software de control remoto***[670], lo que no deja de conllevar una sensible intrusión seguida de una modificación del estado original del

[667] Vid. Velasco Núñez, Eloy. ADSL y troyanos…*op.cit.*

[668] Esta labor esencial de ponderación propia del actor jurisdiccional habrá de marcar con exactitud la extensión y límites de la medida ablativa de derechos, no sólo cuando la situación fáctica permita una inequívoca valoración de su proporcionalidad en aplicación de concretas previsiones jurídicas, sino cuando no exista una que permita señalarlos con su mera invocación u ofrezca un margen de discrecionalidad más o menos amplio, debiendo recurrir a la aplicación analógica.
Sería el caso, por ejemplo, de la valoración de la necesidad imperiosa de limitar el derecho al secreto ante el ataque criminal a concretos y valiosos bienes jurídicos, que podría ser resuelta idóneamente mediante la instalación inadvertida de *software de control remoto* en determinados dispositivos técnicos de los sospechosos para acceder a sus contenidos codificados y que fueren de interés para el proceso penal, cuando, a estos fines, no existe en la Ley una serie de normas que precisen cómo ha de ejercerse semejante limitación, tanto en lo propiamente jurídico como en lo técnico.
Evidentemente, la formación del auto judicial motivado que contenga la limitación del derecho al secreto de las comunicaciones, bajo este supuesto de hecho, devendrá un ejercicio de una extrema complejidad técnico-jurídica, precisamente, por exigir que se resuelva sobre cuestiones de proporcionalidad en un ámbito ciertamente complejo, en el que será difícil determinar la carga de intrusión en el derecho a la intimidad y el nivel de garantía jurídica que su materialización supondrá y, consecuentemente, la admisibilidad del sacrificio del derecho al secreto de las comunicaciones que de esta manera se considere prudente adoptar.

[669] Al tiempo de escribir este apartado, la sociedad asiste a una auténtica revolución en la forma de comunicarse a través de las comunicaciones telemáticas, basadas principalmente en *software* de mensajería o *VoIP*, que hacen tambalearse el mercado del envío de voz a través de la telefonía fija o móvil, ya clásicas a estas alturas. Sobre estas nuevas formas de comunicarse debe recaer también el derecho de injerencia del Estado. Algunos ejemplos, con protocolos de codificación o no, son: *Skype, Whatsapp, Viber, ooVoo, Line,* etc., cuya instalación en un *smartphone* es de una extrema sencillez o, también, las populares redes sociales como *Twitter, Tuenti, Facebook, Linkedin,* etc., con centenares de millones de usuarios registrados en todo el mundo con identidad real, supuesta, oculta o sometida a tratamientos informáticos que impiden su trazabilidad.

[670] En palabras de VELASCO, *"este método de investigación oficial se basa en la introducción de software de agente autónomo, previamente programado, que con imitación de las técnicas malware, sólo que esta vez puestas al servicio de la Justicia, busca de forma remota datos y comunicaciones internas en el ordenador del sospechoso, para copiar lo preseleccionado y enviárselo al operador para su análisis incriminatorio".* Vid. Velasco Núñez, Eloy. ADSL y troyanos…*op.cit.*

dispositivo que, aunque inocuas en realidad ambas, suscitan los recelos de los medios jurídicos más proclives al hipergarantismo.

A la ya mencionada ausencia de derecho positivo, se sumarían en este caso las dudas sobre la posible aplicación analógica, por considerar que el procedimiento resultaría altamente invasivo siquiera para ser usado frente a las modalidades delictivas más graves, como sería el caso del terrorismo.

Tiene que ser una vez más la PJE la que, como en demasiadas ocasiones y a falta de una legislación específica, lance un guante que habrá de ser recogido por una Autoridad Judicial que, bajo la más estricta observación del principio de proporcionalidad, motive y resuelva sobre el uso de esta herramienta tecnológica.

Nuevamente, por tanto, se han de considerar dos posibilidades: la intrusión en un terminal para copiar su contenido (abierto o protegido mediante contraseñas) o mediante la instalación de *software de control remoto* (mediante técnicas de ingeniería social[671]).

En el primer caso, se hablaría de un ***registro virtual*** pues, una vez expedito el camino hacia el dispositivo de almacenamiento interno (un disco duro o memoria *flash*, normalmente), nada obstaculizaría el volcado de los datos que contenga.

El problema de la territorialidad, en caso de que el terminal investigado se halle fuera del espacio soberano, es despejado por VELASCO al afirmar que *"el principio de ubicuidad […] formulado por el Acuerdo de la Sala 2ª del TS de 3 de febrero de 2005 ("El delito se comete en todas las jurisdicciones en las que se haya realizado algún elemento del tipo. En consecuencia, el Juez de cualquiera de ellas que primero haya iniciado las actuaciones procesales, será en principio competente para instrucción de la causa"), valida, por razones de competencia judicial para España, las inmisiones y aprehensiones que por meras razones de intermediación tecnológica se hagan desde cualquier punto del territorio español con autorización judicial – y aún sin ella, para casos de extrema urgencia – aunque pasen y se vehiculicen en parte por el territorio de otros Estados, siempre que tengan relación con la investigación de un delito que en*

[671] La ingeniería social supone en este caso la intrusión utilizando técnicas de manipulación del sujeto investigado para que actúe de una determinada forma que permita la instalación en su terminal del *software de agente autónomo*.

todo o en parte despliegue parte de su acción o de sus efectos en el territorio jurídico legal a que se refiere la protección recogida en el art. 23 LOPJ". Y comenta el autor: *"…el mero viaje de ceros y unos por la red internacional, o la transmisión no rectilínea de los mismos, no convierte en propietario del lugar por donde circulan en cable o magnéticamente – wireless – […] el criterio de la ubicación tecnológica del prestador del servicio tampoco otorga exclusiva [...] salvo ne bis in idem"*[672,673].

Otro problema se deduciría del cumplimiento del art. 579 LCRIM en aquellos casos en que no fuera posible contar con la presencia del investigado para el acto del registro, lo que exigiría una especial resolución y control reforzado de la medida por parte del Juez que la dispusiese.

El segundo caso, más problemático, en mi opinión, debiera quedar resuelto por la propia consideración de la labor de la PJE como primera salvaguarda de la pureza de la prueba, unido al uso de medios técnicos de certificación segura y al eficiente control jurisdiccional de la medida.

Siendo así, ninguno de los procedimientos descritos, por intrusivos que parezcan, deben excluirse de un proceso penal que ha de saber servirse de la tecnología para combatir a aquellos – estos sí – que la utilizan para socavar las libertades de los demás, lo que sin duda merece que sus derechos fundamentales, que no son absolutos, queden limitados en lo estrictamente necesario para los legítimos fines de la impartición de Justicia.

[672] Vid. Velasco Núñez, Eloy. *Delitos cometidos a través de Internet…op. cit.,* pág. 123 y ss.

[673] Sobre la cuestión de la *"deslocalización"* de las fuentes de información en Internet, con cita al CCib y al Acto del Consejo de la UE de 29 de mayo de 2000, sobre el *Convenio de Asistencia Judicial en Materia Penal* entre los países miembros, GONZÁLEZ-CUÉLLAR se refiere a la necesidad de reacción de los estados con independencia de la ubicación territorial de la evidencia digital. Vid. González-Cuéllar Serrano, Nicolás. *Garantías constitucionales…op. cit.,* pág. 152.

B. Estudio sobre los DACE

Como alternativa a la expresión "datos de tráfico", comúnmente utilizado en la doctrina, he elegido deliberadamente la expresión "datos asociados a las comunicaciones electrónicas", o su acrónimo DACE, en un intento de conciliar todos aquellos aspectos técnicos distintos del contenido material de las comunicaciones que, por el efecto expansivo de las TIC, produzcan o puedan producir nuevas tipologías cuya categorización responda a un concepto amplio de dato.

He tenido también en consideración que no todos los DACE se vinculan con concretos actos de comunicación, sino que pueden ser también independientes de su materialización al estar alternativamente relacionados con determinadas posibilidades o prestaciones técnicas de los dispositivos y de las redes de comunicaciones electrónicas y que no tienen relación con la comunicación entre personas. Dentro de los que sí se hayan generado durante un acto de comunicación personal, será necesario distinguir con nitidez también su vinculación temporal, según se relacionen con una comunicación en curso o ya finalizada[674].

La legislación de conservación de datos, como parte de las disposiciones generales relacionadas con la intervención legal de las comunicaciones, se orienta exclusivamente, con toda evidencia, a contribuir a la seguridad pública y a servir con éxito al proceso penal. Para lograr estos propósitos, busca instaurar, con vocación de permanencia, un *quantum* de eficiencia - dentro de los estándares democráticos de la legislación europea y nacional -, y sea cual fuere el estado de desarrollo actual o futuro de las TIC. De esta situación, se deduce la exigencia de lograr una adaptabilidad atemporal de la legislación a las necesidades que puedan emerger de la realidad social.

Esta visión utilitaria de los DACE, con sus correspondientes e innegables efectos jurídicos, no tiene otro fin, por tanto, que la de sistematizar las categorías de datos que puedan interesar al proceso penal, ahora o el futuro, de modo que el contenido formal de las comunicaciones electrónicas sea suficientemente conocido y razonablemente

[674] Vid. Pérez Gil, Julio. *El nuevo papel de la telefónia móvil…op. cit.*, pág. 197 y ss y González López, Juan José. *Los datos de tráfico…op.cit.,* pág. 63 y ss.

incorporado al proceso de contradicción y valoración de la evidencia digital, teniendo en cuenta además el principio de proporcionalidad.

Deben entenderse proscritas, si no se acompañan con decisiones complementarias precisas, las fórmulas abiertas para describir categorías genéricas de datos a conservar pues, semejante indeterminación, desdibujaría la moderación que debe presidir la imposición de determinadas obligaciones a los ciudadanos – que además son tan intrusivas como la que se está describiendo -, lo que conlleva *a priori* asociada la imposición a los sujetos obligados de gravosas cargas de orden logístico para materializar el derecho de acceso del Estado a los DACE conservados[675,676]. Por ello, es de exigir que se diga con precisión en la Ley cuáles de ellos son objeto de su interés y cómo y en qué condiciones deberán ser conservados y accedidos.

En este sentido, la LCDCE, como legislación transpuesta en España de la DCD, pese a los defectos que se dirán, debe considerarse un cuerpo legislativo de referencia – apto por su calidad, en cualquier caso, para acoger reformas adecuadamente estructuradas sin necesidad de introducir cambios radicales - porque, a mi juicio, cumple con los mínimos estándares de eficiencia indispensables para regular la conservación de los DACE.

Esta apreciación se debe, entre otras cosas, a que categoriza en su art. 3.1 una amplia - pero ajustada y precisa - lista de los DACE específicos que tienen utilidad directa para analizar con suficiencia el contenido formal de las comunicaciones,

---

[675] En palabras de PÉREZ SÁNCHEZ, sobre el análisis de la LCDCE, *"la transposición de la Directiva 2006/24/CE está suponiendo un gran reto de adaptación organizativo y técnico a los Operadores de Telecomunicaciones y los Proveedores de Internet en nuestro país…la implantación de las medidas necesarias, está provocando muchas dificultades técnicas, muy complejas y costosas…a un sector que, por otro lado, se le pide que sea el motor de la Sociedad de la Información, invirtiendo en infraestructuras y en nuevas tecnologías y que genera riqueza externa, pero que sin embargo sufre una gran carga fiscal…"*. No obstante, el art. 14.1 DCD contiene previsiones para la revisión de la posición de los operadores a estos efectos. Vid. Pérez Sánchez, Martín. *Posición del sector de telecomunicaciones ante la nueva regulación de protección de datos: Retos y dudas*. [ed.] Agencia Española de Protección de Datos. *La protección de datos en la cooperación policial y judicial.* Madrid: Aranzadi S.A., 2008, págs. 125-132.

[676] Vid. *Informe de evaluación sobre la Directiva de conservación...doc. cit., p*to. 6. En la conclusión introducida en el punto 8.3 de este documento, reconociendo una "*falta de seguridad jurídica para el sector"*, crípticamente se anuncia que *"la Comisión estudiará maneras de proporcionar un reembolso homogéneo a los operadores"*. En mi opinión, el Estado debería asumir íntegramente las cargas de la conservación de datos. De ser así, se proporcionaría además la debida seguridad jurídica para una función que excede al interés comercial de las operadoras. Esto supondría, en términos prácticos de cumplimiento de la Ley, un mayor rendimiento general de este recurso en relación con la satisfacción real de las necesidades de investigación en cuya virtud fue preparado.

siempre, eso sí, que se verifiquen en el ámbito de los operadores del mercado de las telecomunicaciones y a través de las redes púbicas de comunicaciones electrónicas (ya que los DACE de los ISP, por el momento, quedan incomprensiblemente a extramuros de la LCDCE al no ser considerados sujetos obligados *ex* art. 2 LCDCE).

La cuestión es, con carácter general, comprobar en la Ley si están contemplados todos los datos necesarios y si están todos los sujetos obligados que demanda el proceso penal.

Por ello, partiendo de un concepto general que acoja lo que debe entenderse por DACE desde un punto de vista jurídico, se deberá llegar a precisar también qué categorías técnicas concretas son las que interesa conservar, todo ello bajo unas estrictas previsiones que garanticen la debida seguridad jurídica.

1. Generalidades sobre los DACE

Definir qué son los datos de tráfico no es sencillo si se tienen en cuenta los continuos progresos de las TIC y la experiencia criminológica concomitante, lo que configura un panorama de intervención para el Derecho ciertamente singular y complejo, en el que debe actuar atendiendo a las necesidades que impone la realidad social.

En este sentido, y siguiendo a GONZÁLEZ LÓPEZ, puede tenerse la tentación de optar por una definición abierta (*"… los datos de tráfico son definidos, tomando como punto de partida el proceso de comunicación, por oposición a los datos pertenecientes al contenido (material)"*)[677] – lo que el autor define como la ***conceptuación por exclusión*** – heredera de las primarias e incompletas percepciones de los DACE valoradas en la STEDH del Caso *Malone*[678] o, incluso, las de la FGE sobre la materia[679],

[677] Sobre la conceptuación de los datos de tráfico, vid. González López, Juan José. *Los datos de tráfico…op.cit.,* pág. 49 y ss.

[678] Con el correspondiente y decidido apoyo en la consolidada jurisprudencia posterior en la STC 114/1984, de 29 de noviembre (FJ 7) (luego reproducida en otras muchas a partir de la STC 70/2002, de 3 de abril (FJ 9)) en que se declara, siguiendo el criterio ya apuntado del TEDH, que "*el concepto de «secreto», que aparece en el art. 18.3, no cubre sólo el contenido de la comunicación, sino también, en*

que suponen *a priori*, en mi opinión, un rechazable y primario concepto de su realidad e, incluso, de su utilidad en términos de seguridad jurídica del proceso penal.

En el extremo opuesto, puede contemplarse una ***caracterización exhaustiva***, lo que supone de inmediato el recurso a los listados de los DACE que, en un momento dado, puedan identificarse como valiosos para la investigación penal.

Sobre las aportaciones de esta última visión de tan citado autor, interesan los conceptos asociados que se incluyen en el siguiente texto:

> *"Como notas características utilizadas y categorías incluidas pueden distinguirse las de "**externalidad**" (con las categorías de identidad subjetiva de los interlocutores, momento, duración y destino); **"dependencia temporal**" y "**funcional**" (datos indicativos del origen, destino, ruta, tiempo, fecha, volumen, duración o tipo de servicio subyacente), y "**rastreo**" de la comunicación ("huellas informáticas" de las comunicaciones telemáticas y datos de localización de la telefonía móvil)"* [680,681].

La opción por la caracterización exhaustiva, con descripciones muy precisas sobre lo que debe tenerse por dato de tráfico o dato informático, como señala el autor, se ve materializada en el CCib con una amplia influencia en el derecho positivo posterior y para cuyo análisis he de remitirme a un apartado específico incluido más adelante[682].

---

su caso, otros aspectos de la misma, como, por ejemplo, la identidad subjetiva de los interlocutores o de los corresponsales".

[679] En la Consulta 1/1999 a la FGE, de 22 de enero, esta distingue el "*contenido intelectual*" de la comunicación y *"unos datos relativos al proceso mismo de comunicación que sin formar parte del contenido intelectual son indisociables de la realidad misma de la comunicación".* Nótese que la carga de indefinición que aporta haría muy difícil precisar cuáles son los que, en un momento dado, interesan al proceso penal, virtud que se logra con la posterior transposición en la LCDCE, donde con bastante precisión se señalan las categorías de datos en el art. 3.1.

[680] Según anota el autor, esta visión se apoya en las SSTC 123/2002, de 20 de mayo (FFJJ 4 y 5), y 56/2003, de 24 de marzo (FJ 2). Vid. González López, Juan José. *Los datos de tráfico…op.cit.,* pág. 52 y ss.

[681] Sobre la dependencia temporal y funcional, vid. Hernández Guerrero, Francisco. *La intervención…op. cit.,* pág. 350.

[682] El CCib se centra, no obstante, en el uso de la informática como medio instrumental de las comunicaciones electrónicas – y, en mi opinión, indiferenciado -, criterio que no se ha tenido en cuenta en la DCD ni, evidentemente, en la LCDCE, que sólo regulan lo concerniente a los datos relacionados con la telefonía fija o móvil y, muy pobremente, el acceso a Internet a través de las redes públicas de comunicaciones. Esta anómalo y excluyente punto de vista es muy sugerente de la necesidad de dar un enfoque global de las comunicaciones electrónicas que integren todos los aspectos que les sean afines.

Un tercer criterio, al que me adhiero sin dejar de apreciar la seguridad jurídica que ofrecen los listados de datos, sería el de la ***caracterización no exhaustiva***, que permitiría que *"los eventuales datos que se ajusten a dicha característica pasen a integrarse en la categoría de "datos de tráfico", aun cuando en algunos supuestos se lleve a cabo una enunciación no exhaustiva de las categorías de datos de tráfico que se distinguen"* [683].

Este criterio se encuentra representado también en la definición aportada por RODRÍGUEZ LAINZ, para quien son datos de tráfico "a*quellos datos e informaciones que circulan por las redes de telecomunicaciones o de comunicaciones electrónicas, conjuntamente con éstas, y que facilitan información sobre el origen, el destino, la localización, el itinerario, la hora, la fecha, el volumen y la duración de la comunicación, el tipo de servicio subyacente o cualesquiera otros datos o servicios accesorios que sirvan a finalidades similares a las anteriormente descritas, siempre que no constituyan el contenido mismo o parte del contenido de la comunicación*"[684,685].

Estos puntos de vista jurídicos sobre los DACE, por razones de orden práctico y utilitario, basadas, al fin, en la experiencia proporcionada por los años de vigencia de la LCDCE, sugieren, en mi opinión, la necesidad de optar por una definición de corte generalista no exhaustiva, que permita la adopción dinámica de decisiones del legislador para incorporar, en vía reglamentaria, nuevas categorías técnicas específicas de DACE que en cada momento resulten jurídicamente procedentes[686], sean o no de tráfico y distintas, naturalmente, del contenido material de la comunicación, pero que se vinculen con cualquiera de los aspectos relacionados con las comunicaciones electrónicas como fenómeno inherente a la realidad social de las TIC, aún emergente.

---

[683] GONZÁLEZ LÓPEZ pone como ejemplo de esta caracterización la expresada en el artículo 2 b) de la Directiva 2002/58/CE, según el cual es dato de tráfico "*cualquier dato tratado a efectos de la conducción de una comunicación a través de una red de comunicaciones electrónicas o a efectos de facturación de las mismas*". Vid. González López, Juan José. *Los datos de tráfico…op.cit.,* pág. 57 y ss.

[684] Vid. Rodríguez Lainz, José Luis. *La intervención de las comunicaciones telefónicas.* Barcelona: Bosch S.A., 2002, págs. 31 y 32.

[685] En este sentido, con referencia a los conceptos de la Directiva 2002/58/CE, vid. González-Cuéllar Serrano, Nicolás. *Garantías constitucionales…op. cit.,* pág. 171.

[686] Esta posibilidad de remisión al desarrollo reglamentario queda abierta por lo dispuesto en el art. 33 LGT, apdos. 5 y 6, (modificado en la Disposición Final Primera, apdo. Uno, de la LCDCE), donde se dice con la misma redacción que "*los sujetos obligados deberán facilitar al agente facultado, salvo que por las características del servicio no estén a su disposición y sin perjuicio de otros datos que puedan ser establecidos mediante Real Decreto[…]".*

Puede decirse a estos efectos que, aunque sea desde un punto de vista teórico, no todos los datos relacionados con las comunicaciones electrónicas tienen por qué ser automáticamente deudores de la protección del secreto de las comunicaciones, tal y como lo zanja la LCDCE[687,688], sino que estos datos, que interesan a la investigación penal, pueden acogerse bajo una definición amplia que no requiera de este específico modo de protección jurídica en todos los casos.

La finalidad de esta propuesta debería servir, en este caso, para alimentar la necesidad de conservación de datos más allá, incluso, de su utilidad accesoria o funcional para facilitar el proceso de la comunicación[689].

Es evidente que una definición de este tipo – que acoge la denominación planteada de "datos asociados a las comunicaciones electrónicas" -, debe ser de tal calidad que deje conjuradas las tachas de inseguridad jurídica que se deduzcan de la falta de precisión de la Ley.

El concepto de DACE, en mi percepción más amplio que el de los meros datos de tráfico contemplados en la LCDCE, dentro de una legislación claramente orientada a proporcionar efectividad a la perseguibilidad penal de los delitos, puede partir de la definición sobre lo que es un *"dato de tráfico"* a la luz del art. 2b de la Directiva 2002/58/CE[690], que es *"cualquier dato tratado a efectos de la conducción de una comunicación a través de una red de comunicaciones electrónicas o a efectos de la facturación de la misma"*, sistematización que, ampliada al cada vez más extenso mundo de las comunicaciones electrónicas, podría acoger la siguiente propuesta de definición:

[687] Vid. SSTS 316/2000 de marzo; 1235/2002 de 27 de junio y 1086/2003, de 25 Julio, sobre el acceso a los datos de la agenda de los teléfonos móviles y SSTS 249/2008, de 20 de mayo; 777/2008, de 18 de noviembre; 40/2009, de 28 de enero; 688/2009, de 18 de junio y 737/2009, de 6 de julio, sobre la determinación del IMSI mediante el análisis del espacio radioeléctrico.

[688] Sobre el valor de que se haga derecho positivo allí donde hubo confusión de derechos, vid. Fernández de Palma, Rosa. *Análisis de la Ley 25/2007…op. cit.,* pág. 176.

[689] En este último sentido se pronuncia el autor al afirmar *que "en el curso de una comunicación pueden ser tratados múltiples tipos de datos que no responden a la finalidad de hacer posible la comunicación y que, sin embargo, deben reputarse tales, por exceder de lo que cabe entender por contenido material de la comunicación"*. Vid. González López, Juan José. *Los datos de tráfico…op.cit.,* pág. 62.

[690] Bien entendido que esta directiva, *ex* art. 3.1, sólo se aplica a los *"servicios de comunicaciones electrónicas disponibles al público en las redes públicas de comunicaciones"*, lo que exigiría una sensible revisión de la legislación europea para acoger las propuestas que se plantean en este estudio.

*"Se entenderá por **datos asociados a las comunicaciones electrónicas*** (DACE) *aquellos datos, distintos del contenido material del mensaje transmitido, que sean o hayan sido tratados a efectos de la conducción de una comunicación prestada a través de una red de comunicaciones electrónicas por un servicio de comunicaciones electrónicas o como parte de la prestación de un servicio telemático de la sociedad de la información, incluidos los servicios de valor añadido, así como los demás datos afines relativos a la suscripción de cualquiera de estos servicios y los demás producidos por cualquier dispositivo técnico apto para mantener una comunicación electrónica, aún cuando no se vinculen a una comunicación concreta".*

GONZÁLEZ LÓPEZ, por su parte, ante la insuficiencia del criterio vinculado a la dependencia funcional, define como ***datos de tráfico*** los que *"…se generan o tratan en el curso de una comunicación y que difieren del contenido material, entendiendo por tal aquella información cuya transmisión voluntaria por el emisor al receptor motiva la comunicación"*[691]. Definición que el autor en su propuesta – algo parco a la hora de aportar carga semántica a los términos *comunicación* e *información* - acompaña de notas que sugieren una distinta perspectiva constitucional relacionada con el carácter accesorio[692] de tales datos y su temporalidad, pues pueden venir referidos a comunicaciones en curso o ya finalizadas.

De esta percepción, merece destacarse la cuestión de la dependencia temporal de los datos de tráfico, que, en palabras del autor, *"aparece en la referencia al "curso de una comunicación". Es la aparición de estos datos en el proceso de comunicación lo que les otorga su nombre y justifica su pertenencia a este concepto, incluso una vez concluido el mismo. Esto se debe a que, aunque ciertos datos, eventualmente de tráfico*

[691] Vid. González López, Juan José. *Los datos de tráfico…op.cit.,* pág. 62.

[692] Sobre la adjetivación de accesoriedad, muy interesante por su trascendencia jurídico-constitucional, GONZÁLEZ LÓPEZ dice que *"la diferencia entre el contenido material y formal de la comunicación radica en el componente volitivo-teleológico de la comunicación. El proceso de comunicación obedece al propósito por parte del emisor de transmitir una determinada información al receptor, constituyendo éste el contenido material de la comunicación. El resto de datos, ya sean los necesarios para hacer posible la comunicación u otras informaciones que sean tratadas como parte de ésta, constituirá un elemento accesorio de este contenido, que es el que justifica la finalidad primordial de la comunicación: la transmisión de información del transmisor al receptor"*. Propuesta que, sin duda, hace recaer la acción de comunicar en sus aspectos más humanos y, desde luego, distintos de los técnicos, apreciación sobre la que habrá de volverse más adelante. Vid. González López, Juan José. *Los datos de tráfico…op.cit.,* págs. 62 y ss.

(como los de localización geográfica), pueden existir al margen de la comunicación en curso (de ahí que no resistan su inclusión bajo un criterio fundado en la dependencia funcional) es su presencia accesoria a la comunicación lo que los hermana con los datos indubitadamente de tráfico, de modo que, con independencia de que la protección constitucional varíe en función de la actualidad o finalización del proceso de comunicación, pasan a formar parte de una misma categoría de datos, la de los integrantes del contenido formal de la comunicación". Debe repararse, por tanto, en el pronunciamiento final que contiene este fragmento sobre los distintos niveles de protección constitucional que merecen los datos según se vinculen a actos contemporáneos o diferidos de comunicación.

Finalmente, GONZÁLEZ LÓPEZ propone tres nuevos enfoques que permiten una clasificación según la naturaleza de los datos[693]: En primer lugar, los ***datos indubitadamente de tráfico,*** o datos de tráfico en sentido estricto, cuya nota característica es su dependencia funcional del acto de comunicación; En segundo lugar, los ***datos eventualmente de tráfico,*** que serían los que *"sólo ocasionalmente podrán calificarse de datos de tráfico, ya sea porque no siempre aparecen vinculados a la comunicación (datos de localización o de "servicios de valor añadido") o porque se trata de conceptos más amplios que el de datos de tráfico…[porque] se trata de informaciones susceptibles de gozar de existencia al margen de la comunicación o que, incluso, pueden integrar el contenido material de la misma"* y, en tercer lugar, los ***datos afines,*** como categoría ajena a los datos de tráfico, como lo son los datos de suscripción y cualquier otro que, sin ser parte de las comunicaciones electrónicas, mantenga algún vínculo con estas que pueda resultar del interés del proceso penal[694].

Será sobre estos conceptos sobre los que gravitará a su vez el enfoque práctico que pretende darse a los datos asociados a las comunicaciones electrónicas y que se planteará en los párrafos que se insertan a continuación.

[693] Vid. González López, Juan José. *Los datos de tráfico…op.cit.,* págs. 63-74.
[694] Estos datos quedan fuera de la protección del art. 18.3 CE. Vid. González-Cuéllar Serrano, Nicolás. *Garantías constitucionales…op. cit.,* pág. 173.

2. La naturaleza de las comunicaciones electrónicas. Propuestas de definición.

Sobre los aspectos de las comunicaciones ajenos a su contenido material, esto es, sobre su contenido formal, cabe hacer algunas consideraciones más precisas – con las consecuencias jurídicas y de toda índole que se tratará de determinar -, distinguiendo entre:

- ***Datos personales asociados a una comunicación electrónica en curso***, como pueden ser los IMSI e IMEI, los datos de tráfico de llamadas entrantes, salientes o intentadas, los números de abonado o las identidades de los suscriptores de los servicios, los datos de la IP de acceso a la red pública de comunicaciones, los datos de tráfico interno o *logs* de los ISP y de los servicios subyacentes, los datos de enrutamiento, la dirección ***MAC***[695] del equipo informático, etc., en tanto sean producidos en el curso temporal de una comunicación.
- ***Datos asociados a la mera cobertura de red*** o de puesta a disposición de la red a los dispositivos de comunicaciones electrónicas para su eventual conducción técnica, tales como los datos no personales referidos a las BTS en la que se registren temporalmente los dispositivos (la geolocalización de los postes de antenas, la identificación de celdas y, de estas, su inclinación, orientación, zona geográfica de cobertura, apertura, potencia, alcance, etc.) o los datos personales de registro temporal de tarjetas SIM a determinadas BTS, con referencia a su IMSI, el IMEI o, fuera del concepto de dato técnico, la identidad de los suscriptores.
- ***Datos asociados a las comunicaciones electrónicas ya realizadas***, que serían los que conservasen las operadoras de telecomunicaciones y los ISP

[695] Acrónimo del inglés *media access control* o control de acceso al dispositivo, que es un código alfanumérico de 48 *bits* (o 6 bloques hexadecimales) que identifica una tarjeta o dispositivo de conexión a red (Por ejemplo, la tarjeta wi-fi de un ordenador portátil corriente, que se usa para conectar el dispositivo a Internet). No obstante, es necesario aclarar que el potencial individualizador de la dirección MAC es circunstancial, pues los usuarios pueden de una forma relativamente sencilla modificar su configuración alfanumérica mediante la técnica conocida como *mac spoofing.* A pesar de ello, el MAC no deja de tener un importante valor para la investigación policial pues, con modificación o sin ella, su significado indiciario e incluso probatorio puede llegar a ser muy alto.

sobre comunicaciones ya finalizadas y, en su caso, los ***datos conservados de cobertura de red***[696]**.**

Por lo anterior, urge realizar una precisión jurídica que sirva para diferenciar entre sí los conceptos de *acto de comunicación* y *acto de cobertura*[697], cuya naturaleza material es netamente distinta y, consecuentemente, su relevancia en relación con su afectación al contenido esencial del derecho a la intimidad es, en mi opinión, también inequívocamente diferente, dependiendo además de que se refieran a comunicaciones en curso o a comunicaciones ya finalizadas.

Buscando un contenido o definición que responda a tales actos, con la única finalidad de facilitar la comprensión de las explicaciones que en adelante se incluyan e ir recogiendo al mismo tiempo algunas de las aportaciones de los diversos autores estudiados, pueden proponerse los siguientes:

- ***Acto de comunicación electrónica****: "Aquel por el cual se produce una transmisión de voz o datos de cualquier clase en canal cerrado entre un número finito de personas*[698] *e iniciado por cualquiera de ellas, por el que se dan a conocer sus pensamientos, ideas, sentimientos, etc., con independencia de su carácter íntimo o reservado y llevado a cabo mediante el uso de un dispositivo tecnológico apto para mantenerlo".*
- ***Acto de cobertura****: "Acto por el cual un dispositivo tecnológico apto para mantener una comunicación electrónica completa y con independencia de su realización, establece un enlace técnico permanente o temporal con otro dispositivo técnico de igual o distinta naturaleza y destinado a garantizar, llegado el caso, un acto de comunicación de cualquier clase".*

[696] Los datos de cobertura no son objeto de conservación según la LCDCE. No obstante, una interpretación del considerando 23 de la DCD permitiría disponer su conservación, pues se dice en él que "*la Directiva exige que se conserven exclusivamente los datos generados o tratados en el proceso del suministro de servicios de comunicación",* lo que no ofrece dudas al respecto, ya que no existiría comunicación si no se pusiese la red pública de comunicaciones a disposición de los usuarios a través de las correspondientes antenas BTS.

[697] La precisa terminología empleada para enunciar los conceptos jurídicos que contienen hay que atribuirla al Fiscal FRANCISCO HERNÁNDEZ GUERRERO y comentada en entrevista con el autor mantenida el 22 de noviembre de 2011, en la que ambos coincidimos en idénticos conceptos.

[698] De lo definido, aunque sea de una forma tácita, se excluye todo lo relativo a las comunicaciones en las que uno de los interlocutores sea una máquina, materia que se tratará más adelante con mayor profundidad.

Dentro de los *actos de cobertura* deben distinguirse aún dos subcategorías en razón del momento en que se producen:

- ***Actos de cobertura durante el acto de comunicación.***
- ***Actos de cobertura fuera del acto de comunicación***[699].

Debe hacerse una salvedad o aclaración en lo referido al concepto de comunicación electrónica, según la semántica de la definición aportada, ya que, como es de ver, se centra en las comunicaciones personales. En consecuencia, quedan excluidos de la definición los que denominaré ***actos de comunicación técnica***, que serán los que tengan por objetivo *"la transmisión de un mensaje cuyo contenido consista en el envío de paquetes de datos de naturaleza técnica, orientado a la ejecución de determinadas órdenes telemáticas que se basen, a su vez, bien en las prestaciones del propio dispositivo de comunicaciones*[700]*, bien en la ejecución de programas informáticos o software de cualquier clase*[701]*. A estos efectos, será imprescindible que el emisor o el receptor del mensaje, o ambos indistintamente, sean un dispositivo apto para mantener una comunicación electrónica".*

Sobre esta modalidad, dice GONZÁLEZ LÓPEZ que:

> *"La clarificación de esta conclusión exige rechazar con carácter previo que las comunicaciones "técnicas" que conlleva el tratamiento de este tipo de información constituyan comunicaciones comprendidas en el ámbito de aplicación del artículo 18.3 CE*[702]*. Ya se trate de la conexión a Internet, de los "datos de cobertura" o de la IMSI, lo cierto es que este tipo de transferencias de*

[699] Los datos de localización fuera del acto de comunicación, según GONZÁLEZ-CUÉLLAR, son protegibles de acuerdo con el art. 18.4 CE y no por el 18.3 CE, cuestión está central para buena parte de los razonamientos que formarán parte de este estudio, pues motivará una reflexión sobre las diferentes categorías de DACE a la luz de su materialización en un acto de cobertura producido fuera de un acto de comunicación. Vid. González-Cuéllar Serrano, Nicolás. *Garantías constitucionales…op. cit.,* pág. 152.

[700] Por ejemplo, generar una descarga eléctrica en un TMA que actúa como receptor, de forma que sirva de iniciación de una carga explosiva.

[701] Por ejemplo, dar una orden telemática viral para instalar indiscriminadamente *software* de DoS en miles o millones de terminales no protegidos.

[702] Aclara el autor que *"debemos rechazar que el envío de la IMSI del terminal al operador sea comunicación a efectos del 18.3 CE, pues, como afirma la STC 281/2006, de 9 de octubre, "las comunicaciones comprendidas en este derecho han de ser aquellas indisolublemente unidas por naturaleza a la persona, a la propia condición humana; por tanto, la comunicación es a efectos constitucionales el proceso de transmisión de expresiones de sentido a través de cualquier conjunto de sonidos, señales o signos" y que "la comunicación es un proceso de transmisión de mensajes entre personas determinadas"".*

información no tiene otro propósito que permitir las comunicaciones interpersonales[703]*. Precisamente por ello se trata de un tipo de intercambio de información, de comunicación, que no siempre aparece en el marco de comunicaciones en curso, es decir, que sólo eventualmente adquiere el carácter de "datos de tráfico"*[704].

Como puede deducirse de la mera lectura de las anteriores observaciones, la pretensión no es otra que la de distinguir qué actos serían merecedores de la más alta protección de acuerdo con el art. 18.3 CE y qué otros lo serían únicamente bajo el régimen general de protección de datos establecidos en el art. 18.1 CE o el 18.4 CE, asunto este trascendental para la fortuna de las propuestas jurídicas y prácticas contenidas en este estudio, orientadas a mejorar las capacidades operativas de la PJE dentro del proceso penal[705].

[703] Sobre esta cuestión, afirma el autor que *"aún más clara resulta la exclusión en el caso de la orientación vía GPS, que, como se señala en Rodríguez Lainz, J. L. "SITEL y principio de proporcionalidad en la intervención de comunicaciones electrónicas", Diario La Ley, n.º 7689, 7 de septiembre de 2011,* pág. *4, "en sí misma no puede considerarse comunicación, toda vez que no se vale de un servicio de comunicaciones electrónicas disponible al público para la transmisión de información""*.

[704] Vid. González López, Juan José. *Intervención de las comunicaciones: nuevos desafíos, nuevos límites,* en *El Proceso Penal en la Sociedad de la Información. Las nuevas tecnologías para investigar y probar el delito*. Coordinador: Pérez Gil, Julio. VVAA. Ed. La Ley. 2012, págs. 109-172, pág. 122.

[705] Como apunta GONZÁLEZ LÓPEZ, *"así se mantiene en la STC123/2002, de 20 de mayo. En el mismo sentido, en la Memoria Explicativa del CCib (apartado 29) se señala que "la recogida de estos datos [los de tráfico] se estima en principio menos intrusiva, desde el momento en que no revela el contenido de la comunicación, que se estima más sensible". Igualmente, en Italia la doctrina y jurisprudencia atribuyen un mayor grado lesivo de la privacy a la interceptación ("intercettazioni"), frente al acceso a los listados de datos ("tabulati"), como se advierte en la sentenza della Corte Costituzionale italiana n.281 di 1998 (4) y en Camon, A. L'acquisizione dei dati sul traffico elle comunicazioni". Rivista italiana di Diritto e Procedura Penale, Fasc. 2. Aprile-Giugno 2005,* págs. *594-650,* pág. *644. No es, sin embargo, una posición pacífica. Acerca de los argumentos que nos inclinan a diferenciar la intensidad de una y otra injerencia, GONZÁLEZ LÓPEZ, JUAN JOSÉ, Los datos…, op.cit., p.166 y ss"*. Vid. González López, Juan José. *Intervención de las comunicaciones: nuevos desafíos…op. cit.,* pág. 155.

C. Análisis jurisprudencial sobre los DACE

1. Posición doctrinal dominante sobre el secreto de las comunicaciones

a) Los permanentes efectos de la Doctrina Malone del TEDH

La posición jurisprudencial dominante sobre el alcance del derecho a la protección del secreto de las comunicaciones, una de cuyas más estrictas visiones se contiene en la STC 114/1984, de 29 de noviembre, se resume en el siguiente y garantista pronunciamiento del Tribunal Constitucional, que alcanza hasta los elementos más nimios e incluso meramente técnicos del proceso de la comunicación, como lo son los datos de tráfico almacenados[706], y que sería reflejo, de un lado, de la ausencia de modulaciones en el férreo blindaje constitucional del derecho al secreto de las comunicaciones y, en mi opinión, su confusión con el derecho a la protección de datos y, de otro, de la imposibilidad de prosperar la pretensión de introducir modificación alguna en su percepción jurídica:

> *"Este Tribunal [el TC] sí ha elaborado una doctrina, ya muy consolidada, sobre el derecho al secreto de las comunicaciones telefónicas del art. 18.3 CE. Así, a modo de resumen en la citada STC 123/2002, de 20 de mayo, FJ 5, recordamos: «hemos dicho, con palabras de la STC 114/1984, que el derecho al secreto de las comunicaciones (art. 18.3 CE) protege implícitamente la libertad de las comunicaciones y, además, de modo expreso, su secreto. De manera que la protección constitucional se proyecta sobre el proceso de comunicación mismo cualquiera que sea la técnica de transmisión utilizada (STC 70/2002) y con independencia de que el contenido del mensaje transmitido o intentado transmitir -conversaciones, informaciones, datos, imágenes, votos, etc.-*

[706] De esta posición participa GONZÁLEZ-CUÉLLAR, quien afirma que *"en general está salvaguardado por el art. 18.3 CE cualquier dato "externo" o de "tráfico" que el prestador de servicio conserve, con independencia de la razón por la que lo haga"*. Vid. González-Cuéllar Serrano, Nicolás. *Garantías constitucionales…op. cit.,* pág. 173.

pertenezca o no al ámbito de lo personal, lo íntimo o lo reservado (STC 114/1984). El derecho al secreto de las comunicaciones protege a los comunicantes frente a cualquier forma de interceptación o captación del proceso de comunicación por terceros ajenos, sean sujetos públicos o privados (STC 114/1984)»".

Para la exégesis de este inequívoco pronunciamiento, puede tenerse la tentación de considerarlo únicamente referido al "*contenido del mensaje"*, sea cual fuere su naturaleza, incluidas - en mi opinión extemporáneamente - las comunicaciones no personales, y no a sus aspectos de conducción técnica. Pero la frase final, pese a su oscura redacción ("*El derecho al secreto de las comunicaciones protege a los comunicantes frente a cualquier forma de interceptación o captación del proceso de comunicación por terceros ajenos, sean sujetos públicos o privados")* permite colegir la excepcional protección universal e inclusiva de todos los aspectos relacionados con "el proceso" de la comunicación, que alcanzaría, tanto a las comunicaciones no personales, como a la protección de datos, aún en el caso de que se refiriesen a comunicaciones ya finalizadas[707].

Esta percepción jurídica queda rígida e indisolublemente anclada a la caracterización que de los DACE se instituyó en 1984 a través de la STEDH, de 2 agosto, sobre el *Caso Malone,* y que otorgó idéntica protección al contenido material que al formal, doctrina que se recogió de modo diáfano en la inmediatamente posterior y trascendental STC 114/1984, de 29 de noviembre, al admitirse que:

"Puede también decirse que el concepto de «secreto», que aparece en el artículo 18.3, no cubre sólo el contenido de la comunicación, sino también, en su caso, otros aspectos de la misma, como, por ejemplo, la identidad subjetiva de los interlocutores o de los corresponsales. La muy reciente Sentencia del Tribunal Europeo de Derechos del Hombre de 2 de agosto de 1984 -caso Malone- reconoce expresamente la posibilidad de que el art. 8 de la Convención pueda resultar violado por el empleo de un artificio técnico que, como el llamado comptage, permite registrar cuáles hayan sido los número telefónicos

[707] Y, por si esto no fuera suficiente, llegó en 2007 la LCDCE para dejar claro que los DACE son materia de la misma protección que el contenido de las comunicaciones.

marcados sobre un determinado aparato, aunque no el contenido de la comunicación misma".

Es decir, que la determinación de un número de abonado por el contaje (del francés *comptage*) de los pulsos eléctricos de las comunicaciones analógicas de aquellos tiempos y que hoy se pueden antojar primitivas, dicho de manera por el momento muy básica, merecía la misma protección que el contenido material de la comunicación a la que se asociasen.

Sin embargo, frente a esta postura, es necesario recordar cuánto ha evolucionado la tecnología de las comunicaciones de la era de Internet y de la telefonía móvil y sus DACE, lo que debe conducir a intento de comprender cómo ha variado – o cuánto debiera variar - la posición o percepción de los operadores jurídicos dentro del proceso penal en materia del ejercicio del derecho del Estado a la injerencia en el secreto de las comunicaciones o en el derecho a la protección de datos, según proceda jurídicamente, ya que, como se reconoce en la STS 249/2008, de 20 de mayo, en referencia al uso por la PJE del *IMSI Catcher*,

> *"…todo apunta a que la mecánica importación del régimen jurídico de aquellos datos a estos otros, puede conducir a un verdadero desenfoque del problema, incluyendo en el ámbito de la protección constitucional del derecho al secreto de las comunicaciones datos que merecen un tratamiento jurídico diferenciado, en la medida en que formarían parte, en su caso, del derecho a la protección de datos o, con la terminología de algún sector doctrinal, del derecho a la autodeterminación informativa (art. 18.4 CE)".*

Es sobre esta cuestión y sus tensiones, que considero nucleares, en torno a las que girarán buena parte de las propuestas que se contienen en este trabajo[708].

[708] Tarea de difícil abordaje pues, muy en contra de lo pretendido, el TC ha proclamado con meridiana claridad, en línea con lo ya aportado, que *"el ámbito de protección de este medio de comunicación - la telefonía - no tiene limitaciones derivadas de los diferentes sistemas técnicos que puedan emplearse. No sólo la primitiva telefonía por hilos sino también las modernas formas de interconexión por satélite o cualquier otra señal de comunicación a través de las ondas se encuentran bajo la tutela judicial" (STS 137/1999, de 8 de febrero).* Con idéntica visión, la STS 130/2007, de 19 de febrero, afirmó que *"el umbral de la garantía del derecho al secreto de las comunicaciones tiene carácter rigurosamente preceptivo. Por tanto, es el ordenamiento el que establece sus términos y su alcance mismo. Así, como espacio de intimidad garantizado al máximo nivel normativo, no podría quedar, y no queda, a expensas de la evolución de los avances de la técnica, lo que supondría un riesgo permanente de eventual*

b) Injerencia leve e injerencia grave

En el panorama social relacionado con la ITCE conviven de forma poco pacífica la extraordinaria evolución de las TIC y la rigidez de la doctrina jurídica pues, donde esta última ve blancos o negros, la explosiva evidencia muestra que existe – o debiera existir – una amplísima gama de grises.

Por ello, en el capítulo II se presentó someramente el panorama de actualidad al respecto y cómo la comunidad internacional, comenzando por las Naciones Unidas y continuando por cualquiera de los demás organismos supranacionales, trataba de asumir los retos ocasionados por el evolución de las TIC, con probable resultado de naufragio o, todo lo más, con la producción de instrumentos jurídicos de investigación inestables e incapaces de llegar a un mínimo aceptable de eficiencia, pese a sus enjundiosos análisis de la realidad circundante y a su encomiable voluntad de hallar soluciones.

A la relectura de este capítulo me he de remitir para, al menos, dejar representada la distancia, de apariencia insalvable, entre las TIC y el Derecho.

Pero en tanto esta distancia razonablemente se acorte, en la STC 281/2006, de 9 de octubre (RTC 2006/281), se reconoce, en primer lugar, que *"…no existe reserva absoluta de previa resolución judicial respecto del derecho a la intimidad personal, de modo que excepcionalmente hemos admitido la legitimidad constitucional de que en determinados casos y con suficiente y precisa habilitación judicial realice determinadas prácticas que constituyan una injerencia leve en la intimidad de las personas"*[709]; En segundo lugar, que el secreto *"se proyecta tanto sobre el proceso de la comunicación como sobre el contenido de la misma, aunque este no quede en la esfera de lo íntimo"*[710]; Y, en tercer lugar, *"la protección alcanza frente a cualquier forma de interceptación en el proceso de la comunicación mientras el proceso está teniendo*

relativización, con la consiguiente degradación de lo que es una relevante cuestión de derecho a mero dato fáctico".

[709] Ver también las SSTC 37/1989, de 15 de febrero, (RTC 1989,37), F. 7; 207/1996, de 16 de diciembre, (RTC 1996,207), F. 3; y 70/2002, de 3 de abril, (RTC 2002,70), F. 10.

[710] STC 114/1984, de 29 de noviembre (RTC, 1984, 114)

lugar, siempre que sea apta para desvelar, bien la existencia misma de la comunicación, bien los elementos externos del proceso de comunicación, bien su propio contenido". Finalmente, el derecho al secreto de las comunicaciones alcanza a terceros ajenos a los comunicantes[711,712].

La exégesis de algunos elementos del anterior y enjundioso pronunciamiento jurisprudencial resulta muy sugerente a propósito de las finalidades de este trabajo, pues será preciso restarle indeterminación, allí donde sea posible, al concepto de ***injerencia leve en el derecho a la intimidad.*** *Sensu contrario*, se intentará determinar cuándo, decididamente, se está ante una ***injerencia grave*** al hacer su aparición el más mínimo signo de afectación al derecho fundamental.

Esta necesidad de modulación, en mi opinión, se justifica en los variados elementos y circunstancias de todo orden que, en materia de comunicaciones electrónicas, emergen como consecuencia de la diversificación y uso real de las TIC y que no siempre resultarán merecedores de una radical, indistinta y universal protección, como proclama la STC comentada, sino, más bien, de un ponderado juicio de proporcionalidad, según corresponda al peso del sacrificio a los derechos fundamentales que su limitación implique.

Estas posiciones jurídicas trasladan, con poco ejercicio crítico, la visión arcaica de las comunicaciones telefónicas fijas a un mundo por completo diferente, que no es otro que el del uso real de las TIC en la sociedad actual, por lo que se hace necesario un nuevo enfoque de las garantías constitucionales a aplicar a la limitación de los derechos fundamentales en este relativamente novedoso campo de intervención del Derecho.

Se pretende deslindar, entre otras cosas, entre lo que corresponde, de forma directa e inequívoca, al derecho al secreto a las comunicaciones y lo que afectará únicamente al derecho genérico a la intimidad o, más simplemente, determinar que en algunos casos no tenga por qué producirse inexorablemente una afectación a los derechos del art. 18 CE.

[711] SSTC 114/1984, de 29 de noviembre, F. 7 y 56/2003, de 24 de marzo (RTC 2003//56) F.3.
[712] Vid. Lanzarote Martínez, Pablo. *Intervención de las…op. cit.*, pág. 711.

A estos efectos, como punto de inflexión en la jurisprudencia, en la comentada STC 281/2006, nótese que se dice también que la protección del art. 18.3 CE alcanza a la comunicación "*mientras el proceso está teniendo lugar",* dejando aparentemente implícito que disminuye o cesa en cuanto la comunicación finaliza.

El anterior y controvertido punto de vista, muy confuso en mi opinión, genera una gran incertidumbre sobre el peso de los derechos condicionados por esta circunstancia de orden temporal, según se acceda a los DACE durante o después de la comunicación a la que se vinculen.

Indica también que, en algún momento reciente, el valor que se daba a los DACE conservados en relación con el sacrificio de los derechos fundamentales era menor que el otorgado a los accedidos durante el curso de la comunicación.

Este punto de vista jurisprudencial parece, por otra parte, constituirse en un hito desbordado por la legislación y la jurisprudencia posteriores o, al menos, la de los últimos años, donde se ha unificado la protección a los DACE conservados con los producidos en tiempo real durante la comunicación, como es de ver en el espíritu que se trasluce de la LCDCE. Además, no sólo se extiende genéricamente la protección a los que se produjeron en comunicaciones ya finalizadas, sino a cualquier dato que tenga algo que ver con el mundo de las comunicaciones electrónicas, que conlleva una radical y universal protección, cuestión que será también materia de estudio.

De lograrse la pretensión de deslindar el ámbito del Derecho que en cada momento se halle concernido, como conclusión preliminar, se podría llegar a sostener que la IDACE podría tener un mayor valor o, expresado de un modo más funcional, ofrecer un mayor rendimiento para la investigación, al menos desde un punto de vista policial, que el que tiene el propio contenido material de las comunicaciones.

La anterior circunstancia conllevaría, en mi opinión y con toda lógica, una *ratio* menor de penetración en cualquiera de las expresiones del derecho a la intimidad consagradas en el art. 18 CE, hasta llegar incluso a hacer innecesario el acceso al contenido material en algunos casos.

En buena medida, la IDACE, ajena – se debe insistir – al contenido material de la comunicación, llega a estructurar o condicionar la evolución, desarrollo y posibilidad

de éxito de las investigaciones, actuando como un auténtico eje de progresión para que alcancen sus legítimos fines, orientando el conjunto de una inteligencia policial puesta al servicio del esclarecimiento de los hechos delictivos. Su trascendencia y posible valor probatorio, unido a la calidad del proceso investigativo en cuyo seno hayan sido analizados, superarán sin duda en muchas ocasiones al deducido del mero análisis del contenido material de las comunicaciones.

2. Las comunicaciones con máquinas en relación con la protección del art. 18.3 CE.

Habría que estimar también, en relación con las comunicaciones electrónicas intermediadas por un dispositivo técnico, un nuevo y necesario enfoque jurídico para aquellos casos en los que la comunicación no responda al paradigma básico de interlocución entre personas en que se fundó la actual legislación procesal sobre la intervención de las comunicaciones, sino entre estas con máquinas (persona a máquina o vice-versa) y las comunicaciones de máquina a máquina, cuyo nivel de protección de ningún modo puede ser equivalente a las primeras, salvo en aquellas excepciones en que, bien ponderada la injerencia, así se deba determinar.

La doctrina sobre esta materia, no obstante, se cimienta en la que se trasluce de la ya reiteradamente comentada STC 114/1984, de 29 de noviembre, por lo que los autores estudiados no dejan lugar a interpretaciones imaginativas que pretendan restar vigencia a sus pronunciamientos. Muy por el contrario, la rigidez y la ausencia de modulaciones sobre la protección formal del secreto sobre las comunicaciones electrónicas es absolutamente palmaria y se proyecta indistintamente sobre cualquiera de sus expresiones[713].

Pero pareciéndome poco razonable esta posición y, desde luego, ajena en algunos casos a la realidad social impuesta por el desarrollo de las TIC, conviene tratar de comprender y asumir la diversidad alcanzada en su uso cotidiano, que no siempre

[713] Vid. González-Cuéllar Serrano, Nicolás. *Garantías constitucionales…op. cit.,* pág. 168.

representará ese ejercicio de lo íntimo que tanta protección merece en los entornos democráticos o, al menos, no lo será en determinadas aplicaciones criminales.

En este sentido, siguiendo a GONZÁLEZ-CUÉLLAR[714], *"lo relevante, no es la intervención humana en el envío o recepción de los datos, su carácter directo o indirecto, sino la utilización, para la transmisión, de un cauce susceptible de ser incardinado dentro de la categoría de comunicación, según la representación social del término"*, es decir, que prima el componente formal del secreto sobre el acceso al instrumento de transmisión al que representa la comunicación humana en sí misma.

Concluye el autor para sostener la protección formal e indistinta del secreto de las comunicaciones, aún diferenciando entre *sistema* y *canal de comunicación*, que:

> *"Forzoso es advertir que el trasvase de datos entre máquinas en el que los humanos intervienen de forma remota en el envío o la recepción puede muy fácilmente situarse fuera del concepto de comunicación y, en ocasiones, será difícil diferenciar entre una simple transmisión de datos en un sistema y una comunicación protegida[715][…] Sólo deben considerarse incluidos en el ámbito de protección del art. 18.3 CE las transmisiones de datos entre máquinas que empleen un mecanismo de conexión reconocible como canal de comunicación conforme a un criterio socialmente compartido".*

En este contexto, el autor se apoya en algunos ejemplos que podrían considerarse muy comunes en el uso cotidiano de las comunicaciones electrónicas, como la recepción de una señal de alarma (de máquina a persona) o una consulta *web* (de persona a máquina)[716] que, en mi opinión, coincidente en lo esencial con la del

[714] Vid. González-Cuéllar Serrano, Nicolás. *Garantías constitucionales…op. cit.,* págs. 167 y 168.

[715] Adviértase en este fragmento que el autor parece dejar la puerta abierta a la posibilidad de diferenciar comunicaciones protegidas de las que no debieran serlo.

[716] Estos casos, en su simpleza, no representarían en ningún caso un entorpecimiento de la labor policial de investigación pues se obtendrían con toda normalidad, caso de que tuvieran algún interés, en el curso de una intervención de las comunicaciones ordenada por la Autoridad Judicial. Caso distinto es la fenomenología objeto de este trabajo, en que el análisis del *iter criminis* deviene de una complejidad extraordinaria y que sí tiene importantes connotaciones con la cuestión de fondo, lo que se estudiará con más profundidad en un apartado posterior. Sin embargo, el autor, sin entrar en estos últimos casos, opina *a priori* que *"la exclusión [del tipo de comunicaciones cuyos ejemplos menciona] supondría aceptar un alto riesgo de lesión de la privacidad".* Por tanto, con todas las reservas, habré de plantear una opinión contraría a la de GONZÁLEZ-CUÉLLAR.

autor[717,718], son merecedores de una reconocible protección mediante el secreto por contener, al menos, un mínimo significado que los entroncaría sin necesidad de más discusión con lo íntimo (dicho sea, por otro lado, con independencia del contenido formal del secreto que se vierte sobre el canal de transmisión).

Es necesario insistir, desde un punto de vista estrictamente práctico, que si todo ello tuviera algún interés para el proceso penal (como, por ejemplo, saber cuándo un investigado entra o sale de un local propio cuando desconecta o conecta la alarma, cuando retira dinero de un cajero, efectúa un pago, etc.), no sería posible diferenciar el ámbito de la intervención entre las facetas de interés en relación con el resto del tráfico comunicativo del terminal objeto del interés procesal, por lo que sería necesario un mandato judicial que cubriese, con toda lógica, su uso indistinto durante un periodo determinado de tiempo[719].

Pero, utilizando este mismo argumento, es decir, el de la *información significativa,* puede verse que este no es el problema que interesa ahora analizar, pues existen comunicaciones sin contenido "humano" (sin *información significativa*) que, a los efectos que interesan, excede por completo al interesante punto de vista fenomenológico planteado por GONZÁLEZ-CUÉLLAR, aunque, eso sí, tengan en común que tanto unos mensajes como otros circulan por un canal cerrado de transmisión.

Estos ejemplos, relativamente habituales, quedarían representados en el plano casuístico por los miles de llamadas instrumentales automáticas de telefonía móvil (sin interlocución humana) de la OP. LÍNEA ROJA (caso de vaciamiento patrimonial de una

---

[717] Según GONZÁLEZ-CUÉLLAR, no hacerlo *"implicaría situar fuera del concepto constitucional de comunicación a información significativa transmitida por los mismos cauces que los mensajes elaborados y cursados directamente por humanos".*

[718] El autor comentado clasifica los mensajes pregrabados como mensajes de máquina a persona. Sin pretender entrar con profundidad en el tema, podría interpretarse genéricamente su naturaleza como un mensaje diferido de persona a persona, de naturaleza similar al correo electrónico.

[719] Bien el del terminal del usuario, bien el del terminal emisor si está conectado a una línea multipropósito, casos en que el uso sería diverso. En caso de que el terminal de la alarma tuviese una SIM alojada destinada a un uso exclusivo y predeterminado para gestionarla y si el interés del proceso penal sólo consistiese en conocer el tráfico de datos relativos a su conexión y/o desconexión, se estaría ante un caso típico de valoración de la proporcionalidad que exigiría optar por la intervención de la SIM de la alarma y en ningún caso del terminal del receptor, por ser esta posibilidad menos gravosa para los derechos fundamentales del investigado. En cualquier caso, nótese que la carga de sacrificio del derecho al secreto por comunicación de máquina a persona en este caso es ínfima, pues tan sólo consiste en que el investigador sepa cuándo se activa o desactiva un aparato de alarma, más que el hecho subsiguiente de la notificación al usuario, lo que podría no tener el más mínimo interés para la investigación.

promoción comercial) o la infección *DoS* de varios millones de ordenadores en la escena mundial de la *botnet* MARIPOSA (infección viral de ordenadores mediante instalación maliciosa de *malware* controlado)[720], que se estudiarán con más profundidad en apartados posteriores, y que ejemplifican sobre la verdadera trascendencia, a día de hoy, del concepto de comunicaciones máquina a máquina en su más genuina representación criminal y, desde luego, sin relación alguna con comunicaciones personales de ningún tipo.

Estos casos consisten, respectivamente, en el envío ininterrumpido por cada tarjeta de telefonía de un mensaje sin contenido material destinado a agotar el valor de una promoción comercial por la contratación de una línea de telefonía móvil y para difundir *malware* entre millones de ordenadores sin un concreto destinatario personal.

Una intervención de las comunicaciones ofrecería como resultado, en el primer caso, el silencio más absoluto y, en el segundo, durante la fase de infección por *malware,* un ininteligible tráfico de paquetes de datos conteniendo programas informáticos maliciosos ejecutables por una máquina en destino, pero sin que figure persona alguna como su receptora[721].

Es esta clase de comunicaciones el que necesita de un revisión jurídica ya que, en mi opinión, parece absurda la protección ciega y acrítica del canal de transmisión – cual banco pintado al que urge retirarle el cartel - cuando lo que hay que tratar es de proteger realmente la intimidad de las personas.

Será objetivo de este trabajo, por tanto, ofrecer con apoyatura en la experiencia, una visión distinta del uso criminal de las TIC y de lo necesario que es

[720] *Ibídem.*

[721] Las comunicaciones, en este caso, podrían dirigirse a ordenadores pasivos como receptores, tales como, por ejemplo, los que gestionan un proceso industrial o contienen datos de cualquier clase pero sin adscripción a persona alguna. Ejemplos de esta clase de redes informáticas lo constituyen los llamados ***sistemas de scada*** (acrónimo del inglés *supervisory control and data acquisition* que significa supervisión, control y adquisión de datos), que son ordenadores empleados exclusivamente para el control y supervisión de los procesos industriales. Nótese que estas máquinas pueden ser infectadas como *zombies* de una *botnet* sin que esta circunstancia los ponga en peligro o, alternativamente, ser precisamente el objeto del ataque, causando su inutilización previa manipulación telemática. A continuación, puede repararse en el perjuicio que puede sufrir una pequeña o mediana empresa cuya producción dependa de la eficiencia, disponibilidad y seguridad de estos sistemas y, por su gravedad, en otro extremo, en el robo y vaciamiento de los datos de un sistema informático que soporte la gestión, por ejemplo, de la seguridad social, de los sistemas de navegación aérea o de la agencia tributaria.

desprenderse de ciertos anacronismos que impiden una visión jurídicamente racional de lo que hay proteger realmente.

Por todo lo anterior, cuando se hable de las *comunicaciones electrónicas* y de sus DACE, se utilizará, de forma extensiva, un concepto amplio que abarcará a todas aquellas en las que la comunicación se produzca entre personas o máquinas y cualquiera de sus combinaciones, sea cual fuere el procedimiento de comunicación y el medio empleado para configurar el mensaje, venga o no codificado, pero siempre utilizando la intermediación de un instrumento basado en la electrónica, como rama de la física cuyas aplicaciones técnicas propician la comunicación o transferencia, no sólo de la voz o texto sino también, de forma interactiva, de contenidos de cualquier clase.

Se debe concluir respecto de las anteriores reflexiones, que todas las comunicaciones entre personas están protegidas formalmente por el secreto, pero que, al existir diferentes categorías, que responden a una gran variedad de los usos reales de las comunicaciones motivada por la extraordinaria evolución de las TIC y el hecho de que no todas afectan a personas, según el concepto subyacente en la muy deficiente legislación actual, el Derecho debiera tratarlas con la eficiencia que se deduce de su distinta naturaleza, al menos en sus aspectos jurídico-procesales[722].

En consonancia, todo lo anterior debe ser puesto en proporción con el *quantum* de sacrificio que exigirá la limitación de determinados derechos y que afectará intensamente en algunos casos, sin la más mínima duda, al derecho al secreto de las comunicaciones (por ejemplo, una conversación entre personas por vía telefónica), en otros, la afectación será mínima (verbigracia, ordenar una operación de banca electrónica) o nula (por ejemplo, usar una tarjeta de telefonía como detonador de explosivos o para enviar un código malicioso y activar en remoto el *malware* instalado en un ordenador) y, en todos los casos, aspectos que únicamente afectarán accesoriamente a materias directamente relacionadas con el derecho a la protección

[722] Cuando comenzó el uso masivo de Internet y la telefonía móvil, la jurisprudencia ya anotó la necesidad de contar con mejor legislación. En la STS de 20 de diciembre de 1996 (RJ 1996, 9038) ya se atisbaban *"los nuevos peligros cernientes sobre la intimidad"* para lo que sería necesario *"arbitrar instrumentos legislativos adecuados que salvaguarden la integridad del ámbito de privacidad de la persona".*

de datos de carácter personal y, muy lejanamente, al secreto de las comunicaciones (Por ejemplo, un dato conservado de la localización de una BTS en una comunicación finalizada tiempo atrás).

Se necesita además, a falta de precisiones jurídicas que poder invocar en el vigente derecho positivo, tratar esta cuestión desde un enfoque amplio sobre el concepto de las comunicaciones electrónicas – operativo o incluso, si se quiere, extrajurídico – que permita entender que, visto que la finalidad del proceso penal es idéntica en todos los casos, esto es, intervenir las comunicaciones, se puedan asumir todas y cada una de las expresiones actuales y, si es posible, futuras, que tan sensible materia pueda alcanzar, de modo que el proceso penal no se resienta en su eficiencia al no haber sido posible aportarle unos medios de prueba por mor de las insuficiencias comentadas.

3. Inclusión de las comunicaciones orales directas

Antes de progresar en otros aspectos de las comunicaciones, debe quedar despejada la cuestión de la inclusión o no de las ***comunicaciones orales directas*** como acreedoras de la protección del art. 18.3 CE y, consecuentemente, determinar si existe reserva de judicialidad sobre la decisión de injerirse en su contenido.

Lo esencial de este tipo singular de comunicaciones es que se producen con inmediatez de los interlocutores entre sí y sin que hagan uso de dispositivo técnico alguno para mantenerlas, ya que algunos autores[723] sostienen que, siendo así, la alta protección constitucional otorgada por el art. 18.3 a las comunicaciones personales afectaría únicamente a las que se produjeran mediante el uso de los *"servicios*

[723] NOYA lo expone diciendo que *"una interpretación restrictiva determina que las comunicaciones a las que se da protección en el citado precepto [el art. 18.3 CE] y por tanto las únicas cuyo secreto puede levantarse mediante autorización judicial, son aquellas que se mantienen a través de un instrumento técnico interpuesto, y no las desarrolladas de forma directa entre los interlocutores".* Vid. Noya Ferreiro, María Lourdes. *La intervención…op. cit.,* pág. 105. También, vid. Jiménez Campo, Javier. *La garantía constitucional…op. cit.*, págs. 35 y ss, López-Fragoso Álvarez, Tomás. *Las intervenciones telefónicas en el proceso penal*. Madrid, 1991, pág. 51, Pardo Falcón, Francisco Javier. *Los derechos del artículo 18 de la CE en la jurisprudencia del Tribunal Constitucional*. REDC, núm. 34, 1992, pág. 174 y Vegas Torres, Jaime. *Obtención de pruebas…op. cit.,* pág. 43.

especialmente concebidos para la comunicación entre personas distantes"[724], categoría en la que se englobarían sin duda las comunicaciones electrónicas.

Lo anterior podría interpretarse, de un modo restrictivo, en el sentido de que el precepto constitucional dispone una protección de menor intensidad para aquellas otras comunicaciones que se produjesen entre personas no distantes y que, para cuya materialización, no se sirviesen de dispositivos tecnológicos de comunicación de cualquier clase, conocida o por conocer, es decir, para las *comunicaciones orales directas*[725].

Sin embargo, en mi opinión, no cabe deducirse que el secreto de las comunicaciones orales directas no esté protegido constitucionalmente, ya que una lectura precisa del contenido del artículo 18.3 no ofrece duda alguna sobre que el objeto de protección, con carácter general, son las comunicaciones y su secreto – *salvo resolución judicial* -, sin que sea posible hacer distinción alguna entre ellas, excepto en el caso de que sean merecedoras de una especial protección, que debe entenderse superior, si son materializadas mediante el uso de servicios *postales, telegráficos, telefónicos o análogos*[726].

Además, según se zanja en la trascendental STC 114/1984, de 29 de noviembre, la interpretación no puede ser sino la amplia, al proclamar que *"quien graba una conversación ajena incide directamente en el derecho al secreto de las comunicaciones…[con independencia] de mantenerse a través de un instrumento técnico interpuesto"*[727].

---

[724] *Ibídem.* Extráigase de este fragmento de la definición de VEGAS, que se aportó en el estudio sobre la proporcionalidad, su clara precisión de que la comunicación se produce "entre personas" y que estás se hallan "distantes" entre sí. Este autor, para sostener la restricción del ámbito de aplicación del art. 18.3 CE se apoya indirectamente en la STC 281/2006, FJ 3º y, con cierta inestabilidad, en la STS de 9 de diciembre de 2008 sobre el Recurso 848/2008. Para VEGAS, estarían igualmente excluidas de la protección del art. 18.3 CE *"…todas [las comunicaciones] las que se realicen mediante el empleo de cualquier otra herramienta informática o de red no concebida específicamente para la transmisión de mensajes".* Vid. Vegas Torres, Jaime. *Obtención de pruebas…op. cit.,* pág. 41 y ss.

[725] Sería el caso de las que se producen tras la concurrencia, aleatoria o no, de personas en un determinado lugar físico en el que se comunican entre sí directamente (Por ejemplo, en el interior de un vehículo, en un establecimiento público, al aire libre, etc.). Vid. Noya Ferreiro, María Lourdes. *La intervención…op. cit.*.

[726] Gimeno Sendra, Vicente. *La intervención de las comunicaciones,* en Marchal Escalona, Nicolás (Director). *Manual de lucha…op. cit.,* pág. 570.

[727] Vid. Noya Ferreiro, María Lourdes. *La intervención…op. cit.,* pág. 106.

Consecuente con lo anterior, la intervención de las comunicaciones orales directas requiere de un mandato judicial, atendido el principio de proporcionalidad[728].

Desde un punto de vista policial, las dudas que se plantean en los ámbitos de reflexión jurídica quedan resueltas, por defecto y sin mayores problemas, como en tantas ocasiones en que la inseguridad jurídica impera, con una buena dosis de garantías a prevención, mediante la interposición sin reservas de una solicitud judicial para la grabación de las comunicaciones orales directas[729], sin hacer exégesis de la posibilidad de residenciarlas en el régimen general de protección de la intimidad y no en el especial y superior reservado a las postales, telegráficas y telefónicas.

Esta exigencia, perfectamente interiorizada en la praxis diaria de la PJE, plantea, por otro lado, algunos problemas de efectividad en el orden práctico en aquellos casos en que el ámbito espacio-temporal elegido para comunicarse sea espontánea y aleatoriamente determinado por los sujetos concernidos por el interés judicial.

Se trata, por tanto, de unos escenarios criminales en los que la PJE ha de intervenir en tiempo real cuando investiga con inmediatez a los sospechosos, con los consiguientes problemas para la instalación de los medios técnicos destinados a la grabación de sus conversaciones orales directas, dado el dinamismo y la espontaneidad con que se producen, lo que no siempre permite acudir a un Juez de Garantías para que disponga sobre la marcha un mandamiento de intervención con una imposible referencia a los condicionantes que se ignoran de tiempo, lugar y demás circunstancias en que se producirán.

---

[728] A lo que hay que añadir un exigente dominio de los medios técnicos de grabación por parte de la PJE, de forma que queden cubiertas todas las garantías de veracidad, autenticidad e integridad en cuanto al contenido material que se registre y de los correspondientes DACE, lo que se suele poner en práctica, a falta de una regulación procesal y una norma técnica específica, bajo la estricta fe pública aportada por el Secretario Judicial y el empleo de los medios de certificación y salvaguarda disponibles en el mercado especializado que ofrezcan la completa seguridad jurídica sobre este tipo de procedimientos (intervención de la SIM en el SITEL, certificación con firma electrónica, *hash, time stamping* o sellado de tiempo, geolocalización con medios complementarios, etc.).

[729] No obstante, por razones de seguridad jurídica, la instalación de tales medios se hace bajo el régimen del art. 18.3 CE. Vid. AAN del Juzgado Central de Instrucción núm. 6, de 3 de mayo de 2011, en DP 68/2011. Curiosamente, el Magistrado, según el Auto, autoriza "*la restricción de su derecho al proceso telecomunicativo"* que se produce en el interior de un vehículo en el que se instala el sistema de audio lo cual, en mi opinión, contiene una inexactitud que no es necesario explicar.

Estos casos, que son muy comunes, resultan de difícil subsunción dentro del contenido material de la resolución judicial pues, aún teniendo idéntico interés para el proceso penal que las que se producen a través de un dispositivo técnico identificado ante el Juez, se tropiezan con dificultades tales como la descripción del modo en que ha de llevarse a cabo, el desconocerse el escenario en que finalmente se producirán, el periodo de tiempo, el medio técnico de grabación, etc.

Para su solución y aunque sería deseable una forma admisible en Derecho para ello, no están permitidos los mandatos judiciales con fórmulas abiertas que se adapten, con idéntico dinamismo, a su eventual ejecución ante la verificación de un determinado escenario.

Para estos casos, consecuentemente, sería exigible una revisión jurídica de la rígida reserva de judicialidad sobre las cuestiones espacio-temporales planteadas, de forma que permitiese, de una manera flexible y adaptativa, un control posterior de jurisdiccionalidad sobre tales aspectos que, por imprevisibles, no hayan de presuponer una renuncia del juzgador de atender la necesidad de intervenir las ***comunicaciones orales directas sobrevenidas***.

Naturalmente, lo anterior debiera quedar disponible bien aplicado el principio de proporcionalidad, permitiendo a la PJE intervenir en escenarios en los que el exigente panorama de la criminalidad grave, compleja u organizada aconsejara al Estado de Derecho no renunciar a su legítima acción ablativa.

Con toda lógica, este tipo de comunicaciones no producen DACE conservados, por lo que no procede la aplicación de norma alguna de la LCDCE, ya que se está hablando de los que se producen en el curso de una intervención de las comunicaciones ordenada por la Autoridad Judicial, a cuya finalización se retiran los medios técnicos de grabación.

No obstante lo anterior, existen determinados DACE sobre las comunicaciones orales directas, generados por el uso de los medios técnicos, que tienen un extraordinario interés para la investigación, como serían los de localización y los de activación/desactivación del periodo de grabación, datos que, debidamente certificados, pueden tener un extraordinario valor para el proceso penal

Por ello, otra cuestión interesante en torno a los medios técnicos la constituye la cuestión de la certificación tecnológica, de forma que queden garantizadas la autenticidad, veracidad e integridad de los contenidos grabados, según las propuestas que más adelante se incluirán.

4. Comentarios sobre otros aspectos jurisprudenciales de interés

Pero, por más que impere la doctrina nacida del Caso Malone y recogida en la STC 114/1984 y en otras muchas que la corroboran, la jurisprudencia no ha sido en absoluto pacífica en lo que se refiere a la identificación jurídica del derecho fundamental afectado, especialmente cuando se trata del almacenamiento y cesión de los datos de tráfico de las comunicaciones electrónicas ya finalizadas.

Tanto ha sido así, que de las cuatro posturas que identifica GONZÁLEZ LÓPEZ[730], a quien nuevamente he de seguir, tan sólo una – que el autor da por abandonada – considera afectado el derecho fundamental al secreto de las comunicaciones del art. 18.3 CE[731] y que es la que ya se ha tratado en el apartado correspondiente.

De las otras tres posturas doctrinales estudiadas por el autor, paso a ocuparme en el apartado siguiente, en el que las califico de no dominantes:

[730] Vid. González López, Juan José. *Los datos de tráfico…op.cit.,* pág. 316 y ss.

[731] Representativo de esta postura es, según el autor citado, el *"criterio mantenido por la Fiscalía General del Estado en su Consulta 1/999 y también el que parece derivarse de la STS 1231/2003 (Sala de lo Penal), de 25 de septiembre (FJ 8), que, tomando como referentes las SSTS 316/2000, y 1235/2002, presenta un planteamiento sumamente confuso en que se vincula igualmente la obtención de los listados con el derecho al secreto de las comunicaciones, pese a referirse a comunicaciones ya acaecidas".* Sobre la confusión en esta materia, se cita en la STS 1231/2003 la doctrina contenida en la STC 70/2002, donde se afirma a su vez que *"ha de añadirse otra consideración, relativa al momento en que se produce la intervención policial. Pues tal intervención no interfiere un proceso de comunicación, sino que el citado proceso ya se ha consumado, lo que justifica el tratamiento del documento como tal (como efectos del delincuente que se examinan y se ponen a disposición judicial) y no en el marco del secreto de las comunicaciones. La protección del derecho al secreto de las comunicaciones alcanza al proceso de comunicación mismo, pero finalizado el proceso en que la comunicación consiste, la protección constitucional de lo recibido se realiza en su caso a través de las normas que tutelan la intimidad u otros derechos [la comunicación en este caso se refiere a una carta ya abierta]"*. Vid. González López, Juan José. *Los datos de tráfico…op.cit.,* pág. 318.

a) Pronunciamientos doctrinales no dominantes

Sobre los derechos fundamentales concernidos por el almacenamiento de los datos de tráfico – práctica que no nace de los imperativos la LCDCE, sino originada por necesidades de la gestión tecnológica interna de las operadoras del mercado de las telecomunicaciones, lo que motivó el que pudieran estar disponibles para la investigación criminal -, han existido posturas, ocasionalmente presentes en la jurisprudencia, que incluso llegaban a negar la afectación a derecho fundamental alguno[732].

Pero la cuestión candente, sobre la que puede mantenerse una discusión en el plano doctrinal, es sobre si, con la decisión de ceder datos almacenados por las operadoras de tráfico de las comunicaciones, se limita indistinta y automáticamente el derecho al secreto de las comunicaciones o si, por el contrario, la afectación es únicamente al derecho a la intimidad o a la protección de datos personales, materia que, en sí misma, tiene un interés nuclear para intentar comprender bien cuál es la verdadera trascendencia de las diversas alternativas jurídicas para el Derecho[733].

Esta discusión, de otro lado, sólo puede sostenerse desde un punto de vista teórico, toda vez que quedó zanjada *ex* art. 1.1 LCDCE con la imposición de un mandamiento judicial como medio de requerir los datos de tráfico conservados por las operadoras, tras la identificación inequívoca del derecho del art. 18.3 CE como el afectado por el acceso y cesión, sin conceder opción a las otras dos formas de manifestarse el derecho, esto es, a la intimidad o a la protección de datos[734].

---

[732] Véase la STS 1219/2004 (Sala de lo Penal), de 10 de diciembre (FJ 16). Por otro lado, esta visión sería extensiva a los datos de abonado que constan en los contratos de prestación del servicio de telefonía, encuadrables en la categoría de datos afines, según la STS 1338/1998, de 9 de noviembre (FJ 2), lo que no afectaría, según esta doctrina, ni al derecho a la intimidad, ni al secreto de las comunicaciones.

[733] LÓPEZ-BARAJAS ilustra de un modo comprensivo sobre estas tensiones doctrinales, haciendo notar, con referencias a varios autores y jurisprudencia, que *"mientras ex art. 18.3 CE la intervención de las comunicaciones requiere siempre resolución judicial, no existe en la Constitución reserva jurisdiccional absoluta respecto del derecho a la intimidad personal, donde se ha admitido, de forma excepcional, que en determinados casos y con la suficiente y precisa habilitación legal, es posible que la Policía Judicial realice determinadas prácticas que constituyan una injerencia leve en al intimidad de las personas"*. Vid. López-Barajas Perea, Inmaculada. *La intervención de las comunicaciones electrónicas*. La Ley. Grupo Wolters Kluwer, 2011. ISBN 978-84-8126-816-4, pág. 33 y ss.

[734] En el preámbulo de la LCDCE se puede comprobar esta diáfana identificación con el texto siguiente: *"La Ley [la LCDCE] es respetuosa con los pronunciamientos que, en relación con el derecho al secreto de*

En lo que se refiere a la consideración jurisprudencial de reconocer únicamente una afectación al derecho a la intimidad, dice GONZÁLEZ LÓPEZ, que se recogió en "*la citada STS 1219/2004 (Sala de lo Penal), de 10 de diciembre (FJ 16), que, a pesar de negar la existencia de afección a derechos fundamentales, se ocupa de analizar tal posibilidad no desde la óptica del derecho a la protección de los datos de carácter personal, sino del derecho a la intimidad. Aún más claramente en las SSTS (Sala de lo Penal) 1235/2002 (Sala de lo Penal), de 27 de junio (FJ 3), y 1397/2005, de 30 de noviembre (FJ 1), esta segunda haciéndose eco de las SSTS 316/2000, 1235/2002 y 1086/2003, que reconducen al ámbito del derecho a la intimidad la indagación en la memoria de un aparato de telefonía móvil, admitiendo que la misma se practique por la policía judicial en el marco de las diligencias de averiguación y aseguramiento de pruebas, siempre que se respete el principio de proporcionalidad*"[735].

Respecto de la posibilidad de que el derecho fundamental concernido sea el de la protección de los datos de carácter personal, la opción más razonable – que es por la que opta el mismo autor, atribuyéndole en su momento una cierta fortuna - y a la que me adhiero, es la que GONZÁLEZ LÓPEZ indica con el siguiente texto:

> *"Finalmente, se ha abierto paso una corriente jurisprudencial, cada vez más estable, que sitúa la protección de los datos de tráfico recabados de los proveedores en el régimen previsto en la LOPDCP. Así, SSTS 459/1999 (Sala de lo Penal), de 22 de marzo (FJ 2); 2384/2001 (Sala de lo Penal), de 7 de diciembre (FJ 2); 1330/2002 (Sala de lo Penal), de 16 de julio (FJ 4); 1167/2004, de 22 de octubre (FJ 1), que se refiere expresamente al artículo 11.2 de la LOPDCP; 558/2005 (Sala de lo Penal), de 27 de abril (FJ 1); 916/2006 (Sala de lo Penal), de 29 de septiembre (FJ 10), y 101/2007 (Sala de lo Penal), de 23 de enero (FJ*

---

las comunicaciones, ha venido emitiendo el Tribunal Constitucional, respeto que, especialmente, se articula a través de dos garantías: en primer lugar, que los datos sobre los que se establece la obligación de conservación son datos exclusivamente vinculados a la comunicación, ya sea telefónica o efectuada a través de Internet, pero en ningún caso reveladores del contenido de ésta; y, en segundo lugar, que la cesión de tales datos que afecten a una comunicación o comunicaciones concretas, exigirá, siempre, la autorización judicial previa". La doctrina del TC que menciona no es otra que la nacida del Caso *Malone* y de la STC 114/1984, tan reiteradamente mencionada, por su extraordinaria trascendencia y vigor, en el enfoque jurídico dominante sobre el acceso a los datos de tráfico conservados por las operadoras.

[735] Vid. González López, Juan José. *Los datos de tráfico…op.cit.,* pág. 317.

3[736]), que también remiten al citado artículo 11.2 d) de la LOPDCP para exceptuar la necesidad de consentimiento[737].

Nuestra postura a este respecto debe coincidir necesariamente con la última doctrina jurisprudencial[738]. No cabe duda, como ya expusimos, de que los datos de tráfico deben reputarse datos de carácter personal, en este caso claramente sometidos a tratamiento, como se desprende del hecho de que su recabo se produzca en relación con las bases de datos en que constan. Partiendo del hecho de que su obtención se produce una vez concluida la comunicación y de que los datos de tráfico no entran en la categoría de datos especialmente protegidos, ha de rechazarse la existencia de afección al derecho al secreto de las comunicaciones y a la intimidad, con independencia de que ocasionalmente se vean envueltos otros derechos fundamentales, entre los cuales puede encontrarse la intimidad, en el proceso de obtención de los datos. Mas dicha confluencia siempre tendrá carácter instrumental…"[739].

Este interesante pronunciamiento merece alguna precisión más, ya que como se dice en la STS 1167/2004, de 22 de octubre (FJ 1):

"Como doctrina de esta Sala, s. 7.12.2001, debemos recordar que la simple petición de listados de llamadas telefónicas efectuados desde un determinado número de teléfono, no afecta al contenido propio del derecho fundamental reconocido en el art. 18.3 CE. Es una diligencia típicamente de investigación policial y por tanto propia de la fase de instrucción que queda extramuros del secreto de las comunicaciones telefónicas cuya violación -erróneamente- se denuncia".

[736] Salvo error, el fundamento jurídico al que se refiere el autor es el segundo y no el tercero como consta en el texto transcrito.
[737] También, véase la STS 2209/2001, de 23 de noviembre.
[738] Interesa mucho el punto de vista de GONZÁLEZ-CUÉLLAR respecto de los mensajes de correo electrónico o los buzones de voz deliberadamente mantenidos en el servidor tras su lectura, que quedarán fuera del ámbito de protección del art. 18.3 CE, pasando a recibir la del art. 18.4 CE (el llamado "derecho de autodeterminación informativa"). El autor se apoya en Maza Martín, J.M. *La intervención judicial de las comunicaciones a través de Internet. Internet y Derecho Penal*. Cuadernos de Derecho Judicial núm. 10, 2001, págs. 633–643, pag. 643. En este sentido, vid. González-Cuéllar Serrano, Nicolás. *Garantías constitucionales…op. cit.,* pág. 168 y ss.
[739] Vid. González López, Juan José. *Los datos de tráfico…op.cit.,* pág. 318.

A continuación, el tribunal sentenciador afirma, con una rotundidad que no deja lugar a dudas, que "*no hay equiparación posible entre una conversación intervenida y la mera indicación del teléfono y titular al que se efectuó la llamada*", es decir, entre el contenido material y el formal – que los identifica como netamente distintos -, algo que, en mi opinión, ideológicamente no debe ofrecer dudas, deslindado con claridad meridiana qué derecho fundamental se limita con el acceso a los datos de tráfico almacenados: el derecho a la protección de datos personales y ningún otro.

La doctrina contenida en el pronunciamiento, negando tal equiparación de derechos y al punto de reconocer la diligencia como "típicamente de investigación policial", hace gravitar el peso de la limitación del derecho hacia el ámbito de las injerencias leves en los derechos fundamentales que, de un modo perfectamente reconocible, sería el propio o típico de una indagación en sede policial – una parte de las rutinas policiales, podría decirse, consistentes en la recogida de vestigios para orientar el curso de la investigación criminal -, siempre y cuando, naturalmente, todo ello esté dirigido en exclusiva a servir al proceso penal *ex* arts. 549.1.a) LOPJ, 11.2.d)[740] LOPD, 22.2 LOPD[741] y 1, 2 y 4 RDPJ.

Finalmente, en sintonía con lo indicado, el tribunal expone el modo en que ha de procederse para recabar los datos de tráfico de las bases mantenidas por las operadoras del mercado de las telecomunicaciones:

> *"En tal sentido debe citarse la STS 459/99 de 22.3 que entiende que estos listados custodiados en los ficheros automatizados a los que se refiere la LO. 5/92 de 29.10 requieren el consentimiento del interesado al contener datos*

[740] En art. 11.2.a LOPD se dice, sobre la excepción del consentimiento para la comunicación de datos, que será posible "*cuando la cesión está autorizada en una ley*". Sobre otras excepciones del consentimiento, el art. 11.2.d LOPD establece que no será necesario *"cuando la comunicación que deba efectuarse tenga por destinatario al Defensor del Pueblo, el Ministerio Fiscal o los Jueces o Tribunales o el Tribunal de Cuentas, en el ejercicio de las funciones que tiene atribuidas. Tampoco será preciso el consentimiento cuando la comunicación tenga como destinatario a instituciones autonómicas con funciones análogas al Defensor del Pueblo o al Tribunal de Cuentas".*

[741] En el art. 22.2 LOPD se establece que *"la recogida y tratamiento para fines policiales de datos de carácter personal por las Fuerzas y Cuerpos de Seguridad sin consentimiento de las personas afectadas están limitados a aquellos supuestos y categorías de datos que resulten necesarios para la prevención de un peligro real para la seguridad pública o para la represión de infracciones penales, debiendo ser almacenados en ficheros específicos establecidos al efecto, que deberán* clasificarse por categorías en función de su grado de fiabilidad".

personales, pero no es preciso cuando la cesión de tales datos tenga por destinatario el Defensor del Pueblo, el Ministerio Fiscal, Jueces o Tribunales, en el ejercicio de las funciones que les están atribuidas, art. 6.1 y 11.2 de la Ley, régimen que es idéntico al que se deriva de la actual normativa representada por la LO. 15/99 de 13.12 de Protección de Datos de Carácter Personal - BOE 14 de diciembre - pudiéndose entender que los listados de llamadas telefónicas constituyen un fichero de tratamiento de datos[742] *de carácter personal de conformidad con el art. 3 de la Ley para cuyo conocimiento no se exige el consentimiento del afectado cuando "... se recojan para el ejercicio de las funciones propias de las administraciones públicas en el ámbito de sus competencias..."*[743].

Cumplidas así las cosas, todo sugiere que, de obrar la PJE de acuerdo con el principio de proporcionalidad, nada habría de rechazable en que accediese de forma bien ponderada a los datos de tráfico de las comunicaciones electrónicas conservados por las operadoras del mercado de las telecomunicaciones *"en el ámbito de sus competencias"* (que, vistas las cosas, urgen de una precisión *lege ferenda*), cuestión sobre la que habrá de volverse profusamente.

Así se consideró, al menos, cuando entró en vigor el art. 12 LSSI, hoy derogado desde la LCDCE, en cuyo apdo. 3º se disponía lo siguiente: *"Los datos se conservarán para su utilización en el marco de una investigación criminal o para la salvaguardia de la seguridad pública y la defensa nacional, poniéndose a disposición de los Jueces o Tribunales o del Ministerio Fiscal que así los requieran. La comunicación de estos datos a las Fuerzas y Cuerpos de Seguridad se hará con sujeción a lo dispuesto en la*

[742] Art. 5.1.t RLOPD: *"Tratamiento de datos: cualquier operación o procedimiento técnico, sea o no automatizado, que permita la recogida, grabación, conservación, elaboración, modificación, consulta, utilización, modificación, cancelación, bloqueo o supresión, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias".*

[743] Véase también el FJ 2 de la STS 2384/2001 FJ 2 donde se afirma, en términos del derecho de protección de datos, que *"no es preciso [el consentimiento del interesado] cuando la cesión de tales datos tenga por destinatario el Defensor del Pueblo, el Ministerio Fiscal, Jueces o Tribunales, en el ejercicio de las funciones que les están atribuidas --art. 6-1º y 11.2.d, de la Ley--, régimen que es idéntico al que se deriva de la normativa actualmente en vigor, representada por la L.O. 15/99 de 13 Dic. de Protección de Datos de Carácter Personal --BOE 14 Dic.-, pudiéndose entender que los listados de llamadas telefónicas constituyen un fichero de tratamiento de datos de carácter personal de conformidad con el art. 3 de la Ley para cuyo conocimiento no se exige el consentimiento del afectado cuando […] se recojan para el ejercicio de las funciones propias de las administraciones públicas en el ámbito de sus competencias...".*

normativa sobre protección de datos personales[744]". En este contexto, como es de ver, el régimen jurídico de la cesión de los datos se vinculaba al derecho a la protección de datos y no al secreto de las comunicaciones[745].

Es evidente que, con la llegada de la LCDCE, este punto de vista cambió, optándose por una radical visión jurídica ligada a este último derecho y nacida de la doctrina *Malone* que hiciera a su vez fortuna en la STC 114/1984. En consecuencia, la cesión de datos de tráfico conservados se hizo indistinta en su protección constitucional a la de los producidos al tiempo de la intervención de las comunicaciones[746], esto es, bajo la reserva de resolución judicial – necesariamente previa, como indican los autores estudiados - *ex* art. 18.3 CE. Por lo demás, la redacción del art. 1.1 LCDCE y la inequívoca vinculación del espíritu de esta Ley al secreto de las comunicaciones, no ofrecen la más mínima duda sobre este particular.

Así, la LOPD dice en su art. 22.2 que *"la recogida y tratamiento para fines policiales de datos de carácter personal*[747] *por las Fuerzas y Cuerpos de Seguridad sin consentimiento de las personas afectadas están limitados a aquellos supuestos y categorías de datos que resulten necesarios para la prevención de un peligro real para la seguridad pública o para la represión de infracciones penales, debiendo ser*

[744] Se verá también más adelante la posición jurídica de la AEPD sobre el régimen de cesión de los datos de tráfico que, hasta la entrada en vigor de la LCDCE, lo consideró de acceso directo por la PJE.

[745] El autor deja claro en su análisis, en cualquier caso, con referencia a la jurisprudencia reiteradamente estudiada, que *"los datos registrados no pueden ser requeridos por la policía sin autorización judicial"*. Vid. González-Cuéllar Serrano, Nicolás. *Garantías constitucionales…op. cit.,* pág. 172.

[746] Atendida esta identificación, todo indica la necesidad de realizar un juicio de proporcionalidad separado sobre la necesidad de ceder DACE, tal y como lo considera en un Voto Particular el Magistrado Sr. MARCHENA GÓMEZ a la STS (Sala de lo Penal) 316/2011, de 6 de abril, en que señala que "*no cuestiono que esos datos electrónicos, generados durante una conversación telefónica mantenida mediante telefonía móvil, pueden llegar a ser de vital interés para el éxito de las investigaciones. Tampoco pongo en duda la legitimidad de su sacrificio cuando judicialmente se considere que la restricción de ese derecho está justificada con arreglo a los principios que informan la investigación penal en una sociedad democrática. Pero lo que no puedo avalar es que la resolución que autoriza el menoscabo del derecho al secreto de las comunicaciones no dedique una sola línea a explicar el porqué de su necesidad y, además, silencie el ineludible juicio de proporcionalidad. Es aquí donde sitúo mi discrepancia respecto de mis compañeros de Sala. Toda decisión judicial que acuerde, además de las escuchas telefónicas de los sospechosos, el control por la policía de otros datos generados durante la conversación, pero con incidencia sustantiva en el ámbito definido por el art. 18 de la CE, ha de motivar, con el mismo nivel de exigencia que venimos imponiendo para validar las escuchas, las razones que explican y legitiman el sacrificio añadido de otros aspectos íntimamente ligados a la privacidad*".

[747] En su definición del art. 3.a como "*cualquier información concerniente a personas físicas identificadas o identificables".*

almacenados en ficheros específicos establecidos al efecto, que deberán clasificarse por categorías en función de su grado de fiabilidad".

Al respecto de la *frase "la comunicación de estos datos a las Fuerzas y Cuerpos de Seguridad se hará con sujeción a lo dispuesto en la normativa sobre protección de datos personales"* con que finalizaba la cita precedente de la LSSI y en consonancia con la posición jurisprudencial estudiada, los informes emitidos por la Agencia Española de Protección de Datos, ante consultas hechas con anterioridad a la promulgación de la LCDCE, se pronunciaba, en relación con determinadas categorías de datos, que para producirse la comunicación a las Fuerzas y Cuerpos de Seguridad[748], debían cumplirse los siguientes requisitos[749,750,751]:

a) *Que quede debidamente acreditado que la obtención de los datos resulta necesaria para la prevención de un peligro real y grave para la seguridad pública o para la represión de infracciones penales y que, tratándose de datos especialmente protegidos, sean absolutamente necesarios para los fines de una investigación concreta.*

[748] Nótese la utilización de la expresión genérica de "Fuerzas y Cuerpos de Seguridad", todos ellos miembros de la Policía Judicial, pero sin entrar a precisar si éstos deben ser miembros de la PJE.

[749] Pueden leerse en la dirección www.aepd.es, partiendo del informe 1999/0000, de 16 de julio. El informe 213/2004 se pronuncia de una manera más específica ante una consulta sobre la cesión del número IP (atribuyéndole la condición de "dato personal" con arreglo a la LOPD), dando lugar a los requisitos que se transcriben en el texto. Con similar expresividad se pronuncia la AEPD en el informe 297/2005 y 133/2008, este último de fecha posterior a la promulgación de la LCDCE. Sobre la consideración de dato personal de la IP dice GONZÁLEZ LÓPEZ que *"entender que la conexión a Internet, que no necesariamente debe ir acompañada de una comunicación concurrente, constituye una comunicación es equiparable a sostener la condición de comunicación del envío de la señal a la antena de telefonía móvil a efectos de la ubicación del terminal en un área de cobertura. A nuestro entender, estas actuaciones técnicas, si bien pueden considerarse comunicación desde un punto de vista técnico, escapan al propósito ya apuntado de la comunicación (envío de mensaje de emisor a receptor) y constituyen, por ello, un presupuesto técnico necesario para hacer posible la comunicación"*. En esta opinión, entre otras que se aportan en este estudio, pueden residenciarse los puntos de vista que se sostienen sobre la desafección de este tipo de actos de conexión técnica del derecho al secreto de las comunicaciones. Vid. González López, Juan José. *Intervención de las comunicaciones: nuevos desafíos…op. cit.,* pág. 122.

[750] También, vid. Salom Clotet, Juan. *Incidencias de la nueva regulación…op. cit.,* pág. 149 y ss.

[751] Sumándose al parecer de otros juristas, DEL CASTILLO se muestra crítica con los pronunciamientos de la AEPD, considerando necesario el mandato judicial para la cesión de datos que conlleve una limitación de los derechos fundamentales. Vid. del Castillo Vázquez, Isabel-Cecilia. *Protección de datos…op. cit.,* pág. 424 y ss.

b) *Que se trate de una petición concreta y específica, al no ser compatible con lo señalado anteriormente el ejercicio de solicitudes masivas de datos*[752].

c) *Que la petición se efectúe con la debida motivación, que acredite su relación con los supuestos que se han expuesto.*

d) *Que, en cumplimiento del art. 20.4 de la LOPD, los datos sean cancelados "cuando no sean necesarios para las averiguaciones que motivaron su almacenamiento".*

Por ello, según el punto de vista de la AEPD, con arreglo al art. 11.2.a de la LOPD, *"cuando la cesión esté autorizada en una ley"*, los datos podían comunicarse a requerimiento directo de las Fuerzas y Cuerpos de Seguridad. Es evidente, por tanto, que con el nacimiento de la LCDCE queda prohibida en el ámbito de aplicación tan específica y útil cesión por la disposición expresa contenida en el art. 1.

Todo lo anterior, de no ser por el desafortunado defecto de previsión que tenía la derogada LSSI sobre los tiempos mínimos de conservación de datos[753], configuraba una poderosa herramienta para dinamizar las pesquisas de la Policía Judicial siempre que fuese empleada bajo los requisitos genéricos del principio de proporcionalidad.

La antigua redacción del art. 12 de la LSSI conllevaba por tanto, en lo positivo, un deseable y elevado grado de accesibilidad a los datos por parte de la Policía Judicial al no precisarse del mandato judicial que claramente instituye la LCDCE. En lo negativo, suponía un marco excesivamente impreciso que dificultaba una verdadera y eficaz regulación de la materia, urgida de una precisión sobre qué datos había que conservar.

El posicionamiento jurídico de la AEPD sobre el régimen de cesión de datos, de otro lado, es criticado por PÉREZ GIL[754] por considerarlo entusiásticamente invocado

[752] La expresión "solicitudes masivas de datos", huyendo de la búsqueda prospectiva o aleatoria, podría contraponerse al concepto de "obtención de inteligencia de datos" y obtener una mayor indulgencia de la AEPD al contener tal categoría en sus pronunciamientos en la línea de lo que se propugna en este trabajo.

[753] Lo que suponía una puerta de escape para el cedente, al no tener un tiempo mínimo de conservación de datos obligatorio, atribuible a un error en la redacción del precepto.

[754] PÉREZ GIL, en fechas anteriores a la promulgación de la LCDCE, al referirse a la forma de accesibilidad predicada por la AEPD para la PJ, comenta lo siguiente: *"…pero el alto tribunal suele considerar bastante una providencia sin motivación alguna para acordar su solicitud…Eso es lo que ocurre, por poner un ejemplo de en la STS 1219/2004 (Penal), de 10 de diciembre (ponente Saavedra Ruiz), FD 16.º Un dictamen de la Agencia de Protección de Datos fechado en 1999 vino a convalidar la idoneidad de las*

por la PJ como mejor forma de remover los obstáculos que les impiden gozar de una pretendida libertad de acceso.

En mi opinión, nada de esto debe ser interpretado con tanta prevención, pues la actividad de la PJ, en cualquier caso, es reflejo de su adaptación al estado evolutivo actual de la tecnología y de la propia complejidad de una sociedad en la que el actor criminal se inserta con total solvencia. En la satisfacción de este legítimo interés de la PJE, contrariamente a lo temido, la tecnología ayuda la mayoría de las veces a lograr un grado de injerencia menor por parte de los poderes públicos para lograr los mismos y legítimos fines de proteger los derechos fundamentales de las víctimas, que son las grandes olvidadas de nuestro tiempo.

Un avance tecnológico puede sustituir, vistas así las cosas, a un intrusivo registro personal por el pase por un menos intrusivo arco detector de metales. Un dato de geolocalización de BTS hace innecesaria la intervención del contenido de las comunicaciones si lo se desea saber es en qué área aproximada se utilizó un determinado terminal.

Mi punto de vista, por completo contrario a estos pareceres, es que la PJ participa del proceso penal con plena voluntad de servirlo, participando excepcionalmente en la limitación de los derechos fundamentales y contando en todo momento con el permanente respaldo del actor jurisdiccional como mejor garantía de su eficaz proceder y acogimiento a la seguridad jurídica necesaria para su labor diaria.

Por ello, donde realmente se aferra la PJ es a los adecuadamente interiorizados imperativos de raíz constitucional, propios del Estado de Derecho, de actuar con imparcialidad, neutralidad y sujeción al principio de legalidad, a los que se adhiere con tanta intensidad como lo hacen los Jueces, Fiscales y Secretarios Judiciales. A estos factores se unen además las cualidades específicas de la PJ que, de una forma resumida son: La idoneidad del modelo policial español para alcanzar las finalidades del proceso penal, la dependencia funcional de la PJ del Poder Judicial y su inmediatez

solicitudes de datos efectuadas por la PJ sin mandamiento judicial o requerimiento previo del Ministerio Fiscal, un fundamento al que todavía hoy se siguen aferrando los cuerpos policiales en sus requerimientos de aportación de datos". Vid. Pérez Gil, Julio. Investigación penal y nuevas …*op. cit.*, pág. 229.

a Jueces y Fiscales y su completo grado de autonomía respecto de la estructura orgánica para el ejercicio de la función específica consagrada en el art. 126 CE.

Finalmente, hay que añadir otros dos factores esenciales – y no precisamente menores - y que son o deben ser comunes a todos ellos: su exigente formación técnica y científica y la estricta perspectiva ética y deontológica que ha de acompañar a todos sus actos. Todo lo anterior, en mi parecer, configura una PJ merecedora de la más alta consideración dentro del proceso penal español.

Pero, en tanto la labor investigadora de la PJE ha de constreñirse con precisión a los imperativos de la LCDCE y a las orientaciones jurisprudenciales más restrictivas sobre el secreto de las comunicaciones, puede reconocerse en estos pronunciamientos jurídicos, también, alguna luz sobre la intensidad que merece la protección de un derecho fundamental, según sean las circunstancias en que se produce su limitación, lo que permitiría, en mi opinión, justificar alguna liberalidad jurídica más que acercase una mayor eficiencia en la labor policial de obtención de la IDACE, bien modulado sea, en cualquier caso, el principio de proporcionalidad en tan compleja tarea.

En efecto, en los razonamientos contenidos en el FJ 8 de la STS 1231/2003, de 25 de septiembre, se manifiesta una clara adhesión doctrinal a la postura de las SSTC 114/1984 y 70/2002 sobre la afectación al secreto de las comunicaciones y la reserva judicial en la materia pero, al mismo tiempo, se incluye una mención a la STC 120/2002, donde se introducen algunas matizaciones interesantes, que sugieren un menor peso específico del derecho fundamental identificado y que irían en la dirección indicada en los posicionamientos jurisprudenciales que hacen residir la limitación en el derecho a la protección de datos:

> *"La protección del derecho al secreto de las comunicaciones alcanza el proceso de comunicación del mismo, pero finalizado el proceso en que la comunicación consiste, la protección constitucional de lo recibido se realiza en su caso a través de las normas que tutelan la intimidad u otros derechos» ... «pues, y esto se subraya, el art. 18.3 CE contiene una especial protección de las comunicaciones, cualquiera que sea el sistema empleado para realizarlas que se declara indemne frente a cualquier interferencia no autorizada judicialmente».[…] «la entrega de los listados por las compañías telefónicas a la*

policía sin consentimiento del titular requiere resolución judicial, pues la forma de obtención de datos que figuran en los citados listados supone una interferencia en el proceso de comunicación que está comprendida en el derecho al secreto de las comunicaciones telefónicas del art. 18.3 CE pues incorporan datos relativos al teléfono de destino, el momento en que se efectúa la comunicación y su duración para cuyo conocimiento y registro resulta necesario acceder de forma directa al proceso de comunicación mientras esté teniendo lugar»".

Es decir, que una interpretación literal de las frases *"…interferencia en el proceso de comunicación que está comprendida en el derecho al secreto de las comunicaciones telefónicas del art. 18.3 CE…"* y *"…pero finalizado el proceso en que la comunicación consiste, la protección constitucional de lo recibido se realiza en su caso a través de las normas que tutelan la intimidad u otros derechos…",* en lo que haga referencia al acceso a los datos de tráfico almacenados, sugiere una identificación distinta de los derechos concernidos y notoriamente vinculada, a su vez, con la cuestión de la temporalidad.

En este mismo sentido, en la STC 123/2002, de 20 de mayo, se dice: *"…ahora bien, aunque el acceso y registro de los datos que figuran en los listados constituye una forma de afectación del objeto de protección del derecho al secreto de las comunicaciones, no puede desconocerse la menor intensidad de la injerencia en el citado derecho fundamental que esta forma de afectación representa en relación con la que materializan las "escuchas telefónicas", siendo este dato especialmente significativo en orden a la ponderación de su proporcionalidad".* Sobre este sugerente matiz, dice GONZÁLEZ-CUÉLLAR que *"la sentencia añade que la menor lesividad de la injerencia habrá de ser tomada en consideración en la ponderación de la proporcionalidad"*[755,756].

[755] Vid. González-Cuéllar Serrano, Nicolás. *Garantías constitucionales…op. cit.,* pág. 173.

[756] En este mismo sentido, LÓPEZ-BARAJAS dice que *"la aplicación del principio de menor intensidad en la injerencia se proyecta sobre el juicio de proporcionalidad, toda vez que éste determina si está justificado el sacrificio del derecho fundamental afectado en función de las circunstancias del caso concreto".* Vid. López-Barajas Perea, Inmaculada. *La intervención de las comunicaciones…op. cit.,* pág. 41. En materia del principio de menor intensidad de la injerencia, la autora se apoya en la STC 26/2006.

En estas matizaciones, pueden hallarse algunas orientaciones jurídicas que permitirán formar una nueva visión o juicio sobre la proporcionalidad que admita una interpretación ajustada al peso del derecho en trance de limitación y puesto en relación, a su vez, con la realidad social. Esta visión abre indudablemente, por tanto, algunas puertas a una nueva hermenéutica que concilie la realidad y el Derecho en el cada vez más complejo escenario del uso criminal de las TIC.

Consecuentemente, debe interpretarse que el acceso a los datos de tráfico, al tiempo de producirse la intervención de las comunicaciones, queda bajo la inequívoca esfera de protección del secreto de las comunicaciones del art. 18.3 CE, pero que, cuando la intervención ya ha culminado y los datos pasen a formar parte de una base de datos de la operadora, por el imperativo o la liberalidad que fuere, la intensidad de su protección jurídica será menor ya que habrá *"finalizado el proceso en que la comunicación consiste".* En este caso, en términos de su protección, se deberá hablar de las normas que regulen *"la intimidad u otros derechos"*[757].

En refuerzo de la visión que se propugna por mi parte, VELASCO, a quien por el interés de su visión transcribo literalmente sus palabras, poniendo el acento en la cuestión de la reserva de judicialidad, razona, con acierto, del siguiente modo:

> *"Finalmente, se plantea el problema de si hace falta o no mandamiento judicial para la observación de los datos de tráfico de las comunicaciones privadas, o exclusivamente y sólo para el conocimiento de su contenido.*
>
> *En el ámbito de la interferencia de los meros datos en las comunicaciones por soportes tradicionales como el papel, la información no protegida, como pueda ser la persona y dirección a que se remite la carta o el*

[757] En este sentido, RODRÍGUEZ LAINZ, con referencia a la jurisprudencia que viene analizándose, dice que *"los datos de tráfico, como datos relacionados con una comunicación, no dejan de serlo porque se obtengan de una base de datos de las reguladas en la LCDCE; seguirán siéndolo, «...con independencia de que estos datos se tomen en consideración una vez finalizado aquel proceso, bien de la lícita facturación del servicio prestado, bien de su ilícita difusión» — STC 123/2002, de 20 de mayo, Fto. Jco. 6.º—. Pero tales datos sufren en tal contexto una importante mutación, pues se desgajan del contenido de la comunicación, siempre protegida bajo el amparo del art. 18.3 de la Constitución, para pasar a ser datos de carácter personal, aún relativos a comunicaciones. Como nos dirán las SSTC 114/1984, de 29 de noviembre, 70/2002, de 4 de abril y 123/2002, de 20 de mayo: «...la protección del derecho al secreto de las comunicaciones alcanza al proceso de comunicación mismo, pero finalizado el proceso en que la comunicación consiste, la protección constitucional se realiza en su caso a través de las normas que tutelan la intimidad u otros derechos»".* Vid. Rodríguez Lainz, José Luis. *El principio de proporcionalidad…op. cit.*

conocimiento de la fecha en que ha llegado a su destino, es decir, de los datos adláteres, adjetivos o no de fondo y contenido de las comunicaciones privadas, se han considerado informaciones no susceptibles del amparo judicial (v. gr.: cartero o portero que informa a la policía de la fecha y destinatario y remitente de una carta que ha tenido que repartir), por lo que con más razón, dada la multitud de comunicaciones electrónicas que se practican actualmente, en principio tampoco los llamados datos de tráfico de éstas (número o clave identificadora, aparato emisor, receptor, titulares de los mismos, duración y fecha y hora de establecimiento y fin de la comunicación, localización física o destino del usuario, etc.), deben conseguirse bajo el amparo de un mandamiento judicial y su correspondiente auto razonado, porque si bien es cierto que la información que desprenden los datos de tráfico, bien estructurada, puede arrojar información susceptible sobre el investigado, no lo es menos que la policía siempre ha contado con registros a esos solos fines de investigación criminal y de protección ciudadana (principalmente el DNI, los antecedentes policiales, etc.), y el hecho de que ahora los datos de telecomunicaciones los custodien empresas privadas no es óbice para que sólo a la policía, por escrito y a esos efectos, se pueda dar la información sobre los datos de tráfico, tan numerosos, y conducentes a centrar la investigación y autoría definitiva, que el contenido (con intervención judicial) puede además probar o esclarecer.

La protección que dispensa la Constitución en su art. 18.3 a las comunicaciones privadas, y la limitación expresa a que se refiere el art. 18.4 sobre el uso de la Informática, como reservada a la ley, deben entenderse referidas exclusivamente a los datos principales, sustantivos o de contenido y no a los de tráfico.

[…]

En contra, no obstante, se posiciona la doctrina de la Consulta de la Fiscalía General del Estado 1/1999, de 22 de enero, sobre tratamiento automatizado de datos personales en el ámbito de las telecomunicaciones, según la cual todas las comunicaciones, y en especial las postales, telegráficas y

telefónicas son secretas, salvo resolución judicial, por así deducirse de los arts. 18.3 CE y 8.1 del CEDH que declara el derecho de toda persona al respeto de su correspondencia y con cita de la jurisprudencia del TEDH en los casos Amman, Malone y Dugdeon, se centra en la STEDH de 30 de julio de 1998, caso Valenzuela Contreras, cuando califica como injerencia de la autoridad pública en el ejercicio del derecho al respeto de la vida privada y de la correspondencia el registro mediante aparato contador de los números de teléfono marcados desde un determinado aparato, aun cuando este tipo de vigilancia no implique acceso al contenido de la conversación, ya que desde la perspectiva de los derechos fundamentales lo inviolable no sólo es el mensaje, sino todos aquellos datos relativos a la comunicación que permitan identificar a los interlocutores o corresponsales o constatar la existencia misma de la comunicación, su data, duración, y todas las demás circunstancias concurrentes, útiles para ubicar en el espacio y en el tiempo el hecho concreto de la conexión, lo que supone en definitiva que no cabe disociar, sin merma relevante de garantías, realidades tan sustancialmente integradas como son el mensaje y su proceso de transmisión.

Sin embargo no podemos compartir esta obsoleta doctrina, primero porque el derecho a la intimidad se debe graduar en función de lo que es lo íntimo (no se puede proteger igual el contenido que su vía de transmisión en todo caso), y en segundo lugar, de la protección concreta que hace su titular del mismo, que no es idéntica si se hace en lugares públicos, al acceso libre de la ajena discreción, que en privados, y que sólo afectará a los datos de tráfico si los considera tan esenciales al secreto y los protege con la misma intensidad que el propio contenido; de lo contrario se puede llegar al absurdo de proteger el contenido de las comunicaciones escritas más que las orales en función de la peculiaridad de sus modos de transmisión y no de dónde y cómo hayan sido transmitidas"[758].

[758] Vid. Velasco Núñez, Eloy. *Aspectos procesales de la investigación y de la defensa en los delitos informáticos.* Diario La Ley. Año XXVII. Número 6506. Viernes, 16 de junio de 2006.

Sobre los *"datos adláteres, adjetivos o no de fondo y contenido de las comunicaciones privadas"*, el autor introduce un nuevo elemento de contraste que, pese a su obviedad y simpleza, permite comparar y conciliar la indagación en el ámbito de los datos de tráfico de las comunicaciones electrónicas con lo que ha sido la actividad peculiar de la policía de todos los tiempos: buscar sagazmente datos que corroboren y permitan comprobar los hechos en sede penal. Y no sólo esto, sino hacerlo en beneficio exclusivo del proceso penal.

Así, VELASCO, con una particular crítica a la doctrina del TEDH de los casos *Amman, Malone, Dugdeon y Valenzuela Contreras* – que considera obsoleta -, pone esta fuente de datos en relación con otros registros que contienen también una sensibilísima información personal y cita, al efecto, las bases de datos del DNI o la de antecedentes policiales, lo que sugiere la poca pertinencia de sublimar[759] la que, sin inmiscuirse en el contenido material de las comunicaciones electrónicas, contiene los datos de tráfico asociados que, además, en su configuración material o técnica, contienen muy poca o ninguna información que, directamente, ofrezca datos identificativos de la personalidad a la que se vinculen.

La acerada crítica del autor estudiado alcanza también al enfoque dominante, ya expuesto en párrafos anteriores, por el que lo que se protege principalmente es el canal por el que la transmisión discurre y no, como debiera ser en buena lógica, el contenido esencial que motiva la necesidad de protección efectiva, esto es, la intimidad, como expresión genuina y real de lo humano en lo referido al secreto de las comunicaciones personales mantenidas en canal cerrado[760].

[759] Nótese también que el autor ofrece como referencia – un tanto aberrante, en mi opinión – el hecho de que el depósito de los datos de tráfico esté en manos de empresas privadas, como elemento coadyuvante de la necesidad de la protección radical que critica.

[760] En parecidos términos, y aún cuanto el siguiente comentario se refiere a la privacidad del domicilio, GONZÁLEZ-CUÉLLAR dice: *"Parafraseando al Tribunal Supremo estadounidense, la Constitución protege personas, no lugares"* (El autor cita como referencia el Caso *Katz vs EEUU* U.S. 347 de 1967). Por ello, me adhiero plenamente a la visión jurídica relativa a los derechos humanos que se centre, en primer lugar, precisamente, en la persona y no en conceptos artificiosos que, con toda la buena voluntad que se quiera, sacralicen acríticamente determinados aspectos como modo de conjurar los males que no aciertan a prevenir sobre los primeros.

Pero, ya es conocido el carácter formal y la autonomía jurídica del derecho al secreto de las comunicaciones[761,762], de contenido más amplio que el de la intimidad, con el que no existe una identificación absoluta, por lo que, cualquier revisión debe atenerse a estas sensibles circunstancias que tanto peso aportan al sistema jurídico español.

b) La jurisprudencia sobre el análisis del espectro radioeléctrico

En tiempos recientes, el TS se ha pronunciado sobre la injerencia de la PJE en determinados aspectos técnicos relacionados con las comunicaciones electrónicas que, sin tener relación con concretas actos de comunicación, afectaban únicamente a los dispositivos que las facilitan en relación con su inserción en el espectro radioeléctrico, todo lo cual había generado al principio alguna confusión sobre la más exacta naturaleza de los derechos fundamentales concernidos, resuelta finalmente a favor de la consideración de la injerencia leve.

Esta relativamente novedosa producción de jurisprudencia – ya consolidada en la línea claramente definida que se expondrá en este apartado -, hubo de reaccionar ante la evidencia de que no todo lo que se relaciona con las comunicaciones electrónicas supone una automática afectación del art. 18.3 CE[763].

La cuestión nuclear es que la tecnología policial ofrece formas de captar determinados DACE mediante procedimientos de análisis de la inserción de los

[761] Sobre el carácter formal del derecho al secreto de las comunicaciones, que ha llevado a considerar bajo la protección constitucional no sólo las comunicaciones íntimas, sino cualquier clase de comunicación, a modo de resumen, véanse las SSTC 114/1984 de 29 noviembre, 34/1996 de 11 marzo, 127/1996 de 9 julio, 58/1998 de 16 marzo, 123/2002 de 20 mayo, 70/2002 de 3 abril, 56/2003 de 24 marzo.

[762] Resulta clarificador en este punto el trabajo de LÓPEZ-BARAJAS, quien, sobre la proclamada *"autonomía y sustantividad del derecho al secreto de las comunicaciones"* por el TC, afirma que, en consecuencia, *"es perfectamente posible violar el secreto de la correspondencia sin atentar a la esfera íntima de una persona"*. Nótese, por tanto, la extraordinaria transcendencia de esta circunstancia de cara a la interveción legal de las comunicaciones. Vid. López-Barajas Perea, Inmaculada. *La intervención de las comunicaciones …op. cit*., pág. 31.

[763] En contra, vid. Rodríguez Lainz, José Luis. *Dirección IP, IMSI e intervención judicial de las comunicaciones electrónicas.* Córdoba, 2008.

dispositivos electrónicos de comunicaciones en el espectro radioeléctrico, pero con total independencia de su materialización en concretos actos de comunicación electrónica.

Consecuentemente, el acceso por la PJE a este tipo de datos de ningún modo podía tenerse como fruto de una limitación indebida del derecho al secreto de las comunicaciones pues, para obtenerlos, en ningún momento se había intervenido en comunicación electrónica alguna.

En efecto, los medios tecnológicos y los procedimientos operativos de averiguación de los códigos IMSI e IMEI que identifican respectivamente a las tarjetas de telefonía móvil y los terminales en los que se insertan[764], devienen actualmente en un recurso crítico[765] para abordar cualquier clase de investigación criminal. No en vano, los procedimientos de intervención de las comunicaciones y la cesión de sus datos asociados pueden solicitarse y obtenerse con referencia a uno u otro código. En este contexto, no parece posible la concertación delictiva o, al menos, se reducen sus posibilidades de éxito en sus expresiones más complejas, si no se cuenta con alguna forma de comunicarse por medio de la tecnología.

Aunque existen otras formas como la *VoIP*, la radiofrecuencia o los correos electrónicos, la telefonía móvil sigue siendo el recurso de referencia de los delincuentes para este fin. El estudio de las comunicaciones, en general, ocupa un lugar central en el proceso investigativo, dado que permite la obtención de inteligencia sobre la dinámica de la maquinación criminal junto con la adquisición de pruebas válidas para el proceso penal.

---

[764] LÓPEZ-BARAJAS, quien aporta interesante información sobre la materia, aun considerando la injerencia menor, *"no excluye que su tratamiento automatizado [el de las claves alfanuméricas que se obtienen] implique un significativo nivel de injerencia en la privacidad del interesado".* Estando fundamentalmente de acuerdo con esta autora, como trataré de sostener con apoyo en la jurisprudencia, se trata de un injerencia leve propia de la actividad indagatoria de la PJE y, consecuentemente, sin necesidad de control jurisdiccional como el que exige el art. 18.3 CE. Vid. López-Barajas Perea, Inmaculada. *La intervención de las comunicaciones…op. cit.,* pág. 50 y ss.

[765] El uso de los teléfonos móviles reducido a lo mínimo imprescindible, incluso con conexión a la red exclusivamente para su empleo breve e inmediato, la permanente renovación de los terminales o su adquisición sin el cumplimiento de las obligaciones de registro de usuario impuestas por la LCDCE, hacen que el análisis de las comunicaciones electrónicas adquiera una inusitada complejidad, donde la sagacidad y el sentido de la oportunidad de los investigadores se torna esencial.

De unos años a esta parte, los departamentos de apoyo tecnológico de los diferentes cuerpos policiales se han ido dotando de medios técnicos para este fin, como sería el caso del ***IMSI Catcher*** o ***Interrogador de IMSI e IMEI***[766], cuyos usos se extienden también a las funciones críticas de geolocalización de terminales de telefonía móvil, asunto del que se hablará más adelante.

Pero el uso de este imprescindible recurso no ha estado exento de polémica pues, una vez más y como mejor ejemplo de la falta de seguridad jurídica con que opera la PJE por causas que le son ajenas, el avance de la tecnología sobrepasó al Derecho generando dudas sobre la legitimidad de obtener los códigos sin contar con un mandamiento judicial previo[767].

En sentido contrario, por su extraordinario interés y valor ilustrativo sobre la naturaleza de los DACE, se incluye a continuación un análisis específico – y por todas las demás - de la Sentencia 249/2008, de 20 de Mayo de 2008, de la Sala de lo Penal del Tribunal Supremo, en la que se contiene una serie de pronunciamientos relevantes y acertados en cuanto al fondo de lo tratado en este trabajo, que han sido objeto de consolidación en varias STS posteriores.

---

[766] El *IMSI Catcher* es un instrumento de barrido que permite el análisis del espectro radioeléctrico y que, comportándose técnicamente como una más de las BTS de la constelación más próxima de las que dan servicio a los usuarios, registra pasivamente y de forma inadvertida sus códigos alfanuméricos IMSI e IMEI, sin que se interfiera en el normal funcionamiento de sus terminales (su funcionamiento es independiente de que el usuario esté o haya estado comunicando con su terminal). La información, por tanto, es referida a tantos IMSI e IMEI como personas y terminales estén en el momento del rastreo registrados en el aparato a efectos de obtener cobertura. De esta manera, se sabe cuál es el IMSI e IMEI objeto del interés de la investigación, pero únicamente por la mera exclusión de los demás números IMSI e IMEI no sospechosos y no captados de nuevo cuando vuelve a hacerse un rastreo en los diferentes lugares en los que el sospechoso sucesivamente se halla.
Este laborioso procedimiento – de naturaleza táctica por producirse la intervención con inmediatez al objetivo y por la consiguiente necesidad de establecer una específica operación de cobertura y seguridad – permite posteriormente la motivación del mandamiento judicial de intervención telefónica a partir del número IMSI o IMEI, es decir, sin mención alguna en la solicitud del número de abonado del sospechoso. Naturalmente, este proceso de rastreo no facilita la más mínima información sobre la identidad del usuario y, mucho menos, del contenido de las comunicaciones y, para que adquiera toda su eficacia, debe complementarse con informaciones ajenas a los datos meramente tecnológicos, todo ello para acreditar la procedencia de actuar como se solicita del juzgado.

[767] En este sentido, la STS 130/2007, de 19 de febrero, contiene un buen ejemplo, en lo negativo, de lo necesario que es el conocimiento previo y exhaustivo de las facetas técnicas sobre las que la Justicia ha de pronunciarse. La negativa percepción del Alto Tribunal en aquella ocasión sobre la antijuridicidad del procedimiento tuvo como consecuencia la puesta en libertad de varios narcotraficantes. Con posterioridad se ha consolidado la posición jurisprudencial contraria y que es objeto de breve análisis en este apartado.

El estudio de la jurisprudencia en torno al *IMSI Catcher* – aparato que se ha descrito en lo necesario para aclarar su intrascendencia para la limitación de los derechos fundamentales[768] -, metodológicamente debiera ubicarse en el apartado que se dedicará al análisis fenomenológico sobre determinados aspectos de la obtención de la IDACE por la PJE, lugar natural en el que se debería razonar sobre la idoneidad jurídica y técnica de su uso o, en suma, si se prefiere, donde se reflexionase sobre su admisibilidad para los fines del proceso penal de un Estado de Derecho.

Pero es también cierto que la proposición de una definición amplia de DACE incluida en apartados anteriores – lejana por completo de los arcaísmos que hicieron fortuna en los pronunciamientos originados por el Caso *Malone* del TEDH -, permitiría adaptar el concepto a las nuevas exigencias impuestas sucesivamente por la realidad de las TIC. En este sentido, el art. 33 LGT, apdos. 5 y 6, tiene una previsión para que, mediante Real Decreto, se pudiesen acoger en Derecho nuevas tipologías de datos, todo ello con escrupulosa justificación, además, en los principios de proporcionalidad y de mínima intervención.

Una mirada somera a la jurisprudencia, favorable hoy día al uso directo del *IMSI Catcher* por la PJE sin mandato judicial habilitante - que se tornó pacífica en 2008 tras una inicial rechazo del procedimiento en 2007 por considerarlo invasivo del secreto de las comunicaciones y ser por tanto materia de reserva judicial -, refleja las tensiones que se han puesto de manifiesto en apartados anteriores a propósito del disenso sobre sí se sacrificaba el derecho del 18.3 CE o a cualquiera de los demás que afectasen o no a la protección de datos o a la intimidad.

Pero en esta línea, lo que emerge de la discusión es la necesidad de identificar con precisión jurídica los derechos puesto en juego, a ser posible, desprendiéndose de determinados prejuicios en la idea de que la protección no debe situarse radicalmente

[768] Desde un punto de vista policial estrictamente práctico, es muy de lamentar, en general, la trascendencia pública del uso de los medios técnicos para la incautación legal de pruebas que aportar al proceso penal, todo ello, sin perjuicio de la necesidad hallar un punto de equilibrio entre ambas necesidades, sin que se resientan, ni por el debido sigilo de la técnica policial, ni porque se merme el derecho a la tutela judicial efectiva y a la derecho a la defensa consagrados en el art. 24 CE. En este sentido, basta una sencilla búsqueda en Internet para encontrar exhaustiva información sobre este y otros medios técnicos, con lo que se torna ridícula a estas alturas cualquier pretensión de discreción. Además, como es de ver, la jurisprudencia se ha ocupado de este asunto con detalle, contribuyendo de esta forma a su publicidad, cuestión que, por lo demás, no merece más comentarios.

en el derecho al secreto de las comunicaciones, sino que, por el contrario, es posible que no merezca siempre tan específico blindaje. O, dicho de otra forma, que es posible que si la protección de los derechos fundamentales deviene acrítica y radicalmente ubicada en el canal de comunicación, como se desprende del carácter formal y autónomo del derecho al secreto de las comunicaciones, difícilmente podrá centrarse en lo verdaderamente importante, que no es sino la protección de una de las formas más sensibles de manifestarse los individuos: el derecho al secreto de sus comunicaciones y no otra cosa.

De no aceptarse este punto de vista, en mi opinión, se cercenará la posibilidad de tratar racionalmente los fenómenos criminales propiciados por el uso de las TIC – de insospechada evolución en el futuro -, en la medida en que las visiones radicales confundan la protección que ha de darse a una conversación entre personas que está intermediada por un dispositivo técnico, con la que debe brindarse al direccionamiento IP de un ataque masivo de DoS en la escena internacional o, más simplemente, a la adquisición por la PJE de un DACE fuera de un acto de comunicación protegible por el art. 18.3 CE.

Por esta razón, conviene a la línea de argumentación en este momento hacer una parada para incorporar el análisis de la jurisprudencia mencionada, ya que la doctrina que contiene sobre la naturaleza jurídica de los DACE aconseja adelantar esta tarea, todo ello con la esperanza de contribuir a un mejor y más ajustado enfoque jurídico a lo que el Estado de Derecho demanda cuando se ve en la obligación de limitar los derechos fundamentales de sus ciudadanos.

El argumento de partida pretenderá demostrar que existen DACE que no se producen durante comunicación electrónica alguna y que pueden obtenerse por la PJE mediante el análisis del espectro radioeléctrico libremente y sin injerirse en el derecho al secreto de las comunicaciones de los sujetos investigados.

Pero antes de continuar, es necesario introducir algunas notas informativas sobre el escenario objeto de interés.

Con el objeto de situar al lector en la materia, se hace necesaria una referencia previa, más precisa de la ofrecida hasta ahora, de los siguientes conceptos de naturaleza estrictamente técnica:

- ***IMSI***: Es el acrónimo del inglés *International Mobile Subscriber Identity (**Identidad Internacional del Abonado a un Móvil**)*. Consiste en una relación alfanumérica indescifrable integrada en la ***tarjeta SIM***[769], que permite la conexión de los teléfonos móviles a las redes ***GSM*** y ***UMTS***[770] y que, de conocerse, vincularía el terminal móvil a un número de teléfono y este, a su vez, a un abonado[771]. El conocimiento del IMSI en sí mismo permite, con expresión de su única referencia, solicitar al Juez la intervención de las comunicaciones sin necesidad de aportar el número de abonado ni la identidad del suscriptor.
- ***IMEI***: Acrónimo del inglés *International Mobile Equipment Identity*, ***(Identidad Internacional de Equipo Móvil),*** que representa un código pre-grabado en los teléfonos móviles GSM y posteriores. Se trata de una relación alfanumérica que identifica a un terminal concreto de telefonía móvil con independencia de los IMSI y los demás datos de suscripción del servicio. No aporta información alguna sobre el usuario. El conocimiento del IMEI puede relacionar el terminal con diferentes IMSI que en el mismo se hayan utilizado, simultánea o alternativamente[772]. Los mandatos judiciales

[769] Acrónimo del inglés *subscriber identity module*, en español módulo de identificación del suscriptor. Son tarjetas desmontables que se insertan por el usuario en el teléfono móvil y que sirven para almacenar de forma segura la clave de servicio del suscriptor usada para identificarse técnicamente ante la red (no personalmente). Aunque existen diversas variedades de tarjetas según sea la característica técnica de la red de comunicaciones, por comodidad se usará en este estudio la denominación de "tarjetas SIM" para referirse de un modo genérico a los dispositivos que permiten el registro en la red de los usuarios de la telefonía móvil.

[770] El GSM es un sistema global para las comunicaciones móviles (acrónimo del francés *groupe spécial mobile),* también llamado red 2G. El UMTS o 3G es una red posterior de mayor velocidad para las comunicaciones telemáticas y que dispone de algunas características diferentes de la anterior. Actualmente se están implementando las redes 4G, completamente basadas en el Protocolo IP.

[771] Debe aclararse que el número de abonado sólo podrá conocerse si el Juez ordena a la operadora que lo relacione con el IMSI. Naturalmente, la identidad del abonado, por la misma razón, sólo será conocido si lo revela la operadora por orden judicial.

[772] Es común la tecnología que permite que una misma tarjeta SIM contenga diversos IMSI. Estos IMSI pueden corresponder a varios usuarios diferentes. Lógicamente, esta posibilidad permite a los delincuentes "despistar" a los investigadores. De todo esto se sigue la extraordinaria necesidad de intervenir, no la tarjeta de cada usuario, sino las tarjetas de usuario que se sirvan de un mismo IMEI para

permiten la intervención del IMEI, con lo que podrían intervenirse tantos IMSI como usuarios los insertasen en un mismo terminal.

- ***BTS***: Acrónimo del inglés *Base Transreceiver Station*, o ***Estación de Recepción y Transmisión*** de comunicaciones. Indica la posición geográfica de una antena de telefonía móvil a la que el terminal se ha registrado en el transcurso de una comunicación, a veces desde distancias de decenas de kilómetros. Permite la determinación de sectores de cobertura mediante procedimientos de triangulación cuando se lleguen a activar más de dos BTS, ubicando el terminal móvil en un lugar más o menos definido. No sirve para identificar concretos terminales dentro de los que se hallen en la zona triangulada[773].
- ***IP***: Número que determina una conexión a Internet dentro del *Protocolo TCP/IP*. No aporta en sí mismo información alguna sobre el usuario.

Entrando de lleno ya en la cuestión, y comenzando por el primer y negativo pronunciamiento jurisprudencial, se puede mencionar el caso de narcotráfico que fue objeto de la STS 130/2007 de la Sala 2ª, de 19 de febrero, donde la defensa de los acusados invocó en su recurso como motivo de casación, al amparo del artículo 5.4 LOPJ, la vulneración de los derechos constitucionales a la intimidad personal, al secreto de las comunicaciones y a la tutela judicial efectiva de sus defendidos en relación con las intervenciones de las comunicaciones telefónicas, por haberse utilizado por la PJE un dispositivo técnico que supuestamente desvelaba el número de abonado del teléfono móvil de los investigados.

De la lectura de la sentencia, y en lo que ahora interesa, cabe deducirse la inexacta, o más bien ausente, descripción del funcionamiento y utilidad real del aparato contenida en los fundamentos de derecho y sobre todo su posible transcendencia para los derechos fundamentales, al sostener el Magistrado Ponente que *"la policía, antes de acudir al juzgado en demanda de una autorización para intervenir los teléfonos de referencia, habría procedido por sus propios medios técnicos*

comunicar (terminal móvil, si se prefiere). Es decir, interviniendo un IMEI se intervendrán tantos IMSI como el usuario inserte en su dipositivo de comunicaciones.

[773] Si se hallase el usuario, por ejemplo, en un concurrido centro comercial, no sería posible identificarlo entre las numerosas personas que portasen sus propios terminales dentro de la zona de interés.

a injerirse en el curso de algunas comunicaciones telefónicas, consiguiendo así los números de los correspondientes a un determinado usuario", cosa absolutamente incierta ya que, como bien se demostró en sentencias posteriores, la PJE, para hacer uso del *IMSI Catcher*, en ningún momento necesita injerirse en comunicación alguna para obtener los datos IMSI e IMEI del terminal de telefonía objeto de investigación.

Se deduce también que semejante conclusión se extrae de la escasa o nula información técnica incluida en el proceso objeto del interés casacional – lo que no impidió que el tribunal se pronunciase con las graves consecuencias sobre la indebida libertad de los delincuentes que ya se mencionaron - y de la exigua, extemporánea e imprecisa aportación del testigo de la PJE examinado durante el juicio oral, ya que, según el Tribunal Supremo *"es lo que resulta del oficio que abre la causa en relación con la afirmación testifical antes transcrita, en la que el funcionario declarante precisó que el ingenio técnico utilizado permite la detección de "los números de teléfono que se están utilizando". Esto es, los que son objeto de un uso actual, obviamente, para el diálogo entre personas, como es lo propio de tales medios"*.

Es decir, que el Magistrado da por hecho que el PJE se ha injerido en el contenido de las comunicaciones personales, porque, en su opinión, esto sería imprescindible técnicamente para obtener los números de abonado y, todo ello, sin contar con el correspondiente y previo mandato judicial, hechos que, de verificarse, comportarían *"la imputación de una conducta penalmente relevante a los efectos de los arts. 197 y 198 CP"* sobre la revelación de secretos.

Hay que aclarar que lo que el *IMSI Catcher* en ningún caso proporciona, por impedirlo su configuración técnica, son los números de abonado, que sólo pueden conocerse si la operadora los facilita al requerírsele para que los vincule con los IMSI o IMEI aportados por el investigador (puede decirse de un modo sencillo que lo que circula por la red son los IMSI y no los números de abonado, que no son sino un artificio práctico para que el usuario interaccione su IMSI con los de los demás usuarios registrados en la red).

Por otro lado, y por mucho que se esfuerce la PJE en obtenerlo, el número de abonado no tiene tampoco valor identificativo por sí mismo pues, nuevamente, ha de

acudirse a las base de datos de la operadoras para la revelación de los datos del suscriptor.

Sin embargo, lo que sin mucha indagación le pareció obvio al Alto Tribunal resultó ser por completo incierto, no sólo desde un punto de vista técnico sino también jurídico, ya que el aparato en cuestión – un sofisticado analizador del espectro radioeléctrico - ni analiza teléfonos móviles, ni se utiliza en el curso de conversación telefónica alguna y, mucho menos, precisa de la más mínima injerencia en el contenido de las comunicaciones de los investigados[774].

Esta realidad fue luego reconocida en la trascendental STS 249/2008, de 20 de mayo, cuya doctrina fue reiterada en otras posteriores[775], donde de forma solvente quedó clara la no afectación al derecho fundamental consagrado en el art. 18.3 CE por el uso de la técnica en cuestión.

El asunto fue como sigue:

Habiendo sido un individuo condenado por la Audiencia Nacional por un delito de narcotráfico, su defensa basó los motivos de casación de la sentencia, entre otros, *"…al amparo del art. 5.4 de la LOPJ[776] y del art. 849.1 de la LCRIM, al estimar vulnerado el derecho fundamental al secreto de las comunicaciones sancionado por el art. 18.3 de la Constitución, al fundamentar el Tribunal "a quo" la sentencia en una prueba consistente en el empleo de unos mecanismos de barrido que permiten obtener los números IMSI de las tarjetas de telefonía prepago que se emplearon para comunicar con este recurrente, sin haber obtenido previamente la preceptiva autorización judicial"*.

[774] Por decirlo de forma muy simple, basta con que el usuario lleve encendido su móvil y guardado en su bolsillo para que el aparato puede obtener su IMSI e IMEI y, aún puede decirse más, con total independencia de que haya efectuado o no llamadas telefónicas o un uso de los servicios telemáticos a los que tenga acceso.

[775] SSTS 777/2008, de 18 de noviembre; 40/2009, de 28 de enero; 688/2009, de 18 de junio y 737/2009, de 6 de julio. En la STS 40/2009, como apunta LÓPEZ-BARAJAS, el tribunal considera incluso que *"el IMSI y el IMEI difícilmente pueden considerarse datos de carácter personal"* y que, equiparando su obtención a un vigilancia, el IMSI Catcher viene a funcionar como si fuera *"unos prismáticos especiales inalámbricos"*. Vid. López-Barajas Perea, Inmaculada. *La intervención de las comunicaciones…op. cit.,* pág. 56.

[776] Según la LOPJ, motivado por la mera vulneración de un precepto constitucional, en este caso el artículo 18.3 CE.

El Tribunal Supremo desestimó la petición comenzando por desentrañar la naturaleza del número IMSI, lo que no es poco acierto teniendo en cuenta lo difícil que resulta en ocasiones traer a un pronunciamiento jurisprudencial conceptos técnicos complejos, cuyo conocimiento previo y suficiente es fundamental.

Así, la sentencia se refiere al IMSI, tras otras especificaciones técnicas, como *"una serie de algoritmos integrados en la tarjeta SIM […] que integra indudablemente los datos de tráfico generados por la comunicación mediante telefonía móvil"*[777]. La cuestión para el ponente es, a partir de este momento, si el conocimiento mediante un rastreo sin mandamiento judicial expreso supone una injerencia en el derecho al secreto de las comunicaciones tutelado por el artículo 18.3 CE.

La sentencia hace perder vigencia a la doctrina nacida del famoso caso Malone al proclamar que *"a partir de esos datos, resulta obligado plantearse si la numeración IMSI, ajena al contenido de la comunicación propiamente dicho, encierra una información adicional que, pese a su carácter accesorio, se halle tan íntimamente ligada al secreto de lo comunicado que también merezca convertirse en objeto de protección constitucional. Como es sabido, la jurisprudencia constitucional, tomando como inspiración la STEDH de 2 agosto de 1984*[778] *- Caso Malone -, ha venido insistiendo en que la protección alcanza frente a cualquier forma de interceptación en el proceso de comunicación mientras el proceso está teniendo lugar, siempre que sea apta para desvelar, ya sea la existencia misma de la comunicación, el contenido de lo comunicado o los elementos externos del proceso de comunicación (Vid. SSTC 114/1984, de 29 de noviembre; 123/2002, de 20 de mayo; 137/2002, de 3 de junio; 281/2006, 9 de octubre. También, SSTS 1231/2003, 25 de septiembre y 1219/2004, 10 de diciembre*)".

Con fundamento en la sentencia del caso *Malone* – que el ponente identifica como *"un problema"* -, por la que se apreció que la técnica de *"open register o*

[777] En mi opinión, este específico fragmento ha de interpretarse con más precisión, ya que el IMSI, obviamente, es utilizado como dato de tráfico para establecer una comunicación electrónica, pero existe y puede ser accedido con independencia de que se produzca o no tal comunicación. Consecuentemente, tendrá una naturaleza doble, dependiendo de su uso como parte de una concreta comunicación electrónica o como mero elemento básico preordenado al registro técnico del teléfono móvil en la red de comunicaciones públicas.

[778] Nótese que esta trascendental sentencia es anterior a la aparición de la telefonía móvil e Internet.

comptage[779]*"* contravenía la protección otorgada en el artículo 8 CEDH (al considerar los datos de tráfico como parte de la comunicación), el Magistrado incorpora a la sentencia una referencia al cuerpo doctrinal que en su virtud se había constituido en España, para considerar a continuación su evidente inadecuación al Estado actual de evolución de los medios de comunicación privada y a su propia complejidad.

En efecto, y según la sentencia estudiada, el concepto de *"dato de tráfico"* a raíz de la Directiva 2002/58/CE desborda al utilizado en la sentencia del Caso *Malone*, proclamando que *"todo apunta a que la mecánica importación del régimen jurídico de aquellos datos a estos otros, puede conducir a un verdadero desenfoque del problema, incluyendo en el ámbito de la protección constitucional del derecho al secreto de las comunicaciones datos que merecen un tratamiento jurídico diferenciado, en la medida en que formarían parte, en su caso, del derecho a la protección de datos o, con la terminología de algún sector doctrinal, del derecho a la autodeterminación informativa (art. 18.4 CE)".*

A renglón seguido, la sentencia dice *que "la Sala no puede aceptar que la captura del IMSI por los agentes de la Guardia Civil haya implicado, sin más, como pretende el recurrente, una vulneración del derecho al secreto de las comunicaciones".*

Por otro lado, *"que la numeración del IMSI encierra un dato de carácter personal es conclusión que se obtiene por la lectura del art. 3.a) de la LO 15/1999, 13 de diciembre, de Protección de Datos de Carácter Personal, con arreglo al cual, dato personal es "...cualquier información concerniente a personas físicas identificadas o identificables".*

Con estos términos, la sentencia, de una forma altamente clarificadora, resume la aparente contradicción que se pretende poner de relieve en estas líneas y que hace que la obtención de un DACE no vinculado a determinados actos de comunicación haya llegado a merecer la confusa protección del secreto de las comunicaciones

[779] Método cuasi-artesanal al principio y, al final, llevado a cabo mediante un sencillo aparato, por el que se calculaba el número marcado por un usuario a base de interpretar el sonido característico producido por cada una de las diez cifras del dial de un teléfono fijo (o analizar el impulso eléctrico de la marcación). Adviértase que estamos hablando de los teléfonos antiguos de dial de rueda que producían un determinado sonido al girar según cuál fuese el dígito concreto que sucesivamente se marcase para completar el número de abonado. La sucesión de sonidos hacía colegir el número de abonado a los hábiles policías que lo escuchaban.

únicamente por la aplicación, extensiva y extemporánea, de la reserva jurisdicicional establecida en una ley ordinaria[780,781], la LCDCE, cuando la realidad informa sobre la naturaleza inocua de los análisis del espectro radioeléctrico practicados por la PJE para injerirse en el contenido material o formal de comunicación personal alguna.

El ponente, con una referencia previa a la LOPD, lo expresa así*:*

> *"…está fuera de dudas que el IMSI, por sí solo, no es susceptible de ser incluido en alguna de esas dos categorías. Ni es un dato integrable en el concepto de comunicación, ni puede ser encuadrado entre los datos especialmente protegidos. Como ya se razonó supra, ese número de identificación sólo expresa una serie alfanumérica incapaz de identificar, por su simple lectura, el número comercial del abonado u otros datos de interés para la identificación de la llamada. Para que la numeración IMSI brinde a los investigadores toda la información que alberga, es preciso que esa serie numérica se ponga en relación con otros datos que obran en poder del operador. Y es entonces cuando las garantías propias del derecho a la autodeterminación informativa o, lo que es lo mismo, del derecho a controlar la información que sobre cada uno de nosotros obra en poder de terceros, adquieren pleno significado. Los mismos agentes de Policía que hayan logrado la captación del IMSI en el marco de la investigación criminal, habrán de*

[780] No obstante, en relación con el carácter de ley ordinaria de la LCDCE, tal y como afirma DÍAZ MARTÍNEZ refiriéndose de un modo general sobre la limitación de los derechos fundamentales, *"un presupuesto común para todo acto limitativo de algún derecho fundamental lo constituye el principio de legalidad, según el cual toda injerencia del poder público en los derechos fundamentales requiere que haya sido autorizada o habilitada por una disposición con rango de Ley y que la norma legal habilitadora de la injerencia reúna las condiciones mínimas suficientes requeridas por las exigencias de seguridad jurídica y certeza del Derecho, para aportar al individuo una protección adecuada contra la arbitrariedad"*. El autor se apoya en la STC 49/1999 y en las SSTEDH 24 de abril de 1990, caso *Kruslin y Huvig*; 30 de julio de 1998, caso *Valenzuela*; 20 de mayo de 1999, caso *Rekvényi*; 25 de noviembre de 1999, caso *Hashman y Harrup*; 16 de febrero de 2000, caso *Amann*; 4 de mayo de 2000, caso *Rotaru*. Vid. Díaz Martínez, Manuel. *La dudosa constitucionalidad..op. cit*.

[781] Sobre la cuestión de la reserva de ley orgánica, vid. González López, Juan José. *Comentarios a la ley 25/2007…op. cit*., y González López, Juan José. *Los datos de tráfico…op.cit.,* pág. 425. RODÍGUEZ LAINZ la zanja diciendo que *"bastaría con recordar una constante Jurisprudencia de nuestro Tribunal Constitucional, representada entre otras por las SSTC 37/1989, de 15 de febrero, 207/1996, de 16 de diciembre, 70/2002, de 3 de abril, y, por citar entre las más recientes la ya calendada STC 206/2007, de 24 de septiembre, que advierte que la Constitución no establece taxativamente un principio de reserva jurisdiccional para la restricción de derechos fundamentales, más allá de aquellos específicos supuestos en que así se establezca en la Carta Magna o en que la gravedad de la afectación del derecho así lo exija taxativamente (principio de la reserva judicial absoluta)"*. Vid. Rodríguez Lainz, José Luis. *El principio de proporcionalidad…op. cit.*

solicitar autorización judicial para que la operadora correspondiente ceda en su favor otros datos que, debidamente tratados, permitirán obtener información singularmente valiosa para la investigación. En definitiva, así como la recogida o captación técnica del IMSI no necesita autorización judicial, sin embargo, la obtención de su plena funcionalidad, mediante la cesión de los datos que obran en los ficheros de la operadora, sí impondrá el control jurisdiccional de su procedencia".

Es decir que, a partir de esta sentencia, el procedimiento técnico-policial de determinación del IMSI y el IMEI que se ha descrito puede hacerse sin solicitud de una autorización judicial previa y sin basar su régimen jurídico en el art. 18.3 CE. Consecuentemente, el Instructor Policial no tendrá ninguna obligación de desvelar el uso de esta tecnología sin con ello propiciar alguna limitación de los derechos contenidos en el art. 24 CE.

Una vez obtenidos los códigos alfanuméricos, sin valor identificativo alguno por sí mismos, el instructor de las diligencias policiales habrá de dirigirse a la Autoridad Judicial para, de forma motivada, solicitarle que libre el correspondiente mandamiento judicial dirigido a la operadora de que se trate para que ceda "a los agentes facultados" los datos que los individualicen y los demás que, en relación con estos, expresamente consten en el mandato, incluido el inicio de una intervención del contenido material de las comunicaciones conducidas a su través.

D. Las salvaguardas tecnológicas. La polémica del SITEL.

a) La PJE en la instaruación de las salvaguardas

La Ley, *ex* arts. 117 CE y 7 LOPJ, junto con la consolidada doctrina y la jurisprudencia, confían la preservación de las garantías constitucionales del proceso penal principalmente en la figura del Juez, sin perjuicio de las funciones atribuidas al Ministerio Fiscal *ex* arts. 124 CE y 1 y 3 EOMF.

Sin embargo, en mi opinión, el resultado de tan trascendental propósito no puede descansar exclusivamente en la acción de uno o varios individuos, por más que los actores jurisdiccionales se constituyan en el elemento superior de esta función pues, para que se alcancen tan importantes finalidades, necesitarán contar con el auxilio de un conjunto multidisciplinar y equilibrado de recursos personales y materiales que aporten al proceso penal toda su seguridad y eficiencia en este punto, pretensión que, en modo alguno, debe orientarse al logro de un indeseable vaciamiento o invasión de las facultades jurisdiccionales.

Por ello, podría hablarse, en términos generales, de la existencia de tres elementos esenciales: De un lado, el ya mencionado actor jurisdiccional, como depositario principal de las funciones de preservación de las garantías constitucionales; de otro, según lo descrito en el Capítulo II, la acción de la PJE como su auxiliar (en el ejercicio y materialización de la dependencia funcional), dada su sujeción al principio de legalidad, su imparcialidad, neutralidad e idoneidad para las funciones técnicas de investigación y, finalmente, la instauración de las debidas salvaguardas de todo orden, tanto jurídicas como tecnológicas, que contribuyan indubitadamente a las garantías de autenticidad, veracidad e integridad de las evidencias legales de cualquier naturaleza que hayan de someterse al futuro proceso de contradicción y valoración durante el acto de juicio oral.

Es sobre este último punto sobre el que resta reflexionar con alguna mayor profundidad, ya que el ámbito de interés de este estudio, centrado en la evidencia

digital producida por las TIC, necesita de dispositivos técnicos que aseguren su recogida de un modo seguro y eficiente de cara al proceso penal.

En efecto, los diversos medios técnicos suelen gozar, en general, de una previa aceptación jurídica en cuanto a su idoneidad técnica para las finalidades a las que se destinan, lo que no les libra de haber sufrido, lamentablemente, algunas dudas o incomprensiones como las que rodearon el uso del *IMSI Catcher*.

Sin embargo, en el caso de que los avances de la tecnología ofrezcan, ahora o en el futuro, nuevos dispositivos útiles para la recogida de la evidencia digital, se hará necesario extremar las medidas de salvaguarda o certificación sobre la autenticidad y veracidad de su producto, de modo que, por su eficiencia, los debates procesales se centren exclusivamente en la contradicción de la prueba en sí misma, evitándose que, por innecesario, se desplacen al modo o los medios con los que se obtuvo.

Es necesario, consecuentemente, contar con instrumentos técnicos que se apoyen en los recursos que la propia tecnología y las disposiciones legales facilitan, entre los que cabe mencionar desde el principio, naturalmente, la aplicación de la Ley 59/2003, de 19 de diciembre, *de firma electrónica,* a los documentos que se incorporen al atestado.

b) Idoneidad de los medios técnicos de investigación. La certificación

En lo referido a la idoneidad de los propios instrumentos técnicos - cuya existencia y capacidades, por evidentes razones de sigilo, sería necesario que se mantuviesen al margen del conocimiento público, siempre que esto no supusiera un sacrificio inaceptable a los derechos contenidos en el art. 24 CE -, debiera ser objeto de ***certificación*** por algún organismo público habilitado al efecto, como sería el caso del ***Instituto Nacional de Tecnologías de la Comunicación*** (**INTECO**) o la que realizan los servicios del ***Centro Criptológico Nacional***, a través del **CCN-CERT**[782].

[782] Véase https://www.ccn-cert.cni.es/index.php?option=com_content&view=article&id=12&Itemid=32&lang=es

Respecto de la primera institución mencionada, en el *Convenio Marco de Colaboración en materia de ciberseguridad entre la Secretaría de Estado de Seguridad del Ministerio del Interior y la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información del Ministerio de Industria, Energía y Turismo*, se establece, entre otras cosas, la posibilidad de que el INTECO certifique la idoneidad de los medios técnicos de investigación en relación con las necesidades procesales[783].

De forma alternativa al INTECO, podrían ejercerse similares funciones por el ***Organismo de Certificación*** (OC) del ***Esquema Nacional de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información*** (ENECSTI)[784], que se articula en el ámbito de actuación del Centro Criptológico Nacional, según lo dispuesto respectivamente en la Ley 11/2002, de 6 de mayo, *reguladora del Centro Nacional de Inteligencia*, y el Real Decreto 421/2004, de 12 de marzo, *por el que se regula el Centro Criptológico Nacional*[785], llevando a cabo la labor de certificación[786] del producto previa la realización de una evaluación de la seguridad[787].

---

http://www.oc.ccn.cni.es/
http://www.commoncriteriaportal.org/

[783] Véase http://www.inteco.es/. En la cláusula segunda del Convenio Marco, sobre las aportaciones de las partes, se recoge en el apdo. 2 la posibilidad de ofrecer un soporte técnico a las investigaciones y peritajes, en cuyo subapartado b) se incluye la *"certificación de procedimientos y herramientas empleados por las FCSE, de cara a respaldar su validez procesal"*.

[784] Como se indica en la información disponible en el portal *web* oficial del CCN-CERT, "el ámbito de actuación del Organismo de Certificación comprende a las entidades públicas o privadas que quieran ejercer de laboratorios de evaluación de la seguridad de las TI en el marco del Esquema, y a las entidades públicas o privadas fabricantes de productos o sistemas de TI que quieran certificar la seguridad de dichos productos en el marco del Esquema y cuando dichos productos o sistemas sean susceptibles de ser incluidos en el ámbito de actuación del Centro Criptológico Nacional".

[785] El Organismo de Certificación certifica la seguridad de productos y sistemas de tecnologías de la información, según lo establecido en el procedimiento del Capítulo V (Certificación de productos y sistemas), y atendiendo a los criterios, métodos y normas de evaluación de la seguridad indicados en el Capítulo VI (Criterios y metodologías de evaluación del citado Reglamento de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información).

[786] Según informa el CCN-CERT, *"se entiende por certificación la determinación, obtenida mediante un proceso metodológico de evaluación, de la conformidad de un producto o sistema con unos criterios preestablecidos. Es decir, el reconocimiento de la veracidad de las propiedades de seguridad de la correspondiente Declaración de Seguridad"*.

[787] Según informa el CCN-CERT, *"se entiende por evaluación el análisis, realizado mediante un proceso metodológico, de la capacidad de un producto o sistema para proteger la propiedad de seguridad de la información de acuerdo a unos criterios establecidos, todo ello con objeto de determinar si puede ser certificado"*.

c)Análisis del voto particular a la STS 1215/2009 sobre la idoneidad del SITEL

Lamentablemente, los esfuerzos de la Administración, y particularmente de la PJE, por dotarse de los mejores instrumentos de investigación no cuentan siempre con la confianza de los operadores jurídicos.

En efecto, como ejemplo de esta afirmación, en el voto particular de fecha 1 de febrero de 2010, emitido por los Magistrados Sres. MARCHENA y MAZA sobre una de las SSTS que apreciaron con rotundidad la idoneidad del SITEL[788] para el proceso penal (concretamente, la STS 1215/2009, que resolvió el Recurso de Casación 404/09[789]), se contienen afirmaciones del todo inexactas sobre la calidad de las salvaguardas del SITEL[790,791], que comienzan sembrando la duda, tanto sobre su eficacia como evidencia legal, como por la expectativa de manipulación de que podrían ser objeto, hecho este último que no deja de llevar aparejado su correspondiente y desalentador tanto de desconfianza en la PJE[792]:

> *"…la eficacia probatoria a esos DVD [los producidos por el SITEL]...supone un retroceso para las garantías del proceso penal…caracterizada precisamente por su volatilidad y las infinitas posibilidades de manipulación y tratamiento".*

[788] Un interesante y actualizado estudio del SITEL puede leerse en Vid. López-Barajas Perea, Inmaculada. *La intervención de las comunicaciones…op. cit.,* pág. 201 y ss.
[789] *Ibídem*.
[790] El SITEL cuenta con la certificación facilitada en su día por la Fábrica Nacional de Moneda y Timbre (FNMT). La creación con posterioridad del CCN-CERT, que ahora se propone a los efectos de este estudio es, naturalmente, sin perjuicio de otras posibilidades pues, lo que interesa, es la calidad de la certificación en sí misma y su admisibilidad para la seguridad de la prueba digital y no qué organismo la provea.
[791] Aprovecho la ocasión para negar que el SITEL permita el acceso a los datos conservados por la LCDCE, como afirma erróneamente GONZÁLEZ LÓPEZ, sino tan sólo aquellos DACE que se produzcan como consecuencia de la intervención judicial de las comunicaciones en curso y que hayan sido objeto de una orden judicial separada, específica, precisa y motivada sobre los términos de su cesión. Lamentablemente, como ya se ha indicado, los datos que se piden y reciben en cumplimento de la LCDCE, sorprendentemente, circulan entre la PJE y las operadoras "en analógico", vulgo, papel. Vid. González López, Juan José. *Intervención de las comunicaciones: nuevos desafíos…op. cit.,* pág. 135.
[792] Es constante entre los más conspicuos juristas la exhibición de argumentos hipergarantistas que parecen ir orientados a imponer una especie de "notarización", si se permite el neologismo, de la actividad de la PJE, para evitar que contamine la pureza de las pruebas que aporta al proceso penal. La cuestión es que, si se desconfía de un sistema tan sofisticado de salvaguardas como el que protege el SITEL, qué no se hará con los testimonios de la PJE o con sus hallazgos durante los registros domiciliarios, donde no existen salvaguardas de semejante eficacia.

El voto particular, además, contiene un constante lamento por la situación en la que queda el juzgador al verse supuestamente obligado a hacer *"un acto de fe"* sobre la autenticidad e integridad del contenido que en el soporte DVD entrega la PJE, pese a reconocer que el sistema de captación y entrega de los contenidos por la operadora a la PJE mediante un canal tecnológico seguro gozan de todas las salvaguardas impuestas por la Ley y, especialmente, por las establecidas en la Ley 59/2003, de 19 de diciembre, *de firma electrónica*, y la Orden ITC/110/2009, pero que este intercambio tecnológicamente seguro no alcanzaba al Tribunal.

De las anteriores circunstancias cabe extraer o analizar dos aspectos muy interesantes para la finalidad de este estudio: De un lado, el hipergarantismo triunfante en algunos pronunciamientos jurisdiccionales basado, en ocasiones como las que nos ocupa, en apreciaciones infundadas y en la indisimulada desconfianza en la labor de la PJE, que tanto entorpecen el éxito de la Justicia y, de otro, en la necesidad de incorporar urgentemente a la Administración de Justicia, en su conjunto, las facilidades para el enjuiciamiento ofrecidas por las TIC, y entre ellas, muy especialmente, las orientadas al intercambio en canal seguro de documentos de cualquier clase y evidencias electrónicas autenticadas por las más eficaces salvaguardas tecnológicas, todo ello en beneficio del proceso penal y de la más estricta impartición de Justicia (Por ejemplo, para adoptar decisiones limitativas de derechos fundamentales en tiempo y forma).

Estas cuestiones quedan reflejadas de forma comprensiva en el siguiente párrafo del voto particular:

> *"Pues bien, la lectura detenida de ambos textos normativos -en especial, de este último, que fija los requerimientos técnicos exigibles para la ejecución de la orden judicial de interceptación-, pone de manifiesto que todas las garantías y reservas que el sistema incorpora, sólo miran a la relación entre los agentes de policía facultados y las operadoras de telefonía. La citada OM 110/2009, contempla la necesidad de crear lo que denomina "... bloques funcionales o interfaces del sistema de interceptación legal", arbitra varios canales seguros y resuelve los niveles de seguridad exigibles en la dirección bilateral que ha de establecerse entre la Policía y las operadoras para la gestión*

de la orden judicial de injerencia. El problema radica en que todo ese sistema de controles y garantías se arrincona cuando los agentes facultados vuelcan en un DVD las conversaciones que estiman más relevantes y se presentan ante el Juzgado, mediante una comparecencia personal, aportando un soporte electrónico con vocación de originalidad. Éste es el problema de origen que nos impide avalar el funcionamiento del sistema integrado (SITEL) que, si bien se mira, no lleva su vocación integradora hasta sus últimas consecuencias, pues se olvida de integrar a los órganos jurisdiccionales en el esquema que define su funcionamiento"[793].

Su primera parte viene referida a la normativa precitada en relación con la cuestión de la inexplicable ausencia del actor jurisdiccional en el intercambio de la evidencia electrónica a través de un canal seguro, lo que no merece sino la más entusiasta adhesión por mi parte como representación de uno de los elementos claves para la modernización de la Justicia[794].

No obstante, he de mantener mis reservas sobre la aceptación de tales pretensiones por parte de un estamento judicial que pueda sentirse inquietado en su independencia si se le exigiese imbricarse en un sistema de mensajería que, de alguna forma, le reposicionaría dentro del proceso penal frente a otros operadores jurídicos con los que suele mantener una perceptible distancia[795,796].

---

[793] Y un poco más adelante, rematan los disidentes: *"Sin embargo, en el momento decisivo de su incorporación al proceso penal, para su valoración como fuente de prueba, la relación del órgano jurisdiccional con esos mismos agentes, recupera el añejo sabor artesanal de las comparecencias personales, aportando un documento cuyo contenido ha de ser acatado sin cuestionar su integridad"*. Es de hacer notar la poca calidez con que los magistrados se refieren a una PJE que hace años que ha apostado firme y decididamente por la modernidad en términos de investigación, innovación y desarrollo aplicados a sus procedimientos técnicos y, muy especialmente, los orientados a satisfacer las necesidades de los Tribunales de Justicia bajo cuya dependencia funcional actúan.

[794] *"…la existencia de tres sujetos funcionales distintos: a) las operadoras de telefonía - sujetos obligados-; b) los funcionarios de policía - agentes facultados-; c) los Jueces de instrucción que autorizan la interceptación y que se convierten en destinatarios últimos del resultado de las escuchas".* Deseo fervientemente que esto llegue a ser así.

[795] Por ejemplo, reclamando la urgente disponibilidad de un Juez de Garantías para adoptar resoluciones jurisdiccionales en casos de urgencia vital en tiempo real que pudieran provenir de la PJ u otros órganos de las FFCCSS.

[796] PÉREZ GIL a este respecto comenta que "s*in embargo, cuando eventualmente han de presentarse ante un Juez en demanda de tutela jurídica, lo habitual en el marco del proceso es su trasvase al mundo analógico… El fantasma de la burbuja tecnológica se hace presente, así, en el ámbito procesal, imbuyendo la práctica judicial de una desconfianza hacia el formato electrónico no siempre exteriorizada manifiestamente, pero ciertamente presente en la mayoría de las ocasiones".* Vid. Pérez Gil, Julio. *Brecha*

Pero es en la segunda donde los magistrados yerran incomprensiblemente al atribuir a la PJE la potestad de entregar al Juzgado unos DVD conteniendo *"lo que les parece relevante",* es decir, una relación de datos compilada según el particular criterio de la PJE.

Todo esto es indicativo, además de lo dicho sobre la inusitada desconfianza que desprende (aunque esto no se constituya en un valor procesal ni tenga un contenido jurídico reconocible), del pretendido ejercicio de una facultad de la que en ningún caso gozan los agentes facultados, pues los DVD que produce el SITEL[797], precisamente por imperativo de las sofisticadas salvaguardas tecnológicas que contiene de acuerdo con la normativa legal[798], no pueden ser modificados arbitrariamente – y menos maliciosamente - por la PJE sin dejar un rastro perfectamente perceptible, actividad esta que constituiría, por lo demás, un grave delito[799,800].

Lo anterior contraría de forma verificable la errónea idea expuesta por los magistrados disidentes de que el contenido de las intervenciones podría ser fácilmente manipulado por los agentes y, es de imaginar, respondiendo a sus torticeras intenciones, ya que el SITEL produce unos DVD que representan fielmente el contenido auténtico, veraz e íntegro de las intervenciones telefónicas[801].

---

digital en el proceso español: empeños normativos frente a la realidad. INCLUSÃO DIGITAL E GOVERNO ELETRÔNICO. Lefis series. Zaragoza: Prensas universitarias, 2008, Vol. 3, 3, págs. 53-74, pág. 54.

[797] Considerados por el TS con fuerza probatoria documental, con referencia expresa al art. 318 LEC, en SSTS 1215/2009, de 30 de diciembre (FD 1), - que viene comentándose - y 105/2011, de 23 de febrero (FD C, 16), entre otras.

[798] A los DVD del SITEL, como a las hoy obsoletas cintas magnetofónicas que contenían las antiguas intervenciones telefónicas, se les debe conceder valor como prueba documental con su correspondiente valor probatorio siempre *"que venga precedida por su previa introducción en el proceso y su audición en el juicio oral".* Por todas, STS de 6 de abril de 1994 (RJ 1994, 2889).

[799] Nótese que en la STS discutida por los disidentes se hace un comentario sobre la injusta imputación de delito que implícitamente se le hace a la PJE, por mucho que los magistrados quieran ver en este aspecto un "desenfoque" de la cuestión. Es necesario insistir, una vez más y ya parece ocioso, en el hecho de que de lo que se está hablando en este estudio no es de los miembros de la PJE que sean delincuentes, sino del leal ejercicio de la PJ de las funciones encomendadas por el art. 126 CE.

[800] Acierta el Tribunal sentenciador, por tanto, al considerar que *"... la autenticidad del contenido de los discos está fuera de discusión. Si en alguna ocasión las partes personadas estiman que los discos depositarios de la grabación no responden a la realidad, deberán explicar suficientemente en qué basan su sospecha en cuanto que están acusando de un hecho delictivo a los funcionarios que se encargan del control del sistema SITEL".*

[801] En la propia STS comentada, el ponente deja este punto meridianamente claro en los Fundamentos de Derecho al describir el SITEL, afirmando que *"la evidencia legal del contenido de la intervención es aportada por el Servidor Central, responsable del volcado de todos los datos a formato DVD para entrega a la Autoridad Judicial competente…El contenido de los DVD sobre los que se han volcado las grabaciones impresas en el disco duro, gozan de presunción de autenticidad, salvo prueba en contrario"*.

Su estructura lógica no consiste en el mero grabado de una sucesión de archivos de sonido correspondientes a cada llamada telefónica completa y que puedan suprimirse fácilmente y, mucho menos, modificarse a gusto de la PJE. Al contrario, el SITEL produce unos DVD provistos de un sellado tecnológico o *hash* y el correspondiente *time stamping*, de los que ya se ha hablado, que individualizan todos y cada uno de sus archivos e impiden cualquier clase de manipulación.

Pero si esta se produjese, el sistema generaría toda suerte de elementos de contraste que evidenciarían sin género de duda el hecho de la manipulación, incluso a la mera inspección ocular de un lego en la materia y, naturalmente, no resistiría ni el más mínimo análisis forense, ni el cotejo con una segunda copia ofrecida por el SITEL al usuario de la PJE, ni el que se hiciese con la contenida en los servidores centrales del propio SITEL y, muchos menos, el contraste con los DACE conservados por la propia operadora[802], ajena, por supuesto, a las torticeras intenciones de la PJE.

Todos estos contrastes suponen en la práctica un eficaz, sucesivo, inequívoco e ingente medio de prueba para realizar las más exhaustivas comprobaciones orientadas a resolver la más mínima duda sobre la autenticidad, veracidad o integridad planteada por cualquiera de las partes y sin necesidad, por si fuera poco, de presentar una pericia previa que lo justificase sino, tan sólo, una mera conjetura fundada en la más generosa interpretación del art. 24 CE[803] que, eso sí, deberá ser probada en su momento mediante la correspondiente pericia.

Es particularmente injusto, por inexacto y desatento, el siguiente pronunciamiento de los magistrados disidentes:

> *"En ese instante, los canales seguros y las interfaces que la Orden ITC/110/2009 impone a operadoras y agentes facultados, dejan paso a un incontrolado volcado de datos que, lejos de ser transmitidos por vía telemática, se presentan ante el Juzgado de instrucción por un agente de policía que afirma*

[802] Curiosamente, en ninguno de los numerosos documentos que he estudiado para la preparación de este trabajo he hallado la menor reserva o duda sobre el recto proceder de las operadoras, lo cual me parece procedente, faltaría más. Siempre se ha dado por supuesto que, de manipularse algo relacionado con al intervención de las comunicaciones, sería por parte de la PJE. Las operadoras, siempre al margen de cualquier sospecha.

[803] SSTS 1075/2004, de 24 de septiembre, y 1566/2005, de 30 de diciembre. En una interesante apreciación, los magistrados recuerdan la accesibilidad procesal a lograr la impugnación aún no contándose con una previa prueba pericial, según la STS 593/2009, de 8 de junio).

haber seleccionado aquellos fragmentos que considera relevantes para la investigación…Los Jueces de instrucción se transforman así en meros receptores de unos soportes electrónicos cuyo contenido no puede apoyarse en otra garantía que la confianza acrítica en la profesionalidad de los agentes que se los proporcionan".

d) Papel de la PJE en la intervención de las comunicaciones a través del SITEL

Continuando con el análisis planteado en el apartado anterior, lo que los agentes facultados en realidad hacen cuando se sirven del SITEL, además de lo ya expuesto, es lo siguiente:

- Aportar al proceso penal el ***elemento objetivo***[804] proporcionado por el SITEL, entregando en el Juzgado de Instrucción los soportes ópticos originales provistos del sellado tecnológico producido directamente por el sistema, mediante diligencia incluida en el atestado policial[805], con los contenidos íntegros y auténticos de las intervenciones telefónicas y de sus correspondientes DACE, tras haber sido todo ello previamente ordenado a través una resolución judicial motivada. Estas grabaciones, en los momentos procesales oportunos, quedan sometidas a la fe pública judicial y a la disposición de las partes para que sean examinadas sin otras restricciones que las imponga la seguridad de sus propios soportes y la buena fe procesal y, en su virtud, permitir la representación de las objeciones que se estimen pertinentes, incluido la sospecha y prueba de una manipulación[806].
- Aportar al proceso penal el ***elemento subjetivo*** como resultado de la valoración policial, no vinculante, del contenido de las intervenciones

[804] Sobre el material probatorio, véase la STS de 16 de mayo de 2003 (RJ 2003, 4385), donde se indica que *"son las cintas grabadas (sic) y no las transcripciones".*
[805] Y en el futuro, deseablemente, constituirse en mero corresponsal del SITEL si se activa una conexión telemática segura para la Oficina Judicial.
[806] Vid. SSTS de 22 de junio de 2005 (RJ 2005, 5516) y 17 de julio de 2006 (2006, 6302).

telefónicas y de sus DACE, obtenido mediante la paciente escucha y análisis de, a veces, centenares de horas de conversaciones anodinas hasta que los agentes de la PJE abnegada, diligente y sagazmente, son capaces de obtener inteligencia relevante para el progreso de la propia investigación y, en definitiva, posibles pruebas para garantizar el más exacto conocimiento de los hechos.

La anterior distinción no es considerada por los magistrados disidentes, pues basan toda su argumentación en la aportación subjetiva, que parecen creer única, ignorando la existencia concomitante de la objetiva. Ignorancia que podría haberse resuelto por el muy simple procedimiento de conocer técnicamente el funcionamiento del SITEL y de no emitir valoraciones bajo meras suposiciones sobre su funcionamiento. De haber examinado con semejante diligencia en su ordenador cualquiera de los DVD producidos por el SITEL del procedimiento objeto de casación, con gran simpleza habrían comprobado todos los extremos que se vienen poniendo de manifiesto. Esto les hubiera permitido escuchar todas y cada una de las grabaciones, haber practicado todos las pruebas de veracidad, autenticidad e integridad y haber resuelto satisfactoriamente las dudas que se hubiesen suscitado.

Consecuente con lo anterior, evocando algunos aspectos de la prueba de inteligencia policial, es necesario en este momento hacer una exégesis del valor que para el proceso penal supone la aportación subjetiva de la PJE:

- Se trata de la aportación de un valor añadido atribuible al celo profesional de los agentes PJE que participan en una investigación criminal, quienes no tienen obligación procesal alguna de hacerla[807,808,809].

[807] Es relativamente frecuente, por lo demás, que los Jueces de instrucción se dirijan a la PJE para que "examinen y se pronuncien" sobre determinados elementos de prueba, lo que no deja de ser paradójico o suponer un contraste con aquellas líneas doctrinales en las que se propugna para la PJE una posición de mero ejecutor de las órdenes judiciales dentro el proceso penal. Es de suponer que los Jueces no se dirigirían de esta forma a la PJE si no fueran luego a tener en consideración los hallazgos que por su virtud la PJE aportase al proceso penal.

[808] En la STS de 14 de febrero de 2007 (RJ 2007, 1482) se afirma que *"no existe ningún precepto que exija la transcripción ni completa ni de los pasajes más relevantes, ahora bien, si se utilizan las transcripciones, su autenticidad sólo vendrá si están debidamente cotejadas bajo la fe del Secretario Judicial".* Vid. Lanzarote Martínez, Pablo. *Intervención de las…op. cit.*, pág. 830.

[809] NOYA, apoyándose en abundante jurisprudencia, afirma que *"…los funcionarios no están autorizados a hacer copias [de las cintas originales (sic)] o transcripciones".* Noya Ferreiro, María Lourdes. *La intervención…op. cit.,* pág. 263.

- Contiene una valoración subjetiva del Instructor Policial deducida del estudio de los hallazgos propiciados por el SITEL y de su contraste con el resto de la inteligencia recabada durante el proceso investigativo[810].
- Se apoya en los contenidos incluidos en la aportación objetiva, que constituyen la única prueba admisible – y verificable en cualquier momento, bien por el Juez, bien por el Secretario Judicial -, haciendo una referencia expresa a los que específicamente interesan a los meros efectos explicativos, lo que conlleva la búsqueda y selección de los fragmentos que considera subjetivamente relevantes.
- La valoración se incluye en una diligencia de informe en la que se hace constar expresamente su carácter subjetivo o valorativo[811] y deslindándola claramente de aquellas otras cuyo contenido pueda considerarse objetivo[812].
- La aportación subjetiva tiene la única virtud de orientar a los actores del proceso penal mediante las valoraciones del Instructor Policial generadas con el mayor grado de objetividad posible durante el proceso intelectivo originado durante de la investigación criminal. Es innegable, en cualquier caso, su contribución a la formación de la opinión judicial una vez se somete al más exigente proceso de contradicción[813].
- La aportación subjetiva no tiene valor procesal alguno, aunque puede reconocérsele el que la doctrina y la jurisprudencia atribuyen a la prueba

[810] Nótese que un contenido puede adquirir valor investigativo, e incluso de evidencia, si se combina inteligentemente con el proporcionado por otra fuente de prueba. Por ejemplo, la frase anodina "Juan te entregará ahora la mercancía" podría implicar en un hecho delictivo al interlocutor que la pronunciase si su cómplice, Juan, que está perfectamente identificado, en ese momento entregase a un tercero una determinada cantidad de droga como consecuencia directa e inequívoca del acto de concertación descrito.

[811] Es común que la diligencia se inicie con una frase como la siguiente: *"Sobre cómo sucedieron los hechos objeto de las presentes diligencias policiales, el Instructor se ha formado la siguiente opinión…"*, desgranando a continuación en la diligencia informe todos las valoraciones que considere conveniente, con apoyatura en los elementos objetivos incluidos en las diligencias (y no sólo los provenientes del SITEL).

[812] Por ejemplo, incorporando al atestado una diligencia de antecedentes de un investigado, de una reseña fotográfica o adjuntando la declaración de un testigo.

[813] No obstante, la única valoración posible es la que hace el Juez Instructor apoyándose en la fe pública del Secretario Judicial, según apunta NOYA, con apoyo en abundante jurisprudencia. Vid. Noya Ferreiro, María Lourdes. *La intervención…op. cit.,* pág. 262.

pericial de inteligencia o prueba de inteligencia policial. Y, permítaseme, el sentido común.

- En general, la combinación de la aportación objetiva y la subjetiva permite realizar los cotejos y comprobaciones que resuelvan satisfactoriamente cualquier cuestión que se suscitase sobre la autenticidad o integridad de la primera.

Las SSTS de 22 de junio de 2005 (RJ 2005, 5516) y 17 de julio de 2006 (2006, 6302), a los efectos, enumeran los siguientes requisitos para la valoración como prueba del contenido de la intervención:

1) *La aportación de las cintas.*
2) *La transcripción mecanográfica de las mismas, bien íntegra o bien de los aspectos relevantes para la investigación, cuando la prueba se realice sobre la base de las transcripciones y no directamente mediante la audición de las cintas.*
3) *El cotejo bajo la fe del Secretario Judicial de tales párrafos con las cintas originales, para el caso de que dicha transcripción mecanográfica se encargue – como es lo usual – a los funcionarios policiales.*
4) *La disponibilidad de esta material para las partes.*
5) *La lectura de las mismas en el juicio oral, que da cumplimiento a los principios de oralidad y contradicción*[814].

Visto todo lo anterior, lo que se está describiendo en buena medida es una actividad policial que evoca el concepto de la prueba pericial de inteligencia o prueba de inteligencia policial, de la que habrá ocasión de tratar con más profundidad más adelante, y que, en la práctica, es admitida tácitamente por los tribunales en materia de limitación del derecho al secreto de las comunicaciones, ya que es muy dudoso que el Juez, el Secretario Judicial, el Fiscal y, mucho me temo, las partes, se dediquen con el mismo celo que la PJE a escuchar íntegramente las inacabables horas de grabación y, todavía menos, poniéndolas hábilmente en relación con la restante inteligencia elaborada durante el periodo investigativo, más que nada por el frecuente estado de desbordamiento de los juzgados y fiscalías – siendo generoso en el comentario - y,

[814] Vid. Lanzarote Martínez, Pablo. *Intervención de las…op. cit.*, pág. 825.

lamentablemente también, por la desidia de algunos de los abogados defensores de los justiciables quienes, en realidad, se dedican con poca fortuna a tratar de descreditar en el juicio oral, mediante los correspondientes argumentos *ad hominem* -lo que la PJE ha ido minuciosamente elaborando durante extenuantes horas de trabajo. Vano intento, muchas veces, pues si faltase la aportación subjetiva de la PJE en materia de secreto de las comunicaciones, se podría augurar el más completo fracaso del proceso penal, al menos en los casos complejos, que son muchos[815].

Por ello, los comentarios incorporados a este apartado sobre la viabilidad de la admisión de nuevas salvaguardas tecnológicas, son demostrativos de una injusta prevención genérica presente en muchos de los autores estudiados, lo que representa, en mi opinión, un bloqueo de difícil resolución conforme las TIC ofrezcan la posibilidad a la PJE de introducir en el proceso penal determinados medios de prueba, cuya fortuna quedará sin duda sometida a las más obtusas tachas de proporcionalidad ofrecidas por el hipergarantismo que lastra el proceso penal español y, naturalmente, de la producción normativa que eventualmente se decida a acometer el legislador.

La propuesta de solución de este problema pasa – además de por la revisión del concepto de evidencia digital que aporte seguridad jurídica al acto de su incorporación al proceso penal, cuyo estudio excede al propósito de este trabajo -, incontestablemente, por incorporar cuanto antes los sistemas de salvaguarda y certificación para, como se ha planteado, desplazar los debates procesales a su lugar natural, que es la valoración de la prueba durante el acto de juicio oral y, en ningún caso, por no ser ya objeto de cuestión, del medio técnico con que se obtuvo.

[815] Según el Informe de 2011 del Observatorio de la Actividad de la Justicia de la Fundación *Wolters Kluwer*, la media española de litigios celebrados por cada órgano judicial en 2010 fue de 798,44. A finales de septiembre de 2011, sólo en materia penal el "atasco judicial" era de 1.177.193 casos.

E. Análisis de la casuística criminal

Es necesario, en este momento, abrir un nuevo paréntesis en el trazado argumental que se sigue por considerar que deben introducirse algunas reseñas fenomenológicas relacionadas con el uso criminal de las TIC.

No parece posible reflexionar sobre el Derecho sin haber efectuado una previa y profunda introspección en las realidades materiales sobre las que debe intervenir. Consecuentemente, la elección de la casuística responde a un panorama tan amplio como inquietante y su propósito no es otro que el de ilustrar de forma precedente al lector para que, cuando se planteen las propuestas, se puedan conciliar estas realidades con la revisión jurídica que, en mi opinión, incuestionablemente demandan.

He huido, por tanto, de incluir la experiencia en ubicaciones menores, como las notas al pie de página, o con pacatas referencias en cuanto a su contenido. Al contrario, si alguna aportación podía hacerse de mi mano que justificase la necesidad de una revisión jurídica, debía partir, precisamente, de una correcta interiorización de una realidad alterada, cada vez con más intensidad, por el uso criminal de las TIC.

Los recursos que la tecnología brinda a la investigación criminal, determinantes de su éxito en buena parte de las ocasiones, suelen ser usados desde las fases más tempranas como instrumentos de obtención de la necesaria inteligencia operativa dirigida a lograr dos finalidades esencialmente distintas, pero íntimamente conectadas: En primer lugar, para orientar y estructurar el desarrollo de la propia investigación, acercando a su director los elementos de juicio suficientes para hacerla progresar mediante la confirmación o refutación de las sucesivas hipótesis formuladas y, en segundo lugar, proporcionando una forma legítima de obtención de pruebas relevantes para un proceso penal bajo las exigentes premisas del Estado de Derecho.

En todo este procedimiento distinguimos dos fases: Una pre-procesal o de comprobación previa, y otra procesal, que se desarrolla, con toda lógica, bajo la dirección de los Jueces y Tribunales y del Ministerio Fiscal (art. 550.1 LOPJ). El límite entre ambas, no siempre preciso, viene señalado por el cumplimento por parte de la

Policía Judicial de la obligación recogida en el art. 284 LCRIM de dar a conocer a la Autoridad Judicial la existencia de un posible hecho delictivo.

Consecuentemente, y desde un punto de vista estrictamente policial, la frontera entre una y otra fase hay que situarla en el momento de la apreciación de unos elementales indicios racionales de criminalidad sobre la naturaleza del hecho que se investiga, lo que sucede tras el examen de determinadas circunstancias que ocupan lo que hemos llamado la fase pre-procesal y que hacen nacer las obligaciones recogidas en el art. 282 LCRIM.

En todas las fases de la investigación, se producen condicionantes sobre el uso de la tecnología, todo ello en la medida en que su irrupción en el proceso investigativo pueda conllevar una limitación de los derechos fundamentales de los concernidos.

Básicamente, y en lo que interesa a este trabajo, se estaría hablando de la posible afectación al derecho a la intimidad proclamado en el art. 8 del Convenio Europeo de Derechos Humanos y en el art. 18 CE ocasionada por el uso de la tecnología y, de forma más directa, por su afectación al contenido de sus apartados 3 y 4 de este último artículo.

La protección jurídica del derecho a la intimidad, de contundente e inequívoco blindaje constitucional, introduce a través de los apartados mencionados respectivamente dos de las más trascendentales facetas que configuran una de las partes más sensibles de nuestras libertades y que conllevan la consiguiente limitación del derecho de injerencia del Estado: el derecho al secreto de las comunicaciones y el derecho a la autodeterminación informativa.

Ahora bien, los derechos fundamentales no son derechos absolutos, pues en la misma redacción del precepto constitucional se contempla la posibilidad de que el Estado se injiera en la intimidad de las personas, bajo determinados condicionantes que, normalmente, vendrán de la mano de una decisión jurisdiccional adoptada bajo el principio de proporcionalidad.

Debe anotarse también que, cuando se trate de introducir los medios técnicos de investigación como contramedida del uso de las TIC por parte de los delincuentes, sobre la lícita injerencia policial en su intimidad, llevada a cabo de un modo análogo a

cómo se investigarían sus actividades en el espacio físico, se irrumpirá simultáneamente con la necesidad de limitar el derecho al secreto de las comunicaciones cuando se lleve a cabo en el espacio virtual. Es decir, que el secreto de las comunicaciones se yuxtapone sobre otros actos de vigilancia en este ámbito, obligando al investigador a solicitar con más frecuencia la debida autorización judicial.

Es en este punto donde habrá de hacerse un especial hincapié, pues no siempre existe una precisa y suficiente definición jurídica en el derecho positivo – o siquiera una orientación jurisprudencial consolidada - sobre cuándo el investigador se injiere, debidamente o no, en el derecho a la intimidad. Es decir, usando de una mayor precisión, saber cuándo el agente de la PJE, con su recurso a la instalación de medios tecnológicos, está penetrando indebidamente en la esfera de la intimidad de su investigado y afectando al contenido esencial del derecho y, consecuentemente, incurriendo en responsabilidad personal.

Visto que en la bibliografía que acompaña a este trabajo, se hacen referencias a las interesantes aportaciones de otras personas de mayor autoridad en la materia que el que esto escribe, me permitiré centrarme en algunos aspectos concretos de la investigación tecnológica que he seleccionado en razón de su actualidad, utilidad, afectación social, incidencia en la investigación y su carácter controvertido. Me estoy refiriendo a las cuestiones relacionadas con el geoposicionamiento de los objetivos móviles no cooperantes o balizamiento, la captación del IMSI y el IMEI, la geolocalización de terminales móviles, el tratamiento de los datos asociados a las comunicaciones electrónicas, la intervención de Internet y, de forma transversal, a las consideraciones de carácter policial sobre la instalación de medios técnicos.

Con este espíritu y precedidas de unas consideraciones previas sobre la instalación y uso de medios técnicos, a continuación se presenta, aún sin aparente relación entre sí, una selección de casos cuya característica común se residencia en lo sugestivo de la necesidad, no ya de introducir cambios legislativos, sino, de forma antecedente y principal, de informar la percepción y opiniones de quien haya de reflexionar sobre el particular.

1. Consideraciones previas sobre la instalación de medios técnicos.

El primer problema que que es necesario analizar sobre la ***instalación y uso de medios técnicos***[816] (en adelante, IMT) es el de su inevitable exposición al conocimiento del mundo delictivo, hecho controvertido que se produce por dos motivos diferentes: De un lado, por llegar a conocer su existencia por sí mismos, al descubrirlos por causas accidentales o por haber realizado una búsqueda preventiva y, de otro, por su inclusión en el proceso penal o como consecuencia de su irrupción en los debates procesales[817].

Poco hay que comentar de ambas circunstancias, pues si la primera es un defecto atribuible a la habilidad profesional de los agentes que los instalan o a las aptitudes defensivas de los investigados, lo segundo es una consecuencia insoslayable de la observancia del art. 24 CE.

Consecuentemente, la efectividad y el rendimiento de la tecnología que la PJ opone a los actos ilícitos de los criminales quedan en entredicho por esta causa, obligando a los investigadores a desarrollar nuevos instrumentos técnicos que mejoren sus expectativas, siempre bajo los condicionantes de la insuficiencia procesal y los riesgos jurídicos asociados que han de reiterarse.

a) Compromiso del secreto en la instalación de medios técnicos de investigación

Cuando se redactó la preconstitucional Ley de Secretos Oficiales, en el año 1968, se tenía una noción clara de cuáles eran las amenazas contra *"la seguridad y*

[816] Vid. Vallés Causada, Luis. *Apoyo técnico a la investigación. Cuestiones de actualidad*, en *Manual de lucha contra la droga.* ISBN: 978-84-9903-003-6. Cízur Menor (Navarra): Aranzadi. 1ª Edición, 2011.

[817] Existen numerosas STS que contienen minuciosas descripciones de los medios técnicos que se han empleado en las investigaciones y cuyo uso ha sido objeto de intensos debates procesales, no siempre equilibrados. Como consecuencia, los relatos incluidos en las resoluciones judiciales constituyen una magnífica herramienta para que los delincuentes sepan cómo pueden ser investigados y cuál será la validez o no de los métodos tecnológicos empleados por la PJ.

defensa del Estado", según reza su art. 2, lo que podría identificarse, entre otras, con cualquier forma o expresión coetánea del terrorismo, pero presumiblemente nunca con la por entonces prácticamente inexistente delincuencia organizada y, muchos menos, con la potencialidad que hoy exhibe para amenazar la estabilidad del Estado.

Se puede, por tanto, atribuir a las anteriores razones el que en el art. *2.4 del* Decreto 242/1969, *del Reglamento de la Ley de Secretos Oficiales*, se considerase como objeto de protección de la Ley *"…los conocimientos [informaciones] de cualquier clase de asuntos o los comprendidos como materias clasificadas en el citado artículo segundo de la Ley".* Esto, sin duda, propició que las calificaciones de secreto del art. 3 del reglamento se aplicasen, por acuerdo del Consejo de Ministros de 28 de noviembre de 1986 y según su ordinal primero, apartado cuarto, a *"la estructura, organización, medios y procedimientos operativos específicos de los servicios de información, así como sus fuentes y cuantas informaciones o datos puedan revelarlas".* Sin embargo, una redacción más ajustada en mi opinión debiera extenderse, teniendo en cuenta el razonamiento anterior, a *"…las Unidades de Policía Judicial encargados de la lucha contra la delincuencia organizada o grave…".*

Las razones para exigirse tal calificación no son otras que las que se traslucen del contenido de este estudio y que evidencian graves riesgos para el Estado provenientes de las formas transnacionales de la delincuencia organizada o grave, perfectamente parangonables con los males que cabe esperar del terrorismo.

Consecuentemente, el sistema de garantías debiera evolucionar de modo que se evitase en lo posible la exposición de los medios ténicos a los debates procesales, sin que ello hubiera de significar una minoración de la tutela judicial efectiva, del derecho a la defensa y a un proceso con todas las garantías que debe asistir vigorosamente al justiciable.

El modo de lograrse la conciliación de estos aspectos, aparentemente contrapuestos, no es otro que el de la articulación de un procedimiento de garantías basado en la intervención en el proceso penal de terceras instituciones procesales que verificasen y diesen fe de la idoneidad de los medios técnicos, de los procedimientos empleados y de su legítima aplicación a la obtención de la concreta evidencia por la

PJE, todo ello, de un modo neutral e imparcial, así como sin vinculación ni conocimiento directo del concernido.

b) Aspectos prácticos de la instalación de los medios técnicos de investigación

Para un servicio de apoyo tecnológico a la investigación criminal, la IMT presenta dos premisas básicas, aparentemente contradictorias entre sí: De un lado, es necesario un conocimiento suficiente del contenido de la investigación y el logro de una perfecta sintonía con el equipo de investigación y, de otro, la necesidad de preservación de su autonomía en la aplicación de sus técnicas y procedimientos específicos.

Sobre estas dos premisas, debe subyacer la creación de unas condiciones que garanticen la eficacia operativa, la reserva y la seguridad de la intervención y de sus procedimientos operativos. Este último apartado, exige contemplar unas muy rigurosas medidas de seguridad personal de quienes ejecutan la acción operativa. El frecuentemente sensible ámbito de intervención, normalmente en las inmediaciones de los lugares donde los delincuentes hacen su vida, hace necesario extremar las precauciones, sobre todo cuando se trate de países extranjeros, cuyas circunstancias prácticas normalmente se ignoran o, al menos, no se dominan[818].

En razón de lo anterior, a la instalación de un medio técnico debe precederle una adecuada y completa información preliminar para que, en el momento de la instalación, ninguna circunstancia, por imprevisible que resulte, pueda comprometer la seguridad o la eficacia de la intervención.

Una vez se ha practicado la información preliminar, debe elegirse cuidadosamente la herramienta técnica que mejor se adapte a la misión, siempre teniendo en consideración que la IMT es un recurso que no sustituye a la investigación

[818] Las intervenciones en países extranjeros están siempre sometidas a la autorización de los correspondientes gobiernos, bajo la directa supervisión de los funcionarios policiales que corresponda, bajo su inmediata protección y de forma que cumpla con todos los requisitos jurídicos observables tanto en el país requerido como en el requirente.

por procedimientos directos y que la decisión de su empleo debe tomarse con carácter restrictivo.

Los elementos que condicionan la eficacia de la IMT lo constituyen las condiciones de duración de la alimentación eléctrica del aparato y la adecuada configuración de su régimen de funcionamiento de acuerdo con las necesidades informativas por las que se decide su instalación[819].

No son cuestiones menores, por su parte, las labores de mantenimiento, la gestión de las incidencias, cambio de dispositivos, cambios de configuración, gestión de la alimentación, etc., lo que en sí mismas suponen la reproducción de idénticas condiciones de seguridad técnica y operativa que conllevan la instalación o retirada de medios técnicos.

2. Las redes sociales. Formas mixtas de comunicación.

Como ejemplo representativo de las dificultades que surgen en la intervención de las comunicaciones en el mundo de Internet, puede ofrecerse el siguiente, referido a las redes sociales:

La conocida red social *Facebook*[820], que fue fundada el 4 de febrero de 2004, está operada por un proveedor de servicios de la sociedad de la información radicado en los Estados Unidos, cuyas finalidades comerciales están orientadas, principalmente, a poner en contacto a usuarios de todo el planeta que hayan decidido registrarse como suscriptores de una de sus cuentas. La forma técnica de vincularse el usuario con *Facebook* es a través de la suscripción previa de una cuenta de cualquier proveedor de correo electrónico, en la forma que se ha explicado anteriormente.

[819] Pueden configurarse alarmas de zona (movimiento por una determinada área geográfica), activación por movimiento, voz, periodos temporales, intensidad de la señal, forma de constancia de contenidos, forma de descarga, etc. Cuando el empleo conlleve la limitación de un derecho fundamental, el uso de los medios técnicos puede adaptarse a los imperativos contenidos en el mandato judicial, reduciendo el ámbito de intervención a aquella parte que tenga interés para el proceso penal, ignorando aquellas otras cuyo conocimiento deba quedar reservado a la privacidad de los sujetos investigados (Por ejemplo, conocer los movimientos de un vehículo que se sabe va a ser usado en un determinado lugar, lo que aconsejaría establecer una alarma de activación únicamente cuando se aproximase a este).

[820] Vid. www.facebook.com.

Cuando el contenido intercambiado en canal cerrado a través de esta red social deviene interesante para el proceso penal, la PJE solicita de la Autoridad Judicial la emisión de una CRI dirigida a la compañía en los EEUU y que es normalmente gestionada a través de alguna de las agencias de policía con competencia en la concreta materia, como puede ser el FBI o el *Homeland Security*[821] que, a su vez, las dirige a un bufete de abogados de Palo Alto (California).

Recibida la CRI en el bufete, la compañía se muestra plenamente receptiva a atenderla, pero facilitando la información según las categorías de datos y el tiempo de conservación que haya adoptado por decisión técnica o empresarial[822], y elabora los informes solicitados con específicas limitaciones en cuanto a su formato y extensión. La respuesta queda condicionada exclusivamente a entregar copia de los contenidos insertados con anterioridad a la fecha de efectividad que el auto judicial señale y que, en el plazo de varias semanas o meses, esto es, en tiempo diferido, quedan finalmente a disposición de la autoridad requirente, que los incorpora como evidencia legal al proceso penal español[823].

Evidentemente, queda inhábil la intervención en tiempo real de los contenidos y sus DACE y, desde luego, los que sean de urgente necesidad de acceso[824]. Es de hacer notar, además, las dificultades de contradicción y valoración de la prueba documental así obtenida, que operará en la práctica como una prueba preconstituida en un ámbito extraterritorial, sobre todo cuando se plantee por cualquiera de las partes alguna

[821] Ver http://www.fbi.gov/ y http://www.dhs.gov/index.shtm.

[822] Por ejemplo, los *logs* de acceso IP se conservan únicamente durante 30 días. Muchos de los contenidos o de los datos personales introducidos por los usuarios quedan al pairo de que hayan decidido borrarlos o modificarlos con posterioridad a la suscripción del servicio. Vid. *Facebook Law Enforcement Guide*.

[823] Nótese que, por la evidente naturaleza de la prestación de este servicio de la sociedad de la información, el prestador tiene a través de sus servidores acceso al contenido material no borrado por el usuario. En la práctica de la relación de cooperación judicial con los EEUU, los receptores de los requerimientos judiciales, en lo que a datos de contenido formal exclusivamente se refiere, suelen admitir y contestar directamente el mandato judicial español. Si el interés alcanza también al contenido material, exigen en este caso una CRI para facilitarlo. Fuente: GDT. Adviértase también que se está hablado de conservación de contenidos (material y formal) y no de la invocación de cualesquiera de las facultades contenidas en el CCib respecto de la preservación de determinados datos.

[824] En relación con el acceso al contenido material, es muy común en determinados ámbitos, como el de la delincuencia juvenil asociada a los homicidios, lesiones, amenazas, coacciones, etc., el que sus actores hayan dejado un reflejo en las redes sociales previo, e incluso contemporáneo, de las acciones delictivas que cometen o que planean cometer lo que, de conocerse oportunamente, permitiría a la PJE y los servicios de seguridad o emergencias atender en tiempo real casos de extrema gravedad como los indicados o, al menos, hacerse una figuración sobre cómo afrontar la investigación.

necesidad de verificación, autenticación, tacha de integridad, refutación, práctica de pericias, de testimonios, etc.

Buenos ejemplos de lo anterior lo constituyen las operaciones JABÓN[825] y FONTANA[826], ambas llevadas a cabo por la UCO, que tuvieron como protagonista a la red social *Facebook*.

La ***OP. JABÓN*** se inició como consecuencia de haber detectado los responsables de *Facebook* a un pedófilo cuyas IP de acceso a materiales de pornografía infantil correspondían al rango de navegación *web* adjudicado a España por lo que, a través de la agencia estadounidense *Homeland Security*, trasladó formalmente su denuncia hasta la Guardia Civil que, tras resolver las IP de las transacciones delictivas, realizó una compleja investigación cuyos frutos fueron la detención del sospechoso y la incautación de ingentes evidencias digitales conteniendo materiales pornográficos infantiles.

En esta operación se hace evidente, no ya el encomiable sentido ciudadano de los responsables de *Facebook* de denunciar los hechos delictivos que conocieren en la medida en que les obligue la ley en los EEUU, sino el compromiso ético de hacer llegar la acción penal a los ámbitos extraterritoriales que, como en este caso, alcanzó a España.

La ***OP. FONTANA*** fue iniciada como consecuencia de la recepción telemática en la página del GDT de un "colabora" o denuncia presentada a través de un acceso a la página web de la unidad[827]. En el comunicado se ponía en conocimiento la existencia de una supuesta suplantación de la identidad mercantil de una conocida agencia de

[825] DP 224/2012 del JI núm. 2 de Loja (Granada), realizada entre los meses de enero y febrero de 2012.
[826] DP 2008/117/2011 del JI núm. 24 de Barcelona, con posterior inhibición en las DP 6116/2011 del JI núm. 4 de Hospitalet de Llobregat (Barcelona), todo ello entre los meses de junio y octubre de 2011.
[827] Ver https://www.gdt.guardiacivil.es/*web*gdt/colabora.php. La presentación telemática de denuncias a través del software propiedad de la página *web* de la Guardia Civil (El popular "colabora") no exime de su ratificación formal presencial según disponen los arts. 265 y 267 LCRIM para que cause todos sus efectos jurídicos. La ausencia de este requisito, no obstante, no deja de proveer de inteligencia a la PJE en la forma en que sea, también, jurídicamente admisible en un Estado de Derecho, pues no puede admitirse impunidad alguna en determinadas acciones maliciosas por las que la pretensión del supuesto "colaborador" no sea otra que la de causar algún perjuicio a terceros. La PJE es, dentro del compromiso ético y deontológico que cabe exigírsele, especialmente cuidadosa en el manejo de este tipo de sensibles informaciones, lo que incluye la actuación en caso de que se tuviesen indicios sobre la comisión de los tipos contenidos en los arts. 456 y 457 CP, sobre la acusación y denuncia falsas o la simulación de delitos.

modelos que, a través de una acción maliciosa de captación de mujeres insertada en la red social *Facebook*, invitaba a la creación on-line de un "*book"* o archivo de imágenes confeccionado por las propias candidatas a trabajar como modelos para que, inicialmente, enviasen sus fotogramas o videos con imágenes con un contenido neutro en lo que se refiere a la promoción su imagen personal hasta, progresivamente, lograr envíos con contenido un sexual cada vez más explícito, normalmente, mediante la aplicación, subliminal o no, de técnicas coactivas o amenazantes para conseguir maliciosamente la captación y envío de semejantes archivos.

En este caso, la red social *Facebook* fue objeto de un requerimiento judicial mediante CRI, cursado en la forma que se ha comentado anteriormente y que cumplió escrupulosamente enviando en tiempo diferido los datos de contenido material y formal que le fueron requeridos.

Estos dos casos, tal y como han quedado expuestos, muestran un interés policial aparentemente preferencial por el acceso al contenido material, pero es de hacer notar que ningún éxito habrían tenido si no se hubiesen resuelto satisfactoriamente las necesidad de inteligencia sobre el contenido formal, esto es, la obtención de los datos técnicos orientados a enlazar el contenido ilícito con el autor o autores de los hechos, lo que permite llegar físicamente hasta ellos, investigar las circunstancias de todo tipo que los rodean, asegurar las evidencias legales y, en todo momento, anular sus maliciosas acciones.

Tanto sobre el acceso al contenido material como al formal, es necesario reiterar que todo se refiere a un tiempo diferido por lo que, salvo por la oportunidad de la interposición de una sonda pasiva, poco sentido de la oportunidad podría aportársele a otras acciones investigativas que hubiesen de iniciarse como consecuencia del acceso en tiempo real a determinadas informaciones y, desde luego, obviamente, de una forma completamente inútil para lograr la más mínima reactividad policial en aquellos eventuales casos en los que se necesitase una intervención de urgencia.

Aunque no fue esta la ocasión en la OP. FONTANA, por el perfil criminológico del tipo de delitos investigados puede esperarse en cualquier momento ataques de mayor gravedad a la libertad sexual o a la integridad de las personas concernidas, lo

que evidencia una innegable necesidad de que el Estado se dote de las herramientas necesarias para garantizar la libertad de sus ciudadanos.

Es también importante poner de manifiesto que, independientemente de lo hasta ahora observado, los ISP, en general, suelen mantener por su propia iniciativa los archivos con los DACE correspondientes a las operaciones de sus clientes y que, caso de acceder a colaborar lealmente con la Justicia, ponen a disposición de los agentes facultados a la presentación de un mandato judicial expreso. Este plazo de conservación tiene normalmente una duración de treinta días.

Como es obvio, este periodo de conservación, en caso de que exista, es libremente establecido por el ISP y resulta ajeno a obligaciones jurídicas específicas.

3. Usos no comunicativos o instrumentales de los dispositivos de comunicación electrónica.

Tampoco quedan resueltos en el panorama jurídico actual determinados usos de las comunicaciones electrónicas, de ya no tanta novedad, que se producen cuando la comunicación no se verifica entre dos o más personas[828], esto es, entre personas y máquinas o entre estas últimas[829,830] donde, además, suelen transmitirse datos sin contenido semántico reconocible ni expresiones de estricta intimidad protegibles, al menos, desde el art. 18.3 CE, sino, como mucho, por el 18.1 ó 18.4 CE. En estos casos, con cierta lógica, la intrusión por el Estado no debiera revestir más que un leve sacrificio del derecho a la intimidad, de modo que la PJE pudiese acceder a los datos sin mandato judicial y, especialmente, en los *modus operandi* que impliquen la necesidad de una actuación policial con carácter de urgencia.

---

[828] Lo que, en principio, excedería al concepto de dato considerado por el art. 2.d) de la Directiva 2002/58/CE, pues no se referiría a *"un número finito de interesados"*, prescripción de orden cuantitativo que pierde todo su significado en cuanto se habla de comunicación entre máquinas o en el uso masivo propio del direccionamiento masivo de ataques DoS vía IP.

[829] Vallés Causada, Luis. *Usos delictivos no comunicativos de la telefonía móvil: ¿Una excepción a la protección del art. 18.3 CE?* en El Proceso Penal en la Sociedad de la Información. Las nuevas tecnologías para investigar y probar el delito. Coordinador: Pérez Gil, Julio. VVAA. Ed. La Ley. 2012, págs. 219-239.

[830] *Ibídem*. Deben recordarse en este punto las dificultades señaladas por GONZÁLEZ-CUÉLLAR respecto de la identificación de estos actos como "comunicaciones" en el sentido formal de la expresión. Vid. González-Cuéllar Serrano, Nicolás. *Garantías constitucionales…op. cit.,* págs. 167.

Las comunicaciones en canal cerrado, establecidas mediante el uso de los dispositivos de telefonía móvil, gozan de la alta e indistinta protección otorgada por el derecho al secreto proclamado en el art. 18.3 de la CE de 1978 y el art. 8 del Convenio Europeo de Derechos Humanos.

El uso más habitual de estos dispositivos consiste en el establecimiento de una llamada telefónica entre un número finito de interlocutores (normalmente sólo dos) con el objetivo de comunicarse entre sí, verbalmente o por escrito (los populares SMS[831]), ideas y sentimientos o, más prosaicamente, de intercambiar informaciones de cualquier naturaleza que, por neutras o irrelevantes que pudieran parecer a terceras personas, no por ello perderían su carácter de secretas y merecedoras de la más estricta protección constitucional.

El sustrato tecnológico que favorece la comunicación – hoy día basado en dispositivos electrónicos, algunos muy sofisticados, como los *smartphones* – se sirve, además de en una red de comunicaciones electrónicas operada por una determinada compañía de telefonía móvil, de unos aparatos que llevan inserta una tarjeta de telefonía (Tarjeta SIM) que se utiliza para materializar la conexión técnica entre los interlocutores.

Sin embargo, la casuística criminal refleja que no todos los usos de las tarjetas SIM se dirigen a establecer comunicaciones electrónicas como las descritas[832], sino a cumplir fines reprensibles prohibidos en la legislación penal.

Entre estos usos singulares[833] – que por convenio denominaré "no comunicativos" – se pueden distinguir, a título meramente ilustrativo y sin pretensión de exhaustividad, los siguientes[834]:

---

[831] Los mensajes cortos de texto en telefonía, equiparables jurídicamente al correo electrónico, gozan de toda la protección del art. 18.3 CE. Vid. Marchena Gómez, Manuel. *La intervención jurisdiccional del mensaje corto de telefonía móvil (SMS)*. CYBEX The digital forensic company E-newsletter, 2009, págs. 3-7.

[832] El preámbulo de la Ley 25/2007, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones, de 18 de octubre, reconoce que *"las nuevas tecnologías desarrolladas en el marco de la sociedad de la información han supuesto la superación de formas tradicionales de comunicación, que abarcan no sólo la voz, sino también datos en soportes y formatos diversos"*. De este breve texto puede deducirse, tanto el carácter novedoso, expansivo y socialmente integrado de las formas de comunicación…

[833] *Ibídem.* Vid. Salom Clotet, Juan. *Delito informático y su investigación…op. cit.,* pág.95.

- Vaciamiento patrimonial mediante transacciones electrónicas.
- Geoposicionamiento de posibles víctimas.
- Iniciación de cargas explosivas.
- Tráfico instrumental de IP.

En efecto, un breve análisis fenomenológico de los casos criminales recientes debe conducir a una reflexión centrada en dos aspectos clave:

- Si, de acuerdo con la dimensión formal del derecho, todas las comunicaciones electrónicas son tales y deben estar estrictamente protegidas por el art. 18.3 CE.
- Dependiendo de la contestación a la cuestión anterior, si deben revisarse, tanto el concepto de DACE, como su cesibilidad a la PJE, especialmente en casos de urgencia vital.

Se analizarán desde un punto de vista fenomenológico, en primer lugar, algunos de los casos sugestivos de esta creciente necesidad:

a) Vaciamiento patrimonial mediante transacciones electrónicas

Este caso se estudiará a través del ejemplo ofrecido por la **OP. LÍNEA ROJA**[835], por la que se investigó un supuesto delito patrimonial cometido a través de los servicios de comunicaciones electrónicas proveídos en España a clientes particulares por una determinada operadora del mercado de las telecomunicaciones.

La operadora estableció un plan de captación de clientes mediante una generosa oferta comercial pública de adquisición de tarjetas SIM a un determinado precio, pero dándose la circunstancia de que se podía continuar haciendo llamadas

[834] La sorprendente evolución de la tecnología de las comunicaciones, unida a la febril imaginación de los criminales, asombrará sin duda con nuevas fórmulas para delinquir mediante el uso de estos u otros dispositivos.

[835] La operación fue desarrollada por el GDT de la UCO de la Guardia Civil y seguida por el Juzgado Central de Instrucción núm. 2 de la Audiencia Nacional en DP 65/2009. Fuente: Archivos UCO y entrevista con el Instructor de las Diligencias Policiales.

tras agotar el saldo inicial adquirido en la promoción por una cantidad adicional gratuita de un valor notoriamente superior al de la compra[836].

Evidentemente, la operación así diseñada suponía una importante pérdida económica para la compañía que, en sus planes, esperaba resarcirse ampliamente por el eventual efecto posterior de *fidelización* del nuevo cliente. Pero, si este gastaba el saldo y no continuaba en la compañía, la pérdida económica era en muchos casos superior al 100 % del valor contratado.

Personas conocedoras de la promoción se concertaron para aprovecharse de sus características, para lo cual establecieron una sociedad mercantil que contrató numerosas líneas de tarificación adicional (explotación de números de prefijo 905 cuya conexión por los clientes se obtiene mediante precio). A continuación, adquirieron varios miles de tarjetas SIM prepagadas a la operadora a nombre de desconocidas personas (normalmente con incumplimiento de las obligaciones de identificación impuestas por la LCDCE y, en todo caso, bajo imposibles condiciones de uso personal dado el elevado número de tarjetas que había adquirido cada persona física[837]).

Una vez en su poder, las emplazaron supuestamente en unos dispositivos tecnológicos de llamada automática, desde cuyo IMEI establecieron conexión con cualquiera de los números 905 de la mercantil propia sin otro fin que el de agotar el saldo adjudicado por la promoción a cada una de las SIM. Como es obvio, esta operación supuso el vaciamiento de la cantidad adicional gratuita que fue a parar de esta forma a manos de los maquinadores, que no eran otros que los propietarios de las líneas 905, no continuando como clientes por más tiempo y no cumpliendo, por tanto, con la expectativa de negocio de la operadora que, como consecuencia, sufrió un grave quebranto económico.

Percatada la operadora de los hechos, presentó una denuncia penal a la que acompañó de un exhaustivo y altamente eficiente análisis de sus bases de datos[838],

[836] En algunos casos, el desembolso inicial del cliente de 50 € se bonificada con 82 € gratis adicionales, siendo está última cantidad derivada al bolsillo de los autores de este hecho.
[837] Una sola persona física llegó a ser titular de 943 SIM. Nótese, en cualquier caso, la dificultad añadida para la PJE para determinar la identificación del usuario real de las tarjetas en caso de simulación o usurpación de la identidad.
[838] Nótese, a título de mero comentario, la existencia de un posible ejercicio excesivo de las facultades del operador, pues de este caso puede decirse que, presumiblemente, no existió finalmente un fraude,

poniendo en relación el ingente tráfico de datos asociados a las comunicaciones electrónicas producido entre los números 905, los IMEI de los dispositivos de llamada automática, los IMSI de las SIM prepagadas[839], la identidad de las personas físicas adquirentes y la de las personas jurídicas involucradas, atribuyendo a todo el conjunto una unidad de acción.

El análisis ordenado de la PJE de todos estos datos proporcionados por la operadora, expresado gráficamente, produce una intrincada maraña de relaciones que evocan una estructura de crecimiento fractal[840], pues de cada elemento objeto de estudio surgen innumerables nuevas relaciones que, bien analizadas – y aunque no tiendan al infinito -, muestran, como suponía el denunciante, una maquinación extraordinariamente compleja dirigida a un solo fin: apropiarse del dinero de la promoción telefónica.

Una vez presentado el caso – y por el momento sin pretensiones de exhaustividad - , pueden hacerse las siguientes reflexiones a la luz del Derecho Penal y Procesal:

En primer lugar, las comunicaciones electrónicas producidas desde las tarjetas SIM tenían un uso instrumental preordenado a la obtención de un lucro económico y no consistían en la transmisión de voz o datos establecida en canal cerrado entre personas protegido por el art. 18.3 CE, según el concepto clásico de uso de la telefonía fija o móvil, sino en un vaciamiento del saldo a favor de terceros sin el establecimiento de una relación comercial estable como la pretendida por la promoción.

Sin embargo, la Ley no distingue entre unas u otras comunicaciones y todas, sin excepción, gozan del alto blindaje constitucional que les otorga el precepto indicado,

---

sino una desastrosa gestión de la oferta comercial, todo de acuerdo con las limitaciones implícitas, a *sensu contrario,* a lo indicado en el *Considerando 29 Directiva 2002/58*, donde se dice que*: "El proveedor también puede tratar los datos de tráfico necesarios a efectos de facturación a fin de detectar y frenar el fraude consistente en la utilización sin pago de servicios de comunicaciones electrónicas".*
De otro lado, debe suponerse que el operador se hizo una figuración sobre la naturaleza del contenido material de las comunicaciones que estudiaba, adjudicándoles una naturaleza instrumental para la comisión del fraude, lo que es sugestivo del ejercicio de alguna facultad excedentaria de lo que le permitiría la Ley. El caso es que el Juez no dedujo testimonio por vulneración del art. 197 CP sobre la revelación de secretos.

[839] Se atribuyeron a la red el uso de casi 2.000 tarjetas SIM prepagadas en dos meses.

[840] Según el diccionario RAE, *"figura plana o espacial, compuesta de infinitos elementos, que tiene la propiedad de que su aspecto y distribución estadística no cambian cualquiera que sea la escala con que se observe"*.

lo que se extiende, además, a sus datos asociados de tráfico, localización e identificación[841].

En segundo lugar, detectado el posible perjuicio, la compañía operadora analizó por iniciativa propia y gran eficiencia sus bases de datos de tráfico de llamadas e identificación de IMSI, IMEI, número de abonado e identidad personal sin restricción ni reserva alguna sobre los derechos fundamentales que sus clientes gozasen en el marco de sus comunicaciones electrónicas, expurgando los de aquellos que fueron objeto de su interés y desechando todos los demás con el fin de adjuntarlos a una denuncia ante la PJE que fue finalmente admitida en el proceso penal, causando todos los efectos jurídicos que se estimaron procedentes por quien ejerció la potestad jurisdiccional.

A estos fines, las obligaciones de conservación de datos de tráfico, localización e identificación de las comunicaciones electrónicas establecidas en la LCDCE habrían facilitado el acceso y posterior cesión voluntaria a la PJE sin que mediase una expresa resolución judicial al efecto, facultad de la que de ningún modo goza esta última.

Por otra parte, de haberse producido comunicaciones bajo el *Protocolo TCP/IP*, los proveedores de servicios de la sociedad de la información que hubieran tenido alguna participación en su conducción no habrían tenido ninguna obligación de conservar los datos, ni de cederlos a la operadora y, mucho menos, de haberlos cedido a la PJE, especialmente en el muy probable caso de que el tráfico se hubiera producido en la escena internacional[842].

En tercer lugar, la supuesta apropiación económica de cada una de las tarjetas consideradas individualmente no excedería del centenar de euros en el mejor de los casos, siendo dudoso que en el suceso, caso de tener relevancia penal para el concreto titular de la SIM, se hubiera alcanzado el límite objetivo de penalidad para que se considerase grave *ex* art. 1.1 LCDCE y, consecuentemente, no fuese posible usar las figuras procesales que permiten la limitación de los derechos fundamentales.

[841] Así se proclama en la STC 114/1984, de 29 de noviembre, doctrina tantas veces repetida que se recoge también en las SSTC 70/2002, de 3 de abril, 123/2002, de 20 de mayo y 281/2006, de 9 de octubre.

[842] Véanse más adelante los comentarios sobre la *Botnet* "MARIPOSA" donde el direccionamiento IP dio la clave en la identificación de los ordenadores "esclavos".

Supóngase ahora que, fuera del caso anterior, la PJE adquiriese indicios racionales de una maquinación similar a la denunciada pero desconocida para la operadora y que, además, no sólo no supusiese ningún peligro para sus legítimos intereses empresariales sino que, muy por el contrario, le proporcionarse una mejor expectativa de lucro igualmente legítimo.

En este caso, el acceso por la PJE a los datos asociados a las comunicaciones electrónicas se haría exclusivamente merced a la previa solicitud fundada de un mandamiento judicial, que se otorgaría previo juicio de proporcionalidad expresado en un auto escrito motivado, en el que la Autoridad Judicial desgranaría las razones de orden jurídico y factico por las que se optaba por limitar el derecho fundamental al secreto de las comunicaciones, así como el alcance y límites de la medida.

Lógicamente, si se está a lo establecido en el art. 579 LCRIM y a la copiosa jurisprudencia sobre la intervención de las comunicaciones, no sería posible que el Juez autorizase a la PJE a analizar las bases de datos de la operadora (o de los ISP, en caso de que esto fuese posible) para obtener una inteligencia de similar calidad a la que por sí obtuvo e incorporó libremente a la denuncia aquella cuando se descubrió amenazada en sus intereses privados[843].

Para conseguir un nivel equivalente de eficacia como el logrado por operadora en su análisis, la PJE se vería obligada a iniciar una imposible cadena de solicitudes de mandato judicial conforme adquiriese nuevos indicios que le aconsejasen indagar en una determinada o determinadas líneas de tráfico telefónico y demás datos, lo que, obviamente, resultaría ajeno a la realidad por extenderse en el tiempo, por su propia complejidad y por toda clase de impedimentos prácticos y procesales que ya se hace ocioso comentar.

[843] Así se pronuncia MORENO, evidenciando una aparente colisión – que debiera quedar resulta lo más pronto posible - entre las necesidades surgidas para el análisis de las fuentes de prueba generadas por las TIC y su accesibilidad procesal, quien argumenta que *"la autorización debe ser precisa y determinar los datos a los que se refiera, así como el tiempo para el que se solicita, con el máximo legal de los doce meses que se obliga a conservar. Eso significa que la autoridad judicial no puede expedir autorizaciones genéricas, que dejen al criterio del agente que la cumplimenta o del operador que debe ceder los datos cuáles son los que pide o que entrega…[la autorización] será radicalmente nula…".* Vid. Moreno Catena, Víctor. *Ley de conservación ...op. cit*. La solución, en mi opinión, viene de la mano de la revisión del principio de proporcionalidad y de la apoyatura de la acción jurisdiccional en los recursos de las TIC, todo ello en la forma en que se propondrá.

Sin embargo, de ser factible esta posibilidad, con un empleo mínimo de patrones de búsqueda, se completaría – como lo hizo la operadora – una visión real de la naturaleza y apoyatura tecnológica del presunto ilícito investigado y, sin duda, con una *ratio* menor de penetración en la intimidad de aquellos abonados que nada tuviesen que ver en la maquinación, pero cuyos datos fluyesen junto con los de los objetivos[844].

Lo anterior puede resumirse diciendo, desde un punto de vista estrictamente policial, que en aprovechamiento de las facultades legales de la PJE respecto de las operadoras dadas de alta en la Comisión del Mercado de las Telecomunicaciones y por mor de la LCDCE, podría accederse a una cantidad razonable y suficiente de DACE durante los periodos de conservación establecidos en la norma, pero que este acceso vendría constreñido por las limitaciones de orden jurídico que impiden, por la actual interpretación jurisprudencial del principio de proporcionalidad y de la normativa vigente, la implementación de procedimientos eficaces de obtención de inteligencia sobre aquellos datos.

En lo que se refiere a los ISP, al no alcanzarles las obligaciones de la LCDCE, quedaría al pairo de su voluntad el conservarlos y cederlos de acuerdo con el mandato judicial en aquellos casos que, asumiendo el deber genérico de colaboración con la PJE de todo ciudadano, decidiesen atender a semejante solicitud, teniendo en cuenta, además, el exiguo alcance de las medidas que se dictasen y que afectarían, en todo caso, al tráfico producido por el territorio nacional y a lo que diese de sí la cooperación internacional cuando este lo excediese.

En definitiva, la complejidad de las comunicaciones electrónicas actuales no se ve compensada por la calidad de las medidas procesales que pueden activarse para alcanzar un nivel análogo de eficacia al que puede obtenerse en el mundo físico. Parece que el proceso penal español, instalado en la morosidad en cuanto a la

[844] Por ejemplo: En un caso clásico de petición de un listado de llamadas de un determinado abonado en un determinado lapso de tiempo, la operadora contesta al mandato judicial enumerando escrupulosamente los datos completos generados pero sin discriminación de ningún tipo. Si fuese posible un breve análisis previo de la base, previsiblemente la PJE pediría la cesión final de tan sólo uno o dos, o tal vez ninguno, de los datos conservados, en lugar de recibir un listado de centenares o miles de datos inútiles para la investigación y que corresponden a la intimidad de terceras personas no involucradas en los hechos.

necesaria reforma de su normativa, se resigna a no tratar una fuente de prueba indispensable para llegar al completo esclarecimiento de determinadas formas delictivas hoy día muy comunes en nuestra sociedad.

Es decir, en términos prácticos, que el proceso penal en este campo está urgido de la necesidad de introducir cambios legislativos o, entretanto, a servirse de la adaptación de las interpretaciones doctrinales, siempre dentro del principio de proporcionalidad, de forma que se faculte como proceda a la PJ en forma suficiente para desarrollar labores de inteligencia en el marco de las comunicaciones electrónicas.

b) Geoposicionamiento de posibles víctimas

Otro de los *modus operandi* que está adquiriendo importancia en el complejo mundo de la delincuencia que planifica sus actos criminales con la apoyatura de las TIC, lo constituyen las bandas organizadas dedicadas al robo de vehículos de alta gama (normalmente todo-terrenos), como lo sería el caso de la **OP. IBERIA**[845]. El móvil de la sustracción de esta clase de automóviles es para venderlos a determinadas redes de narcotraficantes que, a su vez, los usan para el transporte, ocultación y comercio de drogas. Así expuesta, esta maquinación no representaría ninguna novedad, ya que se trataría de un caso más de la fructífera cooperación entre grupos criminales[846].

[845] Juzgado de Instrucción núm. 2 de Picassent, en DP 264/20111. Determinadas redes criminales roban vehículos todo-terreno que luego venden a narcotraficantes, que los usan para la recepción, movimiento, ocultación y colocación de la droga en el mercado. Antes de la entrega de los vehículos robados, les instalan balizas de forma encubierta que les permiten el seguimiento de los vehículos con el evidente fin de asaltar y robar la droga a los narcotraficantes en el momento más oportuno. Está claro en este caso que los DACE conservados proporcionan una ingente fuente de inteligencia y prueba para el debido control de la investigación y su escenario, permitiendo la oportuna intervención de la PJ por partida doble: Investigar casos de narcotráfico y desmantelar redes de robo de vehículos. Estos DACE se refieren, no sólo a los producidos por las comunicaciones electrónicas de los investigados, sino por la valoración de la fuente de prueba que supone el análisis de las tarjetas SIM de las balizas, que operan dentro del esquema de comunicaciones de máquina a persona.

[846] Adviértase además la previsible y pavorosa cifra negra que se atisba detrás de los hechos delictivos en el intramundo de la criminalidad organizada. ¿Cabe esperar que alguien denuncie ante la Justicia que le han robado una importante partida de cocaína recién alijada? ¿Quién se expone a relatar un ajuste de cuentas? ¿Quién se acusará de haber receptado un vehículo robado?

La diferencia está en que los grupos de sustracción de vehículos los entregan a los narcos previa la instalación de dispositivos de seguimiento GSM-GPS[847], vulgarmente llamados balizas, lo que les permite hacer un análisis en tiempo real de la actividad criminal de sus "clientes" con el objeto de, en el momento más oportuno, sustraerles la droga con toda comodidad y garantías de seguridad[848].

En este caso, como en los demás, se advierte la necesidad de que la PJE pueda hacer un seguimiento de la señal de las balizas (datos de tráfico asociados a las Tarjetas GSM-GPS[849]), tanto para recuperar los vehículos sustraídos como para aprehender las drogas y, naturalmente, para detener y poner a disposición judicial de los miembros de unas y otras redes. Lógicamente, esta actividad no puede ser realizada sin un mínimo de investigación, lo que exige el acopio de la inteligencia necesaria sobre los DACE para que el proceso penal pueda alcanzar todas sus finalidades.

Aunque estos casos suelen ser sensiblemente menos complicados que el anterior, sí necesitan de las mismas habilitaciones para obtenerse y tratarse unos DACE referidos a usos no comunicativos de la telefonía móvil.

c)Iniciación de cargas explosivas

[847] Combinación de una tarjeta de telefonía móvil con un sistema de posicionamiento geográfico preciso. Este tipo de dispositivos no pueden utilizarse para conducir la voz, pues su único uso está limitado a la transferencia de datos geográficos.

[848] Sería muy pobre concluir que estas redes únicamente conocen gracias a las balizas los movimientos de los vehículos de sus víctimas, ya que la cuestión va un poco más allá: como expertos que son, combinan los datos de geolocalización con sus conocimientos sobre las víctimas y su actividad criminal, en lo que son extraordinariamente hábiles, concibiendo con todo ello sus propios planes criminales para obtener el mayor lucro posible, es decir, que obtienen inteligencia práctica que les permite ser altamente eficaces e impunes en su negocio criminal.

[849] Adviértase que, en el marco jurídico-procesal actual, los datos de localización que conservan las operadoras por imperativo de la LCDCE no se refieren en modo alguno a los terminales, sino a la ubicación de las antenas de telefonía (BTS) que les dan servicio en un momento dado. La emisión de la señal GPS en un valor añadido del dispositivo telefónico que únicamente se puede obtener del prestador de servicios de geolocalización de que se trate. En resumen, y esto es importante, los datos de localización del SITEL nunca informan sobre la localización de las personas ni de sus teléfonos móviles sino de las BTS a las que se conectan.

Lamentablemente, debe hacerse una referencia en este punto a alguno de los dolorosos atentados terroristas que ha sufrido España en los últimos años pues ya se ha producido algún ejemplo del uso de los teléfonos móviles como iniciadores de los artefactos explosivos usados por los terroristas.

El *modus operandi* es de una extraordinaria simpleza. Basta colocar una carga explosiva dotada de su correspondiente detonador para iniciarla mediante una conexión al teléfono móvil, de modo que, al recibirse una llamada en el colocado junto al explosivo la energía eléctrica recibida provoque el encendido del detonador y este, a su vez, la explosión de la carga principal. Este sería el sistema utilizado en el atentado contra el Acuartelamiento de la Guardia Civil del barrio de Inchaurrondo (San Sebastián), el 11 de noviembre de 2000[850], o en los atentados del 11 de marzo de 2004 en Madrid, como es bien conocido.

Lógicamente, a la cuestión ya tratada de los usos no comunicativos de las tarjetas, ha de añadirse la evidente perentoriedad de los servicios públicos (no sólo los policiales, sino de todo tipo de asistencias) de intervenir a la máxima urgencia por la inminencia de graves consecuencias para las personas y las cosas.

d) Tráfico instrumental de IP

Sobre el direccionamiento IP de los ataques de DoS y con apoyatura en la experiencia de la OP. MARIPOSA, se han ido presentando someramente algunas observaciones – a cuya relectura he de remitirme en beneficio de la brevedad -, como medio de examinar determinados aspectos jurídicos controvertidos, todo ello en relación con el legítimo derecho del Estado de intervenir en defensa de los bienes jurídicos puestos en peligro por esta concreta forma de delinquir.

[850] La carga explosiva fue activada por los terroristas haciendo una llamada al teléfono-iniciador justo en el momento en que se percataron, a través de la televisión pública, de que algunos guardias civiles se acercaban a la zona donde se hallaba instalada como bomba trampa (artefacto secundario), ya que se había producido una explosión previa y la misión de los agentes consistía, en ese momento, en reconocer los alrededores del lugar para recoger vestigios de la primera explosión. Nótese lo insidioso del procedimiento, la facilidad de prepararlo, lo sencillo de activar el explosivo secundario y el recurso a algo tan simple como decidir cómodamente desde casa el momento más dañino para activarlo. Terrorismo de zapatillas, podría decirse.

Pero el conocimiento de las IP que hayan sido usadas en el *iter criminis*, en el caso presentado y otros hechos similares, deviene un medio insuficiente para su análisis, pues han de complementarse con otros DACE – fuera de las obligaciones actuales de conservación *ex LCDCE* – que, de conocerse, permitirían la consolidación de la evidencia digital.

En este sentido, como sostiene GONZÁLEZ LÓPEZ,

> *"resulta cuestionable que se califique de dato de origen la dirección IP empleada para la conexión a Internet. Esta circunstancia, que parece responder a una identificación automática de la llamada "navegación" con la conexión a Internet, no es, sin embargo, adecuada, ya que el acceso a Internet no es una forma de comunicación, sino el paso previo a la utilización de los diversos tipos de comunicación que permite Internet (correo electrónico, conversación en tiempo real, etc.). En este sentido, la exposición separada que hace la Directiva 2006/24/CE de los datos correspondientes al correo electrónico y VoIP (dos tipos de comunicación) es incompatible con el análisis del acceso a Internet como si de otro tipo de comunicación distinto se tratara. Es por ello que el planteamiento del CCib se antoja idóneo, ya que hace referencia a los distintos servicios y, por tanto, a las diversas formas de comunicación permitidas por Internet, de manera que el origen venga referido a cada tipo de comunicación y no al estadio, previo y subyacente a todas ellas, de la conexión a Internet, los datos correspondientes a la cual ("datos de conexión") únicamente constituirán datos de tráfico cuando aparezcan vinculados a una comunicación concreta"*[851], [852].

Es decir, que en la conformación del mensaje – mediante el acceso a un servicio de la sociedad de la información -, intervienen otros elementos de naturaleza

[851] Vid. González López, Juan José. *Los datos de tráfico…op.cit.,* pág. 64.

[852] En este sentido, LÓPEZ-BARAJAS dice que *"conviene subrayar que las IP no identifican a personas concretas, sino tan sólo a un terminal informático"*, posición que la autora no considera muy congruente con al regulación de la LCDCE, ya que *"esta exigencia choca con el hecho de que se trata de acceder a un dato que el propio interesado ha permitido que sea de público conocimiento".* Estas tensiones le llevan a considera la urgencia *"de una regulación completa y actualizada de esta materia que atienda las peculiaridades de cada caso."* Vid. López-Barajas Perea, Inmaculada. *La intervención de las comunicaciones…op. cit.,* pág. 58 y 59.

estrictamente técnica que conviene desvelar si se pretende acreditar solventemente los hechos mediante la aportación al juicio oral de la plena evidencia digital.

En la estructuración criminal puesta en marcha por los autores de la *Botnet Mariposa* – en el que el direccionamiento IP aportaría únicamente datos del acceso a la red pública de comunicaciones electrónicas -, pueden distinguirse a grandes rasgos dos elementos esenciales: de un lado, la puesta a disposición de la gigantesca capacidad computacional de la *botnet* a posibles clientes criminales, mediante la infección viral previa, indiscriminada, masiva e inadvertida de millones de ordenadores, privados o no, en la escena internacional; y, de otro, el impredecible uso particular que la clientela criminal eventualmente haya hecho de sus prestaciones técnicas, lo que da una idea del imposible control del resultado de la diseminación de los usos criminales individuales, lo que se medirá, en cualquier caso, por sus más o menos gravosos resultados.

Por lo anterior, el investigador, mediante un titánico esfuerzo condicionado por la percepción jurídica sobre el estudio de las comunicaciones electrónicas, puede desvelar lo suficiente para demostrar la dolosa infección de los ordenadores y acreditar la participación de las personas criminalmente responsables de la maquinación, como bien se vio con las detenciones de los que así actuaron en la *Bonet Mariposa.*

Pero estos mismos investigadores deberán esperar a que las víctimas – que lo serán sin duda en la escena internacional – reporten sus diversos casos particulares, la gravedad de cuyos daños dependerá de la naturaleza específica y el grado de éxito material de cada ataque. Las limitaciones de intervenir en la escena internacional, por lo demás, son bien conocidas y se multiplican por el infinito cuando de lo que se trata es de conseguir la extraordinariamente volátil evidencia digital, al punto de poder ser presentada ante un tribunal.

Por la razón anterior, sólo caben las soluciones individuales ante la emergencia de un nuevo caso para el que se precise unificar la evidencia digital disponible y ponerla en relación con los hechos y estos, a su vez, con sus autores.

Un uso elemental e indebido de las posibilidades de la *botnet* – fuera por completo de lo que pudiera considerarse grave criminalmente – podría ser la distribución de publicidad mediante técnicas de *spam*.

Pero también podría usarse de un modo extraordinariamente grave – que podría incluirse en los riesgos catastróficos - si, mediante un ataque DoS direccionado desde la *botnet* se robasen o borrasen datos, se hiciesen caer servidores o se infectasen con virus los ordenadores de una gran empresa, una administración pública, un servicio público, etc.

Como ejemplos se han aportado las consecuencias del *stuxnet,* pero trátese de imaginar qué sucedería si se borrasen de forma irrecuperable los datos fiscales operativos de la Agencia Tributaria, se colapsasen los ordenadores del Sistema Nacional de Salud o de las cadenas de distribución farmacéutica, la gestión de la navegación aérea y aeroportuaria o se formateasen los servidores de una gran entidad bancaria.

Evidentemente, en este punto fracasan, no ya las posibilidades de acceder a datos conservados en la escena internacional sobre las transacciones telemáticas sino, más simplemente, al puro acceso a la multiplicidad de servidores que estarán sin duda implicados en los ataques.

Además, la original estructuración de los *logs* será sin duda diferente en cada proveedor de servicios de la sociedad de la información, lo que dificultará aún más la investigación técnica, a lo que ha de unirse el comentado divorcio entre las posibilidades identificativas de la dirección IP y el dato verdaderamente identificativo que representa los *logs* del uso del servicio telemático.

Expuestas así las cosas, se evidencia que, con la evolución de las TIC, no basta conformarse con la obligación de conservar la IP de acceso a la red pública de comunicaciones – que poca o ninguna información ofrecen sobre la conformación real del mensaje telemático - sino introducir la obligación entre los ISP de conservar los *logs* de las transacciones telemáticas de los servicios que presten, aspectos los anteriores que representan, respectivamente, la insuficiencia de contar únicamente con los datos de acceso a la red pública de comunicaciones electrónicas, de escaso

valor identificativo, y el necesario conocimiento de la información sobre la configuración de las transacciones telemáticas, de un gran potencial informativo.

Lo anterior es representativo del divorcio existente entre el modo de intervenir los DACE de la telefonía fija y móvil y el que pretendidamente quiere llevarse a cabo, mediante aplicación analógica, sobre los servicios telemáticos de la sociedad de la información, lo que supone un evidente distanciamiento del concepto tradicional de la comunicación electrónica y que, de ningún modo resulta transferible al mundo de las comunicaciones vía Internet.

Interesa también en esta apartado adelantar un efecto añadido, puesto que la tipología de las comunicaciones telemáticas, como consecuencia de su propia naturaleza material, deja al descubierto el completo alejamiento del concepto jurídico de comunicación en los casos de direccionamiento IP, en su expresión aceptada por la doctrina y la jurisprudencia sobre la afectación a la intimidad y al derecho al secreto de las comunicaciones, poniendo en cuestión que un ataque de DoS, por el que se difunde *malware* a millones de ordenadores sin el más mínimo rastro de una acción de comunicación humana reconocible (más allá de los actos personales de concertación criminal y diferenciados de estos, que hayan de merecer la radical protección del art. 18.3 CE), cuando lo que la racionalidad indica es que no sucede nada en estas comunicaciones que afecte a la intimidad en la dimensión *ético-psíquica* de la que habla la jurisprudencia[853].

En consecuencia, algo tendrá que revisarse en esta anómala percepción, reservando con radicalidad la protección constitucional a las comunicaciones personales y pensar en abandonar, ahí donde proceda, la protección del canal de comunicaciones cuando fehacientemente se acredite que su uso criminal lo es únicamente para su mero uso instrumental como máquina. Es decir, revisar el concepto jurídico de "comunicación" en la línea que se trasluce de este estudio[854,855].

[853] Véase la STS 534/2011, de 10 de junio.

[854] En la nota de prensa del FBI con identificación (202) 324-3691, de 11 de diciembre de 2012, ampliamente difundida por la prensa, se informa de la continuidad de las investigaciones en un extenso y complejo marco transnacional de actuación.

[855] Presentados en este apartado someramente los aspectos de orden criminológico sobre la *botnet* Mariposa, en otro posterior se analizarán, con apoyatura en los aspectos fácticos e investigativos, los jurídicos que se deducen de tan compleja maquinación criminal apoyada en las TIC.

4. La geolocalización de dispositivos de comunicaciones

En general, los dispositivos provistos de una tarjeta de comunicaciones electrónicas de cualquier clase son en general susceptibles de ser geolocalizados[856,857].

Pero, antes de comenzar este apartado, se partirá de algo obvio: el acceso a la información de geolocalización proveída por este tipo de tarjetas no se usa para determinar la posición de las personas, sino la de los teléfonos móviles[858], las tabletas, las balizas o de cualquiera otro de los dispositivos de comunicaciones electrónicas o vehículos en los que se puedan instalar[859].

Sobre esta cuestión, en el considerando 14 de la Directiva 2002/58/CE se afirma que *"los datos de localización pueden referirse a la latitud, la longitud y la altitud del equipo terminal del usuario, a la dirección de la marcha, al nivel de precisión de la información de la localización, a la identificación de la célula de red en la que está localizado el equipo terminal en un determinado momento o a la hora en que la información de localización ha sido registrada".* Nótese en este contexto que los datos de localización vienen referidos, con mayor o menor precisión, al equipo terminal y no a la persona que eventualmente lo porte, materia que exige una indagación por completo ajena al análisis de las comunicaciones electrónicas y que se refiere a los métodos de investigación clásicos que permitan asociar el terminal a la persona que lo

[856] Sobre la geolocalización puede leerse un interesante panorama de la actualidad técnica en Gómez Gómez, Juan de Dios. *Localización de terminales móviles de comunicaciones, nuevos desafíos para la investigación criminal.* Trabajo de investigación fin de CACES. Academia de Oficiales de la Guardia Civil. Aranjuez, 2012.

[857] Sobre las balizas y el uso de los teléfonos móviles como elementos de geolocalización es muy interesante la lectura del estudio realizado por Vid. Pérez Gil, Julio. *El nuevo papel de la telefónia móvil…op. cit.*, págs. 173-218.

[858] Aunque es evidente la utilidad de georreferenciar los teléfonos móviles, en realidad, como bien apunta PÉREZ GIL, los datos que se obtienen no son precisos, sino estimativos del área en que se pueden encontrar. Además, según es experiencia de la unidad que dirijo, las peculiaridades del espectro radioeléctrico, la configuración de la constelación de BTS que den servicio a un terminal, la posible existencia de antenas *réflex* (que ofrecen los datos de geolocalización, no de está propia antena, sino de la principal de la que dependen), la configuración del terreno e, incluso, las propias insuficiencias de las bases de datos o de los medios técnicos de investigación, pueden producir importantes errores en la estimación del área de posible localización. Vid. Pérez Gil, Julio. *El nuevo papel de la telefónia móvil…op. cit.*, pág. 176.

[859] Así se recoge en la definición de dato de localización que se recoge en el art. 2 c) de la Directiva 2002/58/CE: *"cualquier dato…que indique la posición geográfica del equipo terminal de un usuario…".*

usa, lo que, de ningún modo tiene por qué coincidir con su propietario, ni con el contratante del correspondiente servicio de comunicaciones electrónicas[860].

En el caso de las balizas, se trata de medios técnicos cuyo régimen de funcionamiento puede configurarse para ofrecer información geográfica precisa o estimativa sobre la localización del dispositivo que interesa a la investigación (Información que, integrada con la de otras fuentes, permitirá de forma secundaria estimar – que no precisar - la zona en la que puede residir o trabajar el investigado o determinar sus posibles objetivos criminales e, incluso, contribuir a la prueba de su implicación en hechos delictivos), según las diversas prestaciones técnicas del propio dispositivo o las que proporcionen otros medios técnicos auxiliares como el IMSI *Catcher* u otros analizadores del espectro radioeléctrico.

Consecuentemente, la vinculación de la geolocalización del dispositivo con lo que concierna a la ubicación de la persona y los actos criminales que se le presuman, corresponderá a un ámbito bien distinto de la investigación policial, en el que la señal de la baliza será un mero medio de obtención de inteligencia – bastante pobre y limitado en sí mismo - y, en ningún caso, determinante como instrumento de prueba, salvo lo que se deduzca de la evidencia digital que haya proporcionado[861].

Es común en la doctrina hallar grandes prejuicios sobre el acceso a la información de geolocalización ofrecida por el análisis del espectro radioeléctrico, sin duda en la creencia de que limita el derecho al secreto de las comunicaciones por su

[860] Este es uno de los problemas – a estas alturas ya clásicos, aunque perfectamente conjurados - de la actividad policial investigadora en cuanto al uso de los medios técnicos y de la inteligencia que producen, dado que debe evitarse a toda cosa la tentación del investigador de vincular falazmente los contenidos material y formal asociados a un concreto terminal con los de la persona cuyo uso se le pretende atribuir. Esto es particularmente visible cuando el agente de la PJE pretenda afirmar que "tal persona está en determinado lugar" porque "los datos de localización de su terminal ofrecen las coordenadas y/o ángulo de BTS que así lo indican". Afortunadamente, la profesionalidad de la PJE evita que pueda producirse semejante inconveniencia que en poco o en nada ayuda al progreso de la investigación y, mucho menos, a la seguridad con que debe discurrir el proceso penal cuando se aporten testimonios de tan débil consistencia.

[861] Sobre su utilidad para la determinación de la responsabilidad criminal, véanse la SAP de Madrid 200/2011, de 18 de mayo y la SSTJ de Madrid 14/2011, de 8 de noviembre. Vid. Pérez Gil, Julio. *El nuevo papel de la telefónia móvil…op. cit.*, págs. 179 y 180.

proximidad al uso concomitante, pero radicalmente distinto, de los dispositivos como medios de comunicación personal[862,863].

Sin embargo, atendido el principio de proporcionalidad, ha de valorarse también el beneficio que supone el hecho de que la cesión de los datos de geolocalización en tiempo real haga innecesaria la, sin duda, más intrusiva intervención de las comunicaciones de voz[864].

Este medio técnico es, en general, un sistema auxiliar en la investigación que no sustituye en modo alguno a los procedimientos policiales clásicos, como las vigilancias o los seguimientos, y que aporta un suplemento de seguridad y eficiencia en el control de unos objetivos que pueden acceder con gran comodidad a los medios de transporte, a veces muy rápidos, o que viajan fuera del alcance del seguimiento directo en rutas extraterritoriales por tierra, mar o aire.

Por razones evidentes de su naturaleza, el uso de balizas reduce los periodos de exposición de los vigilados a aquellos sucesos ajenos al interés del proceso penal y,

---

[862] Los datos de localización pueden ser de tráfico, cuando están asociados a una comunicación electrónica (por lo que afectarán, según la jurisprudencia dominante, al derecho al secreto de las comunicaciones), o distintos de los de tráfico, cuando no lo estén (por lo que afectarán al derecho a la protección de datos personales), como los datos de cobertura (o *stand by* o de puesta a disposición de la red) o los de valor añadido (como los servicios de GPS asociados a determinados terminales o los de localización de usuarios de determinados servicios). Vid. Pérez Gil, Julio. *El nuevo papel de la telefónia móvil…op. cit.*, pág. 197 y ss y González López, Juan José. *Los datos de tráfico…op.cit.*

[863] En la STS (Sala de lo Penal) de 18 de marzo de 2010, se dice que los "*datos personales externos o de tráfico que hacen referencia a una comunicación concreta y contribuyen a desvelar todo o parte del secreto que protege el art. 18-3 C.E*" y los "*datos o circunstancias personales referentes a la intimidad de una persona (art. 18-1º C.E.), pero autónomos o desconectados de cualquier comunicación, que caerán dentro del derecho a la protección de datos informáticos o habeas data del art. 18-4 C.E. que no pueden comprometer un proceso de comunicación… [la equiparación supondría un] desenfoque del problema, pues incorporaría en el ámbito de la protección constitucional del art. 18-3, circunstancias cuyo tratamiento jurídico no debería separarse del que se dispensa a la protección de datos o al derecho a la autodeterminación informática del art. 18-4 C.E*".

[864] PÉREZ GIL expresa su preocupación por un sensible y aparentemente injustificado aumento de las cifras de intervención de las comunicaciones. Sin embargo, hay que anotar que las TIC han diversificado y multiplicado exponencialmente su utilidad para el *iter criminis,* por lo que nada de extraño tendría que tener este fenómeno. Además, no todas las intervenciones se refieren a la voz, como sucedía en la época de la telefonía clásica, de limitadas capacidades para favorecer la concertación criminal, sino solamente a datos, a veces muy precisos y simples, pero de suficiente valor para la investigación criminal. Por último, y con asiento en la experiencia propia, el número de intervenciones que solicita la PJE, aunque sólo fuera por razones prácticas y logísticas, tiende a ser lo más bajo posible, incluso por debajo de las necesidades reales de la investigación que, en muchas ocasiones, y sin dudarlo, sería de proporcionado interés para el proceso penal. La buena noticia en esto es que con una ratio infinitamente menor de penetración en el derecho a la intimidad de los investigados, es decir, con unos mínimos datos, puede hacerse progresar una investigación si se combina con las extraordinarias capacidades técnicas de la actual PJE. Vid. Pérez Gil, Julio. *El nuevo papel de la telefónia móvil…op. cit.*, pág. 215 y ss.

consiguientemente, presentan unas ratios muy bajas, e incluso irrelevantes si se comparan con otros medios de investigación, de penetración en el derecho a la intimidad[865].

Sus posibilidades son cada vez más versátiles y sofisticadas, pudiendo combinarse con otros dispositivos técnicos de variadas capacidades, como los que facilitan la intervención de las comunicaciones, en cuyo caso se hace preciso contar con la correspondiente autorización judicial.

Actualmente no existen espacios inhábiles para la emisión o recepción de la señal en ningún punto del planeta pues, aun cuando el investigado haga uso de contramedidas tecnológicas a prevención[866], siempre puede oponerse una determinada combinación de sistemas de comunicación con el medio técnico que las salven.

De esta forma, las balizas que actualmente se usan ofrecen una gran variedad de prestaciones técnicas, según cuál sea su cobertura, que puede ser a través de la red GSM, sistemas satelitales especiales, radiofrecuencia, etc. Todas ellas pueden usar, además, la precisión propia de los sistemas GPS y su información podrá ser servida en tiempo real al investigador habilitado vía *data web* a un ordenador portátil o a un teléfono con conexión de datos o tableta digital. En igual medida, las balizas pueden gestionarse en remoto variando su configuración para adaptarse a las cambiantes necesidades de la investigación.

Pero si el uso de las balizas es un elemento esencial en la estructuración de la investigación en sede policial, lo es aún más el hecho de poder estudiar los terminales de telefonía móvil en sus posibilidades de facilitar su geolocalización por diversos medios, recurso que deviene crítico en las situaciones de urgencia vital o riesgo

[865] No estoy de acuerdo con PÉREZ GIL respecto de la eventual necesidad de contar con un mandato judicial cuando se evidencie el paso del dispositivo vigilado por lugares que supongan una posible revelación de la adscripción religiosa o política, o que tales dispositivos sean usados o portados por terceros, todo ello por razones obvias de su imposible y previa determinación cuando se inicia la vigilancia técnica y por no diferir de los que sucedería en un plano físico con una vigilancia que descubriera tales facetas "sobre la marcha" (Por ejemplo, el objetivo va a misa inesperadamente en un receso de su actividad delictiva). En mi opinión, las limitadas pero eficientes informaciones provenientes de las señales técnicas se constituyen en una injerencia leve de la PJE en el derecho a la intimidad de los investigados. Vid. Pérez Gil, Julio. *El nuevo papel de la telefónia móvil…op. cit.*, págs. 189 y 190.

[866] Véase, por ejemplo, la STS 234/2012, de 16 de marzo, donde se relata el uso de contramedidas por la banda terrorista ETA.

catastrófico[867]. En estos casos, la consideración del terminal como baliza, sin dependencia temporal ni funcional de una comunicación protegible bajo el art. 18.3 CE[868], tanto a efectos jurídicos como prácticos, sólo podrá considerarse una injerencia leve en el derecho a la intimidad, propia de la actividad policial clásica de búsqueda de vestigios que contribuyan al éxito de la investigación criminal y, por ende, del proceso penal en su conjunto[869].

a) Aspectos jurisprudenciales sobre el seguimiento de móviles no cooperantes

El uso de las balizas no supone la limitación de derecho fundamental alguno de los que exigen un previo control de proporcionalidad y subsiguiente mandato judicial habilitador de las medidas limitativas.

En efecto, y evidenciando una vez más la falta de derecho positivo[870] al que acudir y recurriendo por defecto a la muy escasa jurisprudencia, la STS de la Sala 2ª, de

[867] Incluidos los estudios de geolocalización basados en datos conservados *ex* LCDCE o con los datos de cobertura, que quedan a extramuros de esta Ley, caso que se pudieran acceder.

[868] La jurisprudencia reconoce que no todo lo que tiene que ver con un dispositivo de comunicación tiene que estar automáticamente protegido por el secreto, pues *"basta al efecto recordar que tal aparato no solamente está habilitado para permitir el acto de la comunicación sino que suele proporcionar otras funciones ajenas al hecho de aquella comunicación. Pues bien, cuando del mismo se obtiene la información allí contenida, de suerte que lo sabido no es el contenido de una conversación o de un mensaje SMS, ni siquiera información del hecho de que tal comunicación tuvo lugar y, menos aún, entre quienes, no existe ni asomo de infracción del derecho garantizado en el artículo 18 de la Constitución"* (*STS 1474/2011, de 18 de marzo*). Véanse también, entre otras muchas, las SSTS 1273/2009, de 17 de diciembre; 1040/2005 de 20 de septiembre; y 316/2000, de 9 de marzo.

[869] Sobre la consideración de datos de tráfico, dice GONZÁLEZ LÓPEZ , *que "también como perteneciente a esta categoría puede citarse un criterio utilizado en nuestra doctrina que vincula los datos de tráfico al rastreo de la comunicación*". Vid. González López, Juan José. *Los datos de tráfico…op.cit.,* pág. 55, donde el autor se apoya en Corripio Gil-Delgado, María de los Reyes y Marroig Pol, Lorenzo. *El tratamiento de los datos de carácter personal y la protección de la intimidad en el sector de las telecomunicaciones.* Madrid: Agencia de Protección de Datos, 2001, pág. 188, conforme a los cuales, son datos de tráfico las "*trazas de movimientos que dejan los usuarios en Internet*" y "*aquellos relativos a la localización geográfica en el caso por ejemplo de las telecomunicaciones móviles*".

[870] RODRÍGUEZ LAINZ, en un loable intento de hallar algún asidero jurídico, con referencia al muy concreto ámbito de las entregas vigiladas, dice que *"la única norma que podría emparentar con esta última posibilidad [el uso de dispositivos adherido de seguimiento] sería la del art. 263 bis, apartado 2 de la LECRIM, en tanto en cuanto, se permite que la circulación de los bienes sujetos a tal medida de investigación pueda llevarse a efecto bajo la vigilancia de la autoridad o sus agentes; lo que podría suponer sin duda la instalación de dispositivos de posicionamiento para su más discreto seguimiento"*.

23 de enero de 2007, en el asunto sometido a casación (la aprehensión de una embarcación con droga) se invocó por parte de la defensa la *"[…] infracción de Ley con sede procesal en el art. 849.1 de la Ley de Enjuiciamiento Criminal, por infracción de los arts. 17 y 18.2 y 19 de la CE, en relación con el art. 11.1 de la Ley Orgánica del Poder Judicial, y del art. 24.1 y 2 de la CE, la falta de tutela judicial efectiva e indefensión, con la consecuente nulidad de las actuaciones, en relación con el balizamiento del barco […]"*.

Sin embargo, el tribunal, tras tomar en consideración el simple hecho de que no se había acreditado la existencia de la supuesta baliza alegado por la representación del recurrente, no estimó que para su eventual instalación se precisase de mandato judicial alguno, todo ello por no afectar al derecho a libertad ambulatoria ni que la instalación de la baliza hubiese supuesto alguna tacha para considerar idónea para ejercitar el derecho la ocupación por la PJ de la sustancia de tráfico prohibido.

En este mismo sentido, se pronunció mediante STS Sala 2ª, de 22 de junio de 2007, proclamando que para el uso de balizas por la PJ en otra embarcación *"[…] no se precisó ninguna injerencia en ámbitos de intimidad constitucionalmente protegidos"*, añadiendo a continuación que:

> *"Se trata [la instalación de la baliza], en definitiva, de una diligencia de investigación, legítima desde la función constitucional que tiene la policía judicial, sin que en su colocación se interfiriera en un derecho fundamental que requeriría la intervención judicial"*.

En esta sentencia puede comprobarse adicionalmente cómo el tribunal prudentemente desmonta los socorridos argumentos de la defensa que aluden a un uso espurio del dispositivo de seguimiento, al que le atribuían la posibilidad de grabar imágenes y sonidos, tratando así de extender la confusión necesaria para hacer valer sus argumentos en aplicación del art. 850.1 LCRIM, por denegación de una prueba procesal.

El TS arguyó en contra de semejante pretensión que *"la desestimación es procedente dada la impertinencia de la diligencia de prueba que se instó y, por esa*

Vid. Rodríguez Lainz, José Luis. *Los Dispositivos electrónicos de posicionamiento global (GPS) en el proceso penal*. Diario La Ley, Nº 7945, Sección Doctrina, 17 Oct. 2012.

falta de relación con el objeto del proceso fue denegada en su práctica. Dentro del objeto del proceso estuvo la utilización de una baliza para su localización durante la travesía que se sospechaba era para el tráfico de droga. En ese sentido declararon los responsables de su realización, sin que estos advirtieran de otras finalidades que el recurrente plantea como hipotéticas que, en todo caso, no han sido empleadas en la indagación. Se trataría de una posibilidad no amparada en dato alguno para la que no era precisa una actividad probatoria". Lo cierto es que, de existir las posibilidades técnicas concurrentes en el dispositivo de seguimiento como las mencionadas por la defensa, por ejemplo, para la grabación de las comunicaciones orales directas, hubiera sido objeto de la solicitud de un mandato judicial específico y separado, con amparo en los arts. 18.3 CE y 579 LCRIM.

De otro lado, las pintorescas razones argüidas por la defensa sobre la supuesta peligrosidad de la baliza para la embarcación son también desestimadas por el tribunal diciendo que *"tan sólo referir que el peligro para los tripulantes de la embarcación por la colocación de la baliza en el puente del barco, fue objeto de una actividad probatoria específica, sin que se declare relevante la situación de peligro que se denuncia […] En una reiterada jurisprudencia de esta Sala hemos requerido que la nulidad del juicio por denegación de prueba exige, además de la propuesta en los términos previstos en la Ley procesal, la pertinencia de la diligencia de prueba propuesta, su relevancia al enjuiciamiento para conformar una convicción y su necesidad para el derecho de defensa y a la acreditación del hecho objeto del proceso".* Nótese también, la necesidad de contar con una adecuada formación técnica y legal de los agentes encargados de la instalación de los medios tecnológicos para servir al proceso penal, algo que el tribunal proclama diciendo que *"el concreto hecho por el que se postuló la diligencia de prueba fue objeto de una específica prueba a los funcionarios del Servicio […], al tiempo peritos en marinería, quienes informaron al tribunal sobre las características técnicas de la baliza empleada y los posibles riesgos que pudieran comportar, ilustrando sobre la falta de peligrosidad que el tribunal declara en la fundamentación de la sentencia, por lo que la prueba, que no tenía relación con el objeto del proceso, era, además, innecesaria, por lo que el motivo se desestima"*.

Finalmente, sobre la supuesta entrada en domicilio[871] que pueda comportar el proceso de instalación del medio, mediante la STS Sala 2ª, de 11 de julio de 2008, el tribunal resuelve sobre la no consideración como tal del puente de una embarcación, manifestando que *"el submotivo 2 b) [motivo de casación alegado por la defensa] concierne a la vulneración del derecho a la "intimidad de domicilio", reconocido en el art. 18.2 CE. Para lo que se aduce que en el puente [del barco] fue colocada por el [Servicio] una baliza de seguimiento y localización. En primer lugar, no consta que para situar el artilugio fuera necesario entrar en algún recinto que constituyera un domicilio de los previstos en los arts. 554 o 561 LECr. Atendidos los documentos de los folios […] y las declaraciones en el juicio oral de los funcionarios del [Servicio] con números terminados en […] respecto a la colocación exterior de la baliza en la magistral. Por otra parte, nada permite afirmar que la baliza fuera utilizada para clase alguna de injerencia en las conversaciones o mensajes de los investigados"*.

Sin embargo, la jurisprudencia reciente del TEDH[872] parece inclinarse del lado más garantista, al intentar establecer algunas limitaciones a la instalación por la PJE de propia autoridad de medios técnicos de seguimiento en determinados casos pretendidamente tasados, cuya procedencia se ponderaría de acuerdo con el examen de determinados parámetros objetivos de los que resultaría la exigencia de una intervención judicial previa.

Según esta visión jurídica, no sería necesario que la PJE contase con un mandato judicial si la instalación fuese ocasional y por un tiempo reducido. Pero, si existiese una fundada afectación a la vida privada o a una expectativa razonable de privacidad – vista también la gravedad de los hechos y la duración de la medida - se consideraría como invasiva o injiriente hasta el punto de precisarse un mandato judicial previo para la colocación del dispositivo de seguimiento[873].

[871] Si esto fuese necesariamente así, habría que solicitar la previa autorización judicial, lo que no representa problema alguno de índole práctico policial, bien atendido el principio de proporcionalidad que debe informar una decisión jurisdiccional al efecto.
[872] STEDH de 9 de septiembre de 2010, sobre el Caso *Uzun vs* Alemania. Un excelente análisis de esta sentencia y de otros pronunciamientos jurisprudenciales comparados se contiene en Rodríguez Lainz, José Luis. *Los Dispositivos electrónicos…op. cit*.
[873] Entrevista con VELASCO NÚÑEZ y correo electrónico de 21 de diciembre de 2012.

En cierto modo, esta jurisprudencia recogería la preocupación de ciertos sectores jurídicos sobre la localización precisa de las personas sin la intervención judicial previa, como se trasluce de lo afirmado en la STS, de 19 de diciembre de 2008, en la que se consideró que se vulneraría la intimidad si el artificio técnico de seguimiento permitiera *"conocer el lugar exacto en el que el comunicante se encontraba"*[874].

Sin embargo, en mi opinión, la carga de inseguridad jurídica para la PJE contenida en el pronunciamiento del TEDH es muy grande, ya que resultaría muy difícil identificar tales límites por la propia indeterminación jurídica que se trasluce de los conceptos de "ocasional", "tiempo reducido" y, no se diga, de la estimación de la gravedad, materias cuya valoración objetiva excede a las facultades de la PJE y, máxime, en un ámbito tan complejo, dinámico y cambiante como es el de la moderna delincuencia.

Desde un punto de vista técnico-policial, de prosperar tan garantista visión jurídica, se produciría una injustificada constricción de las facultades indagatorias genéricas de la PJE hasta tal punto que le obligarían, de un lado, a intervenir con un exagerado garantismo "a prevención" y, de otro, a renunciar a la eficiencia operativa con que actualmente se instalan este tipo de medios ante una muy sofisticada delincuencia moderna. En este sentido, la pérdida de oportunidad sería notoria caso de tener que acudirse al Juez cada vez que se necesitase instalar un medio técnico en un móvil no cooperante o variasen las circunstancias iniciales con las que se decició la instalación, lo que se comenta por sí mismo[875]. Es necesario, por tanto, contar con derecho positivo eficiente[876].

[874] Inexactitud material sobre la que ya he vertido mi opinión en lo referido a la imposibilidad de que el artificio técnico indique la posición precisa o aproximada de una determinada persona. No obstante, la STS habla del "comunicante" y se refiere, por tanto, a datos de geolocalización obtenidos como consecuencia de un concreto acto de comunicación protegido por el art. 18.3 CE y revelado, obviamente, por la ejecución de una previa autorización judicial de intervención de las comunicaciones. La lógica indica que la obtención de esta información no es consecuencia sino, precisamente, de la habilitación judicial de los agentes facultados al efecto, por lo que es de entender que el Juez ha valorado positivamente la proporcionalidad de semejante medida de localización.

[875] Por ejemplo, si el investigado decide utilizar breve e inopinadamente un vehículo que hasta ese momento no es conocido por la PJE sino como consecuencia de la observación directa de sus actos. Pero, además, si lo que en principio se consideró ocasional y limitado en el tiempo, ¿cómo determinará la PJE cuándo esta medida traspasa los límites y es necesario someterla a un mandato judicial? De ser así, ¿habría que retirar el dispositivo y volver a instalarlo cuando así lo determinase el Juez? ¿Cómo se

Los aspectos más interesantes, a modo de resumen, son dos: de un lado, declarar falso el silogismo *"si el dispositivo de comunicaciones electrónicas está en tales coordenadas y el titular del contrato es el objetivo de la investigación, entonces el objetivo está físicamente ubicado en esa misma localización"*[877] y, de otro, afirmar que existen formas de acceder a los datos de localización de los dispositivos de comunicaciones electrónicas sin que ello suponga una injerencia en derecho reconocido en el art. 18.3 CE, siempre y cuando ello se infiera de su desvinculación temporal o funcional de un determinado acto comunicación, como se duduce de la obtención técnica de datos mediante el análisis del espectro radioeléctrico.

b) Geolocalización de dispositivos de telefonía móvil

Dada la evolución actual de la telefonía móvil[878], la geolocalización se convierte en una de los más sensibles recursos policiales para intentar resolver aquellos casos en que, o se ha de localizar a una persona al tiempo de ir a cometer un delito (relación espacio-temporal dinámica en relación con los demás actores y elementos de la maquinación criminal), o que se halla en riesgo vital (secuestro, desaparición, accidente, violencia de género, desorientación, etc.) o porque puede producirse una

---

averigua la identidad de la persona previamente a que use un vehículo que es en sí mismo del interés de la investigación? (Por ejemplo, un vehículo que ha sido cedido a los criminales y que se sabe que lo utilizarán personas desconocidas para cometer delitos).

[876] Sobre la necesidad de contar con normas claras a las que ceñirse la actividad de la PJE, dice RODÍGUEZ LAINZ que *"de nuevo volvemos a proclamar la urgente regulación de estas técnicas de investigación de tanta utilidad. Al menos el malogrado Anteproyecto de Ley de Enjuiciamiento Criminal de julio de 2011 dedica varios preceptos a lo que define como vigilancias sistemáticas, entre las que se encuentran aquellas en las que sean utilizados medios técnicos de localización y seguimiento –art. 315.2; en una regulación que recuerda bastante el precedente alemán analizado en la sentencia del caso Uzun v. Alemania: Sometimiento a la decisión del Fiscal investigador, salvo supuestos de extremada urgencia, y limitación temporal de su vigencia –art. 319-, son las claves sobre las que se asienta tal regulación"*. Vid. Rodríguez Lainz, José Luis. *Los Dispositivos electrónicos...op. cit*.

[877] Sobre la preocupación de la jurisprudencia por el sacrificio que suponen estos medios técnicos en cuanto a la ubicación precisa de la persona, con mención a la STS 906/2008, de 19 de diciembre, vid. Pérez Gil, Julio. *El nuevo papel de la telefónia móvil en el proceso penal: ubicación y perfiles de desplazamiento,* en El Proceso Penal en la Sociedad de la Información. Las nuevas tecnologías para investigar y probar el delito. Coordinador: Pérez Gil, Julio. VVAA. Ed. La Ley. 2012, pág. 191 y ss.

[878] De masiva aceptación por parte de los ciudadanos y de imprescindible uso para la concertación de los diversos actores de los hechos criminales. Esta última categoría incluye no sólo a los delincuentes, sino también a sus víctimas y a cualquier otro usuario cuyo terminal haya jugado algún papel relevante en la producción del suceso criminal.

situación de riesgo catastrófico para las personas o las cosas (atentado, ataque masivo DoS, daños en sistemas informáticos sensibles, etc.).

Junto con la escucha y grabación del contenido hablado (voz) o escrito (SMS) de una intervención telefónica, el SITEL ofrece sus datos asociados de tráfico, localización e identificación en tiempo real con referencia exclusiva al curso de cada comunicación[879] (voz, SMS, datos, etc.). En lo referido a la geolocalización del terminal, estos datos corresponden únicamente a la identificación de la ubicación física de la BTS o estación base principal de telefonía móvil en la que se ha registrado para efectuar una determinada llamada, expresada mediante sus coordenadas geográficas y en referencia a su ***CGI***[880].

Independientemente de lo anterior, estos mismos datos, sin que haya precedido una orden de intervención de las comunicaciones, habrán sido conservados durante un año por las operadoras del Mercado de las Telecomunicaciones en cumplimiento a las obligaciones que la LCDCE y, por tanto, consistirán en datos diferidos de comunicaciones que se verificaron en el pasado y de cuyo contenido material no hubo jamás constancia, salvo que se haya dado la coincidencia de haber existido alguna intervención legal precedente.

Los datos de localización "en bruto" son muy imprecisos pues, en el mejor de los casos, permitirán estimar que el terminal se halla en un área más o menos próxima a la ubicación de la citada BTS o, como máximo, en el sector que al que dan servicio una de sus celdas.

[879] Los teléfonos móviles encendidos, aunque no estén en plena comunicación, se van registrando en las sucesivas BTS cuya posición geográfica les sitúe en condiciones técnicas de ofrecerles servicio, bien a requerimiento del propio usuario, bien de un tercero que quiera comunicar con éste.

[880] Acrónimo del inglés *cell global identify* o identidad global de cada una de las celdas en que se divide una antena BTS con relación al sector circular al que prestan cobertura. Estos sectores, frecuentemente de 120 grados de amplitud, quedan identificados direccionalmente por el ángulo de su bisectriz (por ejemplo, 277 grados). El ángulo de cobertura no es fijo sino estimativo, pues su abertura depende de las condiciones radioeléctricas de propagación, lo que es indicativo de la falta de precisión del sistema, que puede estimar áreas sectoriales de superficie extraordinariamente amplia. Nótese que, con estos medios, difícilmente puede atenderse a una urgencia vital si hay para lograr precisión en la localización hay que recurrir a determinados medios técnicos adicionales por completo ajenos a la información facilitada por las operadoras. Además, hay que hacer constar que existen antenas multidireccionales que cubren todo el espectro desde una sola celda, con lo que la geolocalización se complica extraordinariamente.

Los trabajos para ganar una mayor precisión – lo que en puridad se ha llamado "geolocalización" – exigirán un complejo procedimiento técnico basado en el análisis de coberturas mediante el uso del *IMSI Catcher* o mediante el empleo de otros recursos tecnológicos actualmente disponibles en el mercado especializado[881]. Estos equipos, de elevado coste económico y manejados por personal de altísima capacitación técnica, por razones obvias, no pueden usarse sino en casos extremos debidamente justificados[882].

Para tratar de minimizar la insuficiencia o inexistencia de datos de localización del terminal móvil objetivo durante lo que se ha denominado el "periodo de ceguera de datos", en tanto se resuelve la solicitud de mandamiento judicial, la tecnología facilita la posibilidad de generar datos de localización[883]. Este sistema permite ganar alguna reactividad, pero limitada al momento a partir del cual estén disponibles los datos conservados por imperativo de la LCDCE y por expresa resolución judicial[884].

Las dos modalidades de análisis de la geolocalización que permiten dos tipos diferentes de investigación:

A.- Geolocalización en tiempo real bajo intervención telefónica:

El SITEL ofrece en tiempo real los CGI que se correspondan con la antena o célula de telefonía móvil empleada para la realización de una llamada telefónica o el envío o recepción de un SMS por un terminal de telefonía móvil, que quedan representados mediante un punto en el plano o representación gráfica ofrecida por el sistema.

En una primera fase de gabinete, se trata de delimitar el sector que cubre la celda problema. Si el teléfono móvil estuviera en movimiento durante la conversación, gracias a la orientación de los sucesivos sectores de las BTS que activara, podría

[881] GÓMEZ GÓMEZ informa sobre determinadas tecnologías de geolocalización no basadas en el acceso al GPS, como la de la *"la empresa norteamericana Trueposition, la cual oferta una solución U-TDOA que ofrece precisiones de localización de terminales móviles de comunicaciones con márgenes de error de un máximo de 50 metros en cualquier circunstancia, incluidos interiores, en los que los GPS no funcionan".* (Véase www.trueposition.com). Vid. Gómez Gómez, Juan de Dios. *Localización de terminales…op. cit.*, pág. 70.

[882] Muchos de ellos ajenos al interés del proceso penal, como es el caso de la localización de las personas en riesgo.

[883] Vid. Pérez Gil, Julio. *El nuevo papel de la telefónia móvil op. cit.*, pág. 180.

[884] Si el mandato judicial finalmente no llegase por cualquier razón, el procedimiento que se describe no supondría en ningún caso el acceso al conocimiento alguno de datos asociados a las comunicaciones.

estimarse una determinada ruta. En esta fase se estudia también si el terminal inmóvil ha recibido cobertura de otras BTS, complementándose los anteriores trabajos con un estudio del solapamiento de las coberturas del conjunto de las BTS intervinientes[885].

En una segunda fase, sobre el terreno, en tiempo real y sobre un terminal parado, el investigador pertrechado con un interrogador IMSI/IMEI y un amplificador, recorre el sector acotado en la fase de gabinete. Así, se captan todos los IMSI e IMEI de la operadora que se está buscando hasta que, finalmente, se capte el IMSI e IMEI del concreto terminal intervenido.

A continuación debe realizarse un análisis de la intensidad de la señal y su vector de orientación para aumentar la precisión sobre la situación del emisor. A estos efectos, el interrogador funciona como un goniómetro que permite determinar "la ganancia ideal en una determinada dirección". La repetición de esta operación desde diferentes puntos de estación permite delimitar un área cada vez más reducida mediante la triangulación señalada por el cruce de los sucesivos vectores de máxima ganancia.

B.- Geolocalización con datos conservados por la LCDCE.

Es útil para tratar de localizar posiciones conservadas por las operadoras[886] durante los periodos permitidos por la Ley y cedidas de acuerdo con al LCDCE.

Depende del hecho de que, en el periodo de tiempo en que se ha cometido el suceso delictivo investigado, el objetivo haya hecho uso de su terminal[887] y que esta

[885] A este procedimiento es al que se refiere PÉREZ GIL al explicar las posibilidades técnicas de lograr más precisión mediante el análisis de la constelación que forman la BTS principal y junto con las demás que, en su proximidad, también se sitúan en posición técnica de dar servicio al terminal. Hay que aclarar que esta posibilidad se refiere, en primer lugar, a una estimación más precisa de la posición de un móvil que está parado en un momento dado, en segundo lugar, que su determinación exige un notable despliegue operativo y técnico y, en tercer lugar, que exige al equipo de investigación situarse tácticamente en la zona de intervención, es decir, sin posibilidad de hacerlo desde un gabinete de trabajo. Estas grandes y obvias limitaciones alejan el temor a una PJE con ínfulas de "Gran Hermano" para controlar la vida de quienes le plazca. Vid. Pérez Gil, Julio. *El nuevo papel de la telefónia móvil…op. cit.*, pág. 178.

[886] Un gravísimo problema para los investigadores es poder relacionar los datos conservados por las operadoras y cedidos por mandato judicial con referencia a la ubicación exacta de la BTS en el tiempo en que los recibió, dado que su instalación es variable según la distribución que vaya haciendo cada operadora, instalando o retirando cualquiera de sus antenas o celdas. Es decir, que el análisis del dato puede conducir al error si no se sabe la posición correcta de la celda en el momento de su generación.

[887] En casos no delictivos, como la desaparición de una persona, la situación exigiría que, antes de perder sus capacidades personales (por ejemplo, por pérdida del sentido) o el uso del terminal móvil

circunstancia tenga un interés directo para la investigación, por razón de la oportunidad, tiempo, lugar, tráfico, etc. En esta modalidad y por razones obvias, no pueden generarse datos adicionales de localización por el investigador.

La fase de gabinete es idéntica a la realizada para la modalidad A, pero lo que realmente se estudia es la cobertura real que las BTS de la zona dan al terminal móvil, sabiendo previamente de qué operadora se trata y cuál es el IMSI e IMEI del terminal objetivo.

El procedimiento sobre el terreno consiste en hacer un rastreo en zona de cobertura para estudiar la intensidad de varios puntos de estación del interrogador IMSI/IMEI. La BD de la operadora informará del canal y la frecuencia (GSM o UMTS).

Una vez finalizado el rastreo se dibujan sobre la cartografía de la zona las BTS interesadas y el solapamiento de sus coberturas, tratando de obtener finalmente un polígono lo más reducido posible en que se estime que pudo estar localizado el terminal.

c)Pericias de geolocalización

Suponen una variación del caso B que se ha explicado en el apartado anterior y se orientan principalmente a realizar un estudio pericial sobre el geoposicionamiento de los terminales de los actores de un hecho delictivo.

La finalidad de este estudio – muy complejo por exigirse estudios de DACE conservados y de análisis de coberturas de BTS - no es otra que facilitar al investigador y al juzgador una estimación pericial de la relación espacio-temporal de los terminales de los actores involucrados en los hechos, de las que puedan extraerse conclusiones de valor para el progreso de la investigación o para su eventual valoración como pruebas en el proceso de contradicción del juicio oral.

(por ejemplo, por avería o falta de alimentación electríca) hubiese hecho en las inmediaciones algún uso de su terminal. Adviértanse, por tanto, las extraordinarias dificultades que el investigador-rescatador tiene que afrontar para resolver con angustiosa urgencia la situación.

d) Los datos de cobertura

En apartados anteriores quedó propuesta una definición de *acto de cobertura* como un *"acto por el cual un dispositivo tecnológico apto para mantener una comunicación electrónica completa y con independencia de su realización, establece un enlace técnico permanente o temporal con otro dispositivo técnico de igual o distinta naturaleza y destinado a garantizar, llegado el caso, un acto de comunicación de cualquier clase".* Al mismo tiempo, se puso de manifiesto la naturaleza dual de determinados datos de localización, entre los que se pueden incluir a los de cobertura, y que, siguiendo a GONZÁLEZ LÓPEZ, se clasificaron como *datos eventualmente de tráfico*, ya que podían aparecer o no vinculados funcionalmente con los actos de comunicación[888,889].

En efecto, el contenido de la definición de *acto de cobertura* propuesta se materializa, en el plano de lo práctico, en el enlace vía radio que establece un dispositivo de comunicaciones electrónicas (que tiene insertada una tarjeta SIM de voz y/o datos), como un teléfono móvil, un *smartphone* o una tableta, con la antena o BTS que le da acceso a la red pública de comunicaciones. El propósito de este enlace no es

---

[888] GONZÁLEZ LÓPEZ proporciona abundantes referencias sobre estos datos: *"En Italia se habla de "celle di apertura", como se pone de manifiesto en CAMON, A. "L´acquisizione...", op.cit., p.631. En Alemania se han empleado los términos "Stand-by-Daten", definidos en ALBRECHT, H-J., DORSCH, C., KRÜPE, C., Rechtswirklichkeit und Effizienz der Überwachung der Telekommunikation nach den §§ 100a, 100b StPO und anderer verdeckter Ermittlungsmaßnahmen, Max-Planck-Institut für ausländisches und internacionales Strafrecht, Freiburg i. Br. 2003, nota a pie de* página *20, p.8 como "aquellos datos que se presentan en el ámbito de empleo de un equipo de telefonía móvil como datos de localización ["Standortdaten"] permanentes e independientes del hecho de que el usuario en ese momento telefonee con el equipo (encendido) de telefonía móvil", y, simplemente, "Standordaten" ("datos de localización"), BREYER, P., Die systematische..., op.cit., p.86, término que puede inducir a equívocos con el siguiente tipo de "datos de localización", pero que se distingue claramente de éste atendiendo a la definición que proporciona el autor citado: "aquellos que envía a intervalos periódicos un teléfono móvil en funcionamiento, con el que todavía no se telefonea, a la estación base de difusión de la red"*. Vid. González López, Juan José. *Los datos de tráfico…op.cit.,* pág. 69 y ss.

[889] Sobre si los datos de cobertura son datos de tráfico, el autor dice que *"el problema que se plantea entonces es: ¿existen datos de tráfico desvinculados de la transmisión de información en tiempo real correspondiente a una comunicación? A nuestro entender, no"*, aclarando a renglón seguido que *"nuestra respuesta negativa se refiere a que el hecho que otorga a unos determinados datos la condición de "datos de tráfico" es su tratamiento en el curso de una comunicación en tiempo real"*. Sin embargo, en mi opinión, la promulgación de la LCDCE tuvo un efecto integrador sobre los DACE – si se exceptúa, claro está, su inoperancia respecto de los servicios de la sociedad de la información -, al acoger en su ámbito objetivo conjuntamente a *los "datos de tráfico, localización e identificación"* lo que, en el orden práctico, permite el planteamiento jurídico unificado. Vid. González López, Juan José. *Los datos de tráfico…op.cit.,* pág. 69 y ss.

iniciar una comunicación electrónica sino, simplemente, que el dispositivo quede registrado técnicamente en la red para el eventual establecimiento de comunicaciones electrónicas, pues esto es algo que dependerá únicamente de la libre voluntad del usuario o de la de los terceros que quieran comunicar con él, mediante el marcado del numero de abonado respectivo en el teclado del dispositivo o mediante el acceso a un servicio de comunicaciones prestado por un ISP y conducido por la red.

Lo anterior significa que, mientras el dispositivo esté encendido en un lugar con la suficiente cobertura de una o varias antenas, las BTS lo mantendrán registrado en la red pública de comunicaciones y listo para establecer una comunicación. La operadora que gestiona la red, por su parte, tendrá constancia material de los datos concretos de cobertura con referencia a la localización geográfica de la BTS o de la celda concreta que cumpla esta función[890]. Obviamente, conforme el dispositivo se vaya desplazando a otros lugares, se irá produciendo una serie de conexiones y desconexiones de las sucesivas BTS que estén más próximas en cada momento.

La versión más avanzada del SITEL ofrece en tiempo real los datos de localización de una llamada activa intervenida judicialmente, según el tráfico de conexiones:

- LU[891] ROJO: Significa en el terminal está en cobertura pero sin mantener una comunicación.
- LU VERDE (o *Attach*): Momento en que se produce la conexión a BTS.
- LU NEGRO (o *Dettach*): Momento en que se produce la desconexión de la BTS.

Los datos de localización que posteriormente se conservarán por las operadoras *ex* art. 3.1.f) LCDCE[892], con independencia de que hayan sido intervenidos

[890] "*Como se explica en la respuesta facilitada por la CMT a una consulta particular, "el operador sí puede saber dónde se encuentra el abonado en relación al área cubierta por una antena de telefonía [en este sentido se habla coloquialmente de "tener cobertura"] (son los llamados "datos de localización")",* disponible en http://www.usuariosteleco.es/Derechos/ProteccionPersonales/TratamientoDatosPersonales/Datos+de+localización.htm". Vid. González López, Juan José. *Los datos de tráfico…op.cit.,* pág. 70.

[891] Acrónimo del inglés *localization update* o actualización de la localización. Los datos se ofrecen en referencia la CGI de la BTS que registra la cobertura. Estos datos pueden obtenerse a través del SITEL siempre que haya sido previa y expresamente dispuesto en el mandato judicial.

[892] Es decir, según el 3.1.f) LCDCE "*1º La etiqueta de localización (identificador de celda) al inicio de la comunicación y 2º Los datos que permiten fijar la localización geográfica de la celda, mediante*

o no judicialmente, serán los producidos en el tiempo como consecuencia de los actos de comunicación hechos mediante el uso del terminal, consistiendo únicamente en los referidos a la ubicación geográfica de la BTS a través de la que se dio la primera cobertura. Esto quiere decir que, si una comunicación se ha iniciado a través de una primera BTS y, por haberse producido un desplazamiento del terminal durante un periodo de tiempo los suficientemente largo (por ejemplo, durante un viaje por carretera), el terminal puede haber recibido cobertura sucesivamente desde un número indeterminado de BTS diferentes. Sin embargo, como ha quedado dicho, sólo se conservarán por la operadora los datos geográficos de la primera de ellas.

Pues bien, de la simple lectura del listado de datos de obligada conservación por las operadoras del mercado de las telecomunicaciones establecido *ex* art. 3.1 LCDCE, se constata la ausencia de obligación de conservar los datos de cobertura[893], cuya utilidad para la investigación es incuestionable, especialmente en los casos de urgencia vital o riesgo catastrófico, materia de la que me ocuparé con mayor detenimiento en apartados posteriores.

Sin embargo, la Directiva 2002/58/CE acoge en su definición de datos de localización a los de cobertura *ex a*rt. 2.c): *"datos de localización»: cualquier dato tratado en una red de comunicaciones electrónicas que indique la posición geográfica del equipo terminal de un usuario de un servicio de comunicaciones electrónicas disponible para el público"*[894]. Es evidente que las operadoras se ven en la necesidad técnica de tratar los datos de cobertura en la forma que se indicado y que, por tanto, deberán tener una referencia geográfica de su producción en tiempo real para situarse en disposición de prestar una servicio de comunicaciones electrónicas al usuario registrado en la red.

---

referencia a la etiqueta de localización, durante el período en el que se conservan los datos de las comunicaciones".

[893] Los datos de cobertura, sin comunicación activa, sólo se producen por el uso de la red GPRS (2,5 G) y UMTS (3G).

[894] En el Considerando 3 de la Directiva 2006/24/CE se dice: *"Los artículos 5, 6 y 9 de la Directiva 2002/58/CE definen las normas aplicables al tratamiento, por los proveedores de red y de servicios, de los datos de tráfico y de localización generados por el uso de servicios de comunicaciones electrónicas".*

Consecuentemente, desde este punto de vista, pueden constituirse los razonamientos fácticos y jurídicos que permitan plantear la necesidad de integrarlos en las obligaciones de conservación *ex* arts. 33.5.i).

Es cierto que las gravosas cargas de conservación de datos impuestas a las operadoras *ex* LCDCE aconsejan prudencia a la hora de imponer otras nuevas, todo ello sin perjuicio de sopesarse vías logísticas alternativas para soportarlas. Además, no es difícil prever que el volumen de los datos de cobertura que se han descrito, si se refiriesen al periodo regular de conservación previsto en el art. 5.1 LCDCE, que es de doce meses, se generarían unas necesidades de almacenamiento de proporciones gigantescas.

Por ello, ponderados los criterios de necesidad de contar con este tipo de datos, fuertemente vinculados a la urgencia de intervenir, el planteamiento de una nueva carga de conservación sobre los datos de cobertura debiera referirse, no a la accesibilidad a un extenso repositorio histórico de datos – aunque esto sea muy tentador para cualquier investigador vocacional -, sino a disponer de ciertas capacidades reactivas plenamente justificadas para resolver situaciones graves y perentorias con datos inmediatos a los momentos de su producción.

Hechas las anteriores reflexiones y conocido que las operadoras, en general, conservan los datos de cobertura por razones de gestión técnica interna durante un periodo tiempo que oscila entre las 24 y las 72 horas[895], no sería descabellado plantear un periodo de 72 horas de conservación formal *ex* LCDCE de los datos de la ubicación de la BTS principal (con expresión de sus datos de CGI), e incluso algo superior, para atender reactivamente las necesidades urgentes de intervención, todo ello bajo un régimen jurídico especial de cesión de datos que será objeto de propuesta en apartados posteriores.

5. Necesidad policial de obtener IDACE. La urgencia vital y el riesgo catastrófico.

[895] PÉREZ GIL confirma este último periodo. Vid. Pérez Gil, Julio. *El nuevo papel de la telefónia móvil…op. cit.*, pág. 200.

Uno de los ejemplos más claros de la necesidad de obtener IDACE temprana o, si se prefiere, oportuna – término este intensamente ligado al anterior -, lo representan aquellas investigaciones cuyo signo sea el de la perentoriedad en la reacción policial, bien porque los hechos hayan adquirido o puedan adquirir una extraordinaria gravedad si no se interviene rápida y efectivamente, bien porque razones de urgencia vital perfectamente identificables así lo aconsejen.

Entre los primeros casos, podríamos incluir los hechos protagonizados por las bandas terroristas y grupos de delincuencia organizada o, en cualquier caso, por la necesidad de minorar los riesgos subyacentes a la diseminación de ataques telemáticos sobre importantes intereses públicos o privados[896], como los que se han analizado con la casuística aportada; y, entre los segundos, cualquiera de los casos en que se ponen en riesgo importantes bienes jurídicos entre los que, naturalmente, hemos de considerar la defensa de vida y la libertad. Por ello, y en referencia a estos últimos, se podrían mencionar los homicidios, los secuestros, la violencia de género y las desapariciones de personas, ejemplos que subliman la necesidad de obtener IDACE de forma inmediata y, a veces secundariamente, acceso al contenido de las comunicaciones.

La última aseveración puede parecer extraña, en la frecuente e inexacto entendimiento de que la reacción policial oportuna sólo pueda obtener éxito como consecuencia de la interpretación del contenido material de las comunicaciones mantenidas por los actores que forman parte de la maquinación criminal; pero lo cierto es que lo que, sin pretender restar importancia al contenido material de las comunicaciones, lo que verdaderamente se necesita primariamente es, por ejemplo, lograr la geolocalización del objetivo y poder analizar los demás datos de tráfico e identificación, esto es, de obtener con toda urgencia IDACE[897].

[896] Por ejemplo, para evitar la caída de los servidores desde los que se preste un servicio público esencial, como los de salud, comunicaciones, transporte, protección civil, etc.

[897] Se debe hacer, por otra parte, un inciso en este razonamiento en lo que se refiere a los datos de identificación, que ayudarán a reforzar la idea que viene siendo expresada: los datos de identificación pueden ser falsos o erróneos como consecuencia de la inadecuada legislación española contenida en la disposición adicional única de la LCDCE, en relación con la obligación de los operadores de registrar la identidad de sus clientes, por la acción perturbadora de algunas personas que, de forma maliciosa, adquieren bajo su identidad real o supuesta los terminales móviles de tarjeta prepago para luego derivarlos a usos indeterminados de terceros a los que se los transfieren, haciendo posible la elusión de

Un ejemplo de necesidad de geolocalización de urgencia lo representa un caso sucedido en Requena (Valencia)[898], por el que la familia de un hombre, cuyo paradero desconocía en ese momento, temía que la razón de la desaparición fuera la de usar de forma inminente un arma de caza para suicidarse. Finalmente, se logró su localización tras varias horas de intensa búsqueda física y tecnológica, hallándolo muerto en el interior de su vehículo particular junto a su arma y a su teléfono móvil.

Otro ejemplo, del que no se necesitan mayores explicaciones, lo constituiría la localización de un teléfono móvil que vaya a ser usado como detonador de explosivos en un atentado terrorista y la urgentísima interrupción de sus comunicaciones para evitar su detonación mediante una llamada del asesino[899].

De estos ejemplos, se deduce también el importante papel que juegan las operadoras en el escenario policial, en la que medida que, de su intervención de altísma especialización y acceso a la información, pueda obtenerse el mayor rendimiento posible de la IDACE. Perspectiva que, dada su posición jurídica en relación con el proceso penal – al que alimentan como consecuencia de sus trascendentales obligaciones legales respecto de las comunicaciones electrónicas -, puede llegar incluso a extenderse a una participación activa de naturaleza pericial, algo de lo que se hablará también en los apartados siguientes.

Actualmente, el éxito de este tipo de intervenciones, en lo que refiere a la obtención de datos en tiempo real y con toda lógica, depende de la generación de los DACE que se analicen tras la entrada en eficacia de una intervención de las comunicaciones ordenada por la Autoridad Judicial, lo que implica periodos medios de tiempo de activación de un mínimo estimado de 4 horas, por completo incompatibles con las obvias necesidades de actuar con toda urgencia. A estos periodos de tiempo hay que sumarles, además, los incrementos adicionales como consecuencia de haber emergido nuevos actores en el escenario criminal, lo que generará nuevas y urgentes

---

sus responsabilidades penales que, por otro lado, no alcanzarán presumiblemente a los primeros. Por ello, la identificación del usuario, con ser urgente, lo será menos que los demás datos a los que se ha hecho referencia. Esta perspectiva indica, *sensu contrario,* cuán necesario es obtener inteligencia sobre los datos de tráfico y localización, pues representan una posibilidad efectiva y segura de resolver la emergencia.

[898] DP 2997/2011 del Juzgado de Instrucción núm. 1 de Requena (Valencia).

[899] Bien urgiendo a la operadora a interrumpir las comunicaciones del móvil-detonador, bien haciéndolo mediante el uso táctico del IMSI-Catcher.

necesidades de IDACE. A esas alturas, el explosivo ya se ha consumido, el secuestrador ha ocultado o agredido a su víctima o el desorientado ha sufrido un accidente, por reiterar algunos ejemplos.

Pero la necesidad de IDACE en estos casos no se limita a los que se produzcan como consecuencia de la intervención judicial de las comunicaciones, sino también la que se obtenga del análisis urgente de los DACE conservados *ex* LCDCE, todo ello en la medida en que su estudio pueda clarificar algún aspecto que oriente o revele, al menos, una línea de investigación nueva para resolver la cuestión[900].

Por tanto, independientemente de las consideraciones jurídicas que se dirán, una reacción policial adecuada para tratar alguno de los casos de urgencia vital o riesgo catastrófico que se han enumerado, exigiría la automática conexión a las fuentes de IDACE y la pertinente cesión de datos[901], lo que supondría, según la legislación vigente, una injerencia en los derechos fundamentales de los concernidos sujeta en su apreciación al criterio de proporcionalidad de quien ejerce la acción jurisdiccional, expresado mediante auto motivado y dirigido a la operadora de telecomunicaciones[902] como sujeto obligado por la LCDCE[903].

Pero la LCDCE, no viene dotada de previsiones jurídicas adecuadas para tratar la urgencia, de modo que queden fijadas en el derecho positivo las facultades que puedan ejercer los servicios de emergencia, seguridad o investigación para atender debidamente la excepcionalidad de estas situaciones críticas. Excepcionalidad que

[900] Por ejemplo, imagínese que una persona ha desaparecido y que su teléfono móvil está apagado al tiempo de conocerse los hechos y que, además, no haya sido usado en ningún momento para comunicar desde hace varios días. Sin embargo, para fortuna de la víctima, puede que el teléfono, antes de haber sido desconectado (por pérdida, sustracción, manipulación maliciosa, avería, voluntad propia, agotamiento de la batería, etc.), se haya registrado a una BTS próxima al lugar de su desaparición. En este caso, de conocerse los datos de cobertura, puede estudiarse el terreno por técnicos de la PJE y estimar el lugar donde debe socorrérsele. Naturalmente, de haber comunicado, se podrán estudiar los datos de localización *ex* LCDCE. Si, además, se tratara de un caso de violencia de género, podría obtenerse inteligencia combinada con los relativos a un posible sospechoso.

[901] Adviértase que se está hablando de lo que podría denominarse con mayor propiedad "una cesión dinámica de datos", en la medida en que la necesidad de obtenerlos se revelaría en la medida en que la investigación se fuese desarrollando, a veces, por caminos absolutamente imprevisibles, generando sucesivas y cambiantes necesidades de IDACE (Por ejemplo, la aparición sucesiva de nuevos actores en un secuestro o el seguimiento de una persona desorientada).

[902] Naturalmente, previa identificación de la operadora concreta que esté prestando el servicio de acceso a la red pública de comunicaciones, de acuerdo con las obligaciones impuestas por el art. 33 LGT.

[903] Sobre el estrecho ámbito de los prestadores de servicios de telecomunicaciones a los que alcanza esta ley, vid. Vallés Causada, Luis. *Memoria para la obtención del Diploma de Estudios Avanzados*. Madrid: UNED, 2011. Esta cuestión se tratará con más profundidad en el capítulo siguiente.

debe entenderse respecto del régimen jurídico general pero, en ningún caso, en razón de su frecuencia fenomenológica pues, lamentablemente, son bastante comunes y, desde luego, con una grave y a veces irreparable trascendencia a un sinnúmero de bienes jurídicos protegidos.

Puede decirse, como resumen, que la LCDCE se ata vigorosamente a las muy específicas limitaciones de la persecución penal, como si las conservación de los DACE sólo fuera útil a sus necesidades, llevando automáticamente aparejado un exquisito respeto y cuidado sobre la limitación de los derechos fundamentales de aquellas personas contra las que un día pueda dirigirse la Justicia, lo que sucede de una forma claramente orientada al esclarecimiento de unos hechos que ya han finalizado por completo en el tiempo.

Lo expresado en el anterior párrafo, que no merece en sí mismo la menor crítica, no se compadece bien con otras necesidades propias del carácter dinámico de la investigación penal, que no es estática en modo alguno ni se limita a ver por el retrovisor unos hechos que ya son historia, sino que necesita alimentarse de un proceso continuo de obtención de inteligencia que, en muchos de los casos, no se cierra con la producción de un concreto resultado criminal y su eventual esclarecimiento[904].

Pero, sin olvidar los hechos criminales que requieren una intervención de urgencia, como en un secuestro o un posible atentado, la situación se compadece aún menos en la resolución de las emergencias genéricas - que no suelen tener el más mínimo interés para el proceso penal, como los accidentes o las desapariciones de personas por causas no criminales, como las desorientaciones -, que deben resolverse desde la perspectiva de la seguridad de los ciudadanos y que son atendidas, en muchos casos, directamente por los servicios de emergencia.

[904] Por ejemplo, una red de pornografía infantil no se desmantela porque se haya detenido a un número determinado de pedófilos que hayan intercambiado archivos con contenidos ilícitos en un momento dado, sino que habrá que desmantelar también las diversas estructuras de captación de menores para la obtención de las imágenes. Esta actividad puede, en muchos casos, ocasionar investigaciones de años compuestas, a su vez, de otras investigaciones concomitantes cuyo desarrollo exija un gran dinamismo en la obtención de inteligencia.

a) IDACE en casos de urgencia

En el documento de evaluación de la DCD[905] se informa sobre el modo en que los países miembros, en el ejercicio de sus facultades, la han transpuesto a su Derecho interno, así como sobre los resultados que ha ofrecido la experiencia adquirida.

Según las finalidades de la conservación que han sido admitidas en cada estado miembro, los países pueden agruparse en tres categorías:

Dos de ellas vinculan el acceso a los datos sólo al hecho de que se haya producido un delito grave y sea necesario investigarlo por este medio. La diferencia entre ambas categorías sólo reside en lo que se debe entender por delito grave, pues en unos casos se vincula a una determinada retribución penológica fijada por cada estado miembro, como es el caso de España[906], y en otros, sencillamente, no se define en qué consiste la gravedad[907], lo que, sin duda, causará una notable inseguridad jurídica. Ambas tienen en común, en cualquier caso, la necesidad de que exista un delito de forma precedente como finalidad admisible para la cesión de los datos.

Sin embargo, la tercera categoría, que es la que más interesa ahora, admite que las finalidades por las que se pueda acceder a los DACE no se limiten al tratamiento de la delincuencia grave, pues han reparado en que los DACE sirven también para atender determinadas necesidades generales relacionadas con la delincuencia, así como las emergencias o situaciones de perentoria necesidad de intervención[908].

---

[905] La Directiva es una disposición normativa del Derecho europeo que vincula a sus estados miembros o, alternativamente, al Estado destinatario en la consecución de determinados resultados u objetivos concretos en un plazo dado, dejando a las autoridades internas competentes, sin embargo, la debida elección de la forma y los medios adecuados a los fines perseguidos. Vid. *Informe de evaluación sobre la Directiva de conservación...doc. cit.* Más adelante se incluye un estudio más pormenorizado sobre este importante documento.

[906] Bulgaria, Estonia, Irlanda, Grecia, Lituania, Luxemburgo, Hungría, Países Bajos y Finlandia.

[907] Chipre, Malta, Portugal y Reino Unido.

[908] Bélgica, Dinamarca, Francia, Italia, Letonia, Polonia, Eslovaquia y Eslovenia. Según el documento de evaluación de la DCD, *"estos países, exigen que los datos deben conservarse no sólo para la investigación, detección y enjuiciamiento de delitos graves, sino también en relación con todos los delitos y para la prevención de la delincuencia, o por razones generales de seguridad nacional, estatal o pública"*.

De forma expresa, y sin entrar en el grado de determinación y previsibilidad[909] jurídica exigible, algunos países incluyen entre estas finalidades la búsqueda de personas, como en Bulgaria[910], el salvamento de una vida humana, como en Irlanda[911] o la protección de la seguridad pública, como en Letonia[912].

En el caso de España, el proceso de transposición de la directiva en la LCDCE produjo un texto firme y exclusivamente vinculado con la investigación de los hechos delictivos ya producidos, según las tipologías criminales que tuviesen asociadas penas graves[913,914]. Así, en el art. 1.1 se establece que podrán accederse los DACE conservados:

> *"…a través de la correspondiente autorización judicial con fines de detección, investigación y enjuiciamiento de delitos graves contemplados en el Código Penal o en las leyes penales especiales",*

y en el art. 7.3, referido a los plazos de cesión de los datos, en los que se contempla difusamente la cesión urgente, que:

> *"El plazo de ejecución de la orden de cesión será el fijado por la resolución judicial, atendiendo a la urgencia de la cesión y a los efectos de la*

[909] Sentencia del Tribunal de Justicia de la Unión Europea de 20 de mayo de 2003, en los asuntos acumulados C-465/00, C-138/01 y C-139/01 (Petición de decisión prejudicial: *Verfassungsgerichtshof y Oberster Gerichtshof): Rechnungshof* (C-465/00) contra *Österreichischer Rundfunk* y otros, y entre *Christa Neukomm* (C-138/01), *Joseph Lauermann* (C-139/01) y *Österreichischer Rundfunk* (Protección de las personas físicas en lo que respecta al tratamiento de datos personales - Directiva 95/46/CE - Protección de la intimidad - Divulgación de datos sobre los ingresos de empleados de entidades sujetas al control del *Rechnungshof*). Vid. *Informe de evaluación sobre la Directiva de conservación...doc. cit.*, pág. 9.

[910] Artículo 250 bis, apartado 2, de la Ley sobre Comunicaciones Electrónicas (modificada) de 2010.

[911] Artículo 6 Comunicaciones (Ley de Conservación de Datos) de 2011.

[912] Artículo 71, apartado 1, de la Ley de comunicaciones electrónicas.

[913] Algunos autores consideran que la LCDCE puede usarse en las fases pre-procesales de una investigación. En este sentido, para MORENO CATENA *"esta disposición [la LCDCE], no sólo extiende su ámbito a la explotación de esos datos encaminados a la investigación penal, es decir, a la intervención de los poderes públicos una vez que es conocida la existencia de un hecho delictivo y toma estado ante los tribunales del orden jurisdiccional penal, sino que también comprende la explotación de los datos para la detección de los delitos, fundamentalmente en lo que se refiere a la labor de los servicios de inteligencia (CNI), en situaciones predelictuales o, en todo caso, con independencia de que se haya abierto un procedimiento penal para la persecución de un concreto delito"*. Vid. Moreno Catena, Víctor. *Ley de conservación...op. cit*.

[914] Puede plantearse también la discusión sobre si la LCDCE tiene también una finalidad preventiva. Es evidente que le mera existencia de la ley hará precaverse a los delincuentes más advertidos sobre las posibilidades de que se obtengan por su mediación pruebas eficientes sobre los hechos delictivos que puedan protagonizar. Puede existir, por tanto, una más que reconocible previsibilidad en la Ley que aconsejará a las personas ajustar su conducta para evitar vulnerarla.

investigación de que se trate, así como a la naturaleza y complejidad técnica de la operación.

Si no se establece otro plazo distinto, la cesión deberá efectuarse dentro de las setenta y dos horas contadas a partir de las 8:00 horas del día laborable siguiente a aquél en que el sujeto obligado reciba la orden".

De la simple lectura de la anterior norma, desde el punto de vista de la intervención policial de urgencia, se deben destacar tres elementos:

- Que la cesión queda condicionada a la previa emisión formal de un orden judicial.
- Que el plazo de entrega es el que fije la Autoridad Judicial en la resolución, pero que, en cualquier caso, habrá de valorarse la urgencia en la cesión.
- Que los condicionantes de orden técnico y la "complejidad de la operación", aunque esto sea obvio, comprometerán la viabilidad de la cesión en cuanto a su calidad.

Evidentemente, la cuestión de la perentoriedad de la intervención policial queda condicionada a los tiempos asociados a la disposición material de una resolución judicial motivada y los que impongan las operaciones técnicas de acceso, selección y cesión de los datos al agente facultado. Es decir, en la práctica, a unos tiempos muy dilatados y absolutamente incompatibles con la urgencia sobre los que no es necesario incidir más por el momento.

Puede concluirse, por ahora parcialmente, que la LCDCE no se orientó en absoluto al tratamiento de la urgencia, sino a alimentar un supuestamente pausado discurrir de la investigación puramente criminal sobre hechos ya acaecidos, pues no reparó en la utilidad de los DACE para resolver gravísimas situaciones de hecho como las que se han comentado en la reseña fenomenológica, ni dotó a las FFCCSS ni a los servicios de emergencia de los instrumentos jurídicos suficientes – o, al menos, a los primeros - que requerían, no sólo ya la excepcionalidad de estas situaciones, sino su carácter dinámico y cambiante.

Así las cosas, el acceso de los ciudadanos en situación crítica a los diversos servicios de emergencia puede hacerse a través de una llamada telefónica al número

112, como servicio público genérico para este fin, o a los números de atención ciudadana 062, de la Guardia Civil, o 091, del CNP, siempre que, naturalmente, estén en condiciones de hacerlo pues, en caso contrario, la oportunidad de recibir auxilio queda a merced de las insuficiencias de la LCDCE.

Lo anteriormente expuesto describe, por tanto, los dos modos diferentes de acceder a los DACE en casos de urgencia: De un lado, el que habilita la LCDCE para investigar exclusivamente los delitos graves y, de otro, el acceso de los servicios de emergencia a determinados DACE, que se realiza a través de la legislación sobre el número telefónico de emergencias 112 y referidos exclusivamente a la llamada por la que se solicite un auxilio.

Comenzando por la segunda modalidad, en transposición de la Directiva 91/396/CEE del Consejo, de 29 de julio de 1991, *relativa a la creación de un número de llamada de urgencia único europeo*, se legisló en España lo relacionado con la materia mediante el Real Decreto 903/1997, de 16 de junio, *por el que se regula el acceso, mediante redes de telecomunicaciones, al servicio de atención de llamadas de urgencia a través del número telefónico 112.*

La finalidad, en la faceta que afecta al interés de este estudio, no era otra que conocer los datos de identificación y localización de los ciudadanos en riesgo, pero siempre constreñida a que estos hiciesen una llamada al número 112, 062 ó 091. Es decir, en ningún caso, para acceder a los datos partiendo del conocimiento más o menos preciso de la situación de emergencia en sí misma, ni de los números de los abonados a los que fuese preciso asistir. En consecuencia, las facultades indagatorias se reducían exclusivamente a acceder los concretos datos de la llamada entrante que permite la legislación nacional.

Así, según reza el art. 3.3 del RD, *"…dichos operadores facilitarán la identificación automática de la línea o zona geográfica desde donde se efectúen las llamadas al número telefónico 112, dentro de las posibilidades técnicas de la red y de acuerdo con la regulación que sobre las facilidades de presentación y limitación de la línea llamante se establezcan en la normativa nacional y comunitaria para salvaguardar la seguridad nacional, la defensa, la seguridad pública y la prevención, investigación y persecución de delitos, la seguridad de la vida humana o razones de*

interés público. En todo caso, lo establecido en el párrafo anterior se entenderá sin perjuicio de las medidas que se adopten para garantizar el secreto de las comunicaciones, de acuerdo con lo establecido en el artículo 18.3 de la Constitución, y la protección de los datos personales, conforme a lo dispuesto en la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal, y en sus normas de desarrollo y disposiciones complementarias"[915].

De esta constricción legal no se libran las FFCCSS en el ejercicio de otros cometidos, pues su faceta de servicios de emergencia no es transferible a las funcionalidades de la PJE, por más que esta última se inserte orgánicamente en aquellas, de lo que es fiel reflejo el contenido del Informe 2005-0297 de la AEPD, donde se dice en respuesta a una consulta sobre la materia que:

> *"Para resolver esta cuestión no será posible estar a la Resolución de la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información de 28 de septiembre de 2004, aportada junto con la consulta, dado que la habilitación otorgada en dicha Resolución a la Dirección General de la Policía y a la Dirección General de la Guardia Civil lo es al amparo de lo dispuesto en el artículo 38.5 de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones y en la Orden CTE/711/2002, de 26 de marzo.*

[915] En la Orden de 14 octubre de 1999, *sobre condiciones de suministro de información relevante para la prestación del servicio de atención de llamadas de urgencia a través del número 112*, se precisa en su art. 2, sobre la Información que facilitarán los operadores, que *"los operadores obligados a los que se refiere el artículo 1, deberán facilitar a las Comunidades Autónomas, a las Ciudades de Ceuta y Melilla o a las entidades prestatarias autorizadas que hayan asumido la prestación del servicio de llamadas de urgencia a través del número telefónico 112 (en adelante, entidades prestatarias), a petición de éstas, las correspondientes bases de datos que permitan relacionar e identificar el número de la línea llamante y la dirección (como mínimo, cuando estén disponibles: Provincia, municipio, núcleo de población, código postal, calle, número de casa, planta y piso) o zona geográfica desde la que se efectúa la llamada, en el ámbito territorial de la competencia de aquéllas.*
En ambos casos, las mencionadas bases de datos contendrán, en la medida en que estén disponibles por parte de los operadores, el nombre, apellidos, documento nacional de identidad y dirección correspondiente al titular de la línea telefónica fija o móvil desde donde se efectúa la llamada.
En el caso de llamadas realizadas al número 112 desde el servicio de telefonía móvil automática, en su modalidad analógica, los operadores obligados que prestan dichos servicios realizarán, bajo petición de las entidades prestatarias, los correspondientes traceos de llamadas para determinar la ubicación de la correspondiente situación de la celda que ha recogido la llamada.
Los operadores obligados colaborarán para que se realice de forma efectiva el traspaso de la información que suministran a las entidades prestatarias. Los programas para la explotación de las bases de datos se podrán suministrar por los operadores, de manera voluntaria, si así se pacta entre las partes".

De este modo, la citada Resolución autoriza la comunicación de datos de abonados a los citados Órganos en tanto prestan servicios de atención de llamadas de urgencia a través de los números 091 y 062 y no atiende a las funciones atribuidas a los integrantes de los mismos por el artículo 549.1 de la Ley Orgánica del Poder Judicial".

En mi opinión, la realidad de las emergencias exige inequívocamente la confluencia de ambas legislaciones pues, independientemente del interés final que los hechos puedan tener para el proceso penal, lo cierto es que su resolución necesita de un amplio enfoque en materia de acceso a los DACE, que aúne las facultades reactivas con las investigativas y, todo ello, con el despliegue de sus sofisticados recursos humanos y tecnológicos, de modo que el Derecho resuelva adecuadamente esta contingencia mediante la positivización de las normas que sean precisas.

No obstante, las facultades de acceso a los DACE que ampara el RD 903/1997 se agotan en las prestaciones que actualmente facilitan los servicios de emergencia, no siendo posible extenderlas por tratarse de un más que meritorio servicio, pero cuya principal aportación es, únicamente, la de alertar en su significado más genuino.

Por ello, una vez conocida y comprobada la naturaleza de la contingencia (por ejemplo, un accidente de montaña), y conocido el número de abonado de la víctima, sus demás datos personales y los de localización de su terminal, pueden los servicios de emergencia transferir y documentar básicamente la inmediata actuación de las asistencias (en el ejemplo, la localización de un familiar que dé razón del paradero exacto de la víctima, el aviso a un servicio de rescate en montaña y a un helicóptero de transporte sanitario, como los que dispone la Guardia Civil, que ya sabrán desde un primer momento a dónde dirigirse sin necesidad de mayor información).

Pero imagínese ahora que el accidentado ha perdido la consciencia, se halla en riesgo de desangrarse o congelarse y que el sector cubierto por la celda de telefonía desde donde el accidentado llamó antes de que su situación se agravase, sea de tal amplitud que exija un estudio más detallado para determinar la ubicación precisa del terminal.

Es notorio, en este caso, que las posibilidades del servicio de emergencias no darán más de sí, entrando en juego los recursos técnicos de geolocalización que se han descrito en apartados anteriores.

Pero aún hay más: Piénsese ahora en un secuestro, en el que además se producen desplazamientos de la víctima y en que la información no provenga de un servicio de emergencias (los secuestradores no les suelen comunicar sus intenciones), sino de un particular que avisa a las FFCCSS de la situación. En este caso, deberán activarse dinámicamente las facultades contenidas en la LCDCE pero, lamentablemente, con las insuficiencias que se han expuesto.

Lo urgente en este caso será, en rasgos generales, analizar en tiempo real los datos de cobertura de los teléfonos de los actores del suceso – fuera de la regulación de la LCDCE -, estudiar los demás datos conservados, integrar la información de estas fuentes con las demás de las que se disponga y, en definitiva, activar todas las posibilidades en las que el legislador pensó cuando se determinó a imponer a todos los ciudadanos la conservación de sus datos de tráfico, localización e identificación.

Para resolver el problema de un modo jurídicamente admisible, es necesario establecer *lege ferenda* un sistema de cesión urgente de los DACE según los condicionamientos fácticos y jurídicos planteados.

a) El requerimiento de cesión urgente de los DACE.

RODRÍGUEZ LAINZ, al comentar diversas cuestiones sobre la proporcionalidad en relación con las materias tratadas en el LCDCE, afirma que:

> *"Como no podía ser de otra forma, el legislador somete la concreta utilización de los datos almacenados por mandato de su art. 1 a las exigencias clásicas de cualquier restricción de derechos fundamentales, cuales son: en primer lugar la previsión legal; en segundo la reserva de decisión judicial motivada, que podría ser salvada por una actuación de la Policía Judicial en supuestos de urgencia, cuando no existiera una reserva estricta de decisión*

judicial; y en tercer lugar, «...la estricta observancia del principio de proporcionalidad, concretado en tres requisitos o condiciones: idoneidad de la medida para alcanzar el fin constitucionalmente legítimo perseguido (juicio de idoneidad), que la misma resulte imprescindible o necesaria para ello, esto es, que no existan otras medidas menos gravosas que, sin imponer sacrificio alguno de derechos fundamentales o con un sacrificio menor, sean igualmente aptas para dicho fin (juicio de necesidad), y, por último, que se deriven de su aplicación más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o intereses en conflicto, o dicho de otro modo, que el sacrificio impuesto al derecho fundamental no resulte desmedido en relación con la gravedad de los hechos y las sospechas existentes (juicio de proporcionalidad en sentido estricto)» (SSTC 234/1997, de 18 de diciembre, 70/2002, de 3 de abril, 25/2005, de 14 de febrero y 206/2007, de 24 de septiembre entre otras)".

Sin embargo, la voluntariosa apuesta del autor para que la PJE pueda requerir de propia autoridad los DACE en los supuestos de urgencia choca frontalmente, en mi opinión, con la contundencia del art. 1.1 LCDCE respecto de la exclusiva reserva judicial que, por otro lado, el mismo autor reconoce. Por ello, si en el plano doctrinal pueden considerarse pronunciamientos de esta naturaleza, la realidad policial mostrará hasta qué punto, con semejante redacción del precepto legal, sería imposible lograr una cesión de datos aún basando la petición en el más execrable de los crímenes. No sólo eso, sino que, a no dudar, en el enjuiciamiento posterior de los hechos, tal cesión sería invocada en los debates procesales como causa de nulidad de las actuaciones.

Pero lo que sí se puede hacer constar es la más absoluta razonabilidad de la posición de RODRÍGUEZ LAINZ, ya que sería completamente necesario que la PJE pudiese contar con la posibilidad de efectuar un ***requerimiento de cesión urgente*** de los DACE que hiciera confluir las facultades legales mencionadas en el apartado anterior de un modo jurídicamente eficiente.

Pero, para que esto gane toda su eficacia, y visto que las soluciones prácticas de la casuística relacionada con la urgencia vital vienen de la mano, en muchas ocasiones, de las facultades propias de la función de policía judicial, deben introducirse algunos

cambios en la LCDCE, que es la norma en la que, sin excederla en la orientación de la DCD, deberá plantearse una revisión o mejora[916].

En este sentido, el art. 11.2.a LOPD establece sobre la excepción del consentimiento para la comunicación de datos, que será posible "*cuando la cesión está autorizada en una ley"*. Consecuentemente, la Ley debe establecer cuándo el consentimiento podrá eludirse en casos excepcionales, como los que, con toda lógica, suponen las situaciones de urgencia vital o riesgo catastrófico.

Algunos de los condicionamientos deberían ser tenidos en cuenta para tratar la excepcionalidad relacionada con la urgencia son los siguientes:

En primer lugar, en atención al principio de proporcionalidad, que no exista un medio alternativo menos gravoso para resolver favorablemente la situación y sin que esta decisión comporte riesgos inasumibles.

En segundo lugar, es exigible que la PJE haya actuado con la debida diligencia en el análisis de los indicios que permitan identificar, sin dudas más allá de lo razonable, que se trata de una situación de emergencia que exige la instauración de las medidas excepcionales contempladas en la Ley.

En tercer lugar, deben reiterarse todas las obligaciones incluidas en los arts. 549.1.a) LOPJ, 11.2.d) LOPD, 22.2 LOPD y 1, 2 y 4 RDPJ, que demandarán de la PJE la más exigente acreditación de las causas que le obligaron a activar las facultades excepcionales contenidas en la norma y a informar de todo ello al Juez.

Es evidente que el procedimiento de urgencia no está orientado a eludir la acción de este último sino, dadas las circunstancias, a actuar de acuerdo con la proporcionalidad de unas medidas previstas para atender dinámicamente y con toda urgencia situaciones de claro carácter excepcional y grave, dándole inmediata cuenta de lo actuado junto con la documentación que le permita instaurar, a la mayor brevedad, su más eficaz control de jurisdiccionalidad sobre lo ya iniciado, así como la

[916] Sobre la excepción de la urgencia y las posibilidades de intervención de la PJ de propia autoridad ante *"la imposibilidad de recabar la autorización judicial sin riesgo de que se pierda o borre la información"*, vid. Martín Pallín, José Antonio. 2008. *El equilibrio entre la conservación…op. cit.,* pág. 161.

tutela judicial efectiva de los actores del suceso con todas sus consecuencias, incluida la declaración de la eventual improcedencia de lo actuado[917,918].

Sobre este último aspecto, es evidente también la necesidad de controlar un posible uso desviado o desproporcionado de las facultades excepcionales por parte de la PJE, mediante las debidas medidas correctoras que resulte procedente aplicar.

En cuarto lugar, comunicar a las operadoras el requerimiento de cesión de datos con expresa de aclaración de ampararse en un procedimiento de urgencia establecido en la Ley y en las obligaciones que, al efecto, se contraigan.

En quinto lugar, disponer de sistemas seguros de transferencia telemática de documentos con las partes implicadas.

En sexto lugar, facilitar el acceso al registro telemático y de auditoría que se active sobre los datos accedidos, todo ello como modo de garantía y salvaguarda de la procedencia de haber actuado de un modo proporcional a la emergencia tratada. Este elemento objetivo que, con apoyo de la tecnología, aporta un contraste jurídicamente seguro, debe ponerse a la inmediata disposición de la Autoridad Judicial.

Las soluciones que se proponen para establecer un marco adecuado a las finalidades anteriores, son las siguientes:

---

[917] El acceso urgente y excepcional a los datos para resolver situaciones de urgencia no es extraño en el Derecho pues, como comenta VELASCO respecto de los contenidos de un teléfono móvil incautado por la PJE – y nótese que no sólo habla de contenido formal, sino también material -, podría considerarse un control posterior de judicialidad: *"Sin embargo y muy, muy excepcionalmente, en supuestos de eminente e indiscutible urgencia, cabe la apertura policial de propia autoridad sin mandamiento judicial del correo electrónico o SMS aprehendido si existiesen razones de urgencia, necesidad e inmediatez para la prevención y averiguación del delito, el descubrimiento de los delincuentes y la obtención de pruebas incriminatorias, respetándose en todo caso el principio de proporcionalidad (Vid. STC 70/2002, de 3 de abril) y siempre que sea con posterioridad convalidado judicialmente, no mediante un análisis ex post facto en función de lo aprehendido, sino ex ante, considerando la concurrencia o no de esas circunstancias excepcionales, entre las que se encontrará en los dispositivos electrónicos la posibilidad de su borrado, porque, de lo contrario, la actuación policial – al inmiscuirse en la intimidad ajena – debe consistir en acudir al Juez para la apertura del mensaje, mediante la confiscación y envío del soporte físico en que se conserva, si esto garantiza y evita que desaparezca o técnicamente se borre desde otro punto"*. Vid. Velasco Núñez, Eloy. *Delitos cometidos a través de Internet…op. cit.,* pág. 97.

[918] *"En relación a la necesidad de autorización judicial, el criterio general, conforme a nuestra jurisprudencia, es que sólo pueden llevarse a cabo injerencias en el ámbito de este derecho fundamental mediante la preceptiva resolución judicial motivada que se adecue al principio de proporcionalidad (SSTC 207/1996, de 16 de diciembre, FJ 4; 25/2005, de 14 de febrero, FJ 6; y 233/2005, de 26 de septiembre, FJ 4). Esta regla no se aplica, también según nuestra doctrina, en los supuestos en que concurran motivos justificados para la intervención policial inmediata, que ha de respetar también el principio de proporcionalidad"* (STC 173/2011, de 7 de noviembre).

En primer lugar, introducir en las categorías de datos a conservar los de cobertura, en el entendimiento de que su acceso inmediato y dinámico por la PJE contribuye a determinar la localización de los actores del suceso. Los datos de cobertura, accedidos exclusivamente bajo esta etiqueta, no guardan relación con las comunicaciones electrónicas que eventualmente puedan producirse durante el periodo de cesión, por lo que deben considerarse meros datos de localización del terminal pero no de tráfico[919].

En segundo lugar, los datos de GPS tratados en régimen de valor añadido[920] y sin vinculación a los actos de comunicación deben quedar fuera de la regulación de la LCDCE y considerarse jurídicamente una injerencia leve en el derecho a la intimidad análoga a la que supone el uso de las balizas, en consonancia con los pronunciamientos jurisprudenciales que se han estudiado, y propios de la labor indagatoria de la PJE[921,922,923].

En tercer lugar, en el régimen jurídico de los *logs* de las transacciones telemáticas debe considerarse también la eventual cesión urgente de su contenido formal referido a aquellos datos que supongan un elemento de interés para la resolución de la emergencia, como sería, por ejemplo, la ubicación del punto de acceso a la red y los demás datos que racionalmente puedan contribuir a tan necesario fin.

---

[919] Vid. González López, Juan José. *Los datos de tráfico…op.cit.,* pág. 170 y ss.

[920] *Art. 2.g) Directiva 2002/58/CE: "Servicio con valor añadido»: todo servicio que requiere el tratamiento de datos de tráfico o datos de localización distintos de los de tráfico que vayan más allá de lo necesario para la transmisión de una comunicación o su facturación".*

[921] Sobre el ámbito de lo policial al que debe circunscribirse la indagación de los datos de localización no vinculados a las comunicaciones en curso o finalizadas, es decir, cuando estos se traten aisladamente, GONZÁLEZ LÓPEZ hace una referencia al derecho italiano en donde esto se admite, con cita de Camon, A. *L'acquisizione…op. cit*. Vid. González López, Juan José. *Los datos de tráfico…op.cit.,* pág. 171. Este autor observa una mayor amplitud en el rendimiento de los datos de cobertura debido al número de los que se reciben durante el periodo de tiempo accedido, por lo que resultan útiles para el establecimiento de perfiles de movimiento. Todo ello le lleva a concluir que debe contarse con una regulación específica, opción a la que debo adherirme sin reservas.

[922] GONZÁLEZ LÓPEZ dice que *"por lo que se refiere a los datos de localización geográfica (GPS), las dudas son menores, por tratarse de datos cuya utilidad al margen de las comunicaciones en curso es diáfana"* y se apoya en Aprile, E. Spiezia, F. *Le intercettazioni telefoniche ed ambientali. Innovazioni tecnologiche e nuove questioni giuridiche.* Milano: Giuffrè Editore, 2004. Vid. González López, Juan José. *Los datos de tráfico…op.cit.,* pág. 172.

[923] En lo que se refiere a la transferencia europea de datos, esta conceptuación jurídica no impediría el uso de las facultades de intercambio de información contenidas en la Decisión Marco 2006/960/JAI, que impide la trasferencia de datos obtenidos por medios coercitivos, ya que los propuestos no lo serían.

En cualquier caso, bajo situaciones de emergencia, el consentimiento de las víctimas debe presumirse tácito[924] y sin necesidad de requerirse la autorización judicial para acceder a los datos regulados por la LCDCE, en lo proporcional a la situación de hecho producida y en las condiciones expuestas anteriormente en cuanto a la obligación de facilitar el control jurisdiccional de las medidas.

A todos estos efectos, el derecho positivo debería contener alguna regulación al respecto en orden a la instauración de la debida seguridad jurídica que debe respaldar el uso de los medios técnicos de investigación por la PJE.

Reiterados todos los argumentos y prevenciones que se han mencionado en la parte expositiva de este trabajo, la cesión de los DACE a la PJ en los casos de urgencia vital debiera producirse mediante la apoyatura en los canales telemáticos seguros que actualmente están activos y en pleno rendimiento entre las diferentes unidades de PJ y las compañías de telefonía autorizadas a operar en el Mercado de las Telecomunicaciones. Este sistema permite, en un periodo razonable de tiempo, la solicitud y cesión telemática de los DACE relativos a los objetivos a investigar a través de los módulos de comunicación del SITEL, así como de los documentos justificativos de la procedencia de la medida redactados por la PJ y que cumplieran con los requerimientos que a los fines indicados fuesen admisibles en Derecho.

En la actualidad, el Poder Judicial está ausente de este canal[925,926], siendo deseable que a la mayor brevedad se implementen las soluciones telemáticas de

---

[924] *"Tampoco podrá considerarse ilegítima aquella injerencia o intromisión en el derecho a la intimidad que encuentra su fundamento en la necesidad de preservar el ámbito de protección de otros derechos fundamentales u otros bienes jurídicos constitucionalmente protegidos".* (SSTC 159/2009, de 29 de junio, FJ 3 y 173/2011, de 7 de noviembre)".

[925] Sobre los interfaces de comunicación, véase el art. 33.9 LGT: *"Los sujetos obligados deberán tener en todo momento preparadas una o más interfaces a través de las cuales las comunicaciones electrónicas interceptadas y la información relativa a la interceptación se transmitirán a los centros de recepción de las interceptaciones. Las características de estas interfaces y el formato para la transmisión de las comunicaciones interceptadas a estos centros estarán sujetas a las especificaciones técnicas que reglamentariamente se establezcan por el Ministerio de Industria, Turismo y Comercio".*

[926] Es de desear que las iniciativas europeas y española en materia de e-Justicia progresen en esta dirección. Sobre los desarrollos europeos, vid. *Hacia una estrategia europea en materia de e-Justicia (Justicia en línea). COM(2008) 329 final* y la abundante producción documental sobre la materira. En lo que se refiere a los españoles, vid. *Plan de modernización de la Justicia 2009-2012* y la Ley 18/2011, de 5 de julio, *reguladora del uso de las tecnologías de la información y la comunicación en la Administración de Justicia*. A título ilustrativo, véase la labor del CGPJ sobre la e-Justicia en el portal:

integración orientadas a mejorar, en primer lugar, la más estricta observancia de los derechos fundamentales de las personas concernidas y, desde luego, a hacer eficaz la disponibilidad de los DACE en los casos relatados.

b) El requerimiento de preservación de datos

El ***requerimiento de preservación de datos*** debe contemplarse únicamente como una alternativa – sin duda de menor utilidad para la investigación criminal[927] - al procedimiento de cesión urgente de aquellos DACE cuya conservación no esté incluida actualmente en los arts. 3.1 LCDCE y 33.5 LGT[928], todo lo cual se preordena a evitar su pérdida y a minimizar en lo posible las perniciosas consecuencias del periodo de "ceguera de datos" ocasionado por las eventuales demoras en la disposición de una autorización judicial *ex* art. 1.1 LCDCE, todo ello en caso de que el procedimiento de urgencia que se ha propuesto no fuese jurídicamente viable[929].

Consistiría en la práctica en facultar a la PJE en forma análoga en lo esencial a como se previene en los arts. 16 al 18 CCib[930] para los DACE de las transacciones

---

http://www.poderjudicial.es/cgpj/es/Temas/e_Justicia. También, vid. De la Oliva Santos, Andrés, Gascón Inchausti, Fernando y Aguilera Morales, Marién (coordinadores). *E-Justicia en la Unión Europea.* Cízur Menor: Aranzadi, 2012. ISBN 9788499039824.

927 *"…mientras que la conservación tiene como resultado la disponibilidad de datos históricos, la preservación no garantiza la capacidad para establecer pistas de pruebas antes de la orden de preservación, no permite realizar investigaciones si el objetivo es desconocido y no permite obtener pruebas sobre los movimientos de, por ejemplo, las víctimas o testigos de un delito".* Vid. *Informe de evaluación sobre la Directiva de conservación...doc. cit.,* pág. 6.

928 La evolución de las TIC puede producir nuevos datos cuyo acceso por la PJE pueda ser relevante para los legítimos fines de una investigación.

929 Con toda evidencia, este procedimiento se dirige a poder disponer, al menos, de la máxima información sobre los DACE aunque llegue tarde.

930 En el pto. 3.3 del documento de evaluación de la DCD se aclara que *"la preservación de datos es distinta de la conservación de datos (también llamada «congelación rápida»), en virtud de la cual los operadores notificados con una orden judicial están obligados a conservar los datos relativos únicamente a determinados individuos sospechosos de actividad delictiva a partir de la fecha de la orden de preservación".* Además de los requerimientos que para los casos de urgencia se proponen en este apartado para ser ejecutados de propia autoridad por la PJE, mediante orden judicial, podrían preservarse también aquellos datos, fuera de los casos de urgencia, no conservados por exigencia de la LCDCE o no cancelados por las operadoras o ISP, sobre aquellas personas objeto del interés del proceso penal (en el documento mencionado se habla del "*procedimiento de congelación plus",* que iría *"más allá de la preservación de datos, en el sentido de que un Juez puede también conceder acceso a datos que aún no hayan sido suprimidos por los operadores. Además, se establecería una exención muy limitada por ley de la obligación de suprimir, por un breve período de tiempo, determinados datos de*

telemáticas de modo que, de propia autoridad, pudiese dirigirse a los operadores e ISP para que preservasen determinados DACE de interés para la investigación, pero sin acceder por el momento a ellos, según el deber de colaboración *ex* arts. 118 CE y 17 LOPJ, cosa que quedaría reservada al resultado del control *ex post* de la Autoridad Judicial bajo los condicionamientos que finalmente estimase procedente adoptar y que no tendrían por qué ser coincidentes con la preservación señalada por la PJE.

Técnicamente, la preservación no supondría un acceso por la PJE a los datos, que está prohibido por el art. 1.1 LCDCE, sino una salvaguarda de los que pudieran interesar por razones objetivas de la investigación[931], condicionada a lo que indicase posteriormente el Juez *ex* art. 1.1. LCDCE en auto motivado, por el que se habilitase a los agentes facultados en la extensión y límites que considerase proporcionados, momento en que la aplicación de la ley adquiriría toda su eficacia.

6. Conclusiones preliminares

Deseando aportar seguridad jurídica al proceso de cesión de datos sobre las comunicaciones ya finalizadas, de forma precedente a la LCDCE, no sólo la doctrina y la jurisprudencia españolas apuestan por el mandato judicial previo, sino también algunas recomendaciones que pueden hallarse en el derecho internacional, así como en el derecho comparado[932], en lo que supone de facto una equiparación jurídica de

comunicación que no se almacenan normalmente, como datos de localización, datos de conexión a Internet y direcciones IP dinámicas de usuarios que tienen una suscripción de tarifa plana, y cuando no es preciso almacenar tales datos a efectos de facturación"). En el texto insertado en primer lugar, por otra parte, se habla de contar con una orden judicial pero, como es de ver, se hace necesario un procedimiento que evite el riesgo de demora en los justificados casos de urgencia en que sea jurídicamente admisible. Vid. *Informe de evaluación sobre la Directiva de conservación...doc. cit.,* pág. 5 y ss.

[931] Esta posibilidad podría ser muy útil en aquellos casos en que los DACE no fuesen de ordinario solicitados por los investigadores por su excepcionalidad de uso o por cualquier otra razón que aconsejase reserva en la decisión de su conservación legal. Por ejemplo, en las tareas de geolocalización, sería muy conveniente analizar, no sólo los datos de cobertura de la BTS principal, sino los de las demás que temporalmente formen parte de la constelación que estén dando cobertura secundaria al terminal. Esto permitiría mejorar la calidad, precisión y oportunidad de la geolocalización. Además, podrían mejorarse los datos de CGI con la aportación de la intensidad de la señal, la dirección, etc.

[932] En la exposición de motivos del CCib se manifiesta que debiera optarse por que la revelación de estos datos *"haya sido ordenada por autoridades judiciales"*. En igual sentido, en los pronunciamientos del Grupo del Artículo 29 y en el derecho comparado. Por su interés, se reproducen las referencias

los datos de tráfico en tiempo real a los conservados sobre las comunicaciones ya finalizadas.

Esta rígida perspectiva, al hacer tabla rasa en la protección de cuanto tuviera que ver mínimamente con las comunicaciones electrónicas, no reparó en los grises que había entre blancos y negros, produciendo una norma que, sin ocultar sus aciertos, se compadece poco con algunos aspectos de la realidad del uso social de las TIC y, consiguientemente, de su dimensión criminal.

Así, como defectos más notorios, podrían señalarse la ausencia de normas sobre los procedimientos de cesión de urgencia en casos de peligro por demora, la falta de categorización de determinados datos que no tienen relación con los actos de comunicación, como los del cobertura o los de valor añadido – e incluso sobre la propia conceptuación de lo que debe entenderse por comunicación -, el tratamiento automatizado de determinados DACE y, naturalmente, la omisión de imponer determinadas obligaciones de conservación de los *logs* de las transacciones telemáticas.

En toda esta discusión subyace la cuestión del secreto y la reserva judicial, que se extienden claramente cuando se hace residir el núcleo de los derechos fundamentales en el art. 18.3 CE y no tanto cuando de lo que se habla es del arts. 18. 1 y 18.4 CE.

Pero discutir a estas alturas esta materia no sólo parece condenado al fracaso, pues la LCDCE optó claramente por la reserva judicial, sino que, como es de ver en

---

aportadas al efecto por GONZÁLEZ LÓPEZ: *"Por lo que respecta al acopio de datos de tráfico, puede consultarse Martínez Martínez, R. Tecnologías..., op.cit., p.266, Pérez Gil, J. "Medidas...", op.cit., p.915, y Rodríguez Lainz, J. L. Intervención..., op.cit., p.498. Se reclama previo requerimiento judicial también en Guerrero Picó, M. C. "Protección...", op.cit., p.135, y Cabezudo Rodríguez, N. "La Administración...", op.cit., nota a pie de* página *63, p.187. Incluso en Velasco Núñez, E., "Aspectos...", op.cit., p.6, a pesar de la postura que mantiene en cuanto a la vulneración de derechos fundamentales, se aconseja buscar la intervención judicial, en el marco de un proceso penal abierto. En relación con ello, en cuanto que datos de carácter personal, también se reclama en* DE LA ROSA CORTINA, J.M., *"Análisis...", op.cit., p.4, respecto del acceso a datos médicos, si bien se vincula la afección al derecho a la intimidad. A este respecto, en Guerrero Picó, M. C. El impacto..., op.cit., p.470, se afirma que "los únicos que pueden autorizar una injerencia en el derecho fundamental a la protección de los datos de carácter personal por necesidades derivadas de una investigación criminal son los jueces". En Marchena Gómez, M. "Dimensión...", op.cit., p.15, por su parte, sin emitir un pronunciamiento rotundo, se advierte, a la luz de la jurisprudencia, del ·"fundado riesgo" de incurrir en el supuesto del artículo 11.1 LOPJ, en caso de recabo de los datos por el MF sin autorización judicial previa"*. Vid. González López, Juan José. *Los datos de tráfico…op.cit.*, pág. 337 y ss.

documento de evaluación de la DCD, una buena mayoría de los países miembros de la UE decidieron por esta vía en su derecho interno, sin contar con el rechazo a la transposición por los tribunales constitucionales de tres de los países. Intentar residenciar la cesión de datos de tráfico en el derecho a la protección de datos sería considerado, sin duda, regresivo y no sólo en un plano temporal sino, claramente, en lo que tuvo de avance democrático frente a la controvertida decisión del legislador europeo de ordenar la masiva conservación de los datos de tráfico de las comunicaciones de sus ciudadanos.

Por ello, las propuestas de este trabajo no se orientan a sustraerse del control judicial sino a hacerlo más dinámico y adaptado a las necesidades de los tiempos.

No se discutirá, por tanto, la intervención de la Autoridad Judicial y el secreto de las comunicaciones allí donde deba imperar, sino de su modulación, pues en nada debe entorpecer la intervención judicial a la necesaria operatividad de la investigación criminal si se han interiorizado bien por la PJE los imperativos del art. 126 CE y la extensa legislación que lo desarrolla y, en igual modo, se posibilita la adecuación de la Ley a las exigencias impuestas por las nuevas realidades. Antes bien, la reserva judicial supone una garantía sobre el recto proceder del investigador quien, recurriendo y sintiendo su tutela, progresa con seguridad jurídica en la investigación[933].

Es tarea inacabada, por tanto, la regulación del mandato constitucional contenido en el art. 18.4 CE, que bien podría haber canalizado, tanto la percepción jurídica de los DACE, como de su tratamiento automatizado pues, al *"limitar el uso de la informática"* – por más que este precepto se haya redactado en modo negativo -, se pueden también establecer normas respecto de su utilidad para un proceso penal firme, inequívoca y eficientemente dirigido por la Autoridad Judicial con el auxilio de la PJE.

En este sentido, GONZÁLEZ-CUÉLLAR, dice que:

> *"Lo que se reclama es el desarrollo legal del derecho constitucional que el art. 18.4 CE, hermenéuticamente reconstruido conforme a la realidad social*

[933] En este sentido, MARTÍN PALLÍN, afirma que *"el acceso directo de la Policía Judicial a las fuentes de datos sin previa autorización judicial, puede conducir al naufragio de la actividad probatoria".* Vid. Martín Pallín, José Antonio. 2008. *El equilibrio entre la conservación…op. cit.,* pág. 154.

actual, contiene, como condición necesaria para su eficacia, no sólo frente a la recopilación, tratamiento automatizado y utilización de datos personales, sino también ante el aprovechamiento por los órganos de persecución penal de los sistemas de almacenamiento y comunicación de datos digitales para la investigación y la prueba de los delitos"[934].

Legíslese entonces.

[934] Vid. González-Cuéllar Serrano, Nicolás. *Garantías constitucionales…op. cit.,* pág. 153.

V. CAPÍTULO QUINTO: LA INTELIGENCIA SOBRE LOS DATOS ASOCIADOS A LAS COMUNICACIONES ELECTRÓNICAS

Mucho se ha hablado ya de la IDACE, concepto del que podía intuirse un significado de utilidad para la investigación criminal, al menos, en sus trazos más gruesos.

Sin embargo, hablar de inteligencia y proceso penal no es precisamente sencillo, pues los prejuicios que acompañan al desarrollo de la actividad indagatoria de la PJE, en la medida en que pueda sospecharse una colisión con los derechos fundamentales de los investigados, aconseja cautela a la hora de intentar conciliar ambos conceptos.

Para poder iniciar una discusión en la materia, se haría notoria la necesidad de este maridaje si sólo se atendiese a la realidad de la casuística criminal y al uso social de las TIC y, por el contrario, devendría controvertida si no se pusiese en inmediata relación con el exigente marco jurídico democrático al que semejante actividad debe severamente ajustarse de forma que, del resultado del proceso de obtención de la inteligencia para el proceso penal, no se resintiesen importantes bienes jurídicos de superior e imprescindible consideración.

Es, por tanto, en este difícil punto de equilibrio, donde deben buscarse la soluciones. Un punto, donde el control jurisdiccional ha de ajustar con precisión el fiel de la balanza de forma que se propicie una verdadera y fructífera relación entre la PJE y el actor jurisdiccional y, todo ello, orientado a la verificación de un proceso penal con todas las garantías. Consecuentemente, no parece ajustado a sus necesidades el desplazamiento de los equilibrios logrados, ni por el lado del exceso de facultades de la PJE, ni por un exacerbado garantismo que impida un ajuste a los tiempos de las verdaderas necesidades del proceso penal que requiere la sociedad moderna.

Como corolario de todo lo anterior, el objetivo de la inteligencia, entendida como un instrumento legítimo destinado a facilitar las finalidades indicadas, fracasaría en su mismo origen si se alcanzase sin respeto a los límites impuestos por los consolidados principios democráticos en que se fundamenta la Constitución Española.

Por ello, ligar una propuesta con su proporcionalidad – su razonabilidad en suma - debe ser la tarea básica que no rompa este afortunado equilibrio entre seguridad y libertad. Con esta argamasa habrán de unirse los demás elementos que

coadyuven al éxito de un proceso penal dirigido por la Autoridad Judicial, entre los que, por derecho propio, se encuentra la PJE, con su legislación, técnicas y procedimientos y con el auxilio de los instrumentos de garantía y salvaguarda que representa el uso de la tecnología.

Es hora, por tanto, de profundizar en el significado de lo que aporta el concepto de inteligencia para justificar, desde un punto de vista práctico, las propuestas de todo orden que se plantearán, que se pretenden conciliadoras con el exigente marco jurídico de referencia en lo tocante a la limitación de los derechos fundamentales.

A. Delimitación del término inteligencia

1. Concepto amplio de inteligencia: El ciclo de inteligencia

Aunque se ha hablado hasta ahora, repetida pero someramente, del término ***inteligencia***[935,936], es en este capítulo donde debe delimitarse en consonancia con las propuestas de índole práctica que se formularán.

Aunque no de forma exclusiva, el concepto genérico de inteligencia, en la orientación que se pretende dársele en este trabajo, tiene en su origen importantes connotaciones con su aplicación a las necesidades de la defensa nacional, en cuyo beneficio se han desarrollado complejas teorías y metodología y adquirido sensibles experiencias que lo convierten en toda una ciencia, no exenta de grandes controversias y debates.

Vista desde este ámbito, la inteligencia puede definirse como:

> *"El producto que resulta de la evaluación, la integración, el análisis y la interpretación de la información reunida por un servicio de inteligencia. Su elaboración es objeto del proceso conocido como ciclo de inteligencia"*[937].

No obstante lo anterior, una mirada superficial parece sugerir un agotamiento de sus utilidades en sus expresiones o facetas más preventivas o de anticipación ante determinadas situaciones o amenazas que, si en un principio son tan sólo mínimamente intuidas o sospechadas, deberán estimarse con la mayor precisión posible si se han de afrontarse el futuro con las máximas garantías de éxito.

---

[935] En lo que interesa, es en la combinación de las acepciones tercera y quinta del diccionario donde se encuentra la primera aproximación a su contenido semántico ya que, respectivamente, significa *"conocimiento, comprensión, acto de entender"* y *"habilidad, destreza y experiencia"*.

[936] En la *teoría triárquica de la inteligencia*, elaborada por ROBERT J. STERNBERG, se establecen tres categorías para describir la inteligencia, cuya traslación al campo de estudio de este trabajo es evidente:

- *Inteligencia componencial-analítica: la habilidad para adquirir y almacenar información.*
- *Inteligencia experiencial-creativa: habilidad fundada en la experiencia para seleccionar, codificar, combinar y comparar información.*
- *Inteligencia contextual-práctica: relacionada con la conducta adaptativa al mundo real.*

[937] Vid. Esteban Navarro, Miguel Angel. *Glosario de Ingeligencia.* Ministerio de Defensa, pág. 74.

Sin embargo, siendo esto así, el ciclo de inteligencia tiene una utilidad determinante para ordenar el proceso intelectivo en que ha de consistir cualquier tipo de investigación, sea o no su finalidad atinente al proceso penal, proporcionando al investigador la necesaria metodología para garantizar su éxito.

En este sentido, lo más interesante de la definición de inteligencia es el concepto de ***información*** en sus acepciones más directamente relacionadas con el proceso penal, que están contenidas en los ordinales tercero y quinto del diccionario, respectivamente: *"Averiguación jurídica y legal de un hecho o delito"* y *"comunicación o adquisición de conocimientos que permiten ampliar o precisar los que se poseen sobre una materia determinada"*.

Tras ponderar el interés de la RAE en incorporar al diccionario las acepciones de mayor contenido semántico-jurídico, es necesario reparar en que las informaciones, por sí mismas, raramente contendrán una carga probatoria significativa y que será necesario adquirir *conocimientos que las amplíen o precisen*, tal y como es reclamado en su definición. Es de esto, precisamente, de lo que se ocupa el ***ciclo de inteligencia***[938]: de ***evaluar, integrar, analizar e interpretar*** la información o las informaciones y, si ha de servir al proceso penal, suministrarla de acuerdo con el marco jurídico en que discurre.

2. Obtención de inteligencia para el proceso penal. La inteligencia criminal

Una definición del concepto de ***inteligencia criminal*** indica que es el:

> *"Tipo de inteligencia llevada a cabo por los servicios de información policiales para resolver delitos y luchar contra el crimen organizado. La inteligencia criminal se caracteriza, al mismo tiempo, por tener un carácter preventivo de actividades delictivas y por complementar la acción judicial*

[938] Un interesante resumen del panorama actual sobre el ciclo de inteligencia puede leerse en Navarro Bonilla, Diego. *El ciclo de inteligencia y sus límites.* Cuadernos constitucionales de la Cátedra Fadrique Furió Ceriol ISSN 1135-0679, núm. 48, 2004, págs. 51-66.

represiva mediante la aportación de pruebas en la puesta del delincuente ante la Justicia"[939].

En esta definición convergen dos facetas netamente distintas: la *preventiva* – que no es objeto del interés de este trabajo - y la *resolutiva*. Con respecto a esta última – y usando un término ciertamente abrupto -, la finalidad de la inteligencia sería la de proveer el proceso *represivo* unido a la acción judicial -, lo que sugiere más bien la idea de su utilidad para comprender qué necesita el proceso penal y cómo hay que proporcionárselo de una forma admisible en un Estado de Derecho, esto es, cómo se ha de llegar a la adquisición de una prueba susceptible de contradicción y valoración en el acto de juicio oral[940].

En lo que se refiere a las funciones de la PJE para la ***obtención de inteligencia para el proceso penal***, pueden proponerse como ***elementos del ciclo de inteligencia criminal*** los siguientes:

> *"La identificación y adquisición legítima de todas aquellas informaciones de cualquier naturaleza que, de una forma objetiva, puedan contribuir al cumplimiento de sus finalidades (**evaluación**); la verificación de un proceso comprensivo de contraste con otras cuyo contenido pueda concurrir a un mismo fin, esto es, a servir al esclarecimiento final, completo e inequívoco de los hechos delictivos (**integración**); el descubrimiento y determinación del significado objetivo de las informaciones tras haberlas relacionado entre sí (**análisis**); y todo ello, finalmente, orientado a facilitar la concepción, ordenación y expresión intelectiva de la realidad (**interpretación**) de forma que sea útil para la formación de la opinión jurisdiccional sin la contaminación de elementos subjetivos o cualesquiera otros que hayan sido deficientemente incorporados al proceso penal (**contradicción y valoración de la prueba**)"*.

[939] Vid. Esteban Navarro, Miguel Angel. *Glosario…op. cit.*, pág. 77.

[940] *"La prueba penal es un elemento de acreditación de un hecho que tiene trascendencia penal en el enjuiciamiento de unos hechos. Las partes del proceso mediante la utilización de pruebas tratan de reconstruir lo que sucedió con anterioridad. En un Estado de Derecho, caracterizado, entre otros aspectos, por la naturaleza del proceso penal como instrumento de control social formalizado, se exige que sólo puedan utilizarse en esa reconstrucción los medios de prueba y de investigación previstos en la Ley procesal con observancia de los requisitos establecidos en la Ley"*. (STS 1509/2003, de 12 de noviembre). En mi opinión, la prueba de inteligencia debiera estar perfectamente prevista en la Ley Procesal, sin que diese lugar a polémicas que le restasen virtualidad como prueba valorable en el juicio oral.

Por ello, en lo que interesa a las funciones atribuidas a la PJE por el art. 126 CE y la legislación que lo desarrolla, debe aportársele al término inteligencia, procedente de fuentes abiertas o restringidas, humanas o técnicas, una dimensión orientada a la resolución de los problemas connaturales al proceso penal.

Se trata, consecuentemente, de suministrar, como parte del atestado, un producto elaborado con vocación de adquirir la condición de prueba evaluable desde un punto de vista jurisdiccional en el acto de juicio oral, cuestión que, en cualquier caso, será decisión libre y exclusiva del director del proceso penal.

Es por ello esencial que la labor de la PJE se desarrolle con absoluta transparencia, huyendo con decisión de cualquier técnica o procedimiento de inteligencia viciado de obscuridad o subjetividad y sirviéndose, al mismo tiempo, de la metodología científica y la apoyatura en pruebas documentales e indiciarias, lo que incluye el recurso a los medios proporcionados por la tecnología.

La cuestión más controvertida hay que residenciarla en el papel relativo que el Instructor Policial juegue dentro del proceso penal cuando lo que aporte no sea únicamente una mera sucesión de pruebas materiales y objetivas, sino que, además, exprese una valoración subjetiva de su idoneidad para que el juzgador alcance el más exacto conocimiento de los hechos, alimentando objetivamente el proceso de contradicción y valoración de la prueba propio de la fase de juicio oral.

Esta actividad será tanto más sensible cuanto más relevante haya sido la propia incorporación de inteligencia al proceso investigativo la que haya propiciado la apertura de nuevas líneas de indagación y, consecuentemente, de adquisición legítima de posibles pruebas, algo en lo que se debe ser especialmente cuidadoso para no incurrir en vicios de nulidad que las hagan inviables para el proceso penal.

Evidentemente, cuando esto haya conllevado la limitación de un derecho fundamental (como por ejemplo, la solicitud y ejecución de una intervención telefónica o un registro domiciliario), la previa apreciación de su proporcionalidad por al Autoridad Judicial habrá debido estar respaldada por un proceso de impecable metodología policial en el trámite de aportación de los suficientes elementos de juicio.

En caso contrario, el proceso penal devendrá inestable y lo que habría parecido en sede policial de inequívoca trascendencia para consolidar la responsabilidad penal de los justiciables, resultará a la postre inservible para la valoración de los hechos en sede judicial, cuando no causa suficiente del fracaso del procedimiento penal en su conjunto. Nótese, por tanto, el extraordinario papel que ha de jugar la PJE para conjurar todos estos problemas.

Otro elemento, tan interesante como controvertido, podría encontrarse de una manera elemental en la progresiva distancia que, conforme avanzan las TIC y, en general, en cualquier ámbito de intervención en torno a la moderna delincuencia, se abre entre el concepto de información y el de inteligencia, a veces enorme e, incluso, mediando las correspondientes dosis de hipergarantismo, insalvable.

En la vetusta LCRIM el paradigma de un hecho, un autor, un lugar, sin pretender restar complejidad ni mérito a las investigaciones de la policía propias de los tiempos en que se promulgó, la indagación consistía básicamente en reunir las suficientes informaciones que permitiesen el completo esclarecimiento de los hechos, su enjuiciamiento y el pronunciamiento de una sentencia.

La inteligibilidad de todo el proceso no exigía una elaboración demasiado compleja de las informaciones, esto es, la obtención de inteligencia, por consistir en la recopilación de testimonios, análisis de restos orgánicos (fluidos corporales, huellas digitales, manchas, etc.), restos inorgánicos u otras huellas (marcas instrumentales, análisis balísticos, análisis de sustancias, etc.), testimonios del resultado de las vigilancias, seguimientos, la presentación de lo recogido durante los registros domiciliarios, etc.

Todas estas informaciones eran aprehensibles para cualquier inteligencia mediante su mero examen o descripción, a veces incluso superficial, sin mayores necesidades de elaboración, salvo en algunos casos excepcionales (como, por ejemplo, la identificación mediante una huella digital).

Estas informaciones, sin necesidad de someterlas a una elaboración muy sofisticada, podían servir para formar de un modo seguro e indubitado la opinión

jurisdiccional y, sin aventurar en exceso, ser incorporadas directamente al contenido material de la sentencia.

Pero, hoy en día, con la LCRIM del siglo XIX aún inexplicablemente vigente y conteniendo un criticado art. 579 LCRIM que no fue capaz (aún en su relativamente reciente reforma operada mediante ley orgánica de 1988), no sólo ya de adaptarse a la evolución de las TIC que ya se atisbaba en el horizonte, sino tan sólo de ofrecer un tratamiento jurídico-procesal medianamente seguro para las que ya existían, las informaciones recabadas a lo largo del proceso investigativo no son en modo alguno inteligibles por el hecho de su mero examen o descripción.

Para demostrar el anterior aserto baste recordar que las informaciones que debió tratar el equipo de investigación de la Guardia Civil que se ocupó de la *botnet* MARIPOSA consistieron, entre otras muchas cosas, en incorporar al proceso penal una ingente cantidad de direcciones IP (informaciones) correspondientes a una maquinación preordenada a conseguir ataques de DoS a través de, al menos, once millones de ordenadores.

Imagínese ahora que la forma de entregar esta información al Juez de Instrucción consistiese en presentar un sinnúmero de hojas de papel con las direcciones IP pulcramente listadas y sin acompañar de una explicación sobre su utilidad para el *iter criminis* y pretender que, de esta forma, el Juez pueda adquirir la más exacta dimensión de lo que ha de juzgar.

Con toda evidencia, es necesaria una elaboración eficiente de las informaciones (inteligencia), hecha desde un punto de vista técnico y con el respaldo de una sólida formación específica y contando por añadidura con alguna experiencia práctica en la materia, que permita comprender o, al menos, intuir, su posible valor para la determinación de la responsabilidad penal, lo que inevitablemente no estará exento de incluir una interpretación subjetiva del analista, siempre valiosa si se incorpora al atestado dentro de una diligencia perfectamente diferenciada de aquellas otras que contengan exclusivamente elementos objetivos.

La sempiterna cuestión en este punto es, únicamente, la confianza que el Juez ha depositar en la PJE que realiza los informes de inteligencia basados en esos datos,

siempre y cuando, naturalmente, los haya elaborado con el más sólido basamento metodológico, técnico y documental[941], de suerte que las protestas de nulidad no puedan basarse en esta circunstancia sino, tan sólo, en la validez intrínseca de su fundamentación como prueba y, en todo caso, mediando una impugnación presentada por la parte interesada en forma de solicitud motivada de auditoría de determinados aspectos controvertidos.

Pero no debe olvidarse que nada impide que, de forma materialmente diferenciada, el Instructor Policial se refiera a la inteligencia que ha adquirido durante el proceso investigativo, presentando y defendiendo las tesis o formulando los juicios de inferencia que la apoyatura documental e indiciaria y las demás pruebas recabadas la permitan lealmente sostener.

Nada hay de inquietante en esta compleja labor, que no es nueva, tal y como reconoce PÉREZ GIL al decir que *"el «análisis de información» o los informes de «inteligencia policial» no son novedosos medios de prueba, sino una forma de actuación policial imprescindible para afrontar con garantías de éxito la lucha contra el delito"*[942], perspectiva que recuerda la idea de su validez dicotómica que admite la jurisprudencia, tanto para la obtención directa de la prueba, como para alimentar el propio progreso de la investigación[943].

3. Otros elementos de la inteligencia

[941] Sobre el necesario equilibrio que ha de hallarse para que los informes de inteligencia ganen toda su utilidad para el proceso penal, dice PÉREZ GIL que *"no parece conveniente ni tendría ningún viso de prosperar pedir que la Policía desvelase detalladamente cómo ha llegado a un resultado, cómo ha obtenido unas fuentes de prueba, etc. Pero tampoco parece convincente que permitamos que el resultado obtenido, libre de todo control, se deslice subrepticiamente y acomode en la sentencia sin posibilidad de refutación, dejando las expectativas de la defensa reducidas a una mera presencia escénica y el papel del juzgador capitidisminuido".* Vid. Pérez Gil, Julio. *Entre los hechos y la prueba: Reflexiones acerca de la adquisición probatoria en el proceso penal*. León, Revista jurídica de Castilla y León núm. 14, enero de 2008, pág. 241.

[942] Vid. Pérez Gil, Julio. *Entre los hechos…op. cit.,* pág. 242.

[943] Por todas, recuérdense las SSTS de 17 de noviembre de 1994 (RJ 1994, 9276) y de 24 de marzo de 1999 (RJ 1999, 2052), mencionadas en capítulos anteriores.

Para concluir la mirada sobre los conceptos relacionados con la obtención de inteligencia, hay que incorporar otros elementos para avanzar en las finalidades de este estudio:

Así, por ***inteligencia de comunicaciones*** se entiende el *"tipo específico de la inteligencia de señales que se elabora a partir de la obtención y el procesamiento de datos provenientes de la detección, interceptación y descifrado de transmisiones efectuadas por cualquier medio, por un receptor que no es quien pretendía el emisor*[944]*. En general se ocupa de las señales de transmisión en serie como las de radio y video, ya que no es difícil la interceptación, mediante el empleo del equipamiento adecuado, del espectro radioeléctrico, de la redes de comunicaciones alámbricas o inalámbricas y de las redes basadas en infrarrojos"*[945]. De la inteligencia de comunicaciones no son ajenas, por tanto, las emisiones de los dispositivos de comunicaciones electrónicas, como el análisis de las BTS o de TMA en materia de geolocalización o la realización de pericias en este ámbito (que es objeto de estimación pericial), el estudio del espectro radioeléctrico, el uso de los servicios de valor añadido, etc.

Como ***inteligencia básica*** se entenderá aquel *"tipo de inteligencia cuyo fin es satisfacer los requerimientos de inteligencia permanentes y generales de la organización. Que no es otro que lo que consta en sus propios archivos y que, bajo determinadas circunstancias, puede adquirir insospechado valor en la resolución de nuevos casos"*[946].

Y por ***inteligencia de fuentes abiertas*** u OSINT[947], se entenderá el *"tipo de inteligencia elaborada a partir de la información que se obtiene de fuentes de información de carácter público. Por fuente abierta se entiende todo documento con cualquier tipo de contenido, fijado en cualquier clase de soporte (papel, fotográfico, magnético, óptico...) que se transmite por diversos medios (impreso, sonoro, audiovisual...) y al que se puede acceder en modo digital o no, puesto a disposición*

[944] Debe entenderse en este caso, según lo dispuesto en el art. 579 LCRIM, la PJE debidamente comisionada a los efectos por el Juez de Instrucción cuando exista limitación de los derechos fundamentales o, alternativamente, también la PJE de propia autoridad cuando sus análisis no conlleven tal limitación.
[945] Vid. Esteban Navarro, Miguel Angel. *Glosario…op. cit.,* pág. 78.
[946] Vid. Esteban Navarro, Miguel Angel. *Glosario…op. cit.,* pág. 75.
[947] Acrónimo del inglés *open source intelligence.*

pública, con independencia de que esté comercializado, se difunda por canales restringidos o sea gratuito. También se suele considerar fuente de información abierta el conocimiento suministrado por los expertos que forman la reserva de inteligencia de un servicio"[948,949].

B. La prueba de inteligencia policial

1. Concepto general de prueba de inteligencia policial

Una vez delimitado el término de *inteligencia* en sus aspectos generales y técnico-policiales, como elemento metodológico orientado a facilitar el proceso investigativo y la subsiguiente adquisición de posibles pruebas, debe buscársele un ulterior significado o valor dentro de las finalidades últimas del proceso penal.

Con este propósito, debe traerse necesariamente a este trabajo una reflexión sobre lo que se viene denominando la ***prueba pericial de inteligencia***[950,951] o, según

[948] La jurisprudencia constitucional, sensible a la exquisita protección de la intimidad, incluso en los ámbitos donde la información circula en abierto, dice que *"en este mismo sentido diversas disposiciones tomadas a nivel europeo se han ocupado de esta materia. Así procede citar en primer lugar el Convenio núm. 108 del Consejo de Europa sobre protección de los datos informatizados de carácter personal (1981), vinculante para España, y las recomendaciones del Comité de Ministros que lo desarrollan, en particular, la recomendación sobre datos personales utilizados en el sector policial (1987) y la recomendación sobre privacidad en Internet (1999). El preámbulo de esta última recomendación - R(99) 5, de 23 de febrero de 1999 - pone de relieve que "el desarrollo de las tecnologías y la generalización de la recogida y del tratamiento de datos personales en las 'autopistas de la información' suponen riesgos para la intimidad de las personas naturales" y que "las comunicaciones con ayuda de las nuevas tecnologías de la información están también sujetas al respeto de los derechos humanos y de las libertades fundamentales, en concreto al respeto a la intimidad y del secreto de las comunicaciones, tal y como se garantizan en el artículo 8 de la Convención Europea de los Derechos Humanos". Además, recuerda esta recomendación que "el uso de Internet supone una responsabilidad en cada acción e implica riesgos para la intimidad" (introducción), por cuanto cada visita a un sitio de Internet deja una serie de "rastros electrónicos" que pueden utilizarse para establecer "un perfil de su persona y sus intereses" (apartado II, 2), subrayando también que la dirección de correo electrónico constituye "un dato de carácter personal que otras personas pueden querer utilizar para diferentes fines" (apartado II, 6)" (STC 173/2011, de 7 de noviembre).*

[949] En este sentido, la STEDH de 3 de abril de 2007, *caso Copland contra el Reino Unido*, considera en su § 41 que *"están incluidos en el ámbito de protección del art. 8 del Convenio europeo, por cuanto pueden contener datos sensibles que afecten a la intimidad, tanto "los correos electrónicos enviados desde el lugar del trabajo" como "la información derivada del seguimiento del uso personal de Internet"*.

[950] GUERRERO dice que *"salvo error, la primera sentencia en la que se utilizó la expresión "pericial de inteligencia" fue dictada por la Sección Tercera de la Sala de lo Penal de la Audiencia Nacional, con fecha*

han querido conceptualizarla algunos autores, la ***prueba de inteligencia policial*** (admitidas mayoritariamente por la jurisprudencia, en sus primeras expresiones, sobre asuntos de terrorismo y ampliada luego también al tratamiento de la delincuencia organizada[952]), en ambos casos con un inestable asiento en la deficientísima legislación procesal[953] y, desde luego, generando no pocas dudas en algunos sectores de la doctrina y la jurisprudencia[954], por más que está última haya ido asentado algunas posiciones mayoritariamente favorables a su admisión como prueba valorable en el acto del juicio oral[955].

En consideración de PÉREZ GIL, *"la prueba de inteligencia policial está siendo configurada por la jurisprudencia como una pericial singular que tiene por finalidad*

---

de 20 de enero de 2000 (nº 3/2000, rec. 45/1989)". En la sentencia – que se ocupó de un caso de terrorismo - se indica que *"estamos ante una auténtica prueba pericial que consiste en relacionar datos".* El carácter de prueba pericial fue avalado mediante la STS 2084/2001, de 13 de diciembre, que resolvió el Recurso de Casación 1048/2000 y perfilado por la STS 786/2003, de 29 de mayo, rec. 945/2002. Vid. Guerrero Palomares, Salvador. *La denominada "prueba…op. cit*., pág. 78. *Relacionar datos,* en lo que interesa a este trabajo, devendrá una pieza angular para sus proposiciones.

[951] También, vid. Rives Seva, Antonio Pablo, y otros. *La Prueba en…op. cit.,* pág. 633 y ss.

[952] Como oportunamente señala GUERRERO, el origen de la prueba pericial de inteligencia hay que situarlo en su orientación al enjuiciamiento de hechos terroristas, siempre graves, dedicación específica sobre la que la jurisprudencia ha atribuido incluso alguna exclusividad (como en la STS 124/2009, de 13 de febrero, que, además, la calificó de *atípica*). Sin embargo, la delincuencia organizada, sobre cuya peligrosidad y extrema complejidad ya me he pronunciado en diversas ocasiones, hace a todas luces injustificada semejante reserva, por lo que esta prueba está absolutamente indicada para su contradicción y valoración en el acto del juicio oral. Otras sentencias recientes a favor de la condición de pericial serían las SSTS 352/2009, de 31 de marzo, 480/2009, de 22 de mayo y 985/2009. Vid. Guerrero Palomares, Salvador. *La denominada "prueba…op. cit*., pág. 80.

[953] DOLZ – autor que reconoce la progresiva eficacia probatoria de los informes policiales apoyándose en la STS 1345/1997, de 5 noviembre - reclama una nueva regulación procesal de la prueba que solvente tal inestabilidad, acogiendo las novedades que las modernas formas de prueba están evidenciando, afirmando que *"podría decirse que la aportación de la Policía científico-judicial al proceso penal está rompiendo los esquemas decimonónicos de la prueba, tal y como viene diseñada en nuestra vetusta LECrim de 1882 y exigiendo reformas legislativas para adaptarlas a la realidad de los tiempos presentes, ya que en los clásicos moldes probatorios de la LECrim (medios de investigación y pruebas; pruebas personales: testificales y periciales; pruebas reales: documentales), no acaba de encajar la actividad de esta Policía científico-judicial, la cual puede transitar entre los actos de investigación y los medios de prueba y por todos los medios probatorios conocidos y que, por otro lado, empezaba a germinar en aquellos tiempos de promulgación de la LECrim, como instrumento objetivo e imparcial de investigación de los delitos".* Vid. Dolz Lago, Manuel-Jesús. *La aportación científico-policial…op. cit.,* pág. 5 y ss.

[954] PÉREZ GIL anota esta circunstancia con referencia a la STS de 19 de enero de 2007, donde, constatando las dudas sobre este tipo de prueba, se afirma que *"se denomine como se denomine la prueba especial practicada, creada sobre las imprecisiones de la propia LECrim, y fuere cual fuere su consideración, en cuanto participa de características propias tanto de la pericial como de la testifical…".* El autor, crítico con la doctrina estudiada, la describe descarnadamente como resultado de una *"predilección del TS"*, que le llevaría a aceptar *"comida preparada, sin tener que asumir el esfuerzo de cocinar".* Vid. Pérez Gil, Julio. *Entre los hechos…op. cit.,* pág. 240.

[955] A título ilustrativo sobre la utilidad real de esta prueba, valorada durante el enjuiciamiento de los hechos terroristas del 11-M, léanse las aportaciones del Magistrado que lo presidió en Gómez Bermúdez, Javier. *No destruirán nuestra libertad.* Madrid: Ediciones Planeta Madrid S.A., 2010.

suministrar al juzgador "una serie de conocimientos técnicos, científicos, artísticos o prácticos cuya finalidad es fijar una realidad no constatable directamente por el Juez y que, obviamente, no es vinculante para él, sino que como el resto de probanzas, quedan sometidas a la valoración crítica, debidamente fundada en los términos del art 741 LCRIM". La pericia es realizada por expertos (normalmente en la lucha antiterrorista) "que con apoyo abrumador en multitud de hechos objetivos, que a su vez reseñan y constatan, llegan a conclusiones que permiten evidenciar circunstancias que no se descubren en un primer examen""[956]. Las conclusiones a que se refiere el autor no son otra cosa que ***juicios de inferencia*** por los que se trata de representar la verdad de los hechos únicamente en el caso de que tengan una sólida vinculación con los elementos fácticos incontrovertibles en que se basen.

Sin embargo, esta catalogación de la prueba de inteligencia policial como una pericial – o *pericial singular,* como refleja el autor citado - no es pacífica siquiera en la propia evolución del jurisprudencia, como oportunamente anota por su parte GUERRERO, autor al que seguiré con profusión en este interesante asunto, al plantear las dudas por la contraposición con un posible y menor valor alternativo de la prueba de inteligencia policial – desprovista ahora del calificativo de pericial -, esto es, únicamente como ***prueba testifical***[957].

Para DOLZ, que se refiere a esta prueba como una variante de la pericial en la que la intervención de la PJE se manifiesta bajo la dualidad testigo[958] - perito, *"debe decirse, en primer lugar, que la prueba pericial es una variante de las pruebas personales integrada por el testimonios de conocimiento emitidos con tal carácter por especialistas del ramo correspondiente de más o menos alta calificación científica, a valorar por el Tribunal de instancia conforme a los arts. 741 y 632 de la LECr y 117.3 de la Constitución. (Sentencia 970/1998, de 17 de julio, entre muchísimas otras)"*[959].

---

[956] PÉREZ GIL se apoya en la siguiente jurisprudencia: *"STS 786/2003, de 29 de mayo, Ponente: Giménez García (RJ 2003, 4242), FD 2.º, con cita de la STS 2084/2001, de 13 de diciembre, pero también otras: STS 1215/2006 (Sala 2, Secc. 1), de 4 diciembre, Ponente: Monterde Ferrer, FD 2.º; STS de 19 de enero de 2007 (misma sala, sección y ponente), RJ 2007 1771; STS 585/2007 (Sala 2.ª, Sección 1), de 20 de junio, Ponente: García Pérez (RJ 2007 3440) FD 2.º; STS 655/2007 (misma sección, sala y ponente), de 25 de junio"*. Vid. Pérez Gil, Julio. *Entre los hechos…op. cit.,* pág. 240.

[957] Vid. Guerrero Palomares, Salvador. *La denominada "prueba…op. cit*., pág. 75 y ss.

[958] Directo o de referencia.

[959] Vid. Dolz Lago, Manuel-Jesús. *La aportación científico-policial…op. cit.,* pág. 29 y ss.

2. El posible valor como prueba de los informes de inteligencia policial

Sea como fuere lo introducido en el apartado anterior, y centrando la discusión en el tema práctico de fondo, para la correcta apreciación del posible valor de la prueba de inteligencia policial, han de conjugarse diversos elementos que, en mi opinión, contribuirán a dotarla de la necesaria perspectiva de utilidad – y singularidad, podría decirse - para el enjuiciamiento en sede penal de determinados hechos complejos.

Estos elementos, que responden a necesidades generales perfectamente identificables del proceso penal, son:

En primer lugar, el reconocimiento de la existencia de hechos complejos relacionados con el terrorismo y la delincuencia organizada que deben ser desentrañados recurriendo a la tecnología, a la ciencia o a determinados conocimientos prácticos.

A las anteriores categorías, sin duda, habría que añadir determinadas casuísticas que podrían calificarse de graves, esto es, con independencia de que sean atinentes al terrorismo o a la delincuencia organizada, o complejas, por ser el escenario criminal de un dificultoso esclarecimiento por razones de índole diverso (fáctico, procesal, territorial, etc.).

En segundo lugar, la necesidad de analizar una ingente cantidad de datos y documentos procedentes de diversas fuentes de prueba dentro del procedimiento inductivo policial (*pericial de análisis de la información*). Esta faceta expresa el ***factor cuantitativo*** en el sentido de la necesidad de recurrir a métodos que permitan una visión global, íntegra y segura de todos los elementos materiales e inmateriales que forman parte de una investigación. Esta circunstancia resulta especialmente visible en el caso de la evidencia digital.

En tercer lugar, la necesidad de poner a disposición del Juzgador una serie de *"conocimientos técnicos, científicos, artísticos o prácticos"*, en lo que se podría definir,

según un amplio sector de la jurisprudencia, como una variante de la prueba pericial de los arts. 456 LCRIM y 335 LECIV. Esta faceta expresaría el ***factor cualitativo*** que debe permitir al Juez la más exacta determinación de la naturaleza de los hechos y su relevancia penal, permitiendo ver de una forma transparente y segura la vinculación de un hecho con su consecuente.

En cuarto lugar, la existencia de realidades no constatables directamente por el Juez y que, lógicamente, necesitan de una representación inteligible, auténtica, veraz e íntegra, susceptible de contradicción y valoración a efectos de enjuiciamiento criminal *ex* art. 741 LCRIM. La inteligibilidad y la seguridad jurídica que deben presidir todo el proceso de generación de inteligencia son y deben ser, por tanto, las señas esenciales de esta faceta[960].

3. Aspectos jurisprudenciales controvertidos de la prueba de inteligencia policial

Frente a la postura mayoritaria de la jurisprudencia respecto de la consideración jurídica de pericial de la prueba de inteligencia policial[961], se han producido también sentencias contradictorias que argumentaban, básicamente, lo siguiente:

[960] Sobre la complejidad del producto obtenido del ciclo o proceso de inteligencia, dice NAVARRO que *"la naturaleza informativa o documental de los materiales con los que llevar a cabo el análisis de Inteligencia, obligan a instalar una concepción muy amplia de los formatos, procedencias, lenguas, soportes, etc., de las informaciones que deben ser obtenidas e integradas en un entorno abiertamente digital. Dicho de otro modo, el producto final de Inteligencia como resultado de una destilación de fuentes y recursos, muchos de ellos procedentes de* páginas web, *tablas estadísticas, informativos de medios de comunicación, informes multimedia, mapas conceptuales, imágenes capturadas por satélite, transcripciones en papel procedentes de sistemas de escucha telefónica, fotografías digitales o en papel, etc. El término que contempla la globalidad de toda pieza de información susceptible de integrarse en un análisis de inteligencia, generada o recogida en cualquier soporte o formato posibilitando la integración eficaz de una multitud de fuentes de información para la generación de inteligencia se denomina multi-int, all source intelligence o inteligencia "holística". Es decir, redes de información internas compatibles con software y sistemas basados en la world wide web, compatibles entre sí y capaces de integrar los resultados de todas las formas de –int (HUMINT, OSINT, MASINT, SIGINT, ELINT, etc.) proporciona un mapa integral, global capaz de ofrecer en un único producto final una metáfora visual del asunto en cuestión".* Vid. Navarro Bonilla, Diego. *El ciclo de inteligencia…op cit.,* pág. 60.

[961] *Ibídem.*

- No se trata de una pericial en sentido propio, puesto que no tratan saberes no jurídicos ni corresponden al bagaje cultural del ciudadano medio no especialista, pero sí al saber empírico. En este sentido, no se trata de un saber cualitativamente distinto, ni especializado en sentido propio (STS 1029/2005, de 26 de septiembre, rec. 1396/2004).
- Los informes de inteligencia deben tener la consideración de testificales y su valor vendrá determinado por la documental en que se apoyen y no por las opiniones personales del funcionario de policía (STS 556/2006, de 31 de mayo, rec. 1158/2005).
- Los informes de inteligencia sólo pueden considerarse pruebas de indicios, cuyo valor únicamente podrá determinarse en conjunción con otros medios de prueba (STS 119/2007, de 16 de febrero, rec. 10461/2006)[962].

4. Valor procesal de la prueba de inteligencia policial

No obstante la jurisprudencia contradictoria que se ha expuesto en el apartado precedente, otros pronunciamiento contemporáneos a los anteriores[963] reforzaron su visión de la prueba como pericial de inteligencia, unificando su visión dogmática en la STS 783/2007, de 1 de octubre, al describir sus singulares características del siguiente modo:

> *"En suma, este tipo de prueba, se caracteriza por las siguientes notas:*
>
> *1º) Se trata de una prueba singular que se utiliza en algunos procesos complejos, en donde son necesarios especiales conocimientos, que no responden a los parámetros habituales de las pruebas periciales más convencionales;*
>
> *2º) En consecuencia, no responden a un patrón diseñado en la Ley de Enjuiciamiento Criminal, no obstante lo cual, nada impide su utilización en el*

[962] Vid. Guerrero Palomares, Salvador. *La denominada "prueba…op. cit*., págs. 78 y 79.
[963] SSTS 585/2007, de 20 de junio y 655/2007, de 25 de junio.

proceso penal cuando se precisan esos conocimientos, como así lo ha puesto de manifiesto la jurisprudencia reiterada de esta Sala;

3º) En todo caso, la valoración de tales informes es libre, de modo que el Tribunal de instancia puede analizarlos racional y libremente: los informes policiales de inteligencia, aun ratificados por sus autores no resultan en ningún caso vinculantes para el Tribunal y por su naturaleza no podrán ser considerados como documentos a efectos casacionales;

4º) No se trata tampoco de pura prueba documental: no puedan ser invocados como documentos los citados informes periciales, salvo que procedan de organismos oficiales y no hubieran sido impugnados por las partes, y en las circunstancias excepcionales que señala la jurisprudencia de esa Sala para los casos en que se trata de la única prueba sobre un extremo fáctico y haya sido totalmente obviada por el Tribunal sin explicación alguna incorporada al relato de un modo, parcial, mutilado o fragmentario, o bien, cuando siendo varios los informes periciales, resulten totalmente coincidentes y el Tribunal los haya desatendido sin aportar justificación alguna de su proceder;

5º) El Tribunal, en suma, puede apartarse en su valoración de tales informes, y en esta misma sentencia recurrida, se ven supuestos en que así se ha procedido por los jueces «a quibus»;

6º) Aunque cuando se trate de una prueba que participa de la naturaleza de pericial y testifical, es, desde luego, más próxima a la pericial[964]*, pues los autores del mismo, aportan conocimientos propios y especializados, para la valoración de determinados documentos o estrategias;*

7º) Finalmente, podría el Tribunal llegar a esas conclusiones, con la lectura y análisis de tales documentos"[965].

[964] En este mismo sentido, DOLZ afirma que "*consideramos aplicable esta doctrina a las pruebas policiales científicas, dado en las mismas concurren los requisitos examinados para las periciales de inteligencia en orden a la su doble cualidad de testifical-pericial, si bien prevalece esta última, y a la necesidad de su ratificación en el plenario, salvo que procedan de laboratorios oficiales y no hayan sido impugnadas por las partes, así su carácter no vinculante para el Tribunal y su no consideración de documentos a efectos casacionales, excepto en los supuestos que así lo admite la jurisprudencia, como son los de un solo informe o varios coincidentes y el Tribunal se haya apartado del mismo sin justificación razonable*". Vid. Dolz Lago, Manuel-Jesús. *La aportación científico-policial…op. cit.,* pág. 35.

[965] Vid. Guerrero Palomares, Salvador. *La denominada "prueba…op. cit*., pág. 79.

Sobre las tensiones que subyacen en las posiciones doctrinales y jurisprudenciales aportadas, que reflejan la necesidad de dar un nuevo enfoque al concepto procesal de prueba, un informe de inteligencia policial representaría una categoría singular y de posible e inusitado valor para el proceso penal, sin que con ello hubiere de ponerse en cuestión el principio de libre valoración de la prueba ni se le diese necesariamente valor como prueba documental.

Sin embargo, el pronunciamiento jurisdiccional insertado no acaba de descifrar su naturaleza procesal ya que, de acuerdo con el ordinal sexto, la Sala la ubica en un lugar indefinido entre la pericial y la testifical, aún atribuyéndole más cercanía a la primera que a la segunda categoría. Esta circunstancia no puede considerarse menor si se atiende a la escala de valores que cada tipo de prueba representa para la formación de la decisión judicial, dado que una prueba pericial está llamada a tener más peso específico que la testifical.

En efecto, siguiendo a DOLZ, se consideran ***pruebas directas o primarias*** "*la **confesión, la testifical, la documental***[966] *y la **inspección ocular***"[967] y por ***prueba indiciaria***[968] se entiende *"la que se obtiene por presunciones o indicios, según la cual se induce un hecho a partir de otro hecho básico en virtud de una relación de inferencia apoyada en criterios de racionalidad"*[969], resultando en su opinión que la ***prueba pericial*** *"es de difícil clasificación entre estos dos conceptos [prueba directa y prueba indiciaria], ya que proporciona al Tribunal las máximas de experiencia que es incapaz de conocer por carecer de conocimientos científicos, técnicos o artísticos para ello (cfr. art. 456 LECrim) y puede ser considerada prueba directa cuando es incontrovertible o científicamente inobjetable el razonamiento pericial o recibir el calificativo de prueba indiciaria cuando formula juicios de inferencia"*[970].

Sobre este interesante punto de vista debe definirse, en mi opinión, el concepto de prueba de inteligencia policial en su perspectiva procesal, entendida

[966] También, vid. Rives Seva, Antonio Pablo, y otros. *La Prueba en…op. cit.,* pág. 671 y ss.
[967] GIMENO enumera como tales "*la declaración del acusado, prueba de testigos, prueba pericial y documental*". Vid Gimento Sendra, Vicente. *Derecho procesal.* AAVV, Madrid, 1999, pág. 641.
[968] También, vid. Rives Seva, Antonio Pablo, y otros. *La Prueba en…op. cit.,* pág. 233 y ss.
[969] Debe anotarse, en cualquier caso, la indeterminación de la expresión "*criterios de racionalidad*", factor al que, sin duda, ha de contribuir la PJE en sus nada desdeñables labores técnico-policiales de auxilio al Juez.
[970] Vid. Dolz Lago, Manuel-Jesús. *La aportación científico-policial…op. cit.,* pág. 19 y ss.

como un instrumento de investigación a constituir sobre un sólido fundamento de pruebas directas o primarias con preferencia, pero sin minusvalorarlos, también sobre la elaboración de presunciones o la recogida de indicios[971], de forma que el cada vez más complejo proceso inductivo policial – que en diligencia diferenciada podrá contener un juicio de inferencia realizado por el Instructor Policial, aunque de naturaleza, evidentemente, no vinculante para el actor jurisdiccional - tenga como resultado final su perfecta idoneidad para servir, con los más altos niveles de seguridad jurídica, al proceso de contradicción y valoración propio de la fase de juicio oral.

Por ello, en relación con la naturaleza de la prueba en que se base, el contenido un informe de inteligencia policial podrá ponderarse ante el Tribunal según que la aportación del Instructor Policial *"pueda considerarse como prueba directa (cuando lo hace como testigo), como prueba indiciaria (cuando elabora juicios de inferencia en sus informes periciales) o como prueba pericial (si argumenta sin juicios de inferencia)"*[972].

Sin embargo, en el análisis de GUERRERO se incluyen determinados elementos sensibles, en relación con la naturaleza jurídica de los informes de inteligencia y de su eventual consideración o no de periciales, que conviene estudiar con algún detenimiento y, si se hace preciso, establecer alguna referencia respecto de la IDACE:

En primer lugar, sobre las dudas sobre la naturaleza de los *conocimientos especiales* cabe decir que en las leyes procesales no existe una relación tasada en la que se precisen o enumeren las categorías que merecerían tal calificativo, pues en el art. 456 LCRIM se habla de forma indeterminada de "*conocimientos científicos o artísticos"* sin que, además, *ex* art. 457 LCRIM y 340 LECIV sea requisito indispensable la aportación de un título oficial cuando no se trate de incorporar saberes reglados, por más que el Juez deba optar preferentemente, y si ello es posible, por el perito

[971] Sin perjuicio, naturalmente, del valor procesal que tienen reconocidos los indicios como prueba, tal y como señala el autor estudiado basándose en el ATS 1671/2007, de 18 de octubre, donde a su vez se cita dos SSTC confirmando esta misma posición. De esta forma, en el auto comentado se dice, en clara referencia al proceso inductivo que podría otorgar valor de prueba a la prueba de indiciaria, que "*se necesita una pluralidad de hechos básicos y que todos ellos, apreciados en su globalidad, no estudiados uno a uno, nos conduzcan al hecho consecuencia, por ser concomitantes entre sí y por hallarse relacionados unos con otros en esa perspectiva final que es la acreditación de un dato que de otro modo no puede quedar probado".* Este importante pronunciamiento ofrece una interesante perspectiva jurídica y práctica al concepto de informe policial de inteligencia en su posible consideración procesal como prueba. Vid. Dolz Lago, Manuel-Jesús. *La aportación científico-policial…op. cit.,* pág. 19 y ss.

[972] Vid. Dolz Lago, Manuel-Jesús. *La aportación científico-policial…op. cit.,* pág. 23.

titulado oficialmente *ex* art. 458 LCRIM, resultando bastante, en cualquier caso, que los peritos no titulados tengan "*conocimientos o práctica especiales en alguna ciencia o arte"*. Tampoco en el art. 335 LECIV, por su parte, se enumeran los conocimientos especiales, indicándose únicamente que tendrán que ver con "*los científicos, artísticos, técnicos o prácticos"*.

Lo anterior pone de manifiesto que el legislador optó por flexibilizar el concepto de perito de suerte que, para la práctica de la prueba pericial, pudiesen ser nombrados quienes de forma acreditada pudiesen contribuir al más exacto esclarecimiento de los hechos a enjuiciar, lo que obviamente debe ser a su vez objeto del estricto control jurisdiccional específico como lo demandan los arts. 474 y 477 LCRIM, entre otras disposiciones legales. No parece descabellado, por tanto, incluir a los miembros de la PJE en esta categoría cuando realicen funciones propias de la obtención de inteligencia.

En segundo lugar, debe descartarse vehementemente desde un principio el hecho que la PJE proceda mediante conocimientos secretos o saberes arcanos, pues sus métodos, por sofisticados que puedan parecer, deben ser y son perfectamente transparentes, precisamente, por pretender servir bien y fielmente al proceso penal, evitando decididamente cualquier tacha de oscuridad o ineficiencia que provocase su insuficiencia o nulidad procesal. Obrar de otra forma sería un absoluto despropósito cuyo único resultado sería el del fracaso del proceso penal y, consecuentemente, el de la PJE.

Debe añadirse, tal y como se argumentó en las breves referencias al atestado incluidas en capítulos anteriores, que de cualquier actuación de la PJE debe quedar un reflejo documental de sus fundamentos materiales o inmateriales en este preciso instrumento de constancia. En ningún caso puede situarse la PJE en la mala disposición de no poder contestar a una pregunta durante el proceso de contradicción en el juicio oral, por rebuscada que sea y, además, con una ajustada referencia a la masa documental admitida a examen jurisdiccional.

Muy al contrario, cualquier elemento inferido de otro puede y debe ser objeto de la reconstrucción en su tracto, con expresa y preferente referencia a las pruebas directas o indiciarias en las que se base, todo con objeto de aportar la necesaria

seguridad jurídica orientada a fundamentar las decisiones de actor jurisdiccional y a verificar en las persona del justiciable la estricta verificación de los derechos contenidos en el art. 24 CE. La actuación de la PJE, por tanto, obra siempre en las actuaciones hasta en sus más nimias expresiones.

En tercer lugar, los métodos y saberes de la PJE, de altísima capacitación profesional, sin duda *"escapan a la esfera de discernimiento de una persona de nivel medio de capacidad intelectual"*[973] en buena parte de sus facetas, en analogía a los que, como peritos, puedan acreditar los profesionales de otros ámbitos del saber humano, estén reglados o no, sin que ello suponga la más mínima nota diferencial con estos, por lo que su concurrencia como peritos ante un proceso penal no sólo es idéntica, sino que viene revestida por añadidura de todas las presunciones de neutralidad, imparcialidad[974], sujeción a la legalidad y las demás que fueron objeto de estudio en el capítulo segundo de este trabajo y que ya se hace ocioso reiterar.

Estas circunstancias hacen idónea a la PJE para intervenir con la más absoluta seguridad jurídica en el proceso penal y, muy especialmente, cuando concurran mediante la aportación de un informe de inteligencia policial. Las desatentas dudas *ad hominem* sobre este particular, que suelen plantearse pobremente por algunas defensas con resultado de fracaso durante las comparecencias de los agentes de la PJE a juicio, están por completo fuera de la realidad.

---

[973] Vid. Guerrero Palomares, Salvador. *La denominada "prueba…op. cit*., pág. 81.

[974] Según GUERRERO, *"las recientes SSTS de 22 de mayo de 2009 y de 31 de marzo de 2010, los peritos de inteligencia, miembros de las Fuerzas y Cuerpos de Seguridad del Estado son, en general, totalmente imparciales, y además, de su testimonio resulta, en palabras de la sentencia de 22 de mayo de 2009 "un alto poder convictivo", es claro que la posible contradicción efectiva de este medio de prueba desplegado por las acusaciones es mínimo".* Hay que anotar que esto será así únicamente respecto de la conclusión científica que aporten los peritos de los laboratorios forenses oficiales en aquellos casos en que haya sido posible materialmente lograr una, pues no todo les es siempre posible. De ser así, por efecto de la capacitación técnica de los peritos oficiales, la calidad de los métodos e instrumentos técnicos y de su exquisita imparcialidad, efectivamente, poca contradicción tendrán sus informes respecto de aquellos otros de que se sirvan las partes. De otro lado, parece olvidar GUERRERO que los efectos de la contradicción no nacen de la naturaleza intrínseca de la prueba, sino de su significado para la acreditación de la responsabilidad penal, materia que admite todas las posibilidades dentro del sistema acusatorio, incluida la absolución del justiciable. Por ello, es injusto y contradictorio acusar a la PJE por aportar un elemento objetivo para alcanzar este trascendental propósito. Vid. Guerrero Palomares, Salvador. *La denominada "prueba…op. cit*., pág. 87.

En cuarto lugar, los periodos de formación, perfeccionamiento y actualización de los agentes de la PJE y las intensas actividades de especialización, los habilitan como investigadores o peritos en muy variados campos del saber.

Si a ello se añade la experiencia en el campo de intervención de que se trate y el conocimiento profundo de cada concreta investigación, se constatará su idoneidad para el ejercicio de las labores señaladas. Particularmente, en el campo de la IDACE, se debe considerar su preparación para el manejo de *software* muy complejo y que requiere ingentes horas de adiestramiento y actualización para lograr su dominio (programas informáticos de análisis de fuentes abiertas o restringidas, análisis relacional, SITEL, hojas de cálculo, bases de datos, etc.), conocimientos profundos sobre telecomunicaciones en telefonía móvil o fija, comunicaciones telemáticas, técnicas de análisis de dispositivos o del espectro radioeléctrico, realización de estudios o pericias de geolocalización, análisis de código, etc.

En este sentido, me parece una trivialización, al menos en materia de IDACE –con un intenso componente pericial -, que pueda llegar a sostenerse, como sugiere GUERRERO con apoyatura en la STS de 2 de febrero de 2007, que *"esos conocimientos no puedan ser más que, únicamente, informaciones derivadas del análisis de documentación obrante en autos",* pues, con total seguridad, los documentos que se manejan como evidencia legal en determinados informes de inteligencia no son meros "papeles en claro", de cristalina interpretación sino que, en muchas ocasiones, su contenido material se verá necesitado de interpretación y puesta en relación con otros datos de cualquier naturaleza extraídos del escenario criminal, lo que incluye evidencias digitales cuya aprehensión intelectual no puede lograrse sino con el auxilio, precisamente, de los altamente formados y experimentados agentes de la PJE y de los sofisticados recursos tecnológicos de análisis que manejan. En consecuencia, me parece inadecuado despachar el informe de inteligencia policial como *"un resumen"*, como de forma tan destemplada se dice en la sentencia comentada[975] y, por ello, me

[975] En la STS se afirma que *"es discutible la necesidad de un resumen de la misma [de la documentación obrante en autos] por parte de los funcionarios"*. Pues bien, y por poner un ejemplo, entréguense en el Juzgado los listados en texto plano conteniendo miles o millones de comunicaciones (como IP, IMSI, IMEI, números de abonado, husos horarios, etc.) de los diversos actores de una trama criminal compleja para que S. Sª. pueda extraer conclusiones a su mera inspección ocular, sin tener que padecer la

muestro en contra de la opinión de GUERRERO cuando afirma que *"en los informes de inteligencia no se aplica ninguna ciencia ni arte"*[976].

En quinto lugar, los informes de inteligencia policial no tienen una finalidad valorativa sino interpretativa (según el diccionario, interpretar es *"explicar o declarar el sentido de algo"*), no contienen pronunciamientos jurídicos, no califican los hechos ni pretenden formular acusaciones y, en cualquier caso, tienen la obligación de analizar objetivamente – sin efectuar pronunciamiento alguno -, tanto lo que presuntamente incrimina a los justiciables, como lo que les pueda exculpar[977,978].

Actuar de otro modo se constituiría en un intolerable ataque al Estado de Derecho, una invasión inadmisible de las facultades del actor jurisdiccional y un cuestionamiento del derecho a la tutela judicial efectiva, a la defensa y a un proceso con todas las garantías consagrado en el art. 24 CE.

Sobre la cuestión de la supuesta tendencia a acusar de la PJE, que merece algún comentario adicional, dice GUERRERO en su crítica a los "peritos de inteligencia" que:

> *"La función real que realiza el perito de inteligencia no es otra cosa que coadyuvar con las acusaciones, exponiendo su propio informe (en el sentido del art. 743 LCRIM), valorando el material probatorio obrante en las actuaciones y*

---

contaminación de los "resúmenes" de la PJE. Vid. Guerrero Palomares, Salvador. *La denominada "prueba…op. cit*., pág. 82.

[976] Vid. Guerrero Palomares, Salvador. *La denominada "prueba…op. cit*., pág. 85.

[977] El art. 2 LCRIM dice que "*todas las Autoridades y funcionarios que intervengan en el procedimiento penal cuidarán, dentro de los límites de su respectiva competencia, de consignar y apreciar las circunstancias así adversas como favorables al presunto reo; y estarán obligados, a falta de disposición expresa, a instruir a éste de sus derechos y de los recursos que pueda ejercitar, mientras no se hallare asistido de defensor".* Obrar en contra de este precepto supondría una grave responsabilidad penal para el agente de la PJE que así procediese, lo que debe incluir no sólo la ocultación o manipulación de pruebas, sino cualquier tipo de deslealtad dolosa o culpable que supusiese una alteración de la realidad. El término "apreciar", por otro lado, significa según la acepción quinta del diccionario "*reducir a cálculo o medida, percibir debidamente la magnitud, intensidad o grado de las cosas y sus cualidades"*, lo que no deja de resultar sugerente en cuanto al ejercicio práctico de las facultades que encomienda al funcionario el art. 2 LCRIM.

[978] Sobre la imparcialidad de la PJE, afirma DOLZ que *"es cierto que en algunos supuestos se ha cuestionado la parcialidad de tales peritos-testigos en tanto son funcionarios de cuerpos y fuerzas de seguridad del Estado, interesados en la persecución y castigo de los delitos, o en el caso de los Inspectores de Hacienda, funcionarios de las Agencias Tributarias, a cuya instancia se persigue penalmente el fraude fiscal. Pero reiteradamente se inclina la jurisprudencia de esa Excma. Sala por afirmar la imparcialidad que se presupone a los funcionarios (Sentencias 1688/2000, de 6 de noviembre de 2000, 20/2001 de 28 de marzo, 776/2001, de 8 de mayo), incluso cuando en la causa estuviera personado como acusación particular el Abogado del Estado (Sentencia 1368/1999 de 5 de octubre)"*. Vid. Dolz Lago, Manuel-Jesús. *La aportación científico-policial…op. cit.,* pág. 31.

realizando alegaciones fácticas y, a veces, hasta jurídicas. Cuando así ocurra, la deposición del perito, en sí misma, no aportará ningún conocimiento técnico ni científico, ni ningún hecho presenciado por este, sino inducciones y opiniones de corte policial basadas en experiencias anteriores exentas de prueba objetiva en el caso concreto, pero sazonadas con expresiones grandilocuentes y aparente contundencia expositiva"[979].

Con este poco afortunado comentario, su autor parece querer atribuir a los agentes de la PJE la calidad de charlatanes o embaucadores, así como una candorosa inocencia a los demás actores del proceso penal ante sus ocurrencias, lo que es ajeno por completo a la realidad del día a día de la administración de Justicia, donde los agentes de la PJE contribuyen solventemente a su eficiente desarrollo con todas las garantías posibles. Ninguna pulsión por acusar hay en la PJE.

Tampoco acierta el tan citado autor con la pintoresca figuración que se hace del ***razonamiento policial*** al afirmar que *"se expresa en conceptos como prevención, anticipación, enemigo y seguridad del Estado"*[980], frase que contiene en sí misma una estupefaciente simplificación de la cuestión y que parece describir a unos agentes de estrechas miras juramentados para destruir a unos inexistentes enemigos, desprendidos de todo sentido de la imparcialidad y la mesura, antes de que sean capaces siquiera de pensar en delinquir. Nada más alejado de la realidad.

Debe a este respecto insistirse, a título de reiterado comentario, que la primigenia función de la PJE nace del art. 126 CE y no del 104 CE, donde se verifica una estricta separación constitucional entre ambas perspectivas policiales y que son, la de la dependencia funcional de Jueces, Tribunales y Ministerio Fiscal para la averiguación de los hechos delictivos ya producidos, de un lado, y la de la constitución de la Policía de Seguridad, de otro.

La PJE no es, por tanto, en sentido estricto, una fuerza policial para "luchar contra el crimen", salvo por los eventuales efectos disuasorios que puedan seguirse de sus intervenciones, por efecto de su eficiencia en el esclarecimiento de los delitos o, finalmente, por las consecuencias jurídicas que la Justicia señale para sus autores. La

[979] Vid. Guerrero Palomares, Salvador. *La denominada "prueba…op. cit*., pág. 86.
[980] Vid. Guerrero Palomares, Salvador. *La denominada "prueba…op. cit*., pág. 86.

PJE nada previene, nada anticipa, no tiene enemigos ni contribuye a la seguridad del Estado sino desde la faceta subyacente a su labor principal que se ha indicado.

Nada que ver con la Policía de Seguridad del art. 104 CE, pues de otra forma se incumpliría el mandato constitucional del art. 126:

> *"La policía judicial depende de los Jueces, de los Tribunales y del Ministerio Fiscal en sus funciones de averiguación del delito y descubrimiento y aseguramiento del delincuente, en los términos que la Ley establezca".*

Nada más y nada menos. Es necesario reiterar esta visión, pues la PJE, a la aparición de indicios racionales de criminalidad, busca instaurar, con inmediatez personal, la relación de dependencia funcional de Jueces y Fiscales que se consagra en la legislación[981], tan deficientemente interiorizada por los sectores menos advertidos de la doctrina y la jurisprudencia, cuyo mayor mérito es el de haber llenado de prejuicios la pobre percepción de las realidades de la PJ que exhiben, lo que supone un lamentable reduccionismo y una minusvaloración de sus funciones que es urgente resolver.

En sexto lugar, los informes de inteligencia policial lo que aportan es, únicamente, una interpretación técnica objetiva que esté racionalmente fundamentada en el contenido documental e indiciario incorporado en su integridad en el atestado, allí donde se estime necesario por su complejidad y utilidad para el proceso penal (sin reserva, por tanto, de su asociación a determinados tipos delictivos o fenómenos criminales, no suponiendo en sí mismos el más mínimo ataque a derecho fundamental alguno, por lo que resultan asépticos en su eventual examen procesal), lo que debe reiterarse sin perjuicio de incorporar en el atestado una valoración adicional subjetiva a incluir en diligencia de informe, pero de una forma expresa y diferenciada de la anterior, de suerte que esta opinión sea percibida en su más exacta dimensión como mera figuración intelectiva del Instructor Policial sobre cómo pudieron suceder los hechos.

---

[981] Tanto es así, que en el argot de la PJE se le da una segunda acepción del diccionario al término "*judicializar",* que podría definirse en el sentido de *"poner en inmediato conocimiento del Juez los indicios criminales que la PJE haya recabado sobre un determinado hecho de apariencia delictiva"*, todo ello para conseguir tempranamente la debida tutela judicial de los actos de investigación que se inicien y su exquisita sujeción al Derecho.

Esta aportación, que puede ser resultado tanto de la iniciativa judicial como de la policial, debe estar orientada al auxilio a la propia Autoridad Judicial[982] y a facilitar de una forma sencilla y accesible el proceso de contradicción y valoración de las pruebas en el acto de juicio oral, sin que en sí mismas supongan el más mínimo compromiso para la seguridad jurídica con que el proceso penal debe desarrollarse. No supone, desde esta perspectiva y en ningún caso, el más mínimo ataque al principio de presunción de inocencia, que no se desvirtúa ni contamina por la cabal exposición ante el Tribunal de hechos de naturaleza perfectamente objetivable.

5. Posición del perito de inteligencia en el proceso penal

La cuestión jurídica más interesante en relación con la consideración procesal de la prueba de inteligencia policial, hay que residenciarla, según todo lo expuesto hasta el momento, en su ubicación singular entre la pericia y el testimonio, sin que pueda en principio el Derecho decantarse por una de ellas, cuestión de la que cabe extraer algunas consecuencias para la debida percepción de este instrumento de innegable valor para la formación de la opinión judicial[983,984].

No tiene la PJE, desde luego, vocación alguna de que sus informes de inteligencia policial devengan en prueba sino, primigeniamente, la de ordenar

[982] Este factor de auxilio o colaboración con la Autoridad Judicial es resaltado por RIVES SEVA. Vid. Rives Seva, Antonio Pablo, y otros. *La Prueba en…op. cit.,* pág. 664.

[983] Vid. Guerrero Palomares, Salvador. *La denominada "prueba…op. cit*., pág. 84.

[984] Aunque con redacción aparentemente contradictoria, el siguiente pronunciamiento jurisdiccional viene a reconocer, como no puede ser menos, que existen facetas de la labor policial de inteligencia que, por tener un marcado carácter técnico, deberán ser consideradas como pericias: *"Como dijimos en la Sentencia nº 556/2006, de 31 de mayo , que, a su vez, cita la Sentencia nº 1029/2005, de 26 de septiembre, los denominados «informes policiales» no pueden calificarse de prueba pericial. En el proceso, es pericia la que se emite a partir de saberes que no son jurídicos y que tampoco corresponden al bagaje cultural del ciudadano medio no especialista. Consecuentemente, no pueden darse por supuestos y deben ser aportados al juicio, para que su pertinencia al caso y su concreta relevancia para la decisión sean valorados contradictoriamente. De este modo, es claro que apreciaciones como la relativa a la adscripción o no de alguien a una determinada organización criminal, o la intervención de un sujeto en una acción delictiva a tenor de ciertos datos, pertenecen al género de las propias del común saber empírico. Salvo, claro está, en aquellos aspectos puntuales cuya fijación pudiera eventualmente reclamar una precisa mediación técnica, como sucede, por ejemplo, cuando se trata de examinar improntas dactilares".* STS 2251/2007, de 16 de febrero (FJ 5º). Otros ejemplos que podrían añadirse serían: análisis del espacio radioeléctrico, análisis relacionales de DACE, captación del IMSI o el IMEI, pericias de geolocalización, etc.

técnicamente la investigación con toda la eficiencia que de su contenido pueda lograrse, de suerte que pueda servir al éxito del proceso penal, si ello procede, como bien indica PÉREZ GIL:

> *"La* actividad *policial de persecución del delito se ha de desarrollar siempre a través de análisis de información, cuanto más depurada mejor, porque solo así podrá cumplir idóneamente su función…El concepto de inteligencia policial es por tanto plenamente válido y asumible, pero alude al plano operativo policial, sin que parezca que debamos admitir que genere alteraciones en la actividad probatoria. De otra manera habríamos de asumir la preponderancia de una valoración confeccionada en sede policial frente a la que realice el tribunal, el cual estaría condicionado hasta el extremo".*

En la doctrina procesal clásica, el ***testigo*** debía declarar según su experiencia, que debía adquirir mediante su presencia personal al tiempo de producirse los hechos y con la condición jurídica de tercero respecto de aquello sobre lo que testimoniase.

El ***perito***, por su parte, tenía una aparición posterior a la de los hechos, en los que intervenía por reclamación de una autoridad que los hubiese de entender y lo hacía con el propósito de que sus especiales conocimientos contribuyesen a su esclarecimiento. Una diferencia esencial entre ambas figuras podría resumirse en que *"al testigo se le llama porque conoce ya el hecho; al perito para que pueda conocerlo"*[985].

Según esta percepción clásica, los agentes de la PJE que confeccionan un informe de inteligencia policial de ningún modo pueden tener la condición de testigos, pues su intervención no es contemporánea con los hechos, salvo que en el marco de las actividades investigativas adquiriesen determinados conocimientos propios de esta figura procesal como, por ejemplo, durante su participación en un seguimiento o en un registro domiciliario respecto de aquello que presenciasen.

[985] GUERRERO aporta un interesante panorama que resume la teoría clásica. Vid. Guerrero Palomares, Salvador. *La denominada "prueba…op. cit*., pág. 84

Sí podrían, por el contrario, ser peritos en aquellos estudios que practicasen según lo que establecen las leyes procesales y que tuviesen una perfecta diferenciación formal como tales dentro del informe de inteligencia policial[986].

En efecto, y adhiriéndome a las opiniones predominantes entre los autores estudiados, sería necesario, como sugiere GUERRERO, *"distinguir dentro del "informe de inteligencia", lo que puede ser considerado como una auténtica pericia, de aquello que deberá ser tenido, según explica la sentencia [vid. nota al pie], como una testifical de referencia"*[987]. Según esta posición, sería posible que, dentro del conjunto del informe policial, se tomasen determinadas aportaciones de la PJE expresamente como periciales y, otras, como testimonios de referencia, todo lo cual conllevaría la pacífica aceptación de este instrumento en su ponderada calificación como prueba en el marco de los debates procesales y sin necesidad de constituirse en una nueva figura procesal[988].

En este contexto, la definición de ***testigo de referencia***, con asiento en el art. 710 LCRIM[989], se encuentra en las SSTS de 3 de octubre de 1995 –RJA 1995, 7589– y 18 de julio de 1996 –RJA 1996, 5919–, donde se dice que *"testigo es la persona física que, sin ser parte en el proceso, es llamada a declarar, según su experiencia personal, acerca de la existencia y naturaleza de unos hechos conocidos con anterioridad al proceso, bien por haberlos presenciado como testigo directo, bien por haber tenido*

[986] DOLZ, en contra de las dudas que puedan suscitarse sobre la especialización de los agentes de la PJE en comparación con la que indubitadamente se atribuye a los peritos de otros organismos oficiales, así quiere verlo cuando afirma que *"el supuesto, no idéntico, sí se asemeja a la pericial oficial que pueden configurar los inspectores de Hacienda en procesos por delitos contra la Hacienda Pública, o los expertos de la Comisión Nacional del Mercado de Valores, en delitos societarios o defraudaciones, tal como se ve en la Sentencia de 464/2003, de 27 de marzo. Aunque las fuentes de conocimiento y especialización de unos y otros sean diversas, es cierto que, sobre todo los últimos, como los funcionarios policiales, obtienen sus conclusiones del examen del propio material de la investigación en relación con sus conocimientos especializados en la materia que se investiga, sean las transacciones bursátiles – lícitas e ilícitas y el modo en que éstas puedan operarse - en el mercado de valores, sean actividades de grupos terroristas de uno u otro signo".* Vid. Dolz Lago, Manuel-Jesús. *La aportación científico-policial…op. cit.*, pág. 31.

[987] El autor se refiere a la SAP de Madrid, Sección 7ª, de 17 de julio de 2009, (Núm. 79/2009, rec. 46/2008). Vid. Guerrero Palomares, Salvador. *La denominada "prueba…op. cit.*, págs. 88 y 89.

[988] El TC no considera que existan limitaciones, según ATC 193/1987, en el que se reconoce que no existen *numerus clausus* en el listado de medios de prueba que pueden practicarse en el acto de juicio oral. Vid. Dolz Lago, Manuel-Jesús. *La aportación científico-policial…op. cit.*, pág. 19.

[989] Con excepción de los delitos de injuria y calumnia vertidos de palabra *ex* art. 813 LCRIM.

noticia de ellos por otros medios como testigo de referencia"[990]*.* De esta definición cabe extraer la posibilidad de adquirir el conocimiento de unos hechos por medio de la inferencia de otros de los que no tiene un conocimiento directo, entre los que se puede incluir, obviamente, los análisis de inteligencia tal y como vienen siendo descritos a lo largo de este capítulo.

Esta figura procesal genera, no obstante, una débil valoración en la jurisprudencia del TC[991], por considerarla poco fiable y por presentar, en definitiva, problemas de credibilidad, tal y como se expresa, entre otras, en la STC 217/1989, de 21 de diciembre, que mostró su recelo a la admisibilidad incondicional de esta prueba, al afirmar que *"en la generalidad de los casos la prueba de referencia es poco recomendable, pues supone eludir el oportuno debate sobre la realidad misma de los hechos y el dar valor a los dichos de personas que no han comparecido en el proceso*".

En algunas sentencias del TC, de otro lado, se llega incluso a afirmar puede *"implica[r] la elusión de la garantía constitucional de inmediación de la prueba"* y *"soslayar el derecho que asiste al acusado a interrogar al testigo directo y someter a contradicción su testimonio"*, según la STC 209/2001[992].

Sobre la cuestión de la fiabilidad, como oportunamente apunta RIVES en referencia a la jurisprudencia del TS, *"la STS de 19 de julio de 1996 –RJA 1996, 6071– ha calificado a los testimonios de referencia de "prueba poco responsable", y las SSTS de 20 de septiembre de 1996 –RJA 1996, 6618– y 24 de febrero de 1997 –RJA 1997, 1374– de prueba "poco recomendable", consolidándose la doctrina sustentada, entre otras, en las SSTS de 5 de marzo de 1993 –RJA 1993, 1840– y 10 de febrero de 1997 –RJA 1997, 718–, en el sentido de que "su valor probatorio es muy reducido" y, en*

[990] Vid. Rives Seva, Antonio Pablo. *El testimonio de referencia en la jurisprudencia penal, en* Noticias Jurídicas (http://noticias.juridicas.com/articulos/65-Derecho%20Procesal%20Penal/200001-testimoniojpenal.html), 2000.

[991] Sería necesario también comentar el carácter excepcional y supletorio con que ha de recurrise a este tipo de pruebas, tal y como sostiene ALONSO PÉREZ, con apoyo en las SSTS, de 11 de septiembre de 1992 y 11 de marzo de 1994, entre otras, constatando al mismo tiempo la dificultad en extraer carga probatoria suficiente de semejantes testimonios. Vid. Alonso Pérez, Francisco. *La Policía Judicial…op. cit.,* pág. 183 y ss. Sobre la excepcionalidad, con apoyo en la STC 261/1994, de 3 de octubre, entre otras, vid. Rives Seva, Antonio Pablo. *El testimonio de referencia…op. cit.*

[992] Vid. Guerrero Palomares, Salvador. *La denominada "prueba…op. cit*., pág. 87.

ningún caso puede constituir la única prueba, actuando más bien como indicios corroborantes junto a otro tipo de pruebas de carácter directo o indiciario"[993].

Sin embargo, en este desalentador y repetido pronunciamiento jurisprudencial se encuentra, en su frase final, respecto de la utilidad de los informes de inteligencia policial, la exacta dimensión de su valor para proceso penal, en la medida en que se basen en *"otro tipo de pruebas de carácter directo o indiciario"*, como fuente segura de conocimiento, y no en controvertibles o endebles referencias a testimonios de terceros de nula consistencia real, máxime cuando estos sean, además, desconocidos.

Esta perspectiva solventa cualquier tacha de inseguridad, falta de fiabilidad o de credibilidad, permitiendo que los debates procesales sobre su contenido en el acto de juicio oral, alcancen todas sus finalidades por ser asequibles al entendimiento común y aptos para el escrutinio de las partes ya que la cuestión del testimonio de referencia no se agota en el testimonio personal de lo que hicieron otros, sino en cualquier otra fuente de prueba que coadyuve a su firme sustento[994,995,996].

---

[993] La siguiente jurisprudencia del TS afirma que *"de esta manera, los llamados «informes de inteligencia» no son prueba pericial, sino que participan de la naturaleza de la prueba de indicios, en la medida que aportan datos de conocimiento para el Tribunal sobre determinadas personas y actividades. Y esos datos si son coherentes con el resultado de otros medios de prueba pueden determinar, en conjunción con ellos, la prueba de un hecho, siempre que éste fluya del contenido de todos esos elementos valorados por el órgano sentenciador. De esta manera, los llamados «informes de inteligencia» no son prueba pericial, sino que participan de la naturaleza de la prueba de indicios, en la medida que aportan datos de conocimiento para el Tribunal sobre determinadas personas y actividades. Y esos datos si son coherentes con el resultado de otros medios de prueba pueden determinar, en conjunción con ellos, la prueba de un hecho, siempre que éste fluya del contenido de todos esos elementos valorados por el órgano sentenciador".* STS 2251/2007, de 16 de febrero (FJ 5º).

[994] Vid. Rives Seva, Antonio Pablo. *El testimonio de referencia…op. cit.*

[995] Y sí adherirse, en contra de la opinión de GUERRERO, a la visión expresada por la Audiencia Provincial de Sevilla en Auto de su Sección 1ª núm. 106/2009, de 2 de febrero, en el que se dice que *"la irrelevancia de que la declaración del mismo sea prestada en una u otra cualidad [testifical o pericial], pues una y otra están sometidas a la libre valoración de la prueba, conforme a lo dispuesto en el artículo 741 ante la LCRIM"* y, puede añadirse, en ambos casos, a su apreciación en conciencia por el juzgador. Ciertamente, en mi opinión y desde un punto de vista policial y extrajurídico, si son galgos o podencos poco importa si la función jurisdiccional puede ejercerse en plenitud y seguridad con el auxilio, entre otros instrumentos procesales, del informe de inteligencia policial. En este mismo sentido, el TS se pronuncia diciendo que *"por tanto, no se acreditan los hechos por los «informes de inteligencia», sino que los datos que en ellos se contienen se contrastan con el material probatorio obrante en la causa y sus conclusiones se aceptan o se desvirtúan por el resultado del mismo. Y a estos efectos es indiferente que los agentes autores fueran citados como peritos o como testigos. Lo relevante es que las partes conocieron el contenido de los informes elaborados y que pudieron rebatir el mismo con respeto a los parámetros derivados de los principios de publicidad y contradicción".* STS 2251/2007, de 16 de febrero (FJ 5º).Vid. Guerrero Palomares, Salvador. *La denominada "prueba…op. cit*., pág. 84.

[996] Sobre la eficiencia de control de jurisdiccionalidad sobre los informes de inteligencia policial y su falta de oscuridad o secreto, asegura DOLZ que *"todo ello permite un pleno control de legalidad por parte de*

Como conclusión de este apartado, y tratando de congregar todos los elementos estudiados en uno, opto por escoger, entre la prueba pericial de inteligencia y los informes de inteligencia policial, la expresión intermedia de ***prueba de inteligencia policial*** como la más adecuada y comprensiva para describir, en sus más exactos términos, su naturaleza genuinamente policial y su eventual utilidad como prueba para el proceso penal cuando así lo admita el actor jurisdiccional.

6. Propuesta de definición de la prueba de inteligencia policial

En consonancia con lo planteado en los apartados anteriores, cabe proponer la siguiente definición de ***prueba de inteligencia policial***:

> *"Por* prueba de inteligencia policial *se entiende aquella que, habiendo sido incorporada al proceso penal a través del atestado policial, contenga juicios policiales de inferencia estrictamente fundamentados, tanto en los estudios periciales practicados, como en referencia a las pruebas directas e indirectas o indiciarías que hayan sido del conocimiento de la PJE durante las fases de investigación y que, a su vez, hayan sido realizadas bajo la dependencia funcional de Jueces y Fiscales y legítimamente admitidas para su contradicción y valoración en el acto de juicio oral".*

los Tribunales de Justicia sobre la actuación policial. Un control que en el caso del informe de "inteligencia" aquí debatido pudo ser y fue, como se verá, intenso ya que su intervención, en su faceta o componente de prueba pericial, no aporta en realidad elementos técnicos que no sean perfectamente comprensibles y fiscalizables por el Tribunal a la luz del resto de pruebas de la causa; a diferencia de lo que ocurriría con otras pruebas periciales que aporten aspectos científicos o técnicos inaprensibles, por puras limitaciones de la inteligencia humana, por los Tribunales, el componente pericial de los informes de inteligencia, exclusivamente limitado al tratamiento, agrupación y análisis de información con arreglo a experiencia, y, lo que es más importante, los juicios de inferencia alcanzados a la luz de todo ello, resultan fiscalizables en todos sus aspectos por la Sala sentenciadora", Vid. Dolz Lago, Manuel-Jesús. *La aportación científico-policial…op. cit.,* pág. 33.

C. Generalidades sobre la IDACE

1. La necesidad de adquirir indicios por la PJE

En los apartados anteriores se ha presentado un amplio panorama sobre la cuestión de la inteligencia y de su eventual utilidad para el proceso penal. Con tan trascendental propósito, a través de los autores estudiados se ha reflexionado sobre la prueba de inteligencia policial, atribuyéndole un papel singular para la formación de la opinión jurisdiccional.

Sin embargo, en el proceso de valoración de esta herramienta, centrado en la elaboración de los elementos de inteligencia ya disponibles en la sede policial y dispuestos para su incorporación al atestado policial, donde no se había reparado hasta ese momento era en que, necesariamente, debían ser previamente obtenidos y, resulta ocioso añadir, de una forma admisible para el Estado de Derecho.

En efecto, queda aún mucho por decir respecto de los actos de investigación que propician la adquisición de las pruebas directas e indirectas o indiciarias que habrán de ser sometidas al ciclo de inteligencia, tanto si proceden de fuentes abiertas como restringidas o si, dicho de otra manera, habiendo mediado, en este último caso, una medida de limitación de derechos fundamentales legítimamente instaurada, se pueda proceder conjuntamente a su integración a este proceso de un modo jurídicamente seguro.

Pero de las fases de integración, análisis e interpretación propias del ciclo de inteligencia ya se ha hablado, al menos por el momento, de una forma suficiente a los propósitos de este trabajo y conviene ahora profundizar un poco más en el qué y el cómo se obtienen los elementos indiciarios que sirven de alimento básico del ciclo de inteligencia criminal, con vocación de hallarles una futura utilidad procesal como prueba, de forma que, hasta tanto esto sea así, enerven el proceso intelectivo policial propio de las fases primarias de la investigación, toda vez que en el escenario de intervención han cambiado las cosas de forma tan intensa y singular que se hace necesaria una profunda revisión de las formas de obtención.

Por ello, la percepción que se tenga de este proceso deberá desprenderse de los prejuicios hipergarantistas y descansar en una ajustada visión de la realidad que lo acoge y que no es otra que la que se deduce del bien ponderado garantismo que trasluce el texto constitucional, que en nada empece, en cualquier caso, a un correcto planteamiento de la función policial.

2. Búsqueda y recopilación de vestigios inmmateriales por la PJE

Las funciones generales encomendadas a la PJE *ex* art. 126 CE exigen, en su materialización práctica, una continua búsqueda y recopilación de vestigios sobre los hechos criminales que alcance a conocer, que debe entenderse como un proceso mantenido de una forma dinámica y constante en el tiempo.

El desarrollo jurídico de este precepto constitucional hay que ubicarlo principalmente en los arts. 282, 326 y 770 LCRIM, mereciendo una especial mención el mandato que contienen de evitar el riesgo de desaparición de los indicios, tal y como se establece genéricamente en el 282, que ordena a la PJE *"…recoger todos los efectos, instrumentos o pruebas del delito de cuya desaparición hubiere peligro"* y, de una forma especialmente exhaustiva, en el contenido del art. 770 LCRIM, lo que otorga a la PJE, no sólo un deber de aseguramiento de lo que halle a su alcance, sino un diáfano deber de anticipación diligente a la posible desaparición o destrucción de pruebas sin que para ello deba contar con una previa y específica encomienda judicial[997].

Otras normas que obligan a actuar con tanta prevención son las contenidas en el art. 11.1 g) LCFSE, referida a la custodia de los efectos, instrumentos o pruebas del

[997] La STC 173/2011, de 7 de noviembre, dice a este respecto, resaltando el sempiterno problema de la indeterminación jurídica, que *"entre esas diligencias (que la Ley no enumera casuísticamente, pero que limita adjetivándolas y orientándolas a un fin) podrá encontrarse la de examinar o acceder al contenido de esos instrumentos o efectos, y en concreto, de documentos o papeles que se le ocupen al detenido, realizando un primer análisis de los mismos, siempre que - como exige el propio texto legal - ello sea necesario (estrictamente necesario, conforme al art. 14 de la Ley Orgánica 1/1992), estricta necesidad que habrá de valorarse atendidas las circunstancias del caso y que ha de entenderse como la exigencia legal de una estricta observancia de los requisitos dimanantes del principio de proporcionalidad. Así interpretada la norma, puede afirmarse que la habilitación legal existente cumple en principio con las exigencias de certeza y seguridad jurídica dimanantes del principio de legalidad, sin perjuicio de una mayor concreción en eventuales reformas legislativas*". Como es de ver, toda una invocación a la necesaria y eficiente labor reformadora que cabe exigírsele al legislador.

delito cuya desaparición hubiere peligro, el art. 14 de la Ley Orgánica 1/1992, de 21 de febrero, de protección de la seguridad ciudadana y el art. 28 e) del RD 769/1987, de 19 de junio, de Policía Judicial y la copiosa jurisprudencia[998].

Es evidente que, frente a la diligencia que la PJE debía oponer ante la posible desaparición o destrucción de pruebas en el mundo físico, para el que el legislador decimonónico preparó la ley procesal vigente, en el virtual, esta necesidad de actuar con eficacia y efectividad se torna más notoria, haciendo extremadamente dificultosa la intervención policial en un espacio condicionado por el sustrato o factor que suponen los actos de comunicación constitutivos de la evidencia digital inmaterial –millones de datos circulando por las redes públicas de comunicaciones que, expresados en *giga o terabytes,* pueden desaparecer instantáneamente y a escala planetaria con un simple *click* del ratón del ordenador -, que perturban o limitan la habilitación procesal de la PJE para intervenir con un *quantum* análogo de eficiencia.

La anterior circunstancia es de unánime reconocimiento entre todas las fuentes consultadas y se basa, además, en la experiencia de la práctica policial. Es por ello imperioso, una vez más, insistir en la necesidad de lograr una percepción equilibrada sobre el alcance real del sacrificio que para los derechos fundamentales suponen determinadas formas de obtención de los indicios por parte de la PJE.

Sin embargo, la recogida de la evidencia digital y, en general, el almacenamiento y tratamiento de los datos personales, sea cual fuere su fuente originaria, se constituye en uno de los concernimientos más sensibles del entorno democrático en que se desenvuelve la sociedad española y que debe ser manejado por los poderes públicos bajo sensibles limitaciones.

Sobre la controvertida cuestión de la protección de datos personales en relación con las comunicaciones electrónicas, baste decir que en el Considerando Séptimo de la Directiva 2002/58/CE, del Parlamento Europeo y el Consejo, de 12 de julio de 2002, *relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas* (Directiva sobre la privacidad y las comunicaciones electrónicas), se manifiesta con meridiana claridad esta

[998] SSTS 7/10/1994, 9/5/1997, 26/02/1999, 26/01/2000, 4/09/2000 y 27/12/2006. Vid. Velasco Núñez, Eloy. *Delitos cometidos a través de Internet…op. cit.,* pág. 222.

preocupación, diciendo que "e*n el caso de las redes públicas de comunicación, deben elaborarse disposiciones legales, reglamentarias y técnicas específicas con objeto de proteger los derechos y libertades fundamentales de las personas físicas y los intereses legítimos de las personas jurídicas, en particular frente a la creciente capacidad de almacenamiento y tratamiento informático de datos relativos a abonados y usuarios"*.

Pero aún siendo esto así, el legislador deja una puerta abierta a la satisfacción de las necesidades especiales de intervención en el amplio espectro que representan las formas de comunicación electrónica actuales, propiciadas por el espectacular y universal desarrollo de las TIC[999], con una también clara referencia a la proporcionalidad de las medidas que los Estados Miembros hubieren de arbitrar, al establecer en el Considerando Decimoprimero que "*en consecuencia, la presente Directiva no afecta a la capacidad de los Estados miembros para interceptar legalmente las comunicaciones electrónicas o tomar otras medidas, cuando sea necesario, para cualquiera de estos fines y de conformidad con el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales, según la interpretación que se hace de éste en las sentencias del Tribunal Europeo de Derechos Humanos. Dichas medidas deberán ser necesarias en una sociedad democrática y rigurosamente proporcionales al fin que se pretende alcanzar y deben estar sujetas, además, a salvaguardias adecuadas, de conformidad con el Convenio Europeo para la Protección de los Derechos"*, idea que luego se desarrolla en el art. 15 de la Directiva.

De los anteriores considerandos pueden extraerse algunas conclusiones de interés:

- Las previsiones se centran en las *"redes públicas de comunicaciones*" como si fuesen el único elemento a tener en cuenta a la hora de arbitrar medidas de protección de datos, olvidando el papel de unos ISP que, por otro lado, se sirven de ellas para la transferencia telemática de sus contenidos.

[999] Sin ir más lejos, podría mencionarse como ejemplo el caso de las posibilidades de geolocalización de terminales de telefonía móvil o del acceso inconsentido a una wi-fi privada, con la correspondiente y compleja discusión sobre aspectos tecnológicos y jurídicos, cosa impensable cuando, en los años de modificación del art. 579 LCRIM, sólo existía la posibilidad de geolocalizar un terminal de telefonía por el muy sencillo procedimiento de averiguar el domicilio en que lo había instalado la operadora o, sencillamente, no se tenía la más remota idea de lo que iba a ser un acceso wi-fi a una cuenta de ADSL.

- La necesidad de que el Derecho alcance al mundo de las comunicaciones electrónicas y que los Estados cuenten con una legislación específica, garantizando la tutela judicial efectiva, el derecho a la defensa de los ciudadanos y a un proceso con todas las garantías.
- La necesidad de intervenir para controlar el ámbito virtual donde también se desarrolla la vida humana, pero haciendo frente a la vez a la "*creciente capacidad de almacenamiento y tratamiento informático de datos relativos a abonados y usuarios".*
- El imperativo o exigencia de que el Estado democrático actúe de una forma proporcional a los hechos ilegítimos cuya interdicción deba procurar.
- El valor de las salvaguardas como garantía de la seguridad jurídica en el proceso de obtención de datos, lo que sugiere a su vez una reflexión sobre la urgente disponibilidad de determinados medios, de naturaleza mixta, normativa y tecnológica, que pudieran aportar eficiencia adicional a las medidas de control jurisdiccional.
- A diferencia de lo que sucede en el mundo físico, para actuar policialmente en el virtual con análogas capacidades procesales, es necesario, según la directiva, "*interceptar legalmente las comunicaciones electrónicas o tomar otras medidas".*

Es prudente anotar, aún sin mencionar el factor condicionante de la capacidad procesal de la PJE por el hecho de la yuxtaposición de los actos de comunicación electrónica sobre el acceso legal a la prueba digital, la evidente insuficiencia de la normativa española de protección de datos - la LOPD y legislación derivada -, centrada en los entornos cerrados donde existan ficheros de datos, cuyo eficiente control está al alcance de la capacidad interventora del Estado, pero inútil en cuanto los datos personales salen a la red con absoluto descontrol y pérdida real y efectiva del dominio por parte de las personas físicas y jurídicas que, en algún momento, consentida o inconsentidamente los vertieron a Internet[1000].

[1000] Dice VELASCO que la obsoleta LOPD, "*prevista para entornos informáticos cerrados, no alcanza a valer para entornos abiertos como Internet, a cuyas dimensiones no puede poner efectivo coto".* Vid. Velasco Núñez, Eloy. *Delitos cometidos a través de Internet…op. cit.,* pág. 138. Tanto es así, que el llamado "derecho al olvido en la red" – una creciente preocupación dentro de los órganos de gobierno

Consecuente a la anterior circunstancia, la recogida y tratamiento automatizado de datos por la PJE - cuyo producto más expresivo es, precisamente, la obtención de inteligencia para el proceso penal - es uno de los más graves concernimientos de la legislación europea y nacional de protección de datos. Sin embargo, la PJE debe quedar excepcional y procesalmente habilitada para obtenerla y de un modo acorde al ámbito donde ha de intervenirse, esto es, el de la producción de la evidencia digital en modo análogo a como lo haría en el espacio físico.

Una primera exigencia, derivada de la necesidad de obtener evidencia digital sobre las comunicaciones electrónicas, sería la de determinar, lo más tempranamente posible, la exacta naturaleza jurídica de la que se produzca dependiendo del empleo real del dispositivo por parte de los investigados, ya que, cuando exceda a sus finalidades primigenias de facilitar técnicamente sus comunicaciones personales, rigurosamente tuteladas por el art. 18.3 CE, se hará necesario diferenciarlas, material y formalmente, de aquellos otros que, no consistiendo en tales comunicaciones personales sino en otros usos instrumentales diversos – impensables en la época de la exclusividad de la telefonía fija -, no merecerían siquiera la protección genérica del art. 18 CE o, dicho de otra forma, que la injerencia en su contenido no afectaría a ningún aspecto de la intimidad consagrado en el texto constitucional y en el CEDH.

Es evidente, en este sentido, que la exigente protección del art. 18.3 CE debe quedar reservada, en el marco de una investigación en sede penal, únicamente al espectro de las comunicaciones personales de los justiciables, cosa que puede ser

---

de la UE - se ha convertido en un anhelo para el 75 % de los ciudadanos de la Unión Europea, anhelo con pocas posibilidades de éxito sólo sin pensamos en lo extraordinariamente fácil que es hacer una búsqueda de fuentes abiertas de datos personales y luego almacenarlos en cualquier intrincado fichero de datos alojado en cualquier ordenador o servidor del mundo. Vid. http://www.europarl.europa.eu/news/es/headlines/content/20120120STO35905/html/D%C3%ADa-Europeo-de-la-Protecci%C3%B3n-de-Datos-el-derecho-a-ser-olvidado-en-Internet, en la página del Parlamento Europeo, información ampliamente difundida por la prensa.

Véase también el dictamen del SEPD en *«Un enfoque global de la protección de los datos…doc. cit., p*to. 174.

Sobre similares concernimientos relativos a la previsión del art. 18.4 CE, respecto de la autodeterminación informativa, el *common law* anglosajón ha desarrollado toda una teoría acerca del "*right to control information about oneshelf",* de un modo conexo con el derecho a la privacidad, tal y como el autor estudiado indica. La preocupación por tan sensible cuestión no puede ser desoída por el Estado democrático y sí gestionada con rigor garantista pues, fuera de las debidas precauciones, en mi opinión, deviene un riesgo para la calidad democrática de la vida de los ciudadanos. La excepcionalidad de su sacrificio debe siempre estar bien ponderada. Vid. Velasco Núñez, Eloy. *Delitos cometidos a través de Internet…op. cit.,* pág. 139.

diligentemente delimitada en fases tempranas de la investigación, lo que sin duda contribuirá al esclarecimiento de la maquinación criminal desde los aspectos más directamente relacionados con el devenir de sus actores en el escenario criminal.

Puede decirse sobre todas las reflexiones anteriores que, en el inquietante panorama actual de la criminalidad, pueden hallarse conspiraciones de extraordinaria complejidad en las que medie un abuso ilimitado, instrumental y, desde luego, no personal de las TIC, pero que siempre tendrán entre sus protagonistas a un número finito de personas cuyo uso personal de las comunicaciones será, por el contrario, siempre diferenciable y limitado. Si sobre los segundos cabe la más estricta protección del art. 18.3 CE, sobre los primeros nada puede parangonarse.

Actuar de otra forma, en mi opinión, equivaldría a renunciar a la tutela judicial efectiva y al derecho a la defensa del interés público en aquellas situaciones en que los dispositivos de comunicación sólo pudiesen ser considerados en sí mismos como instrumentos del delito y, en ningún caso, como elementos de comunicación personal de los justiciables.

D. La IDACE sobre datos de tráfico de telefonía y comunicaciones IP

1. La IDACE, entre el secreto de las comunicaciones y la protección de datos

El término inteligencia aplicado a los DACE adquiere una dimensión inusitada con la evolución de las TIC. Si al comienzo de la telefonía fija lo que se pretendía a través de una intervención judicial de las comunicaciones era escuchar su contenido material y saber quiénes eran los interlocutores, con el fin de obtener algún indicio que orientase la investigación o que permitiese anticiparse a nuevos hechos delictivos (normalmente, sucediendo todo en un reducido espacio territorial nacional y con un número de actores también muy limitado, esto es, no más de diez o doce personas concertadas en una determinada maquinación criminal). Consecuentemente, el volumen de DACE podía perfectamente analizarse mediante métodos artesanales de lápiz y papel.

Sin embargo, en la era de las comunicaciones de telefonía móvil o Internet puede que el interés de proceso penal no consista en escuchar ningún mensaje inteligible ni saber quiénes son sus protagonistas y, sin dudarlo, excederá al ámbito nacional. Pero además, a poco que los casos adquieran alguna complejidad, los DACE que se manejen podrán contabilizarse por millones. No valen ya ni el lápiz ni el papel, sino el uso de sofisticados instrumentos tecnológicos y *software* de análisis de datos.

También se han puesto de manifiesto algunas rigideces de la adscripción jurídica de la cesión de los datos de tráfico al art. 18.3 CE y cómo, en buena lógica, el tratamiento de los DACE hubiera sido más adecuado acogerlo en el art. 18.4 CE a los fines que ocupan este trabajo, mediando siempre las debidas garantías.

Sobre esta cuestión, en un caso anterior a la entrada en vigor de la LCDCE, el TS, *"sin pretensiones ni mucho menos de sentar doctrina",* duda de la necesidad de mandato judicial para los DACE, con la misma y reiterada posición de la AEPD:

"Queda en pie la duda, de si para solicitar el número telefónico o identidad de una terminal telefónica (cabría extenderlo a una dirección o identificación de Internet: Internet protocols), es necesario acudir a la autorización judicial, si no han sido positivas las actuaciones policiales legítimas integradas por injerencias leves y proporcionadas, que puede respaldar la Ley Orgánica de Cuerpos y Fuerzas de Seguridad del Estado o Ley de Seguridad Ciudadana, en la misión de los agentes de descubrir delitos y perseguir a los delincuentes.

A nuestro juicio, sin pretensiones ni mucho menos de sentar doctrina (obiter dicta), los datos identificativos de un titular o de una terminal deberían ser encuadrados, no dentro del derecho al secreto de las comunicaciones (art. 18-3 C.E .) sino en el marco del derecho a la intimidad personal (art. 18.1º C.E .) con la salvaguarda que puede dispensar la Ley de Protección de Datos de Carácter Personal, L. O. 15/1999 de 13 de diciembre: art. 11.2 d. o su Reglamento, Real - Decreto 1720/2007 de 21 de diciembre, que entró en vigor el 31 de marzo de 2008, sin despreciar la Ley 32 de 3 de noviembre de 2003, General de Telecomunicaciones y su Reglamento, R.D. 424 de 15 de abril de 2005 , en los que parece desprenderse que sin el consentimiento del titular de unos datos reservados, contenidos en archivos informáticos, no pueden facilitarse a nadie, salvo los casos especiales que autorizan sus propias normas, entre las que se halla la autorización judicial, que lógicamente estaría justificada en un proceso de investigación penal.

Tampoco debe pasar por alto, aunque sólo sea con carácter dialéctico, el contenido de la Ley nº 25 de 18 de octubre de Conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicación, que al igual que el Reglamento de la Ley de protección de datos son posteriores a los hechos aquí enjuiciados y por ende no aplicables"[1001].

Finalmente, en un ejercicio de aceptación de la realidad y buscando no plantear propuestas regresivas en cuanto a la estricta visión jurídica que se ha impuesto sobre la materia, debe optarse por soluciones alternativas e integradoras, que aúnen una

[1001] STS 236/2008, de 9 de mayo, FD 1º.4.

eficiente modulación de la reserva judicial en lo que admita la exégesis del principio de proporcionalidad, con la admisión de determinadas facultades de análisis en favor de la PJE y el contraste de integridad, veracidad y autenticidad que supongan los medios jurídicos y tecnológicos de salvaguarda. A todo ello, debe precederle una correcta percepción sobre la naturaleza de las comunicaciones electrónicas y la realidad social que las acompaña actualmente.

Sobre estas diáfanas necesidades VELASCO opina que:

> *"Los instrumentos de trabajo de los investigadores públicos preprocesales deben ponerse a la altura de los tiempos, deben acabarse las desconfianzas infundadas en la profesionalidad y convicciones democráticas de los cuerpos policiales, y entenderse que el ejercicio de las facultades legales que les procuran los arts. 22.2 y 12.3 LSSICE, son autónomamente compatibles con la supervisión judicial de los derechos fundamentales del investigado, y la corrección a los hipotéticos excesos, fraudes o posibles abusos que pudieran darse, entrarla más en la responsabilidad penal o disciplinaria del concreto investigador infractor, que en la forzada nulidad probatoria (que más que corregir futuras actuaciones policiales y abogar por la prevención general, desemboca en impunidades intolerables y en "castigos" a la inocente sociedad que debe soportarlas). Por eso la obtención de datos procedentes de fuentes no accesibles al público por parte de los cuerpos policiales…siempre que no redunden en la vulneración de derechos fundamentales de la persona de única restricción jurisdiccional, está permitida y es legal sin necesidad de mandamiento judicial alguno"*[1002].

Esta opinión, como es de ver, viene referida al tiempo en que aún mantenía su vigencia el art. 12 LSSI, luego derogado por la LCDCE, pero contiene una muy equilibrada visión del problema.

Es de resaltar, en primer lugar, que la evolución y la complejidad de las TIC en nada empecen la función de control jurisdiccional, que puede instaurarse desde un

[1002] Vid. Velasco Núñez, Eloy. *Delitos cometidos a través de Internet…op. cit.*, pág. 138.

primer momento y mantenerse con absoluta eficiencia durante toda la vida de la investigación y aún después con todas las garantías posibles.

En segundo lugar, que la PJE es el auxiliar idóneo, no sólo para resolver satisfactoriamente los retos que la complejidad técnica y fáctica del caso impongan, sino para facilitar, precisamente, la acción de control jurisdiccional.

En tercer lugar, que deben disolverse los prejuicios, no ya sobre la tradicional desconfianza de la doctrina y la jurisprudencia sobre la PJE, sino admitir que la tecnología ha avanzado más que la propia sociedad y que deben abrirse las puertas a nueva concepción de la investigación que admita esos propios medios como única garantía de éxito siempre que medie, al mismo tiempo, una análoga eficiencia en su control policial y jurisdiccional.

En cuarto lugar, que todo lo anterior está orientado al servicio del proceso penal pero que, si esto deviene espurio, como no puede ser menos, la Ley contiene sus propios medios correctores, lo que, sin duda, puede apoyarse en los mismos contrastes tecnológicos que se hayan usado en las intromisiones, leves o graves, en la intimidad de los justiciables. Y, por supuesto, sin suponer una automática causa de nulidad de lo actuado a menos que medie una bien definible conexión de antijuridicidad.

Y sobre todo lo anterior, reparar en dos cuestiones primordiales, que no todo tiene que ser hecho bajo el amparo de una estricta y previa orden judicial, pues hay intromisiones que son leves y propias de la actividad indagatoria clásica de la PJE, y que, en cualquier caso, la figura del Juez de garantías emerge en todo el proceso de investigación – tanto para actuar emitiendo autorizaciones previas para la limitación de determinados derechos fundamentales, como para admitir la idoneidad de las que se adoptaron directamente por la PJE de propia autoridad por ser del todo ajustadas a derecho - pues, no debe olvidarse, que la función investigadora de la PJE se ampara exclusivamente en las facultades otorgadas desde el art. 126 CE y que, consecuentemente, nada se hace de su mano que no sea en beneficio del proceso penal y en apoyo y auxilio de una función jurisdiccional de tan honda raigambre constitucional.

Dicho lo anterior, considero necesario en este momento, abrir un paréntesis en la línea de argumentación que se sostiene, con el propósito de volver sobre algunos casos prácticos que ya se expusieron con finalidad descriptiva y sobre los que se deben extraer ahora algunas enseñanzas.

2. Consecuencias que se extraen del análisis fenomenológico

Las lecciones aprendidas durante la investigación de las operaciones LÍNEA ROJA y MARIPOSA, suponen un revulsivo sobre la mirada clásica que aún se mantiene incomprensiblemente desde la vetusta legislación procesal española sobre los fenómenos criminales actuales y su afectación al derecho al secreto de las comunicaciones o al de protección de datos de carácter personal. Es necesario realizar una reflexión sobre ambas experiencias con el propósito de adquirir una nueva percepción de los derechos concernidos en cada caso y de las medidas de orden jurídico que sería aceptable adoptar en consecuencia.

a) Aspectos fácticos y jurídicos sobre el uso instrumental de la telefonía móvil

Sobre los hechos que motivaron a apertura de la OP. LÍNEA ROJA que, como se recordará, se produjo enteramente dentro del territorio de soberanía nacional, la operadora, como supuesta víctima, denunció el uso de más de mil quinientas tarjetas SIM para la apropiación del saldo extraordinario de llamadas de una promoción comercial sin la pretendida consolidación posterior de una relación contractual comercial basada en el precio básico de cada tarjeta, todo ello mediante la realización de llamadas automáticas continuadas sin contenido material a determinadas líneas de tarificación adicional, contratadas por la propia red delictiva, con la finalidad de derivar el vaciamiento patrimonial de la promoción extraordinaria a favor de los titulares de las mercantiles contratantes de las líneas de pago, causando un grave quebranto a la operadora.

La operadora analizó con total libertad y profundidad sus bases de DACE[1003] para adjuntar a la denuncia penal un completo y complejísimo esquema de las comunicaciones máquina-máquina, además de los que se refirieran a los supuestos autores del hecho. Estas comunicaciones no respondían a un concepto de comunicación personal clásico y protegible desde el art. 18.3 CE y, consecuentemente, tampoco sus DACE. Sin embargo, el rígido sesgo garantista español las mantiene bajo tan alto blindaje constitucional, con la correspondiente reserva de judicialidad.

Debe suponérsele a la operadora, con toda lógica, una elevada capacidad de análisis de sus propias bases de datos, que debe presumirse, a su vez, apoyada en el uso de un *software* especializado para estos fines de elevadas prestaciones técnicas, hasta el punto de poner en relación un número ingente de ellos de suerte que les permitiese alcanzar determinados juicios de inferencia porque, de no ser así, le hubiera sido imposible dirigir con tanta eficiencia sus sospechas contra las personas físicas y jurídicas sobre las que volcó su denuncia penal.

Debe también suponerse que la operadora pudo además hacerse una figuración intelectiva sobre el contenido material de unas comunicaciones que denunció como fraudulentas, además de vincularlas con la identidad de determinadas personas físicas y jurídicas a las que atribuyó la maquinación y su beneficio ilícito.

Esta conclusión es evidente pues, resultado del expurgo, es la fijación de determinados números de abonado a las tarjetas SIM, como llamantes sin contenido material (y que sirven para vaciar el saldo de la promoción en una sola llamada automática), y de determinados abonados a números de de tarificación adicional a nombre de concretas sociedades mercantiles (que reciben como beneficio el gasto de la promoción). Todo este estudio permitió también identificar a los actores físicos y jurídicos de la conspiración y la naturaleza mediata de sus comunicaciones instrumentales, diferenciándolas de las demás comunicaciones telefónicas que tuviesen como fin la concertación criminal u otros usos legítimos alternativos.

[1003] Debe entenderse bajo el amparo del art. 6.5 de la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, *relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas).*

Pero este caso no agota su interés en el uso instrumental de las llamadas, tal y como se ha descrito, sino que permite realizar alguna observación adicional sobre sus propias características.

En efecto, si la maquinación no hubiera concitado el interés de la operadora o, más aún, si la ilicitud del uso le hubiera reportado beneficios económicos sin incurrir por ello en alguna clase de infracción, no habría sido posible para la PJE realizar una investigación/pericia de minería de datos[1004] de análoga calidad y eficacia sobre un caso de parecidas dimensiones como la que realizó con tanta liberalidad la operadora (por ejemplo, para estudiar un ataque de DoS), por impedirlo las insuficiencias de la legislación procesal y la limitada visión doctrinal y jurisprudencial sobre la aplicabilidad del principio de proporcionalidad, en relación con la habilitación de la Policía Judicial para llevar a cabo un estudio de semejantes características, cuestión sobre la que habrá de volverse algo más adelante.

En este último caso, y de resultar ajustado a derecho, la pretensión de la PJE de acceder a los DACE partiría, con toda seguridad, de un conocimiento indiciario de algunos elementos de orden fáctico, de unos breves datos de tráfico mínimos y, probablemente, de la identidad de alguna de las personas físicas o jurídicas sospechosas, que permitirían intuir desde un primer momento una maquinación de dimensiones amplias, merecedora de una investigación criminal.

Salvado el espinoso asunto de la gravedad penológica que, como elemento objetivo, se contempla en la LCDCE para motivar la cesión de DACE, la capacidad de maniobra de la PJE resultaría constreñida por una imposible sucesión de solicitudes de mandatos judiciales concedidos conforme penosamente avanzase la intrincada investigación y se suscitasen nuevas necesidades de información circunscritas a pocos y concretos parámetros estrechamente justificados con los escasos datos sobre los que se basase cada nueva solicitud.

[1004] El concepto que se pretende encerrar en esta expresión, pretende integrar el concepto de minería de datos y el de pericia de inteligencia pues, si el primero sugiere arbitrariedad o carácter indiscriminado en la búsqueda de datos, el segundo puede conciliarlo con el proceso penal si es dirigido o controlado por la Autoridad Judicial bajo un expreso mandato judicial de acuerdo con el principio de proporcionalidad.

Este farragoso procedimiento, de una gran duración en el tiempo y complejidad técnica, con grandes esfuerzos, permitiría obtener alguna prueba de suficiente solidez como para evidenciar la existencia de un hecho punible, pero es del todo impensable que, condicionado por la evidente complejidad tecnológica de la maquinación en relación con el inflexible marco procesal, pudiera alcanzarse un resultado tan esclarecedor de su magnitud criminal como el que la operadora logró por sí misma, quizá, con un sencillo y rápido análisis de sus bases de datos.

La realidad material de los hechos, el ámbito tecnológico en que se producen y la escasa afectación que ocasionan en cuanto a la limitación de determinados derechos, aconsejaría revisar el anterior y último planteamiento, en el sentido de habilitar a la PJE para que hiciese sus análisis con análogo nivel de diligencia al que asistió a la operadora, cuestión que debe ser objeto de revisión y propuestas en este estudio[1005].

b) Aspectos fácticos y jurídicos del uso instrumental de la comunicación vía IP

En lo que hace referencia al caso de la *botnet* MARIPOSA[1006], la exigencia de acceder a los DACE – esta vez a escala planetaria – no necesitó del acompañamiento de una intervención concomitante del contenido material de las comunicaciones electrónicas de los supuestos responsables de la infección viral de más de 11 millones

[1005] NIETO MARTÍN afirma que *"…la ley ha optado por invocar genéricamente el principio de proporcionalidad, lo que quiere decir que deja en manos de los jueces que vayan modulando su control. Creo, en este sentido, que el juicio de ponderación y la intensidad del control debe ser distintos, en aquellos casos que se pidan datos en relación a una investigación en fase preliminar, que en aquellos otros en que se pida una ingente cantidad de información en relación a una persona determinada. Es decir, nada empece a que la práctica judicial cree de facto distintos regímenes de autorización más o menos exigentes, por ejemplo, en lo tocante a la motivación".* Vid. Nieto Martín, Adán. *Análisis de la Ley 25/2007, de 18 octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones,* en *La protección de datos en la cooperación policial y judicial.* Madrid: Aranzadi S.A., 2008, págs. 178-181, pág. 180.

[1006] La descomunal potencia de ataques lógicos a través de la *botnet* llegó a ser de tal magnitud que, en una medición de su actividad durante un periodo de quince minutos, contaba con la suma de las potencias de más de cuatro millones de ordenadores infectados y conectados simultáneamente en red, principalmente en países asiáticos, y dispuestos a canalizar ataques de una dimensión que se hace difícil imaginar.

de ordenadores (es decir, de lo que se refiere a sus acciones de concertación criminal), sino de acreditar, de un lado, las acciones de posesión y diseminación viral del código binario responsable de la *botnet* y, de otro, de la cesión eventual de su dominio a terceros interesados en usarla para el lanzamiento de los ataques.

Consecuentemente, al anterior planteamiento investigativo hay que atribuirle diversas facetas, no todas ellas orientadas a la resolución de un caso criminal en su sentido clásico – y menos aún a practicar en el ámbito soberano de intervención del Derecho -, sino distinguirle una faceta dedicada a las acciones de índole paliativa, tanto orientadas a evitar que se pudiese usar en el futuro la *botnet* para elucubrar y ejecutar nuevos y originales ataques a insospechados bienes, como a favorecer las acciones de la comunidad internacional para limpiar los millones de ordenadores *zombie* del *malware* inadvertida y maliciosamente instalados por quienes manejaban el "panel de control" de la *botnet*.

Es necesario añadir que los ataques DoS conocidos y lanzados a través de la *botnet,* entre los innumerables que sin duda permanecerán inéditos en el futuro por la inabarcabilidad de las posibles acciones criminales que podrían llevarse a cabo, variaron desde la simple infección con *malware* de millones de ordenadores para su puesta a disposición de eventuales empleos criminales ya descrita, esto es, sin daño al dispositivo infectado ni uso mediato para otros fines delictivos, hasta a la realización de ***fraudes o estafas de click***[1007] o, en algunos inquietantes casos consumados, gravosos ataques DoS a servicios telemáticos esenciales de algunas administraciones públicas, de diversas consecuencias materiales, como los que sufrieron algunas *web* del gobierno y universidades de la República de Corea.

Por tanto, la investigación, siguiendo con la identificación de sus facetas de naturaleza instrumental, se dirigió básicamente a cumplir dos objetivos:

[1007] Estas estafas, inimaginables en los años ochenta del siglo pasado, consisten en atacar inadvertidamente las *web*s comerciales que insertan entre sus contenidos propios elementos de publicidad contratados por terceros, cuyo precio depende del número de usuarios que los accedan *clicando* en los ***banners*** o hipervínculos residentes en la *web* principal (que sufrirá el perjuicio económico perseguido). El medio de valorar el precio de la inserción publicitaria no es otro que el de contabilizar el número de clicks o consultas de un *banner* en concreto por parte de quienes visiten la *web* principal, por lo que basta con automatizarlos masiva y maliciosamente a través de ataques DoS lanzados con los ordenadores *zombie* (infectados inconsentidamente por la red criminal) para que se logre el daño patrimonial debido a un aumento artificioso de su valor publicitario.

En primer lugar, desde el punto de vista de la responsabilidad criminal de los autores de la diseminación y control de la *botnet*, se llevaron a cabo acciones con el propósito de acreditar que los sospechosos tenían el dominio de los medios de ataque, esto es, del *malware* que se diseminó y de las acciones que con él se podían realizar, una vez puesto a disposición de los posibles atacantes. Esto exigió la identificación de las direcciones IP de las máquinas que les permitían acceder al panel de control o de administración telemática de la *botnet* y, posteriormente, efectuar un registro domiciliario para asegurar la evidencia digital contenida en los ordenadores de los sospechosos.

En segundo lugar, en relación con las acciones de control y paliativas sobre los posibles usos delictivos en curso y futuros de la *botnet*, fue necesario identificar la práctica totalidad de los ordenadores infectados a escala mundial, de forma que se agrupasen según sus rangos de direcciones públicas IP[1008], así como los proveedores de acceso a los que pertenecían, hasta donde fue posible, y como modo de facilitar la identificación de las potenciales víctimas, de suerte que la comunidad internacional dispusiese de la información concreta que le permitiese abordar la limpieza dentro de cada ámbito de intervención. Esta posibilidad de intervenir, como es de ver, excede por completo al control de los investigadores, por suceder en los espacios soberanos de los países en los que se hubiese diseminado el *malware.*

En este sentido, una de las enseñanzas de la OP. MARIPOSA es que la investigación debió ser estructurada, en un principio, únicamente sobre el régimen de accesos a la red pública de comunicaciones de los ordenadores *zombies* o esclavos que constituían la *botnet*. A su vez, estos ordenadores esclavos se conectaban con el panel de mando y control (C&C[1009]) desde el que los delincuentes ordenaban las acciones maliciosas a realizar o ponían la *botnet* a disposición de terceros[1010], y no por el análisis

[1008] Por ejemplo, el rango adjudicado a Movistar o a la Universidad de Seúl. Como es de ver, la información pública de rangos se interrumpe en la compañía a la que se atribuyen, pero nunca a concretos usuarios finales.

[1009] Del inglés *command and control.*

[1010] El contenido material de los ataques consistió en la transferencia de información y datos sobre los diversos ataques lanzados. Así, los administradores de la Red MARIPOSA lograron la obtención de datos personales o credenciales bancarias para su uso ilegitimo o su comercialización, así como para la adquisición de nuevos dominios y servidores en los que alojar los paneles de control de la red y continuar con la comercialización entre sus colaboradores y otros individuos. Emplearon también ataques distribuidos de denegación de servicios o DDoS para extorsionar económicamente al

de las transacciones telemáticas concretas. Es decir, que el investigador conoció los procesos de transmisión de los paquetes de datos a través de la red pública de comunicaciones, por el acceso a los datos de las diferentes IP públicas, pero nunca el contenido material y formal que se verificó en los ISP que fueron accedidos durante los procesos maliciosos de infección y, particularmente, los que se correspondieran de forma más directa al proceso de formación e instalación del *malware*.

El procedimiento para la investigación y posterior desarticulación se conoce como **"sinkhole[1011]"** o método por el que la PJE sustituye subrepticiamente el servidor que aloja el panel de mando y control por uno propio. Este servidor interpuesto registra las IP públicas de los equipos *bots* conectados para conocer cuáles de ellos se encuentran infectados y cuál es la dimensión de la *botnet*. Con estas acciones, posteriormente pueden avisar a sus usuarios para que realicen la desinfección del equipo.

La segunda finalidad del *sinkhole* consiste en registrar la IP pública de la persona que maneja el panel de mando y control y así identificar al autor o autores del delito, caso de que intenten recuperar el dominio del C&C.

La colaboración internacional se concretó, consecuentemente, en la aportación de los respectivos datos de acceso a la red, lo que permitió configurar el mapa aproximado de diseminación del *malware* objeto del ataque DoS[1012] y, allí donde fue

---

administrador del sitio *web* atacado o, por encargo, para solicitar coactivamente los servicios del administrador de una *botnet* la realización de estos ataques contra páginas *web*.
Otro de los tipos de ataques contra páginas *web* fue el ***defacement*** o desfiguración del contenido *web* ofrecido a la vista de los visitantes de la página.
Hubo también ataques a los derechos de propiedad intelectual de empresas de la competencia y manipulación sistemática del servicio de publicidad que provee la empresa *Google*, denominado *Google Adsense*, mediante el mecanismo denominado fraude por *click* o *click-fraud*, por el que el administrador de una página *web* ve incrementado sus ingresos por publicidad de una forma exponencial gracias a la simulación de visitas y *click* en dicha página *web* por una serie de ordenadores controlados de forma remota y masiva (lo que se entiende por una *botnet*).
Se produjeron ataques de *phishing* mediante la muestra de una réplica de la página *web* del BBVA para captar credenciales bancarias para su posterior uso fraudulento.
También se produjeron estafas, como la creación de una página *web* ofertando un falso antivirus, con el objetivo de poder infectar a más usuarios, y además obtener beneficios económicos por ello.
(Fuente: Informe sobre las actividades de los miembros del grupo DDP y su estructura, de octubre de 2010, del GDT).

[1011] Del inglés "sumidero".

[1012] Debe hacerse constar la determinante colaboración de alguno de los proveedores de servicios, como *MICROSOFT* y *GOOGLE*, que facilitaron a requerimiento judicial los datos de tráfico de las transacciones telemáticas relacionadas con la red MARIPOSA según su régimen de conservación de treinta días

posible, el análisis de las consecuencias de la perturbación ocasionada en determinados procesos telemáticos de las víctimas del delito.

Por ello, si de lo que se tratara es de estudiar los efectos de un uso malicioso concreto de la *botnet* sería necesario estudiar los *logs* de las transacciones telemáticas sospechosas.

Es evidente que la valoración específica de cada ataque individual, con toda su carga de singularidad y efectos criminales, se constituía en una investigación propiamente dicha y, por todo ello, una pieza a sumar en un inmenso puzle en el que habían participado, sólo para el ataque, más de 10 millones de ordenadores de todo el mundo que, a poco daño que pudieran hacer, las cifras del éxito resultante de tales ataques exceden a cualquier capacidad de estimación.

Metodológicamente, la identificación de las IP se hizo por medio de los accesos públicos a la información contenida en las bases de datos de la ICANN[1013], entidad internacional que administra el direccionamiento IP de Internet pero, lógicamente, las acciones de identificación plena y final de las víctimas, al menos en el derecho español, sólo podrían hacerse mediante un mandato judicial por cada uno de los actos de comunicación que devinieran sospechosos.

Lo incongruente y absurdo de esta situación es evidente, pues el investigador, que conoce los rangos de IP por tratarse de información pública y accesible vía *web*, por mor de la LCDCE quedará inhabilitado para dar los pasos siguientes e identificar las miles o millones de los ordenadores conocidos pertenecientes a un mismo rango – que no de las personas - a través de las IP conservadas del tráfico de unas comunicaciones telemáticas, sin contenido material más allá de la difusión del código binario malicioso

---

anteriores a la fecha de efectividad de su ejecución material y que, como se ha dicho, se constituye por la libre decisión interna de las empresas mencionadas.

[1013] ICANN es el acrónimo del inglés de la organización mundial *Internet Corporation for Assigned Names and Numbers* y puede consultarse en http://www.icann.org/. Introduciendo una IP pública en su página de consultas informa sobre la entidad a cuyo rango de IP asignadas pertenece. En el ámbito europeo, se puede consultar IP en http://www.ripe.net/data-tools. Si no existiese esta posibilidad de acceso telemático abierto a la información pública, la ICANN o RIPE serían candidatas a la recepción de los miles de mandatos judiciales o solicitudes de similar propósito que fueran cursadas diariamente por las autoridades de todo el mundo encargadas de la persecución de ilícitos en la red. Es de hacer notar, por tanto, lo absurdo de esta situación. Una vez asignado un rango de IP a un operador de telecomunicaciones, como Movistar o Vodafone, este distribuye sus IP entre los usuarios para que puedan acceder a Internet a través de sus *routers*, quedando estos datos incluidos en el art. 3.1 LCDCE y bajo la protección que les otorga esta Ley en su conjunto.

y, con seguridad, en la mayoría de las ocasiones, de ordenadores de uso no personal[1014].

Explicado de otra forma: existen IP que identifican a personas jurídicas o proveedores de servicios de la sociedad de la información, cuyos datos son accesibles públicamente pero, con las mismas razones, no se puede acceder a idénticos medios de identificación vía IP de las máquinas concretas que sufren la infección viral inadvertidamente. Esta situación compromete de forma insalvable la posibilidad de intervenir para resolver la incidencia. Además, para obtenerse lo datos, en primera instancia, el juzgado debería dirigir un primer mandato, revestido una de una gran dificultad y extensión en lo que se refiere al cumplimiento del requisito de motivación, de modo que se facilitasen los miles de IP sobre las que tuviere eventual interés el proceso penal. Algo inviable, como es de ver, salvo que el Estado no quiera renunciar a esta fuente de prueba y se dote de lo necesario para accederla[1015].

La condición de receptor desdibuja y desborda, en este caso, el concepto jurídico clásico contenido en el art. 579 LCRIM sobre las comunicaciones protegidas por el art. 18.3 CE, pues el emisor diluye sus comunicaciones en un número inabarcable de receptores-máquinas que, inadvertidamente y sin ser sus interlocutores humanos ni desear convertirlos en los específicos destinatarios de mensaje inteligible alguno, habrán sido escogidos aleatoriamente, mediante un *software,* de entre los ordenadores conectados a Internet a escala mundial por el mero hecho de no disponer de un sistema de alerta antiviral o un *firewall* que advierta y impida el ataque.

Lo anterior muestra un panorama inédito con el que intentar enfocar la investigación criminal, ya que su visión clásica lo excede en su propia raíz y en su propia naturaleza jurídica, toda vez que la realidad hace desbordar el concepto de comunicación en su sentido más clásico, haciendo imposible una aplicación analógica eficiente del cuerpo doctrinal constituido para la intervención de las comunicaciones

[1014] Por ejemplo, ordenadores que se usan sólo como máquinas, como los servidores de una empresa, un sistema de alarmas, un ordenador que controla un proceso industrial (como una insertadora de etiquetas o un brazo robotizado) o el gestor de las cajas de un comercio, o de acceso general, como un café Internet, un ordenador de consultas de una biblioteca, una red *wifi* de un ayuntamiento, etc.

[1015] Mirando la experiencia de modo retrospectivo, y a título meramente ilustrativo, hasta la entrada en vigor de la LCDCE se cedían a la PJE las IP a la presentación de un simple oficio dirigido al prestador de los servicios, según el modo de cesión amparado en los informes jurídicos de la AEPD. Pero, al quedar derogado el art. 12 LSSI con esta Ley, esta información queda fuera del alcance de la PJE.

de línea fija, haciendo imposible la tutela judicial efectiva de los demás bienes jurídicos puestos en peligro de no disponerse, con la urgencia que requiera cada caso, de los medios adecuados para tratar las comunicaciones electrónicas de línea móvil o las conducidas por vía telemática.

c)Diferencia entre concertación personal y uso instrumental de las comunicaciones electrónicas

Como elemento común de partida los caso analizados, en lo que se refiere al planteamiento de las intervención de las comunicaciones electrónicas, es que se evidencian dos ámbitos sustancialmente distintos dentro de la comunicación, impensables para el legislador de los años ochenta y de necesario tratamiento jurídico más de treinta años después de la entrada en vigor del art. 579 LCRIM:

De un lado, el que se podía denominar como un ***ámbito de concertación personal*** a través de las comunicaciones electrónicas de cara al seguimiento del *iter criminis* por parte de los delincuentes y, de otro, un ***ámbito técnico instrumental de las comunicaciones***, que es el que les sirve para alcanzar los objetivos ilícitos de la maquinación criminal.

Este segundo ámbito es inexistente en las formas de comunicación clásica[1016], lo que exige, lógicamente, una reflexión sobre su más exacta naturaleza y afectación a los derechos fundamentales.

La cuestión fundamental que emerge es, obviamente, la diferenciación temprana y jurídicamente segura entre ambos ámbitos de forma que, vista la trascendencia del concepto jurídico de comunicación que se ha propuesto en este estudio, el Estado de Derecho dote a la PJE con unas u otras capacidades pre-

[1016] Ni en el periodo constituyente, ni en el que precedió a la redacción del art. 579 LCRIM podían escucharse frases conspiratorias como las siguientes: *"Efectuaré doce millones de llamadas y destruiré el sistema de salud coreano o lo que me plazca"* o *"con un llamada activaré el explosivo que he colocado en el tren"* o *"con unas llamadas me apoderaré de los secretos del gobierno y los difundiré a escala planetaria con otras cuantas más"*.

procesales y procesales de intervención en razón de la gravedad intrínseca de las injerencias.

Sobre el ámbito de concertación personal a través de las comunicaciones electrónicas debe recaer, sin la más mínima duda, todo el peso del blindaje constitucional del art. 18.3, por lo que deben sopesarse con espíritu restrictivo las condiciones de proporcionalidad de cualquier medida de intervención de las comunicaciones, que sería adoptada, en exclusividad y con carácter previo, por el actor jurisdiccional y ejecutada por la PJE con la imprescindible participación de la operadora de turno.

Pero si se acredita la inequívoca existencia de un ámbito instrumental autónomo y perfectamente diferenciado de las comunicaciones, en mi opinión, el acogimiento jurídico de las medidas limitativas a instaurar quedaría por completo fuera de la intervención del art. 18.3 CE y, sus datos, regulados desde el régimen general de protección de datos.

Para profundizar en esta idea, un primer cometido de propósito ejemplificador ha de consistir en hacer una introspección en la casuística planteada, tratando de identificar y diferenciar un ámbito de otro, si ello es posible.

En el caso de la OP. LÍNEA ROJA, podría identificarse el ámbito personal de las comunicaciones en las que mantuvieren entre sí los actores criminales del caso, pudiendo ser posible una medida de intervención legal amparada en el art. 18.3 CE en aquellas situaciones en las que se superase el juicio de proporcionalidad. En consecuencia, y siendo esto así, el Juez de Garantías emitiría un auto motivado de intervención de las comunicaciones personales que sería cursado por la PJE a las operadoras y ejecutado a través del SITEL.

Bien sentado lo anterior, y suponiendo que las tarjetas SIM de la promoción comercial carecen de contenido material en la forma en que se ha definido, cuyo uso se preordena a la comisión de un fraude y que, naturalmente, no tienen el más mínimo interés para la investigación penal que el que se sigue de la mera constatación formal de este hecho, el ámbito instrumental de las comunicaciones diferenciado merece un tratamiento jurídico absolutamente distinto de las primeras. Por ello, su acceso por la

PJE sólo puede considerarse, como máximo, como un injerencia leve que deberá permitir un acceso ponderado a la única información que interesa al proceso penal: a los DACE.

En el caso de la OP. MARIPOSA, toda la maquinación que se ha descrito formaría parte del ámbito instrumental por haberse usado las comunicaciones telemáticas como medio de causar un daños a terceros, pero sin recurrir a su uso personal en las labores de concertación o para los demás usos íntimos ajenos a la maquinación criminal. Puede decirse que las comunicaciones de la OP. MARIPOSA fueron, por tanto, meramente técnicas e instrumentales.

En consecuencia, del concepto de acto de comunicación que se propuso[1017] faltarían algunos requisitos para considerar como tal al ámbito instrumental de las comunicaciones electrónicas:

- No existiría un número finito de personas entre las que se produce la comunicación, al menos en el sentido del el art. 2.d) de la Directiva 2002/58/CE, donde se dice que es comunicación "*cualquier información intercambiada o conducida entre un número finito de interesados por medio de un servicio de comunicaciones electrónicas disponible para el público…".* No existe un número "finito" reconocible de receptores y difícilmente se les podría considerar como "interesados".
- No se trata de "*comunicaciones cerradas, esto es, dirigidas a una o varias personas determinadas de forma que el emisor del mensaje pueda controlar el sujeto o sujetos que lo recibirán" [1018].* Si hay algo que no existió es un control de un círculo íntimo con el que interactuar por medio de las comunicaciones electrónicas.
- No todos los emisores son personas.
- No todos los receptores son personas.
- Hay comunicaciones en que los receptores y los emisores son máquinas.

[1017] *Ibídem.* La definición propuesta fue: *"Aquel por el cual se produce una transmisión de voz o datos de cualquier clase en canal cerrado entre un número finito de personas e iniciado por cualquiera de ellas, por el que se dan a conocer sus pensamientos, ideas, sentimientos, etc., con independencia de su carácter íntimo o reservado y llevado a cabo mediante el uso de un dispositivo tecnológico apto para mantenerlo".*

[1018] *Ibídem.* Vid. Vegas Torres, Jaime. *Obtención de pruebas…op. cit.,* pág. 43.

- En algunos casos, las máquinas de los emisores eligen comunicar automática y aleatoriamente con las máquinas de los receptores que no contengan una protección antivirus, esto es, sin intervención humana directa.
- No existe un *"componente volitivo-teleológico de la comunicación"* ni "e*l proceso de comunicación obedece al propósito por parte del emisor de transmitir una determinada información al receptor "*[1019].
- No existe en la voluntad de la PJE, en el planeamiento de la investigación, de injerirse en *"el derecho de los titulares a mantener el carácter reservado de una información privada o, lo que es lo mismo, a que ningún tercero pueda intervenir en el proceso de comunicación y conocer de la idea, pensamiento o noticia transmitida por el medio"*[1020]. No existen, sencillamente, tales cosas en las modalidades comunicativas estudiadas.
- No existió contenido íntimo alguno, como el que describe la STS 534/2011 de 10 de junio, donde se afirma que la intimidad "*es un concepto psicológico [ético-psíquico, según otro pasaje de la STS] que remite a ese "mundo propio" en el que cada quien desarrolla su "vida interior". Por tanto, un reducto que está más allá de la privacidad y que conecta con los estratos más profundos de la personalidad"*[1021]. No existe un componente psicológico o ético-psíquico reconocible ni estratos profundos de la personalidad en ninguna de las comunicaciones maliciosas descritas.

Más bien se trató, por el contrario, de un uso instrumental preordenado al vaciamiento patrimonial de un promoción comercial de telefonía móvil o a la infección viral de millones de ordenadores arbitrariamente elegidos según su falta de resistencia frente a ataques telemáticos maliciosos, salvo que sus autores fueran capaces de proyectar la riqueza de su intimidad con tal fuerza expresiva que necesitasen, nada menos, que de casi 2000 tarjetas SIM para manifestar su personalidad, en un caso, o más de 11 millones de ordenadores y de las incontables comunicaciones IP que compusieron el total de su maquinación telemática, en el otro.

[1019] *Ibídem.* Vid. González López, Juan José. *Los datos de tráfico…op.cit.,* pág. 65 y ss.
[1020] *Ibídem.* Vid. Gimeno Sendra, Vicente. *La intervención de las comunicaciones,* en Marchal Escalona, Nicolás (Director). *Manual de lucha…op. cit.,* pág. 570.
[1021] *Ibídem.*

Fueron, en mi opinión, - y esto sí parece más real -, pura y simplemente, unas comunicaciones de máquina a máquina sin el más mínimo contenido íntimo, sin la menor relación con *"el estrato más profundo de la personalidad"* de sus autores y, desde luego, dispuestas para causar toda clase de daños por vía telemática o telefónica indiscriminada y masiva, cosa que no se podría hacer con los teléfonos fijos primitivos, pensados exclusivamente para el uso humano verbal.

Por ello, de la reflexión sobre la naturaleza instrumental de algunas comunicaciones sólo restaría comentar un elemento que contraría la apertura del Derecho a un nuevo enfoque sobre su tratamiento jurídico: es necesario resolver el criterio jurídico dominante por el cual lo que se protege formalmente es el canal de comunicaciones, más que el derecho a la intimidad, visión sobre la que la realidad dicta su obsolescencia.

Entre las lecturas adicionales que deben hacerse sobre las tipologías mostradas como ejemplo, se ha de anotar, una vez más, que la mayor parte de estos usos no tendrían la suficiente trascendencia penal según el concepto de gravedad asociado a la retribución penológica por los concretos tipos delictivos intentados o consumados, todo ello a efectos de dispuesto en la LCDCE.

Consecuentemente, un mínimo criterio de razonabilidad exige que el tratamiento jurídico-procesal de las fases de investigación de la PJE, y desde luego, la prosperidad del conjunto del proceso penal, no debieran depender de esta circunstancia formal, permitiéndose una habilitación jurídica más generosa y sin perjuicio del debido control jurisdiccional de las medidas de todo tipo que se arbitren.

Por ello, en lo que se refiere al ejercicio del control jurisdiccional, nada empece que se instaure de un modo permanente sobre el conjunto la investigación pero que, sobre las fases de cesión de DACE sobre comunicaciones instrumentales, y a diferencia de las que se refieran al ámbito personal, pueda verificarse únicamente bajo los auspicios de los arts. 549.1.a) LOPJ, 11.2.d) LOPD, 22.2 LOPD y 1, 2 y 4 RDPJ.

Todo lo anterior, hace evidente que lo que se ventila como cuestión de fondo es, en realidad, un nuevo concepto de comunicación, pues las experiencias adquiridas y algunos razonamientos doctrinales así lo sugieren.

En efecto, volviendo a algunos pronunciamientos jurisprudenciales ya analizados, puede hallarse algún criterio que reconoce, o al menos pone de manifiesto su duda, que no todo lo que tiene que ver con un dispositivo de comunicación tiene que estar automáticamente protegido por el secreto, pues:

> "*Basta al efecto recordar que tal aparato [un teléfono móvil] no solamente está habilitado para permitir el acto de la comunicación sino que suele proporcionar otras funciones ajenas al hecho de aquella comunicación.*
>
> *Pues bien cuando del mismo se obtiene la información allí contenida, de suerte que lo sabido no es el contenido de una conversación o de un mensaje SMS, ni siquiera información del hecho de que tal comunicación tuvo lugar y, menos aún, entre quienes, no existe ni asomo de infracción del derecho garantizado en el artículo 18 de la Constitución"*[1022].

Pues bien, en la casuística estudiada se refiere a *"funciones ajenas al hecho de aquella comunicación"*, con la que el ponente sin duda se refiere al uso instrumental del aparato de comunicación, ni que suponga el acceso a un contenido material de los que se acogen a la protección, no ya del art. 18.3 CE, sino al art. 18 CE en su conjunto, esto es, a cualquier asomo de lo que tenga que ver con el derecho fundamental a la intimidad.

En este mismo sentido, como informa VELASCO, *"la SAP de la Sala 7ª de 11 de julio de 2007, […] concluye que intercambiar pornografía no es "comunicación" y utilizar un programa para rastrear en Internet tales intercambios por parte de la policía no vulnera el derecho al secreto de las comunicaciones del art. 18.3 CE, pues con la pornografía infantil no se transmiten mensajes en sentido de los protegidos constitucionalmente por el secreto: expresiones de sentido a través de cualquier conjunto de sonidos, señales o signos, hecha de forma directa entre dos particulares"*[1023,1024]. Es decir que, según esta opinión, la comunicación protegible

[1022] *Ibídem.* (*STS 1474/2011, de 18 de marzo*). Véanse también, entre otras, las SSTS 1273/2009, de 17 de diciembre; 1040/2005 de 20 de septiembre; y 316/2000, de 9 de marzo.
[1023] Vid. Velasco Núñez, Eloy. *Delitos cometidos a través de Internet…op.cit.,* pág. 221.
[1024] En este mismo sentido, en la STS, Sala Tercera, de lo Contencioso-administrativo, Sección 7ª, de 27 de diciembre de 2010 (rec. 1783/2009), se dice que "*en efecto, la STC 281/2006 (LA LEY 110153/2006) , no ha podido evitar de esa vinculación al definirlo. Así, dice: "Pues bien, si el derecho al secreto de las comunicaciones (art. 18.3 CE) constituye una plasmación singular de la dignidad de la persona y el libre*

constitucionalmente es materia de intercambio de mensajes inteligibles entre personas y nunca la que se deriva de un abuso instrumental de sus posibilidades técnicas. Abunda el autor, además, en la idea del rastreo llevado a cabo por la PJE, término que sugiere la necesidad de disponer de unas amplias facultades técnicas de obtención de IDACE en aquellos casos en que ello no tenga asociada una limitación de los derechos fundamentales[1025].

Otro enfoque jurisdiccional interesante es el que se trasluce del contenido de la STS, Sala Tercera, de lo Contencioso-administrativo, Sección 7ª, de 27 de diciembre de 2010 (rec. 1783/2009), en el que el magistrado ponente se pronuncia de un modo sugestivo de la línea de argumentación que se sostiene en este estudio. A continuación, se exponen algunos de sus aspectos más interesantes:

El asunto objeto de casación versó de la posible vulneración del secreto de las comunicaciones por la Comisión del Mercado de las Telecomunicaciones, cuyos inspectores habían accedido a determinadas llamadas en el ejercicio de las facultades reconocidas por el art. 50 LGT, recurso que no prosperó por considerar el tribunal que no existía en tal actividad *"infracción del Derecho al secreto de las comunicaciones, puesto que no [cabía] hablar de comunicaciones privadas sino de controles técnicos"*. Sólo con esta frase, el tribunal ya parece poner el acento en las facetas técnicas accesorias a la innecesaria injerencia en el medio de comunicación inspeccionado que, por otro lado, define como propias de los "controles técnicos" que deben realizar los funcionarios como parte de sus cometidos, es decir, ajena a cualquier pretensión de

desarrollo de la personalidad que son "fundamento del orden político y de la paz social" (art. 10.1 CE EDL 1978/3879), las comunicaciones comprendidas en este derecho han de ser aquellas indisolublemente unidas por naturaleza a la persona, a la propia condición humana; por tanto, la comunicación es a efectos constitucionales el proceso de transmisión de expresiones de sentido a través de cualquier conjunto de sonidos, señales o signos. Aunque en la jurisprudencia constitucional no encontramos pronunciamientos directos sobre el ámbito objetivo del concepto constitucional de "comunicación", sí existe alguna referencia indirecta al mismo derivada del uso indistinto de las expresiones "comunicación" y "mensaje", o del uso de términos como "carta" o "correspondencia" cuando de la ejemplificación del secreto de las comunicaciones postales se trataba (STC 114/1984 (LA LEY 9401-JF/0000), de 29 de noviembre, FJ 7)".

[1025] *Ibídem.* Véase lo aportado sobre el rastreador *HÍSPALIS*. Aunque, ciertamente, el rastreo se refiere a los DACE que circulan en abierto por Internet, no es menos cierto que el uso instrumental de las comunicaciones sugiere un ámbito análogo en cuanto a la generación de DACE y, desde luego, a diferencia de los contenidos de pornografía infantil, con otros de menor o nulo significado como contenido material en sí mismo, cuales son la circulación de *malware*, las llamadas de vaciamiento de saldo, la activación de explosivos o la geolocalización de víctimas.

conocimiento del contenido material de las comunicaciones y centrada en aspectos meramente técnicos de su conducción[1026].

En la sentencia, centrada en las facultades de la CMT en materia de derecho administrativo punitivo *ex* art. 50.6 LGT[1027], se recuerda que *"la sentencia del Tribunal Constitucional de 29 de noviembre de 1984 puso de relieve que, desde el punto de vista material, el derecho a la intimidad lo único que puede proteger es la vida privada o particular de las personas y que no forman parte de ella los demás aspectos de una conversación entre dos personas"* y que, por tanto, una inspección de las facetas técnicas quedaban a extramuros de la protección del art. 18.3 CE.

Independientemente de cualquier otra consideración, la actividad inspectora de la CMT se asemejaría a la que, en un momento dado, reclamaría para sí la PJE si estuviera facultada para examinar técnicamente los DACE que circulan por las redes de comunicaciones o que se conservan por las operadoras o ISP, sin que con ello se pretendiese una injerencia prohibida en los contenidos materiales que tienen o tuvieron asociados o, siendo el caso, contase con el correspondiente mandato judicial habilitante.

En parecidos términos se pronuncia, en esencia, la Abogacía General del Estado[1028] con respecto a las facultades de intervención de la AEPD para la resolución, en vía administrativa, de las denuncias presentadas por los ciudadanos por supuestos abusos en el tratamiento de sus datos personales en determinadas transacciones telemáticas como, por ejemplo, las que consisten en el envío y recepción indeseados de *spam.*

[1026] Los aspectos técnicos consistían en *"(...) supervisar el cumplimiento por parte de Telefónica (...) de sus obligaciones en materias de acceso desagregado al bucle de abonado y, en particular, verificar la existencia de posibles irregularidades en cuanto al suministro de los servicios de acceso desagregado recogidos en la Oferta de acceso al Bucle de Abonado (OBA) que permiten proveer el servicio final al cliente".* Es evidente que ninguna de estas funciones consistía en injerirse en el contenido material de las comunicaciones.

[1027] Siendo particularmente interesantes las que establecen, según esta norma, que *"los operadores o quienes realicen las actividades a las que se refiere la Ley vendrán obligados a facilitar al personal de la inspección en el ejercicio de sus funciones el acceso a las instalaciones. También deberán permitir que dicho personal lleve a cabo el control de los elementos afectos a los servicios o actividades que realicen, de las redes que instalen o exploten y de cuantos documentos estén obligados a poseer o conservar"*.

[1028] Véase el documento de referencia A. G. ENTES PÚBLICOS 182/08, de 29 de diciembre.

En consideración de la abogacía, el hecho de la denuncia llevaría implícito en estos casos el consentimiento del afectado por lo que, con fundamento jurídico exclusivo en la LOPD y no en la LCDCE, sería posible el ejercicio de las facultades inspectoras abiertas, incluyendo la exigencia administrativa de cesión de datos de tráfico de IP frente a los proveedores de servicios, todo ello sin sujeción a lo dispuesto en la LCDCE, es decir, fuera del ámbito procesal penal seguido por delito grave, sin necesidad de previa autorización judicial y, naturalmente, sin la dación de cuenta al Juez de lo practicado.

Yendo más allá en sus razonamientos, la Abogacía del Estado, con remisión al art. 35 LGT[1029], en el que ve un supuesto para el que *"…no se considera necesaria tal intervención judicial para la interceptación de los contenidos de las comunicaciones, no sólo de los datos de tráfico…."*, afirma que *"…la concurrencia de consentimiento del titular [para acceder a sus datos de tráfico] puede no estar siempre presente. En efecto, puede suceder que el titular del derecho no haya prestado su consentimiento y, sin embargo, la AEPD, en el ejercicio de sus funciones, considere necesario conocer los datos a los que se refiere la consulta, protegidos por el secreto de las comunicaciones…pueden existir dos casos…a) El supuesto en que la AEPD inicie una investigación tendente a realizar una comprobación sistemática, o personalizada, del correcto funcionamiento de los dispositivos que un operador de comunicaciones o un prestador de servicios tiene realmente establecidos para la salvaguardia de los derechos exigidos en las leyes, es decir, el sistema de acceso a los datos personales, de corrección de los datos, cancelación y disociación de los mismos…[en relación al caso*

[1029] Art. 35 LGT "*Interceptación de las comunicaciones electrónicas por los servicios técnicos.*
1. Con pleno respeto al derecho al secreto de las comunicaciones y a la exigencia, conforme a lo establecido en la Ley de Enjuiciamiento Criminal, de autorización judicial para la interceptación de contenidos, cuando para la realización de las tareas de control para la eficaz utilización del dominio público radioeléctrico sea necesaria la utilización de equipos, infraestructuras e instalaciones técnicas de interceptación de señales no dirigidas al público en general, será de aplicación lo siguiente:

- *a. La Administración de las telecomunicaciones deberá diseñar y establecer sus sistemas técnicos de interceptación de señales en forma tal que se reduzca al mínimo el riesgo de afectar a los contenidos de las comunicaciones.*
- *b. Cuando, como consecuencia de las interceptaciones técnicas efectuadas, quede constancia de los contenidos, los soportes en los que éstos aparezcan no podrán ser ni almacenados ni divulgados y serán inmediatamente destruidos.*

2. Las mismas reglas se aplicarán para la vigilancia del adecuado empleo de las redes y la correcta prestación de los servicios de comunicaciones electrónicas.
3. Lo establecido en este artículo se entiende sin perjuicio de las facultades que a la Administración atribuye el artículo 43.2".

a)]…la actuación de la agencia difícilmente afectará al secreto de las comunicaciones y no parece necesario solicitar para ello autorización judicial"[1030].

Estas pretendidas facultades – hay que insistir, fuera actualmente de regulación en lo que se refiere a la PJE por imperativo de la LCDCE –, y sensiblemente diferenciadas según se refiriesen a los DACE de una intervención en curso de las comunicaciones o sobre los conservados *ex* LCDCE (bien en el ámbito personal, bien en el ámbito instrumental), evocan la acuciante necesidad de acceder a la inteligencia que puede obtenerse del acceso y análisis de estas fuentes de datos y no sólo a una escueta información ajena a la extrema complejidad del uso criminal actual de las TIC, cual es lo común en la solicitud y cumplimentación de mandatos judiciales a día de hoy, lo que a su vez sería de la máxima utilidad para el proceso penal.

3. Estructura y parametrización de las consultas sobre DACE

a) Consultas simples y consultas parametrizadas

La información sobre los DACE que se solicita en oficio motivado de la PJE a los jueces de instrucción, por imperativos de la respuesta práctica procesal, suele referirse a la contestación a preguntas muy simples, cuyos parámetros, a su vez, son igualmente de un gran sencillez. Las aportaciones de las operadoras son también necesariamente simples, consistentes normalmente en la entrega de unos listados, más o menos largos, con los datos que cumplen con lo requerido en la orden judicial[1031]. No caben,

[1030] Esta visión jurídica, hasta donde se conoce, parece haber causado todos sus efectos, como es de ver en la Resolución R/01716/ de la AEPD, de 27 de julio de 2011, dentro del Procedimiento nº PS/00137 de 2011, en cuyo antecedente cuarto se hace constar que el proveedor de servicios de Internet ha comunicado a la AEPD la resolución de la IP relativa al caso denunciado, con identificación plena del cliente, domicilio y línea telefónica usada.

[1031] Una pregunta típica, objeto de un mandato judicial dirigido a una operadora, podría consistir en que se "facilite a los agentes facultados un listado con las llamadas efectuadas desde el terminal X, entre la hora A del día B hasta la hora C del día D". Evidentemente, la contestación contendrá una lista de abonados llamados, pero sin su identidad asociada, lo que exigiría un nuevo ejercicio de sagacidad policial para que se ponderase la eventualidad de conceder un nuevo mandato para averiguar la identidad de los que justificadamente interesasen. Y así, sucesivamente, con grandes limitaciones prácticas.

pues, las preguntas de una mínima complejidad sino, en todo caso, una sucesión de preguntas o hitos informativos simples debidamente verificados paso a paso por la Autoridad Judicial, todos y cada uno de ellos con su específica expresión de la proporcionalidad de la medida instaurada, que es ordenada en resolución motivada.

Este sistema no permite un expurgo de los que no interesen a la investigación ni permite identificar y analizar los que sí lo hacen, cosa que, por otra parte, alarma a los más garantistas en la idea de que la PJE haya podido eliminar arbitrariamente los que no favorezcan la confirmación de sus sospechas. Aunque ya se ha hablado hasta la saciedad de esto, es necesario recordar que existen el elementos de contraste tecnológico y salvaguardias que permitirían comprobar estos extremos además, naturalmente, de la buena fe de la PJE[1032].

Pues bien, según ha de proponerse en este estudio, dadas las características del extraordinariamente complejo uso criminal de las TIC, se hace necesario ampliar, de forma jurídicamente segura, las facultades de la PJE de modo que se pueda proponer al Juez de Instrucción, cuando la Ley así lo establezca, la posibilidad de introducir ***consultas parametrizadas*** sobre los DACE conservados por las operadoras *ex* LCDCE, todo ello orientado a satisfacer, en realidad, los acuciantes intereses de inteligencia del proceso penal, cuya proporcionalidad debe quedar plenamente garantizada, lo que debe suceder además bajo un extremo cuidado en la observación del requisito extrínseco de motivación[1033,1034].

[1032] En términos de intervención del contenido material de las intervenciones del tráfico IP de las líneas con acceso a Internet, se plantea la necesidad de filtrar los que tienen un gran volumen de datos y que circulan entre el usuario y la red (muchas veces medidos en *gigabytes,* como es el caso de la demanda de acceso a servicios de TV a la carta, visionado de canales de televisión *on-line*, determinadas descargas P2P, etc.) que, *a priori*, carecen por completo de interés para el proceso penal. La posibilidad de que el agente facultado pueda introducir parámetros de filtrado de tales contenidos, con o sin la participación técnica de la operadora o el ISP, supone una limitación material que debe ser objeto de señalamiento expreso en el mandato judicial y sujeta a las debidas medidas de control jurisdiccional y a las demás salvaguardas que sean precisas, todo ello para evitar tachas de nulidad en el entendimiento de que, con semejante filtrado, no se introducen modificaciones significativas que puedan comprometer la pureza del proceso de contradicción y valoración futura de la prueba.

[1033] Una forma de introducir parámetros, siguiendo con el ejemplo anterior, respondería a una pregunta como la siguiente: "Facilite a los agentes facultados un listado con las llamadas efectuadas desde el terminal X, entre la hora A del día B hasta la hora C del día D, cuyo rango de BTS que hayan prestado servicio a los abonados llamados se halle en la provincia de Cuenca o sus limítrofes, así como la localización de tales BTS y de la identidad de los abonados llamados bajo los anteriores condicionantes". Esta pregunta, imposible de ver en la realidad actual, limita el interés del proceso penal a lo estrictamente necesario, sin injerirse, por tanto, en aquellos aspectos de la intimidad de los investigados

b) Auxilio jurisdiccional de las operadoras e ISP

La consulta parametrizada, que en ningún momento ha de ser prospectiva, aleatoria, genérica o abierta[1035,1036], precedida de la valoración de su proporcionalidad por la Autoridad Judicial, puede ejecutarse bajo la dirección de la PJE, con apoyo de las salvaguardas jurídicas y tecnológicas que se han planteado y con el eventual nombramiento de un ***auxilio jurisdiccional*** a las operadoras e ISP, cuyos técnicos podrían intervenir en el proceso penal como peritos[1037,1038].

---

ajenos al *iter criminis.* Además, una mínima eficiencia en el sistema de análisis de las bases de datos de la operadora permitiría la contestación del requerimiento en un breve periodo de tiempo.

[1034] De otra forma sería imposible, por ejemplo, en un ataque de DoS, instaurar medidas preventivas, dar limpieza de ordenadores infectados o en riesgo de serlo, determinar estructuras de ataque, resolver y anular casos de éxito criminal, recuperar, limpiar y restaurar datos sustraídos (por ejemplo, una base de datos de la seguridad social), minimizar fugas de información sensible (sobre activos inmateriales de PII, secretos empresariales, fondos de comercio, secretos de Estado, etc.), restauración de la confianza pública en las administraciones públicas o privadas, en la banca y el comercio electrónico, etc.

[1035] Como recuerda GIMENO, con apoyo en la jurisprudencia, *"no caben tampoco las escuchas predelictuales o de prospección, desligadas de la realización de un hecho delictivo..., no cabe obviamente decretar una intervención telefónica para tratar de descubrir, en general, sin la adecuada precisión, actos delictivos" (ATS 18.Junio.1992). Véase también, y sobre todo, la STS 14.Junio.1993; de conformidad con la doctrina de esta última resolución, la adopción de la medida requiere la existencia, contra una persona determinada de "indicios fundamentados y contrastados...", "no basta con la simple manifestación policial de la existencia de una actividad delictiva inconcreta y difusa cuyo protagonismo no aparece definido, sino por sospechas y conjeturas sin base real alguna...", "No cabe decretar la intervención telefónica para tratarse descubrir actos delictivos que sólo se perfilan en las vagas sospechas de los investigadores policiales". Dicha doctrina es reiterada en las SSTS de 25.Marzo.1994 y 26.Octubre.1995 (Ponente Martín Pallín). Por el contrario, las SSTS, de 28.Junio.1993, 14.junio.1995, 7.Abril.1995 estiman suficientes las "Diligencias Indeterminadas" como cauce procesal para adoptar estas intervenciones".* Vid. Gimento Sendra, Vicente. *La intervención de las comunicaciones* en *Manual de lucha…op. cit.,* pág. 586.

[1036] *Ibídem.* Las propuestas de este estudio, naturalmente, no están orientadas a las peticiones abiertas o genéricas, ya que, como dice MORENO, *"la autorización debe ser precisa y determinar los datos a los que se refiera, así como el tiempo para el que se solicita, con el máximo legal de los doce meses que se obliga a conservar. Eso significa que la autoridad judicial no puede expedir autorizaciones genéricas, que dejen al criterio del agente que la cumplimenta o del operador que debe ceder los datos cuáles son los que pide o que entrega…[la autorización] será radicalmente nula…".* Vid. Moreno Catena, Víctor. *Ley de conservación...op. cit*.

[1037] A ello invita la conclusión contenida en el pto. 8.5 del documento de evaluación de la DCD, donde se considera necesaria *"la elaboración de orientaciones sobre utilización de los datos, incluida la prevención de la búsqueda aleatoria de datos («data mining»)".* Es decir que, en mi opinión, la forma de prevenir la "búsqueda aleatoria de datos" no es otra que la de diseñar una que no lo sea y que, de acuerdo con criterios jurídicamente seguros y de estricta proporcionalidad permita el hallazgo inteligente de evidencias orientadas a satisfacer las necesidades del proceso penal. Vid. *Informe de evaluación sobre la Directiva de conservación...doc. cit.,* pág. 37.

La actividad de integración de estos esfuerzos y salvaguardas en la investigación criminal, bajo la dirección del Juez de Instrucción, podría considerarse inclusa en el concepto de la prueba de inteligencia policial, tal y como se propuso en apartados anteriores, con vocación, por tanto, de ser admitida a contradicción y valoración en el acto de juicio oral.

En este sentido, la actividad empresarial de las operadoras es objeto de un especial interés público que debe entenderse, en buena medida, relacionado con los posibles requerimientos para que presenten un auxilio jurisdiccional amparado en el art. 17.1 LOPJ, siempre en el exclusivo ámbito de sus funciones técnicas[1039].

Esta figura procesal no es nueva en el devenir de las investigaciones criminales revestidas de cierta complejidad en la que la mera acción de la PJE es por completo insuficiente para atender las necesidades informativas y probatorias que exige la naturaleza de los hechos.

Un ejemplo cada vez más repetido, fuera del ámbito de las comunicaciones electrónicas, lo representan las investigaciones de criminalidad económica donde, por sí sola, la PJE no podría esclarecer de ningún modo los hechos sin contar con la concurrencia de los análisis de los eventos económicos de las instituciones públicas encargadas de velar por el correcto cumplimiento de las obligaciones fiscales de las personas físicas y jurídicas.

La cuestión que se plantea es que la inteligencia económica que, por sus propios medios, puede elaborar la PJE[1040] y la inteligencia criminal que, por los suyos,

---

[1038] Sobre esta función, RODRÍGUEZ LAINZ dice que *"el legislador de la LCDCE ha apostado decididamente por la involucración de los operadores de telecomunicaciones en su deber de colaboración con la investigación criminal"*. Vid. Rodríguez Lainz, José Luis. *El principio de proporcionalidad…op. cit.*

[1039] En la STS, Sala Tercera, de lo Contencioso-administrativo, Sección 7ª, de 27 de diciembre de 2010 (REC. 1783/2009), se dice que "*sentada esta premisa, recuerda cuál es la posición jurídica de TELEFÓNICA de la que dice que no es igual o equivalente a la de cualquier empresa, sino especial, pues presta un servicio privado de interés público, razón por la cual se halla en una especial relación de sujeción respecto de la Administración Pública y de la Comisión del Mercado de las Telecomunicaciones*".

[1040] Por ejemplo, la PJE tiene conocimiento por una fuente viva de que un empresario se dedica a la defraudación del IVA. Un buen día, se le incauta en el aeropuerto en vía administrativa una importante cantidad de dinero sin declarar que pretendía evadir al extranjero. Estudiada su vinculación con determinadas sociedades mercantiles, sólo se le conoce una, pero que opera bajo un impecable cumplimiento de sus obligaciones económicas y fiscales. Sin embargo, una suma diversa de indicios aconsejan a la PJE poner los hechos en conocimiento de un Fiscal, que ordena la apertura de una investigación.

pueden obtener los inspectores de tributos de la Agencia Tributaria[1041] (en adelante, AEAT[1042]), son por completo insuficientes para que cada una de estas instituciones pueda resolver aisladamente el caso en toda su dimensión.

Sólo una fructífera y eficiente colaboración, dispuesta bajo el control de un Juez o de un requerimiento del Ministerio Fiscal[1043], puede permitir el intercambio de ambas inteligencias, la criminal y la económica, para que, debidamente integradas, produzcan la verdadera y útil inteligencia elaborada con vocación de servir al proceso penal mediante el esclarecimiento material de los hechos, la determinación de la vinculación de sus autores, la revelación de la estructura mercantil interpuesta, la identificación de testaferros y su relación con los maquinadores en la sombra, determinación de su participación real, el descubrimiento de otros hechos conexos (relacionados o no con la delincuencia económica), la localización del patrimonio evadido o blanqueado, las acciones de resarcimiento civil, etc[1044].

Este proceso de integración de las diversas fuentes de inteligencia – pues pueden concurrir con la proveniente de otras instituciones públicas o privadas - no es estático, es decir, no se limita a que cada institución aporte al juzgado o fiscalía la que tiene a su alcance sino que, el resultado de cada inteligencia será el resultado de la

[1041] Siguiendo el ejemplo planteado, la AEAT sabe que, sin tener una relación aparente entre sí, hay varias personas jurídicas que han dejado de ingresar en la Hacienda Pública importantísimas cantidades correspondientes a la repercusión del IVA por sus actividades comerciales facturadas en un ejercicio económico, en tal medida que se ven obligados a comunicar a las diferentes fiscalías esta situación *ex* arts. 95 y 180 de la Ley 58/2003, de 17 de diciembre, *General Tributaria*, pero sin acumularlas en una concreta investigación, por no haberse identificado una ligazón entre unas y otras personas físicas y/o jurídicas, al menos, en un plano económico o fiscal.

[1042] http://www.agenciatributaria.es/AEAT.Internet/Inicio.shtml.

[1043] Los ejemplos de este tipo de autorización son cada vez más frecuentes. Uno entre muchos lo constituye la orden del Fiscal Jefe de Jaén, adoptada en Diligencias Preprocesales 102/10, de 22 de junio de 2010, dirigido al Delegado Provincial de la AEAT, en cuya parte dispositiva se ordena que un funcionario *"…en forma de Auxilio Jurisdiccional, con fundamento en el art. 17.1 LOPJ, participe y coopere en directo entendimiento con los Agentes de la Guardia Civil encargados en esta investigación, en el desarrollo de la misma, autorizando a los Servicios a facilitarse y recibir cuanta información respecto a los hechos investigados, sea precisa".*

[1044] Siguiendo con el ejemplo, los seguimientos del empresario y el conocimiento de sus relaciones sociales, así como la declaración en sede policial de varios testigos, desvelan una intensa relación con varias personas cuyas empresas reúnen el conocido perfil de defraudación del IVA y que hasta ese momento no se conocía. Al poner a los actores en su escenario, pueden los inspectores de tributos correlacionar la información fiscal y tratar la maquinación en su conjunto. Esto, a su vez, permite el acceso a otras informaciones económicas que habrán de situarse en el escenario criminal, señalando nuevos objetivos para la PJE. La reiteración de este procedimiento tenderá de forma cooperativa a desvelar la verdadera naturaleza y alcance de los hechos, propiciando no sólo su enfoque penal, sino también el resarcimiento de las víctimas y el descubrimiento de posibles bolsas de delincuencia conexa.

progresiva integración dinámica de la que se elabore por cualquiera de las demás, de modo que todos conozcan su contenido y, en su virtud, hagan progresar la investigación mediante su integración en la propia, retroalimentándose unos con otros.

Todo este proceso, bajo este singular enfoque, puede hacerse sin necesidad de una constante autorización jurisdiccional que permita dar cada paso pues, bien el Juez o el Fiscal, habrán establecido el marco habilitante preciso de la actividad de intercambio dinámico de inteligencia de acuerdo con la proporcionalidad de esta medida y el legítimo interés a que se dirige[1045], visto el escenario en el que se ha de intervenir y la seguridad jurídica con que se deberán llevar a cabo todas las actuaciones[1046].

Pues bien, este cometido de prestar un auxilio jurisdiccional altamente especializado, cuya ejecución es a determinadas entidades públicas o privadas *ex* art. 17.1 LOPJ, aunque centrado ahora en la intervención técnica del contenido material de las comunicaciones electrónicas por parte de las operadoras del mercado de las telecomunicaciones – cuyo ámbito de especial protección no se pretende comparar con el de los ejemplos referidos a la información fiscal -, es comentado favorablemente por GONZÁLEZ LÓPEZ, con apoyatura en algunos otros autores:

> *"También frecuente es que la ejecución material recaiga en los operadores de comunicaciones electrónicas, y, desde una perspectiva más amplia, cabe plantearse que en los distintos proveedores de servicios de comunicaciones electrónicas, debido a que son éstos los que, por su condición de tales, mantienen un contacto directo con el proceso de comunicación y se hallan, por tanto, en la mejor situación para acceder a las informaciones transmitidas o datos generados. En este sentido, no sólo se muestra conveniente que el órgano judicial sea asesorado por técnicos en*

[1045] En el ejemplo, demostrar que existe grupo criminal que se lucra de una defraudación de tributos mediante un sofisticado procedimiento ilícito, para lo cual, entre otras cosas, interpone testaferros al frente de sociedades mercantiles que actúan para ocultar la verdadera identidad de los sujetos activos de las obligaciones fiscales.

[1046] En el ejemplo propuesto, además de las normas de la PJE al efecto, ya reiteradamente expuestas, existen otras que obligan a los demás actores del proceso de elaboración de la inteligencia. En el caso de la AEAT, además del marco general de protección de datos contenido en la LOPD y demás legislación, le sería de directa aplicación el art. 95 de la Ley General Tributaria.

comunicaciones electrónicas acerca del método más adecuado para practicar la intervención, sino que la colaboración de los proveedores de servicios de comunicaciones electrónicas es precisa para llevar a cabo la obtención de la información, llegándose incluso, cada vez con mayor frecuencia, a la situación apuntada de que la medida sea practicada por los empleados de la compañía telefónica o del operador de comunicaciones electrónicas, bajo la observancia o control tanto de la policía judicial como, con carácter deseable, del Juez instructor"[1047].

Añade el autor que *"se corre el riesgo, en consecuencia, de que la intervención afecte a una multitud de datos que exceden del propósito inicial de la medida acordada, por lo cual se deberá ser especialmente cuidadoso al seleccionar el tipo de tecnología de interceptación. Por otro lado, también puede suceder que la falta de instrumentos técnicos idóneos provoque la imposibilidad de obtener datos de interés. Estas circunstancias constituyen, de hecho, un argumento más a favor de la delegación de la ejecución material en los proveedores, siempre bajo control judicial"*[1048]. Con este comentario sugiere una participación activa de la operadora en remover los obstáculos que permitan satisfacer en toda su amplitud el requerimiento judicial, allí donde aparezcan determinadas complicaciones de orden técnico que lo puedan condicionar.

Pues bien, la tesis que se sostiene considera que el papel de las operadoras e ISP (o de otros organismos que puedan concurrir a esta finalidad técnica) no debe quedar constreñido a facilitar y resolver sobre lo meramente técnico del instrumento que permite la intervención de las comunicaciones electrónicas – la aparatología, podría decirse -, con ser esto lo más importante, sino extenderlo también, cuando ello

[1047] El autor se apoya, entre otros, en Gimento Sendra, Vicente. *Derecho…op. cit.,* pág. 415. Vid. González López, Juan José. *Los datos de tráfico…op.cit.,* pág. 219 y ss.

[1048] GONZÁLEZ LÓPEZ llega incluso a afirmar que existe un desplazamiento de la actividad de intervención desde la policía hacia las operadoras de comunicaciones electrónicas, cosa que no puedo compartir, pues las obligaciones de cooperación impuestas a aquellas desde los arts. 33 LGT y ss se limitan exclusivamente a la cesión de la señal al SITEL y, en todo caso, a la facilitación, no siempre gratamente recibida y, en ocasiones, tampoco ejecutada, de favorecer determinadas intervenciones especiales de las que deben seguirse desde las instalaciones y medios privados de las operadoras. Naturalmente, cualquier pretensión de que la operadora acceda al contenido material de las comunicaciones, sustituyendo a la PJE, es materia que le queda prohibida por el art. 18.3 CE, lo que debe entenderse únicamente en cuanto exceda de lo preciso para comprobar el correcto funcionamiento de la intervención *ex* arts. 89 RLGT y ss. Debe entenderse, por tanto, que las palabras de tan comentado autor se refieren a la creciente complejidad de sus funciones técnicas frente a las exigencias planteadas por la evolución de las TIC.

sea preciso, al manejo del *software* de análisis que permita una explotación técnica – inteligente - de las bases de DACE en beneficio del proceso penal, bajo la dirección de la PJE y contando con el correspondiente control jurisdiccional[1049].

4. Proporcionalidad de la IDACE

Sobre las cuestiones aportadas hasta el momento, en términos de la proporcionalidad de la propuestas, debe decirse lo siguiente:

La Ley debe establecer con total exactitud la forma y límites en que deben ejecutarse las labores de obtención de la IDACE, conteniendo el derecho positivo una serie de normas que especifiquen cuáles son los procedimientos jurídicamente admisibles.

La justificación teleológica debe orientarse a conseguir un nivel equivalente de eficiencia en el acceso a los DACE ante la evolución de un ámbito de comunicación, nuevo y complejo, pero idéntico en su valor instrumental para la comunicación criminal al que, en su día, justificó la decisión de considerar ajustado a derecho el permitir su limitación. Consecuentemente, la finalidad es idéntica en ambos casos aunque varíe cuantitativa y cualitativamente la forma en que se alcanzan los mismos fines.

[1049] Nótese que, actualmente, cada operadora o ISP se dota de los medios internos de análisis que considera conveniente, lo que produce diversas capacidades de respuesta a preguntas (como se acreditó en el análisis aportado junto con la denuncia del caso LÍNEA ROJA), dependiendo de su complejidad, de una mayor o menor calidad. A ello debe unirse el espíritu de cooperación que exhiban ante cada requerimiento. En este sentido, debe entenderse que, más allá del interés público por sus actividades, son empresas privadas orientadas a la consecución de un lucro legítimo, por lo que la carga de nuevas y onerosas obligaciones de todo tipo debe ponderarse con ánimo restrictivo o, en todo caso, con cargo o transferencia a los organismos del Estado. Esta cuestión, aunque excede al propósito de este estudio, sugiere una posible solución institucional mediante la creación de un organismo técnico que gestionase frente a las operadoras e ISP las capacidades del Estado de intervenir las comunicaciones (lo que unificaría las capacidades materiales de intervención y conservación de DACE bajo un mismo régimen jurídico y técnico), organismo que debiera quedar bajo el control jurisdiccional de una Autoridad Judicial de Garantías al estilo de la propugnada en la Ley Orgánica 2/2002, de 6 de mayo, *reguladora del control judicial previo del Centro Nacional de Inteligencia*. Aún siendo así, mucho me temo que esta solución no sería del agrado de los más garantistas por las más que presumibles tachas de “Gran Hermano” que se verterían sobre tan novedosa institución.

El ámbito y medios de intervención – una base datos y un *software* de análisis -, es el medio idóneo y único para extraer las conclusiones que sirvan de progresión a la investigación criminal, de modo que se propicie el hallazgo de posibles pruebas, no siendo descartable además que esta actividad técnica goce en sí misma de una especial consideración de cara al proceso de contradicción del juicio oral, al atribuírsele la calidad de prueba de inteligencia policial. La idoneidad de las medidas propuestas se completa con el conjunto de salvaguardas tecnológicas, el registro lógico de las acciones de investigación y la eventual participación como peritos de los técnicos de las operadoras e ISP a los que se les haya señalado la ejecución de un auxilio jurisdiccional.

La necesidad de acudir a este medio de prueba sólo puede estimarse en caso de que no exista una forma alternativa menos gravosa de accederlo. Sin embargo, la evolución de las TIC y su uso criminal hace que buena parte de las acciones de concertación criminal transcurran dinámicamente sirviéndose de este medio, llegando incluso a que se den maquinaciones que lo usen como finalidad en sí mismo, no dando lugar por tanto a otra opción que la de intervenir en el ámbito de las comunicaciones electrónicas si es que se desea proteger otros los bienes jurídicos puestos en peligro, todo ello con independencia de la gravedad intrínseca de los hechos.

La motivación de las resoluciones debe ser acorde con la complejidad del problema tratado, ponderando exhaustivamente las razones de limitar los derechos de que se trate, la forma, los medios, su extensión y sus límites. El contenido de la resolución debe, consecuentemente, permitir que queden autorizadas las consultas complejas o parametrizadas sobre los contenidos formales de las bases de datos de las operadoras e ISP, tendentes a obtener la más eficiente IDACE y a restringir, por el contrario, el acceso a los datos que no interesen al proceso penal. Por ello, bajo la dirección de la PJE, deben quedar los técnicos de la operadora o ISP habilitados para analizar las bases de datos en la forma en que se exprese en el mandato judicial y bajo estricto control jurisdiccional.

La intervención judicial previa debe quedar reservada a aquellos ámbitos en que quede afectado el derecho al secreto de las comunicaciones, es decir, en los que se intervengan las comunicaciones personales, reservándose a la iniciativa de la PJE a

los que justificada y exclusivamente tengan que ver con un ámbito instrumental de las comunicaciones electrónicas, en el que no se estime una afectación al derecho fundamental a la intimidad. En todos los casos, no obstante, debe ejercerse un control jurisdiccional adecuado de las medidas que asegure el derecho a la defensa, la tutela judicial efectiva y el derecho a un proceso con todas las todas las garantías, lo que no empece para que se intervenga, en lo que se establezca al efecto de *lege ferenda* (incluyendo la provisión de medidas para tratar adecuadamente los casos de urgencia vital), según el régimen establecido en los arts. 549.1.a) LOPJ, 11.2.d) LOPD, 22.2 LOPD y 1, 2 y 4 RDPJ.

La proporcionalidad en estricto debe tomar en consideración tanto la gravedad de los hechos que se investigan, como la realidad social y el ámbito tecnológico en que se producen, así como las razones de urgencia o el peligro de demora y las demás que permitan ponderar la necesidad de antevenir según la trascendencia de los hechos y la eficiencia previsible de los medios destinados a la investigación.

Y en términos prácticos, vista la evolución del uso criminal de las TIC, el Estado de Derecho debe superar el enfoque por el que la acción jurisdiccional en la limitación de los derechos fundamentales se centra exclusivamente en el mero acceso a los listados de DACE, para extenderse, bajo todas las garantías posibles, a la habilitación de la PJE para la obtención de inteligencia sobre estos mismos datos – conceptos ambos netamente distintos -, contando para ello con el principio de proporcionalidad, las debidas salvaguardas y con la participación como peritos, cuando así proceda, de los técnicos de las operadoras reguladas por la LGT y los ISP regidos por la LSSI. En definitiva, reconocer el valor probatorio que, de una forma jurídicamente segura, pueda tener la prueba de inteligencia policial tras su sometimiento al proceso de contradicción y valoración en el acto de juicio oral.

Sin embargo, esta propuesta ha de chocar irremediablemente – soy plenamente consciente de ello - con los nada desdeñables y alarmante temores que en amplios sectores de la doctrina suscita la cuestión de la "militarización" de la acción policial y el aparente vaciamiento de las funciones jurisdiccionales[1050,1051] en lo que

[1050] En lo que respecta a la LCDCE, según GONZÁLEZ LÓPEZ, una expresión de este vaciamiento se encontraría en la disposición que regula la entrega de los DACE *"a los agentes facultados",* de suerte

podría describirse como "una nueva forma de instrucción de los casos criminales por la PJE y no por el Juez, que queda sepultado bajo sus ímpetus" o "policialización de la instrucción penal", en lo cual he de negar vehementemente la mayor una vez más: La investigación penal, por mor del art. 126 CE, es función exclusiva y excluyente de los jueces pero que, al realizarse con el con el apoyo de la PJE, no puede ni debe evitarse que acuda en su auxilio con sus mejores medios. La cuestión es, únicamente, conocerlos y admitir su idoneidad para servir a un proceso penal propio de un Estado de Derecho.

En efecto, siguiendo una vez más a GONZÁLEZ LÓPEZ[1052], en el ámbito que ocupa este estudio y en referencia al derecho alemán, lo que se ha denominado IDACE se referiría, según el autor, *a "la "Rasterfahndung", cuyo nombre se ha traducido al castellano como "búsqueda entrecruzada de datos"*[1053]*, pero también otras medidas que cobran una especial dimensión merced al tratamiento de datos que permiten, caso de los análisis de ADN, la vigilancia electrónica o la intervención de las comunicaciones"* y que se materializaría en, efectivamente, "*el empleo de técnicas de análisis de datos a fin de dotarse de fuentes de inteligencia propias*"[1054], todo ello ante

---

que *"habiéndose establecido la exigencia de resolución judicial habilitante, lo coherente con dicho presupuesto es que los datos sean cedidos al órgano judicial a fin de que efectúe el control de la medida realizada y que, una vez efectuado éste, sea él el que facilite los datos recabados a los agentes facultados".* Vid. González López, Juan José. *Comentarios a la ley 25/2007…op. cit*. Sin embargo, RODRÍGUEZ LAINZ desmonta semejante prevención en razón del peso de la Autoridad Judicial en el proceso penal: *"… los destinatarios de la información podrán ser o bien éstos [la PJE] o bien la autoridad judicial que los comisiona para que recaben la información de los operadores obligados. Resulta evidente que en uno y otro supuesto la autoridad judicial que autoriza u ordena la cesión de datos es realmente el verdadero destinatario de la información; de hecho el art. 547 de la LOPJ (19) concibe a la policía judicial desde su dimensión de colaboración o auxilio a la autoridad judicial en su función investigadora"*. Rodríguez Lainz, José Luis. *El principio de proporcionalidad…op. cit.*

[1051] Vid. Pedraz Penalva, Ernesto. *Sobre la crisis de la justicia.* en *Constitución, jurisdicción y proceso*, Akal, Madrid 1990, pág. 267.

[1052] Vid. González López, Juan José. *Los datos de tráfico…op.cit.,* pág. 75 y ss.

[1053] GONZÁLEZ LÓPEZ, con referencia a otros autores, describe el concepto de *"Rasterfahndung"* como la *"medida incorporada al ordenamiento jurídico alemán a través de la Ley para la lucha contra el tráfico ilegal de drogas y otras formas de delincuencia formas de delincuencia organizada (Gesetz zu Bekämpfung des illegalen Rauschgifthandels und anderer Erscheinungsformen der Organisierten Kriminalität, OrgKG), de 15 de julio de 1992, que entró en vigor el 22 de septiembre de ese mismo año"*.

[1054] El autor se apoya en Hernández Guerrero, F. J. y Álvarez de los Ríos, J. L. *Medios informáticos y proceso penal,* págs. 9 y 10 y aporta que *"la problemática de la militarización de la policía no es, en todo caso, un fenómeno nuevo, sino que la influencia del modelo militar ya había sido advertida con anterioridad a la dotación con los nuevos medios tecnológicos, y encuentra una clara manifestación en la guardia civil",* con referencia a Barcelona Llop, J. *El régimen jurídico de la policía de seguridad*, Instituto Vasco de Administración Pública. Oñate, 1988, pág. 76 y *ss*. En mi opinión, esta supuesta influencia de lo militar es idéntica en la policía y en las aduanas de todo el mundo avanzado. Sin excepción. No

la *"modernización de las técnicas policiales de investigación [que] han motivado que resulte sumamente dificultosa la dirección de la instrucción por el Juez*[1055]*, hasta el punto de haberse sostenido que esta situación acarrea una duplicidad de diligencias y una menor eficacia en la lucha contra la delincuencia"*[1056].

Pues bien, mi desacuerdo no puede ser mayor con estas respetables pero equivocadas opiniones sino, muy por el contrario, creo que es necesario diluirlas en la razonabilidad de las propuestas que en este estudio se contienen pues, de no de asumir esta realidad – que es la de la sociedad en la que debe imperar la Ley -, sí que supondría la efectiva desnaturalización de las funciones judiciales y un decaimiento de la tutela judicial efectiva, esto es, una desafección de la acción jurisdiccional al ámbito de la vida humana en que ha de intervenir.

Es necesario, por tanto, que la Justicia se apoye en la realidad social y tecnológica y no al revés y que, mediando una auténtica seguridad jurídica en la actividad investigadora de la PJE, se facilite la acción jurisdiccional verdadera al poder juzgar con unos elementos objetivos de juicio que permitan adquirir la más exacta naturaleza de los hechos materia de escrutinio y, consecuentemente, fundar las sentencias desde la más estrecha relación entre estos y la Ley.

Es radicalmente inexacto que, por lo dicho, "*resulte sumamente dificultosa la dirección de la instrucción por el Juez",* sino más bien todo lo contrario, pues queda liberado de la incertidumbre y la inseguridad que supondría la valoración, en un mundo tecnificado, con los más que obsoletos medios de prueba clásicos, llamados irremediablemente a hacer fracasar el proceso penal en este ámbito. Por ello, el

---

entiendo la extemporánea referencia a la Guardia Civil por más que disponga de las técnicas y medios más sofisticados de investigación, pero que, en sus funciones policiales nacidas del art. 126 CE, actúa con idéntica doctrina que los demás cuerpos de investigación.

[1055] El autor lo considera *"una situación que también afecta a la Fiscalía en aquellos ordenamientos o procesos en que tiene conferida la investigación de los delitos"*, con apoyo en Ambos, K., "Control de la policía por el fiscal *versus* dominio policial de la instrucción", *Tribunales de Justicia*, n.º3, marzo 2002, p.18.

[1056] El autor se apoya en Martínez Arrieta, A. "La instrucción de las causas por delitos. Naturaleza. Órgano que debe realizarla. Iniciación", en VVAA, *La instrucción del sumario y las diligencias previas*, Consejo General del Poder Judicial, Madrid 1998, págs. 148 y 149. También en Pastor López, M. *El proceso de persecución: análisis del concepto, naturaleza y específicas funciones de la instrucción criminal*, Universidad de Valencia: Secretario de Publicaciones, Valencia 1979, pág. 42, se advierte la "*hipertrofia de la instrucción*" provocada por la habitual duplicación de las actuaciones, mas destacándose que el modelo de instrucción previsto en la LECrim tiene la ventaja de "*la mayor garantía de imparcialidad desde un principio, en la búsqueda de datos y reunión de pruebas*".

conocimiento de los hechos y las decisiones de orden jurisdiccional, basadas en las aportaciones de la PJE, vendrán amparadas por una actividad probatoria segura que le permitirá ser justo y proporcionado ante el proceso de contradicción y valoración de la prueba.

Ante la frase "sólo el Juez investiga", hay que responder que esto no sería posible en la mayoría de los casos sin el auxilio de la PJE, incluso en los de una mínima complejidad, porque sería difícil ver a S. Sª. atando cabos en una escucha de las comunicaciones, participando en un seguimiento, analizando cuentas, desentrañando el ADN de un sujeto, manejando el *IMSI Catcher* cerca de los sospechosos o analizando bases de datos de cualquier clase.

Decididamente, esto no es posible en la realidad actual, pues la época en que sí lo fue ha quedado enterrada por la fuerza de los hechos y de la modernidad sin que, en modo alguno, se hayan devaluado como consecuencia las funciones jurisdiccionales de investigación dentro del Estado de Derecho que, muy por el contrario, han adquirido una dimensión superior y a cuya seguridad jurídica contribuye, sin duda, la labor de la PJE con plena conciencia de su dependencia funcional de Jueces y Fiscales.

Tampoco parece de recibo que exista *"una duplicidad de diligencias",* pues en esto sí que sirven las previsiones de la prehistórica legislación procesal sobre el atestado, por mucha calidad y peso que se le quiera atribuir, y las diáfanas funciones de la PJE de auxilio judicial, perfectamente diferenciadas y con clara subordinación de las segundas a las primeras, lo que se traduce en la decisión soberana del Juez de incorporar o no el contenido del atestado, o tan sólo alguna de sus partes, a las diligencias judiciales en el preciso marco jurídico del proceso penal.

Y, muchos menos, padecer el proceso penal, por la lógica expansión de las capacidades de la PJE, de *"una menor eficacia en la lucha contra la delincuencia",* pues si se prescindiese de la aportación de la PJE de ningún modo podría el Juez juzgar, sin que el comentario insertado merezca ni una sola explicación adicional por su más que absoluta y evidente irracionalidad.

E. La obligación de conservación de datos de tráfico, localización e identificación.

La comunidad internacional ha ido reaccionando en los últimos tiempos ante las nuevas necesidades de los estados de injerirse legalmente en los contenidos material y formal de las comunicaciones electrónicas. Aunque desbordada por la realidad del moderno uso criminal de las TIC, ha mostrado trabajosamente también una clara intención de entender y luego afrontar sus retos, no exenta a veces de algunos prejuicios garantistas.

Los revolucionarios cambios anejos a esta realidad se han manifestado como factor modificativo del comportamiento social originado por la diversidad y sofisticación de la tecnología de las comunicaciones universalmente disponibles pero, en nigún caso, en cuanto a su utilidad real, que permanece inalterada, y que no es otra que el de favorecer la comunicación humana con medios técnicos cada vez más eficientes y accesibles y, más recientemente, para facilitar también el funcionamiento de las máquinas. Este último y emergente uso es claramente distinto del primero y necesitado de un ejercicio de comprensión en cuanto a su más exacta naturaleza material y, consecuentemente, a su dimensión jurídica.

En ello, la necesidad y el derecho del Estado democrático a injerirse en los derechos fundamentales no ha variado en su esencia, pero sí ha sido necesario que buscase un nuevo enfoque por imperativos de la expansión de la amenaza asociada que el abuso de las TIC puede suponer para su viabilidad y, por tanto, le ha correspondido el intento de dar con las soluciones jurídicas y de todo tipo que garanticen la continuidad en el legítimo propósito de la injerencia.

Por ello, en el capitulo segundo se presentó un panorama de actualidad que incluía los acertados puntos de vista, análisis, posicionamientos y recomendaciones de la comunidad internacional a los estados, de obligada o no adopción en el derecho interno, y que invitan al legislador a hacer, cuando menos, una reflexión sobre los instrumentos jurídicos que sería necesario adoptar o modificar para sortear eficientemente los problemas que sí sabía identificar (la espectacular evolución de las

TIC), pero más difícilmente tratar (establecer un régimen jurídico eficiente para el derecho de injerencia), por existir un derecho precedente de naturaleza formal, de gran rigor en cuanto a su protección jurídica, pero inhábil para adaptarse a la sorprendente evolución operada en este ámbito (el secreto de las comunicaciones).

Estando en estos esfuerzos, la comunidad internacional ha ido invocando diversas propuestas que, aún tímidamente y sin duda entroncando con el derecho penal de lucha, han aportado algunas soluciones efectivas en materia de conservación de datos. Por su directo interés, se estudiarán las siguientes:

- El Convenio sobre la Ciberdelincuencia, hecho en Budapest el 23 de noviembre de 2001, al ser conscientes sus redactores, tal y como reza su preámbulo, *"de los profundos cambios provocados por la digitalización, la convergencia y lay la globalización continua de las redes informáticas y la globalización continua de las redes informáticas"* y, desde luego, de las necesidades de cooperación internacional.
- La Directiva 2006/24/CE, *sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones"*[1057].

En lo que interesa a esta parte del estudio, ambas iniciativas suponen, en lo práctico, un notable intento de compensar el desfase entre los delincuentes y los instrumentos jurídicos que deben garantizar su perseguibilidad, tal y como se proclama en el preámbulo del CCib, al promover "*la asunción de poderes suficientes para luchar de forma efectiva contra dichos delitos, facilitando su detección, investigación y sanción, tanto a nivel nacional como internacional, y estableciendo disposiciones que*

[1057] El marco regulatorio básico de las comunicaciones electrónicas parte de la Directiva 2002/21/CE del Parlamento Europeo y del Consejo, de 7 de marzo de 2002, *relativa a un marco regulador común de las redes y los servicios de comunicaciones electrónicas* (Directiva marco)[1057], conectada con la Directiva 95/46/CE, y se completa con la Directiva 2002/20/CE del Parlamento Europeo y del Consejo, de 7 de marzo de 2002, *relativa a la autorización de redes y servicios de comunicaciones electrónicas* (Directiva de autorización); la Directiva 2002/19/CE del Parlamento Europeo y del Consejo, de 7 de marzo de 2002, *relativa al acceso a las redes de comunicaciones electrónicas y recursos asociados, y a su interconexión* (Directiva de acceso); la Directiva 2002/22/CE del Parlamento Europeo y del Consejo, de 7 de marzo de 2002*, relativa al servicio universal y los derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas* (Directiva de servicio universal) y la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, *relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas* (Directiva sobre la privacidad y las comunicaciones electrónicas).

permitan una cooperación internacional rápida y fiable"; y en la DCD, según su considerando vigésimo primero, dado que sus objetivos son *"armonizar las obligaciones de los proveedores de conservar determinados datos y asegurar que éstos estén disponibles con fines de investigación, detección y enjuiciamiento de delitos graves"*.

Ambos instrumentos jurídicos tienen en común, entre otras cosas, el establecimiento de medidas tendentes a facilitar, no sólo el acceso a las fuentes de datos relacionadas de una u otra manera con las comunicaciones electrónicas, según sus respectivas especificidades, sino también a lograr un grado equivalente de eficiencia en la respuesta internacional al problema mediante el establecimiento de una serie de medidas de cooperación.

Tanto es así, que en el caso de la DCD se establecen obligaciones sin precedentes sobre unos DACE cuyo control por parte del Estado se percibe, no sin razón, con algún escepticismo y reservas por una sociedad muy avanzada y extraordinariamente sensible a cuanto pueda afectar a sus libertades, debido a la estrecha vinculación entre tales medidas y el ejercicio efectivo del derecho a la intimidad, protegido férreamente por los arts. 8 CEDH y 18 CE, en lo que supondría, al decir de muchos autores, un adelantamiento de la acción penal.

Es evidente que la instauración de una medida *ex novo* de conservación de los DACE, además de las connotaciones que sobre el sustrato material puedan contemplarse (una inmensa base de datos en manos de los sujetos obligados por la Ley y accesibles por el Estado), supone una controvertida medida relacionada con la libertad, la protección de datos y el secreto de las comunicaciones que puede concitar el rechazo social en aquellos países que, como los de la Unión Europea, tienen en su acervo democrático la más honda susceptibilidad, no ya sobre el uso supuestamente inadecuado que pudiera llegar a darse a los DACE, sino simplemente por el mero hecho material de ordenarse su conservación, por más garantías y salvaguardas que el Estado haya querido introducir para evitar cualquier desviación de su finalidad.

Sin embargo, sobre la coincidencia en los propósitos de mantener la capacidad de injerencia del Estado ante la realidad del uso criminal de las TIC, el CCib y la DCD son netamente distintos en aspectos de sumo interés para cuanto se pretende

sostener en este trabajo pues, en la síntesis de las facultades que ambos instrumentos jurídicos representan, pueden hallarse algunas de las soluciones que son objeto de propuesta.

En efecto, aunque en los dos textos se habla, de un modo o de otro, de disponibilidad de los datos, las diferencias de tiempos, enfoque y objetivo son notoriamente distintas, pese a lo cual no cabe hablar de ámbitos diferentes de intervención del Derecho, ya que sus hallazgos respectivos concurren a la solución de un mismo problema: garantizar la continuidad en la intervención legal de las comunicaciones electrónicas, tanto en su contenido material, como en el formal, por más que las TIC puedan avanzar facilitando nuevos instrumentos para llevarlas a cabo.

Por ello, trataré de ajustar las propuestas – valorando el extraordinario rendimiento para la investigación que ha supuesto esta herramienta de investigación - a lo que exija el espíritu democrático, el respeto a las libertades, lo que aconseje la experiencia, el sentido común y lo que demande el más estricto concepto de la proporcionalidad que debe imperar en cualquier reacción del Estado de Derecho.

1. La Directiva 2006/24/CE y su transposición

a) La decisión de ordenar la conservación de los datos de tráfico, localización e identificación

No resulta fácil hacer una reflexión introductoria sobre la decisión, sin precedentes en la UE[1058], de imponer la conservación masiva de los "*datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de*

[1058] El Grupo del art. 29 proclamó que *"la decisión de conservar datos de comunicación con el fin de combatir la delincuencia grave es un hecho sin precedentes que tiene una dimensión histórica. Afecta a la vida cotidiana de todos los ciudadanos europeos y puede poner en peligro los valores y las libertades fundamentales que disfrutan y estiman. El Grupo de trabajo recuerda que las consideraciones y las preocupaciones recogidas en el Dictamen antes mencionado mantienen toda su validez. Por lo tanto, es de suma importancia que la Directiva vaya acompañada y sea aplicada en cada Estado miembro a través de medidas destinadas a imitar el impacto sobre la intimidad".* Vid. Dictamen 3/2006 del Grupo de Trabajo del Artículo 29 sobre protección de datos (WP119); Informe 01/2010.

acceso público o de redes públicas de comunicaciones generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones", adoptada mediante la controvertida Directiva 2006/24/CE, que obliga a todos sus ciudadanos, salvo a los nacionales de los tres países cuyo Tribunal Constitucional cerró el paso a la transposición de la directiva a su derecho interno (República Checa, Alemania[1059] y Rumanía)[1060,1061].

Es muy cierto que, mediada la primera década del Siglo XXI, la situación del terrorismo y la delincuencia organizada, bien cimentados en sus inquietantes progresos de los años precedentes, había alcanzado cifras paroxísticas en la escena internacional, con el siniestro ascenso de graves y recurrentes fenómenos – con un insospechado grado de penetración en la sociedad - como el yihadismo, la acción de grupos terroristas de cualquiera de las opciones políticas extremistas, las redes transnacionales de DO, la corrupción y, en general, diversas manifestaciones de lo más execrable del ser humano.

Pero también es cierto que el daño, convenientemente dirigido contra una sociedad de ciudadanos libres, se extiende y manifiesta en el concierto de aquellas naciones avanzadas cuyo signo más sensible es, precisamente, el de haber apostado por el imperio de una Ley justa y por progresar sin renuncias en su sensible acervo democrático. Una sociedad, en definitiva, orgullosa de sus libertades y respetuosa con ellas hasta el extremo de alcanzar, incluso, a los inalienables derechos de sus peores ciudadanos.

En consonancia con este loable espíritu de defensa de las libertades, la conservación de datos constituye, de acuerdo con un parecer unánime, una limitación

[1059] Sobre la decisión del Tribunal Constitucional Alemán, vid. Ortíz Pradillo, Juan Carlos. *Tecnología versus Proporcionalidad en la Investigación Penal: La nulidad de la ley alemana de conservación de los datos de tráfico de las comunicaciones electrónicas.* La Ley Penal, Nº 75, Octubre 2010, Editorial LA LEY.

[1060] Decisión nº 1258, de 8 de octubre de 2009, del Tribunal Constitucional rumano, Diario Oficial rumano nº 789 de 23 de noviembre de 2009; sentencia *del Bundesverfassungsgericht* 1 BvR 256/08, de 2 de marzo de 2010; Gaceta Oficial de 1 de abril de 2011, sentencia del Tribunal Constitucional de 22 de marzo sobre las disposiciones del artículo 97, apartados 3 y 4 de la Ley nº 127/2005 Coll. *sobre las comunicaciones electrónicas y por la que se modifican determinados actos relacionados*, y Decreto nº 485/2005 Coll. *sobre la conservación de datos y su transmisión a las autoridades competentes*. Vid: *Informe de evaluación sobre la Directiva de conservación…doc. cit.,* pto. 4.

[1061] Algunos autores, como GONZÁLEZ LOPÉZ, sostienen la inconstitucionalidad de esta medida. Vid. González López, Juan José. *Comentarios a la ley 25/2007…op. cit.*, y González López, Juan José. *Los datos de tráfico…op.cit.,* pág. 428 y ss.

del derecho a la intimidad, concepto genérico que contiene, a su vez, sensibles expresiones de los derechos fundamentales recogidos, en el ámbito europeo, en los arts. 7 y 8 CEDH y en el art. 16 TFUE.

Consecuentemente, cualquier limitación del derecho a la intimidad deberá ser, con arreglo al art. 52.1 CDF, *"establecida por la ley y respetar el contenido esencial de dichos derechos y libertades. Sólo se podrán introducir limitaciones, respetando el principio de proporcionalidad cuando sean necesarias y respondan efectivamente a objetivos de interés general reconocidos por la Unión o a la necesidad de protección de los derechos y libertades de los demás"*.

En atención a estos pronunciamientos jurídicos, fuertemente enraizados en el principio de proporcionalidad[1062], una limitación de derechos fundamentales debe expresarse de una manera precisa y previsible, de forma que acredite ser necesaria para alcanzar un objetivo de interés general o para proteger los derechos y libertades de otros, ser proporcional al objetivo perseguido y ajustarse al contenido esencial de los derechos fundamentales en sobre los que se aplique.

Además, el art. 8.2 CEDH proclama que el ejercicio del derecho de injerencia de la autoridad pública en el ejercicio del respeto de la vida privada está justificado si es necesario para "*la seguridad nacional, la seguridad pública o la prevención de las infracciones penales"*.

La jurisprudencia del TEDH ha ido precisando las formas en que puede llevarse a cabo una limitación de derechos fundamentales. En materia de conservación de datos, por ejemplo, junto a otros que ya se han mencionado, son relevantes los pronunciamientos como el del Caso *Marper vs Reino Unido* en que el Tribunal consideró que "*el acceso a determinados datos sólo podía justificarse si respondía a una necesidad social acuciante, si era proporcional al objetivo perseguido y si las razones expuestas por la autoridad pública para justificarla eran pertinentes y suficientes"*[1063].

[1062] Vid. *Lista de control de los Derechos Fundamentales de la Comisión control para todas las propuestas legislativas*. *Estrategia para la aplicación efectiva de la Carta de los Derechos Fundamentales por la Unión Europea* COM (2010) 573/4.

[1063] Caso *Marper* contra Reino Unido, sentencia del Tribunal Europeo de Derechos Humanos, de 4 de diciembre de 2008.

Los principios básicos de la protección de datos exigen, por tanto, que su conservación sea proporcionada en relación con la finalidad de su recogida, y que el período de almacenamiento sea limitado y responda al interés general.

Por ello, un análisis simple de las razones por las que adoptó la decisión de conservación de los DACE reflejaría una aparente contradicción entre el profundo respeto por las libertades públicas y la necesidad de asegurarse, al mismo tiempo, una notoria capacidad de acción para intervenir ante unas formas delictivas sólidamente apoyadas en las TIC.

Ya bien entrada la segunda década del Siglo XXI, tras una primera valoración de los efectos la DCD en la vida social de la UE, surge inevitablemente una reflexión sobre la ponderación del sacrificio que esta grave decisión supuso para los derechos fundamentales, centrada en si lo decidido se ajustó a lo necesario y proporcional y, seguramente, dando acuse de recibo de cierta mala conciencia[1064] del legislador europeo, si no sería mejor introducir en la norma, a la mayor brevedad posible, importantes reformas de corte garantista[1065].

Al tiempo de escribirse estas cavilaciones, se cumplen seis años de la entrada en vigor de la directiva y cinco de su transposición en la LCDCE, lo que, a mi juicio, proporciona una corta pero suficiente perspectiva como para valorar su impacto, tanto sobre las libertades públicas, como en términos de eficiencia del Estado de Derecho frente a las expresiones más complejas de la delincuencia.

Es un tiempo, además, en que la UE ha puesto en marcha, a los mismos efectos, sus mecanismos legales de revisión de la directiva *ex* art. 14 y de la normativa

[1064] RODRÍGUEZ LAINZ, al comentar una inicial opción del legislador español, durante los trabajos de transposición de la DCD, por una consideración abierta del concepto de gravedad en el ámbito objetivo de aplicación de la LCDCE, considera que la opción claramente restrictiva que triunfó en el art. 1.1 LCDCE *("…siempre que les sean requeridos a través de la correspondiente autorización judicial con fines de detección, investigación y enjuiciamiento de delitos graves contemplados en el Código Penal o en las leyes penales especiales…"*) se debió a que *"la decisión fue tomada por consenso por todos los grupos parlamentarios, probablemente para atraer el voto favorable de las posiciones más reacias al espíritu y finalidad de una ley que se convertía ya en imperativo para el legislador español"*. Rodríguez Lainz, José Luis. *El principio de proporcionalidad…op. cit.*

[1065] MARTÍN PALLÍN anota la formidable fuente de datos automatizada que supone el cumplimiento por las operadoras de la LCDCE y que exige *"moderar y controlar todo el flujo de información"* comentando, con cierto tono apocalíptico, que *"la única tabla de salvación que paradójicamente nos puede salvar del desastre, es que la explosión de la información puede llegar a anular los efectos de la investigación". Vid.* Martín Pallín, José Antonio. 2008. *El equilibrio entre la conservación…op. cit.,* pág. 155.

transpuesta, para lo que ha contado con los informes previamente remitidos por los países miembros, con una profusa producción de documentos cuyo análisis ocupará un lugar central en esta parte del estudio. Es de esperar que los trabajos de revisión produzcan algunas variaciones en la legislación europea que hayan de ser transpuestas en el española en términos de reforma.

Ante el inicio de los mencionados trabajos de revisión, el Supervisor Europeo de Protección de datos (en adelante SEPD), Sr. PETER HUSTINX, en un discurso de marcado sesgo garantista sobre *"El momento de la verdad para la directiva de conservación de datos"*[1066], enfatizó sobre el carácter de la DCD – que consideraba fracasada en su propósito genérico de armonizar las legislaciones de los países miembros -, diciendo que era *"… sin duda, el instrumento más invasivo de la privacidad jamás adoptado por la UE en términos de escala y número de personas a los que afecta"*, cuya justificación no podía residenciarse únicamente en la utilidad que supusiese para que la policía resolviese graves casos criminales[1067,1068].

El planteamiento de HUSTINX, en clave de proporcionalidad y de cuestionamiento a la baja de las diversas facultades contenidas en la norma, pretende contestar a la pregunta de si serían posibles los mismos logros sin necesidad de recurrir a normas tan gravosas, esto es, sin que hubiese necesidad de imponer una conservación generalizada de datos o, al menos, hacerla menos invasiva.

[1066] Vid. *Conferencia "Taking on the Data Retention Directive". Discurso del Supervisor Europeo de Datos, Sr. Peter Hustinx sobre "The moment of truth for the Data Retention Directive",* Bruselas, 3 de diciembre de 2010.

[1067] Puede decirse, en cualquier caso, que la utilidad de la DCD no se agota en los casos criminales, sino en todo tipo de emergencias y, desde luego, en cuanto tiene de valor técnico para la ordenación del mercado de las telecomunicaciones. Sin embargo, HUSTINX considera inquietante el hecho de que pueda utilizarse más allá de los casos criminales graves o para la prevención criminal, ignorando que su utilidad alcanza a la resolución de emergencias o situaciones de riesgo catastrófico, como hallar a una persona extraviada y en peligro (lo que carece de interés normalmente para el proceso penal) o prevenir la actuación de un grupo terrorista capaz de activar explosivos a placer, cuando lo desee, mediante el uso de tarjetas SIM como detonadores. Hay un grave error de perspectiva, en mi opinión, en los prejuicios de HUSTINX que, por otra parte, no se compadecen con la invocación contenida en los considerandos de la DCD sobre la utilidad atribuida a los DACE, que comprende, sin exclusión, los aspectos de *"prevención, investigación, detección y enjuiciamiento de delitos, en especial contra la delincuencia organizada*".

[1068] De hecho, a la posición de HUSTINX se unen algunas acciones legales promovidas por determinados grupos de derechos civiles por considerar que la DCD restringe los derechos fundamentales, como sucedió el 5 de mayo de 2010, en que el *Irish High Court* autorizó a *Digital Rights Ireland Limited* a acudir al Tribunal de Justicia de conformidad con el artículo 267 del Tratado de Funcionamiento de la Unión Europea.

El argumento del SEPD para sostener su reservas, en mi opinión falaz, se basa en que *"unas cuantas jurisdicciones habían podido sobrevivir"*[1069] sin contar con una legislación similar de conservación de DACE.

Y digo falaz por dos razones: En primer lugar porque, en cualquier caso, todo indica que, en esas jurisdicciones sin transposición de la DCD, la manera de acceder a un idéntico repositorio de DACE podrá verificarse por la PJE, sin duda, mediante el acceso a los datos conservados por las operadoras por las evidentes exigencias de su gestión interna[1070], todo ello bajo un régimen jurídico general de colaboración con la Justicia análogo al propugnado en España por el art. 118 CE; y, en segundo lugar, porque no parece apoyarse en estudios comparativos que muestren hasta qué punto fueron eficientes o ineficientes esas jurisdicciones en resolver casos criminales sin acudir a semejante recurso o, dicho de otra manera, ver dónde fracasaron por no contar con tan sensible información, si es que realmente no fueron capaces de accederla por no existir en la realidad (cosa absolutamente dudosa)[1071,1072].

Sobre estas consideraciones, a mi juicio, ha de alzarse un nuevo y esperanzador punto de vista, que ofrece respuesta a una de las ideas más importantes de cuantas puedan aportarse a este trabajo y que se deriva del hecho de que, por fin, sobre una materia tan controvertida, que además afecta a los derechos fundamentales de millones de ciudadanos de la UE, se introduzca derecho positivo para llenarla de legalidad y así conseguir reducir los indeseables márgenes de indeterminación,

---

[1069] Hasta considerar el garantista *Bundesverfassungsgericht* como un paradigma deseable para los demás países miembros.

[1070] La DCD no ha inventado nada, pues los datos de las operadoras, sean de naturaleza técnica (registro de llamadas entrantes o salientes, la duración, la BTS que presta servicio, etc.) o logística (los datos de facturación, como la identificación del cliente, cuenta bancaria, domicilio, etc.) siempre han sido gestionados con toda eficiencia por las operadoras por razones de lógica empresarial que se hace ocioso comentar. De un modo general, esta circunstancia es recogida en el *Informe de evaluación sobre la Directiva de conservación...doc. cit., p*to. 3.1.

[1071] Hasta donde alcanzo a saber, los alemanes compensan la falta de datos conservados con los que entregan las operadoras por el deber de colaboración con la Justicia ante el requirimiento del Juez o Fiscal de turno.

[1072] No obstante, se recogen algunos ejemplos inquietantes como el que se describe a continuación: *"A escala de la UE, la eficacia de la Operación Rescate (bajo los auspicios de Europol) para la protección de menores contra abusos se vio perjudicada porque la falta de legislación de transposición en materia de conservación de datos impidió a ciertos Estados miembros investigar a miembros de una gran red de pederastas internacional utilizando direcciones IP con una antigüedad de hasta un año"*. Vid. *Informe de evaluación sobre la Directiva de conservación...doc. cit., p*to. 5.4.

inseguridad y riesgos jurídicos[1073,1074], con que se habrían intervenido los DACE hasta la entrada en vigor de la legislación transpuesta de la DCD bajo los imperativos genéricos de colaboración con la Justicia. Sólo restaría, por tanto, mejorarla. Nada más.

La anterior es, precisamente, una de las reclamaciones más insistentes de la PJE: saber a qué atenerse en el ejercicio de sus funciones, saber qué esperar de una determinada fuente de prueba, conocer cómo accederla y cuáles serán sus límites y, en definitiva, tener una expectativa sobre lo que dará de sí una progresión sobre los DACE para el éxito de la investigación.

Sea como fuere, bienvenida sea una revisión que se oriente a lograr el equilibrio entre los conceptos de seguridad y libertad, tan debatidos en las sociedades que se distinguen por su exquisito respeto a los derechos fundamentales, lo que exigirá, sin duda, un sano ejercicio por el que se liberen algunos prejuicios y complejos y se estudie con rigor cómo ha de ser el resultado final y perdurable de la norma.

A los anteriores efectos, este estudio pretende arrojar alguna luz sobre el particular de modo que sus propuestas – que procurarán ser lo más eficientes y lo menos intrusivas – contribuyan, de ser factibles, a lograr tan ansiado equilibrio, en el que la función de la PJE la constituye en uno de sus actores principales.

En los años en que la PJE ha podido disponer racionalmente de una ínfima parte de los DACE conservados por los sujetos obligados por la LCDCE – y bajo un estricto control jurisdiccional -, aún con todas las dificultades y problemas con que se

---

[1073] Si se atienden las cifras apabullantes de dispositivos de comunicación en manos de los ciudadanos, de los miles de millones de comunicaciones diarias de todo tipo y de los ingentes DACE que generan, podrá colegirse que la cantidad accedida en el marco de los diferentes procesos penales a lo largo de la UE será, sencillamente, ridícula. Además, y lo que es más importante, se accede bajo un estricto control de jurisdiccionalidad firmemente establecido en una Ley, mejor o peor armonizada, donde se ponen los más exactos límites a esta función, comenzando por requerir un juicio de proporcionalidad previo a su cesión a los agentes facultados.

[1074] En el propio documento de evaluación de la DCD se reconoce la urgencia de legislar, entre otras cosas, porque la inseguridad sobrevenida con las TIC, propiciaba algunos desajustes *"tales como la proliferación de tarifas planas, servicios de comunicaciones electrónicas de prepago o gratuitos, [que] tuvieron como efecto que los operadores dejaron gradualmente de almacenar datos de tráfico y de localización con fines de facturación, reduciendo así la disponibilidad de dichos datos a efectos de la justicia penal y con fines policiales […]. Los atentados terroristas de Madrid en 2004 y de Londres en 2005 añadieron urgencia a los debates a nivel de la UE sobre la forma de abordar estas cuestiones".* Adviértase en este fragmento, por otro lado, la invocación al derecho penal de lucha que contiene y que evidencia una necesidad insoslayable de actuar mediante al dotación de instrumentos jurídicos y tecnológicos adecuados. Vid. *Informe de evaluación sobre la Directiva de conservación...doc. cit., p*to. 3.2.

ha tropezado, la experiencia práctica policial es excepcional, lo que sin duda se ha reflejado en el éxito del proceso penal.

Puede decirse, sin temor a equivocarse, que esta sensible información sobre los DACE – sin dejar de valorar el sacrificio cuya conservación haya supuesto para los derechos de los ciudadanos – ha sido crucial y, en la mayoría de las veces, decisiva hasta el punto de llegar incluso a convertirse en la única fuente de prueba[1075] y, en la mayoría de las ocasiones, sin asomo de duda, determinante para la resolución de toda clase de graves hechos delictivos.

b) Base jurídica de la DCD

La Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo de 2006, *sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE* (DCD)[1076] contiene las siguientes previsiones en sus considerandos:

El respeto al acervo europeo en materia de protección de datos, cuya primeras normas referenciadas se hallan en la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, *relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos*[1077] (cuya transposición al derecho interno se encuentra en la Ley Orgánica

[1075] Un simple dato de localización espacio-temporal de un teléfono móvil respecto de determinados elementos de hecho ha supuesto, en numerosas ocasiones, la iniciación de toda una investigación, con la seguridad de que los indicios que permitieron a la Autoridad Judicial considerar la proporcionalidad de su cesión de la operadora a la PJE, se orientan al completo esclarecimiento de los hechos.

[1076] Sobre los antecedentes en el derecho europeo de la obligación de conservación de datos, de cuya transposición se ocupa la LCDCE *"con una inusitada predisposición al literalismo"*, se hace indispensable la lectura de Rodríguez Lainz, José Luis. *El principio de proporcionalidad…op. cit.*

[1077] Aunque no es de aplicación a la seguridad pública, la defensa o la seguridad del Estado, tiene como objetivo proteger los derechos y las libertades de las personas en lo que respecta al tratamiento de datos personales, estableciendo principios de orientación para determinar la licitud de dicho tratamiento e intentando armonizar las legislaciones de los países miembros. Cimentada en los más altos valores democráticos de la UE, según su considerando primero, para *"lograr una unión cada vez más estrecha entre los pueblos europeos, establecer relaciones más estrechas entre los Estados miembros de la Comunidad, asegurar, mediante una acción común, el progreso económico y social, eliminando las barreras que dividen Europa, fomentar la continua mejora de las condiciones de vida de*

15/1999, de 13 de diciembre, *de Protección de Datos de Carácter Personal*, donde de forma más escueta se dice en el art. 3.a) LOPD que son datos personales *"cualquier información concerniente a personas físicas identificadas o identificables"*[1078]) y, en materia de los que produzcan en el ámbito de las comunicaciones electrónicas, en la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, *relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas* (Directiva sobre la privacidad y las comunicaciones electrónicas).

Respecto del ejercicio de las facultades anticipadas en el art. 15 de la Directiva 2002/58/CE, se abre la puerta a legislar sobre la conservación de DACE, con vocación de armonizar las dispares legislaciones de los países miembros, con una clara y directa invocación al principio de proporcionalidad[1079], ya que se podrá hacer siempre que *"tales restricciones [constituyan] medidas necesarias, apropiadas y proporcionadas en una sociedad democrática para fines específicos de orden público, como proteger la seguridad nacional (es decir, la seguridad del Estado), la defensa, la seguridad pública, o la prevención, investigación, detección y enjuiciamiento de delitos o la utilización no autorizada del sistema de comunicaciones electrónicas"*.

c)Ámbito objetivo y subjetivo

sus pueblos, preservar y consolidar la paz y la libertad y promover la democracia, basándose en los derechos fundamentales reconocidos en las constituciones y leyes de los Estados miembros y en el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales" y, como se indica en el considerando décimo, *"particularmente del derecho al respeto de la vida privada reconocido en el artículo 8 del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales"*.

[1078] En el desarrollo reglamentario de esta Ley, dado mediante el Real Decreto 1720/2007, de 21 de diciembre, *por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal*, se especifica algo más sobre el concepto, estableciendo en su art. 5.1.f que son datos de carácter personal *"cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables* (según el art. 3.1.o RLOP, es identificable *"toda persona cuya identidad pueda determinarse, directa o indirectamente, mediante cualquier información referida a su identidad física, fisiológica, psíquica, económica, cultural o social. Una persona física no se considerará identificable si dicha identificación requiere plazos o actividades desproporcionados"*).

[1079] En consonancia con el art. 8 CEDH.

El ámbito objetivo de aplicación queda restringido a *"los datos generados o tratados, en el marco de la prestación de servicios de comunicaciones, por proveedores de servicios de comunicaciones electrónicas de acceso público o de una red pública de comunicaciones"* con prohibición absoluta de acceder o conservar el contenido material de las comunicaciones electrónicas, lo que, en términos de la LCDCE, se ha centrado en la conservación de los datos de tráfico, localización e identificación asociados a las comunicaciones electrónicas.

A los efectos del párrafo anterior, es particularmente interesante que, según se dice en el considerando decimotercero de la DCD sobre los sujetos obligados, "*en lo referente a la conservación de datos relativos a los correos electrónicos y la telefonía por Internet, la obligación de conservar datos sólo puede aplicarse con respecto a los datos de los servicios propios de los proveedores o de los proveedores de redes".* Es decir que, de lo comunicado haciendo uso de los servicios de un ISP para la conformación del mensaje, sólo se conservarían los DACE de su paso por las redes públicas de comunicaciones, según la constancia que tuvieren de ello los operadores de tales redes[1080]. Nada de esto afecta, por tanto, a los DACE generados internamente por los ISP, que no tendrán obligación alguna de conservación[1081].

Los DACE, según la directiva, se deben ceder, sin más precisión, "*a las autoridades nacionales competentes de conformidad con la legislación nacional, respetando plenamente los derechos fundamentales de las personas afectadas",* añadiendo *"[y que] se derivan de tradiciones constitucionales comunes de los Estados miembros y están garantizados por el CEDH*". Esta consideración, en el caso de España, se traduce en forma de estricta y garantista reserva jurisdiccional *ex* art. 1.1 y de una

[1080] El valor de los DACE en este caso es tan pobre que, por ejemplo, un acceso de *VoIP* a través de una línea particular ADSL sólo reflejaría el dato de la IP del acceso genérico a Internet. Caso de no apagarse el router Wi-FI, el dato de la IP sería siempre el mismo – o variado unilateral y arbitrariamente por el prestador por razones de índole técnico – pero, eso sí, con independencia de cada uso particular que se haga de esta importante prestación de las TIC. Por no accederse a los datos de los ISP se perderían toda los DACE correspondientes al historial de navegación, lo que incluiría también toda la cadena de servicios subyacentes consultados. Esto evidencia la radical necesidad de contar con los DACE de los ISP – los *logs* – para lograr una identificación plena de la transacción telemática, útil para las finalidades reales de la práctica de la prueba en el marco del proceso penal.

[1081] Así se indica en el considerando vigesimotercero de la DCD: "*Siempre que dichos datos [los DACE] no hayan sido generados o tratados por dichos proveedores, no es obligatorio conservarlos".*

exclusión del Ministerio Fiscal debida a la estricta vinculación de la LCDCE al derecho al secreto de las comunicaciones del art. 18.3 CE.

En el articulado de la directiva, lo más interesante que se precisa es lo siguiente:

El ámbito objetivo se centra en *"los datos de tráfico, localización e identificación"* (art. 1.2) – que deberán estar listos para *"transmitirse sin demora a las autoridades competentes que así lo soliciten* (art. 8) - y, el subjetivo, en "*los proveedores de servicios de comunicaciones electrónicas de acceso público o de una red pública de comunicaciones"* (arts. 1.1 y 3.1) y con reserva de aplicación a los *"fines de investigación, detección y enjuiciamiento de delitos graves, tal como se definen en la legislación nacional de cada Estado miembro"* (art. 1.1).

Sin embargo, se constata que existen datos (no contemplados en el art. 5) que actualmente no son objeto de conservación, como los de cobertura, o que, sencillamente, no entran dentro del ámbito objetivo de aplicación de la DCD, como los que producen los ISP en relación con su participación en los servicios de comunicaciones electrónicas que prestan (los *logs*).

d) El periodo de conservación

En lo referido al periodo de conservación, la DCD, *ex* art. 5, permite un margen entre los seis meses y los dos años, habiéndose optado en la LCDCE por ordenar la conservación únicamente por un año. No obstante, el periodo objetivo de conservación puede ampliarse por los estados de una forma justificada según las facultades otorgadas por el art. 12.

En el art. 7 d) se establece una cláusula de eliminación de los datos a la finalización del periodo legal de conservación, exceptuándose aquellos que hayan sido objeto de cesión a la autoridad competente, lo que se deduce del siguiente texto: *"Los datos, excepto los que hayan sido accesibles y se hayan conservado, se destruirán al término del período de conservación".*

Una previsión particularmente importante al respecto es la contenida en el art. 14.1, orientada a valorar el "*impacto en operadores económicos y consumidores, teniendo en cuenta los avances en la tecnología de las comunicaciones electrónicas y las estadísticas proporcionadas a la Comisión de conformidad con el artículo 10 a fin de determinar si es necesario modificar las disposiciones de la presente Directiva, en particular por lo que se refiere a la lista de datos del artículo 5 y a los períodos de conservación establecidos en el artículo 6. Los resultados de esta evaluación se harán públicos*".

Sería de desear que este espíritu de adaptación, no sólo a la realidad tecnológica, sino a la misma realidad social, sirva para dar acogida a las propuestas que, vista la experiencia, se contienen en este estudio, ahí donde sea razonable y admisible en Derecho.

2. Evaluación de la Directiva 2006/24/CE

a) Cumplimiento del deber de evaluación

En cumplimiento al art. 14 de la DCD, y con el propósito de comprobar la *"aplicación por parte de los Estados miembros y su impacto en operadores económicos y consumidores, teniendo en cuenta los avances en la tecnología de las comunicaciones electrónicas y las estadísticas proporcionadas a la Comisión, a fin de determinar si es necesario modificar las disposiciones de la misma, en particular por lo que se refiere a la lista de datos y a los períodos de conservación"*, la Comisión redactó un informe de situación[1082], cuya más llamativa conclusión es la falta de armonización real de las legislaciones transpuestas, teniendo en cuenta, además, los países cuyos respectivos tribunales constitucionales impidieron la transposición o, más simplemente, la tenían pendiente a la hora de su evaluación.

[1082] *Ibídem.* Vid. *Informe de evaluación sobre la Directiva de conservación...doc. cit.*

Consecuentemente, las disparidades – que ya comienzan con los problemas en la disponibilidad de datos estadísticos homogéneos *ex* art. 10 DCD -, pese a los avances observados, arrojan un poco alentador resultado no exento de inseguridades jurídicas, al menos en materia de cooperación policial y judicial entre los países miembros.

Estas disparidades se centran en materias tan sensibles como las limitaciones temporales de conservación[1083], sus finalidades[1084], las autoridades que pueden acceder a los datos, la necesidad o no de mandato judicial previo o, más prosaicamente, la imputación de los costes de la implementación técnica[1085].

b) Disparidades en el ámbito objetivo y subjetivo

Sobre el ámbito objetivo, se ha detectado que existen países en que las pequeñas operadoras han quedado exentas de la obligación de conservar DACE por la desproporción de los costes y el escaso interés para la función policial o judicial[1086] lo que, en mi opinión, no habrá tardado en ser conocido por los delincuentes.

Otro aspecto interesante lo representa el hecho de la externalización de los servicios técnicos de conservación, que comporta importantes connotaciones, tanto sobre el capítulo de la seguridad material y jurídica que pueda suponer este tipo de servicios de naturaleza estrictamente empresarial, como por lo sugerente de la idea en cuanto a la viabilidad de un posible órgano del Estado que, asumiendo las cargas económicas y tecnológicas, y quedando garantizada la seguridad jurídica mediante un

[1083] En el informe se proclama, como vía alternativa, *"con vistas a cumplir el principio de proporcionalidad, y a la luz de la información cuantitativa y cualitativa sobre el valor de los datos conservados en los Estados miembros, y de la evolución de las comunicaciones y tecnologías y de la delincuencia y el terrorismo, la Comisión estudiará la aplicación de diferentes períodos para diferentes categorías de datos, para las distintas categorías de delitos graves o una combinación de ambos".* Este proceder, en mi opinión, acabará generando arbitrariedades y lagunas jurídicas que entorpecerán el acceso a los DACE.

[1084] Además, no siempre relacionada directamente con la controvertida referencia a la gravedad de los delitos en cuanto a su retribución penológica, para llegar a cuestiones no contempladas en la DCD como el riesgo para la vida y la integridad física

[1085] La opción de la UE tiende al reembolso de los costes.

[1086] Finlandia y Reino Unido, con la consiguiente pérdida de efectividad policial.

Juez de Garantías, gestionase neutral y horizontalmente la conservación de los DACE del conjunto de las operadoras en todo su territorio de soberanía[1087].

Pero la trascendencia de estas inseguridades no se agota en ellas mismas, sino que como se reconoce en el informe, *"esta situación podría no ofrecer la previsibilidad suficiente, que constituye un requisito para cualquier medida legislativa que restrinja el derecho a la intimidad* "[1088], déficit democrático que, de producirse, plantearía un serio problema de legalidad, muy difícil de afrontar en relación con la exigente tutela efectiva de los derechos fundamentales en el ámbito de la UE proclamada en el CEDH y en conjunto del acervo comunitario[1089].

c)Insuficiencias en materia de cooperación policial y judicial

Podría anotarse también un fracaso en la cuestión de la cooperación policial y judicial – siempre de un valor crucial para éxito de las investigaciones - en materia de solicitudes de acceso a los DACE conservados en el ámbito de los países miembros de la UE. Estas solicitudes son en número muy escasas, pero no por su falta de interés para las respectivas investigaciones, al contrario, sino por los obstáculos producidos, precisamente, por las disparidades ya mencionadas, a las que han de unirse las deducidas de la necesidad de cursar farragosas comisiones rogatorias internacionales – de incierta fortuna y peor oportunidad -, así como por la inaplicabilidad de la Decisión Marco 2006/960/JAI del Consejo sobre *la simplificación del intercambio de información e inteligencia entre los servicios de seguridad de los Estados miembros de la Unión*

[1087] Para lo que, en consonancia con al posición del informe comentado en cuanto a la seguridad de los datos, deberá *tener "en cuenta las recomendaciones efectuadas en el informe relativo a la segunda acción común de control y ejecución por el Grupo de Trabajo del Artículo 29 sobre protección de datos, en el sentido de adoptar normas mínimas y medidas salvaguardia y de seguridad técnica y organizativa"*. Vid. Dictamen 3/2006 del Grupo de Trabajo del Artículo 29*…doc.cit*.

[1088] El informe basa esta apreciación en la "*Sentencia del Tribunal de Justicia de la Unión Europea de 20 de mayo de 2003, en los asuntos acumulados C-465/00, C-138/01 y C-139/01 (Petición de decisión prejudicial: Verfassungsgerichtshof y Oberster Gerichtshof): Rechnungshof (C-465/00) contra Österreichischer Rundfunk y otros, y entre Christa Neukomm (C-138/01), Joseph Lauermann (C-139/01) y Österreichischer Rundfunk (Protección de las personas físicas en lo que respecta al tratamiento de datos personales - Directiva 95/46/CE - Protección de la intimidad - Divulgación de datos sobre los ingresos de empleados de entidades sujetas al control del Rechnungshof)".*

[1089] *Ibídem.*

Europea, al tratarse de informaciones obtenidas por medios coercitivos, lo que supone un importante obstáculo para la debida diligencia con que se ha de disponer de tan decisiva y, a la vez, sensible evidencia[1090].

En este ámbito, debe consolidarse un nivel de confianza y efectividad en materia de cooperación policial y judicial de la mayor calidad posible, haciendo que el intercambio de inteligencia en el marco del proceso penal de cada país miembro sea una realidad tangible y no víctima del fárrago e ineficiencias burocráticas de los respectivos sistemas judiciales.

Es necesario, por tanto, contar con un instrumento jurídico específico de cooperación policial y judicial a nivel de la UE, que garantice la ejecución eficiente de las decisiones de acceso a los DACE, según la regulación de la DCD y de acuerdo con el principio de reconocimiento mútuo de las decisiones judiciales y orientado a garantizar su intercambio eficaz por los canales telemáticos seguros que sea preciso instaurar.

d) Valor de los datos para la investigación criminal

Sin duda, lo que sí está perfectamente armonizado es el extraordinario valor que las agencias europeas de policía y aduaneras otorgan a la disponibilidad eficiente de los DACE conservados, que consideran indispensables para la fortuna de las investigaciones.

A los efectos, en primer lugar, los DACE son positivamente valorados en cuanto su utilidad como orientativos del progreso de las indagaciones, es decir, en su mero valor instrumental para establecer o refutar hipótesis policiales, verificar coartadas, incluir o excluir objetivos, identificar testigos, determinar lugares relacionados con la acción criminal, localizar medios de resarcimiento de las víctimas, etc.

[1090] Decisión marco 2006/960/JAI del Consejo, de 18 de diciembre de 2006, *sobre la simplificación del intercambio de información e inteligencia entre los servicios de seguridad de los Estados miembros de la Unión Europea*, DO L 386 de 29.12.2006, pp. 89-100 y DO L 200 de 1.8.2007, pp. 637-648.

En segundo lugar, pueden actuar como primera evidencia o fuente de prueba en aquellos casos en que no se tenga al alcance otro indicio material de la participación en determinados hechos delictivos[1091].

En tercer lugar, aunque no existe una referencia estadística fiable al respecto[1092], la posible prueba fundada en los DACE, hechas todas las salvedades sobre la calidad de los datos, tiene la virtud de su originaria objetividad tecnológica ante al proceso penal. Pero, aunque en sí misma raramente tendrá relevancia procesal como prueba, sí parece evidente que, integrada con otros elementos de prueba e indicios, devendrá con cierta solvencia en un medio de prueba procesalmente eficiente y digno de ser objeto de contradicción en el acto de juicio oral, contribuyendo valiosamente a la formación de la opinión jurisdiccional.

En todos estos casos, el establecimiento de vínculos de llamadas entre personas, el hecho de su presencia en determinados lugares de interés o el uso de determinados accesos IP, suponen una inestimable referencia que permite la reconstrucción fiable de los hechos, la localización e incautación de evidencias o, más simplemente, la estructuración de la investigación mediante una dinámica de comprobación/refutación de hipótesis.

De cualquier modo, reiterando una opinión personal ya comentada, lo excelente y alentador de lo observado durante el periodo de vigencia de la DCD y de su legislación transpuesta es que, por fortuna y para bien, se ha legislado con relativo acierto. Seguir como se estaba, es decir, bajo el peso de una gran incertidumbre e inseguridad jurídicas asociada a la ausencia de derecho positivo significaba no avanzar en el legítimo ejercicio de la limitación de los derechos fundamentales..

[1091] Esto es particularmente visible en el enrutamiento IP, a veces con millones de datos, lo que supone un imprescindible recurso, no ya para la investigación, sino para la prevención de complejas maquinaciones criminales en el ámbito de la ciberdelincuencia.

[1092] Adviértase la aparente inaccesibilidad a los registros judiciales, lo que conlleva la correspondiente carga de ineficiencia para saber, desde un punto de vista meramente estadístico, hasta qué punto los DACE fueron útiles, en una medida u otra, como medio de prueba procesalmente apta e incluso determinante para la formación de la decisión jurisdiccional.

e) Otros aspectos controvertidos de la DCD

Considero necesario introducir en este apartado un párrafo literal sobre las reflexiones del informe de evaluación de la DCD que servirán de referencia, en mi opinión no siempre positiva, sobre cómo debiera ser, en términos de proporcionalidad, de la vida futura de la DCD:

"La Comisión velará por que cualquier propuesta futura sobre conservación de datos respete el principio de proporcionalidad y sea adecuada para lograr el objetivo de la lucha contra el terrorismo y los delitos graves y no vaya más allá de lo que sea necesario para lograrlo. Reconocerá que las excepciones o limitaciones en lo que respecta a la protección de los datos personales sólo se aplicarán en la medida en que sean necesarias. Evaluará cuidadosamente las implicaciones para la eficacia y eficiencia del sistema de justicia penal y para la aplicación de la ley, para la intimidad y para los costes de la administración pública y los operadores, de una regulación más estricta de la conservación, el acceso y el uso de los datos de tráfico. En la evaluación de impacto deberán examinarse los siguientes ámbitos en particular:

- *la coherencia entre la limitación de las finalidades de la conservación de datos y los tipos de delitos para los que los datos conservados puedan consultarse y utilizarse;*
- *una mayor armonización y posible reducción de los períodos obligatorios de conservación de datos;*
- *un control independiente de las solicitudes de acceso y del régimen general de acceso y de conservación de datos aplicado en todos los Estados miembros;*
- *la limitación de las autoridades autorizadas para acceder a los datos;*
- *la reducción de las categorías de datos que deben conservarse;*
- *la elaboración de orientaciones sobre las medidas de seguridad técnicas y organizativas de acceso a los datos, incluidos los procedimientos de transferencia;*
- *la elaboración de orientaciones sobre utilización de los datos, incluida la prevención de la búsqueda aleatoria de datos («data mining»); y*

- *el establecimiento de criterios de medida realistas y de procedimientos de notificación para facilitar las comparaciones sobre la aplicación y evaluación del futuro instrumento".*

Del análisis de estos pronunciamientos pueden extraerse algunas orientaciones para resolver sobre los aspectos controvertidos que se han evidenciado durante el periodo de evaluación.

En mi opinión, con carácter general, una marcada tendencia a la revisión de corte garantista no es incompatible con el reajuste de un marco jurídico eficiente y que no suponga un retroceso en la eficiencia y rendimiento de esta fuente de prueba.

Las cuestiones que merecen una reflexión pausada en este estudio, a mi juicio, son las siguientes:

En primer lugar, las finalidades de la conservación de datos no deben vincularse estrictamente a cuestiones relacionadas con la gravedad y esta, a su vez, con la retribución penológica subyacente, aun resultando este un criterio esencial como fuente de objetividad, sino en el modo amplio que se ha justificado en este estudio.

En el documento de evaluación de la DCD se dice, por otra parte, que hay *"ausencia de una definición en cualquiera de las dos Directivas [*Directiva 2002/58/CE y 2006/24/CE*] de la noción de «delito grave»"*[1093], lo que ha ocasionado sensibles diferencias de un estado a otro en la apreciación objetiva de la gravedad[1094].

Es previsible, por tanto, que, en materia de cooperación policial y judicial entre los estados miembros, se susciten cuestiones disonantes sobre la gravedad subyacente

[1093] Vid. *Informe de evaluación sobre la Directiva de conservación...doc. cit., p*to. 3.2.

[1094] *"Diez Estados miembros (Bulgaria, Estonia, Irlanda, Grecia, España, Lituania, Luxemburgo, Hungría, Países Bajos y Finlandia) han definido «delito grave» con referencia a una pena de prisión mínima, a la posibilidad de que se imponga una pena privativa de libertad o a una lista de delitos definidos en otras partes de la legislación nacional. Ocho Estados miembros (Bélgica, Dinamarca, Francia, Italia, Letonia, Polonia, Eslovaquia y Eslovenia) exigen que los datos deben conservarse no sólo para la investigación, detección y enjuiciamiento de delitos graves, sino también en relación con todos los delitos y para la prevención de la delincuencia, o por razones generales de seguridad nacional, estatal o pública. Las legislaciones de cuatro Estados miembros (Chipre, Malta, Portugal y Reino Unido) se refieren a las «formas graves de delincuencia» o «delitos graves» sin definirlos".* Vid. *Informe de evaluación sobre la Directiva de conservación...doc. cit.,* pto. 4.1.

a los hechos investigados y que deba motivar la cesión o no de determinados DACE al país requirente, con la evidente carga asociada de inseguridad jurídica[1095].

Creo que la gravedad debe ser, sin duda, un referente objetivo para formar y adoptar la decisión jurisdiccional de sacrificar los derechos fundamentales concernidos por la conservación de DACE, pero deben atenderse también la trascendencia social de las conductas, la importancia del bien jurídico protegido y el específico ámbito tecnológico donde se produce la intervención, facetas que, apreciadas de una manera conjunta, permiten la adopción de un juicio de proporcionalidad ajustado a los estándares democráticos y sociales del Estado de Derecho.

En este sentido, la referencias a listas cerradas de delitos – especialmente en ausencia de un derecho penal europeo y de la evidente existencia de realidades sociales dispares - no parecen del todo acertadas si no se acompañan de alguna cláusula que permita alguna excepcionalidad, que esté jurídicamente prevista y atendida su procedencia bajo una estricta razonabilidad. En estos casos, la tendencia parece ser a sobrevalorar determinadas conductas criminales como el terrorismo o formas muy complejas de la delincuencia organizada, sin reparar en las amenazas que suponen otros fenómenos criminales, entre los que cabe destacar, en su aparente levedad, el uso malicioso de las redes de comunicaciones electrónicas.

Por ello, el criterio fenomenológico y el sesgo tecnológico que pueda acompañar a determinadas formas comisivas, deben informar la opinión del legislador sobre la manera en que ha de interpretar la realidad social.

En segundo lugar, el meritorio interés del legislador europeo de armonizar las legislaciones de los países miembros – de una evidente y extraordinaria dificultad – debe incuestionablemente presidir cuanto se haga en mejora de la DCD. Por ello, los defectos de previsibilidad de la Ley exigidos en el acervo europeo sobre derechos fundamentales, deben conjurarse con decisión, logrando una urgente aproximación de

[1095] Por ejemplo, Luxemburgo, que opta por una referencia penológica cuantitativa en su definición, considera delito grave la "condena penal máxima de un año o más" (Artículo 1, apartado 1, de la Ley de 24 de julio de 2010.). Esta retribución es cuantitativamente menor a la española, lo que supondría un grave problema si aquel país se dirigiese al nuestro en solicitud de DACE relativos a aquellos casos cuyas penas no alcanzasen el término retributivo.

la visión jurídica en la materia que evite vicios de nulidad en las resoluciones legales de todo tipo y permita el eficente intercambio de evidencias entre los países miembros.

En tercer lugar, la cuestión – de aspecto imperativo – de rebajar los periodos de conservación de datos, como aparente remedio terapéutico que atempere la mala conciencia adquirida por la decisión de disponerla de forma masiva e indiscriminada, me parece una discusión abierta en falso y que, como previsible consecuencia, quedará cerrada, también en falso, tras reconocerse deudora de una buena dosis de hipergarantismo.

En mi opinión, la carga del supuesto conflicto sobre la decisión del legislador europeo, no gravita en los márgenes cuantitativos del tiempo de conservación previstos en el texto vigente de la DCD y los singularizados en las legislaciones transpuestas – a los que parece querer adjudicárseles alguna tacha de arbitrariedad -. Consecuentemente, nada se soluciona con salvíficos recortes sino, en todo en caso, mediante una adecuada praxis jurisdiccional en lo cualitativo, es decir, en la valoración de la proporcionalidad de acceder a determinados datos históricos que, por su antigüedad y oportunidad, deban ser desvelados si el Estado de Derecho no tiene vías alternativas para defender otros bienes jurídicos puestos en peligro y merecedores de la más alta protección.

En lo demás, pienso que las disquisiciones sobre los presumibles excesos en el señalamiento de los periodos objetivos de conservación devienen una discusión, en todo caso, menor.

Es cierto que la revisión del peso cuantitativo de los meses de conservación es un buen referente objetivo para exhibir una apuesta por la moderación frente a la opinión pública – conviene no olvidarse, en cualquier caso, que en España se optó por la mitad del tiempo previsto como máximo en la DCD, esto es, por un año de conservación -, lo que cae más del lado de la política general que del de la nececesidad de aportar soluciones jurídicas prácticas a problemas perfectamente identificados en la sociedad moderna.

Muy por el contrario, es necesario que una de las más mportantes facetas de la política, la política criminal, informe de la manera más precisa y aséptica posible sobre

cuál es la verdadera trascendencia de los límites temporales de conservación. Esta visión, por otro lado, podría ser sugerente de la necesidad, en todo caso, de progresar optando por la ponderación individualizada del sacrificio que conlleva acopiar determinados datos en el curso de una investigación en sede penal y, no tanto, hasta qué punto temporal puede retrotraerse su acceso legal.

Salvo en los países en que no se ha transpuesto la DCD, la cuestión del periodo de tiempo de conservación, habiéndose cruzado el Rubicón que supuso la decisión de conservar los DACE, no parece haber originado el más mínimo signo de desproporción más allá de las cargas materiales impuestas a las empresas operadoras sino, en todo caso, el que se hubiera producido por cualquiera de las demás causas de auténtica consistencia real, aquellas de las que pueden invocarse durante un proceso penal ordenado con criterios democráticos estrictos (como la gravedad de los delitos, la insuficiencia de la motivación, la forma de acceso a los datos, la autoridad que lo determina, etc.).

El del periodo de conservación de datos establecido en el derecho interno, de un año *ex* art. 5 LCDCE, instaura unos límites temporales objetivos para los que el Juez de Garantías, dentro del principio de proporcionalidad y en el ejercicio de sus facultades discrecionales, señala y precisa los periodos de tiempo para los cuales ordena una determinada cesión de datos a los agentes facultados.

La conservación por un año de los DACE permite a la PJE, en general, una más que razonable capacidad de maniobra para afrontar incluso las investigaciones más complejas[1096]. Por ello, en lo que se refiere a la satisfacción de las necesidades más perentorias de la investigación, si de lo que se trata, por ejemplo, es de resolver un secuestro *express* o la desaparición de una persona[1097], la necesidad de remontarse en el tiempo en los DACE de los actores de los hechos (víctimas y victimarios) no suele pasar de los tres o cuatro días anteriores al del su conocimiento. Los demás DACE que

[1096] Y no siempre para acreditar la responsabilidad penal del justiciable sino, por el contrario, para demostrar su inocencia, como se ha encargado de proclamar el documento de evaluación de la DCD, al tiempo de sumar a los aciertos de la Ley el haber protegido a las víctimas, localizado testigos, etc.

[1097] Nótese que la desaparición de una persona no tiene por qué haber sido causada por la comisión de un hecho delictivo, sino que puede ser, por ejemplo, por haberse extraviado o haber sufrido un desfallecimiento, esto es, fuera del ámbito objetivo de intervención del derecho penal.

se necesitarán serán usualmente los que la intervención de las comunicaciones ofrezca en tiempo real.

Cuando se habla de hechos delictivos relativamente comunes, cuyas maquinaciones hayan tenido algún desarrollo mayor en el tiempo, el periodo objetivo previsto en la LCDCE suele ser también suficiente para colmar las expectativas de los investigadores.

Al menos así se desprende, no sólo de la experiencia práctica policial, sino de los análisis incorporados al documento de evaluación de la DCD, en los que se refleja un uso recurrente de los tiempos medios de antigüedad de los DACE[1098].

Sin perjuicio de lo anterior, la naturaleza de las investigaciones en el mundo de la delincuencia organizada, transnacional, compleja o grave, en número cuantitivamente menor, necesitarán sin duda de la obtención de una muy eficiente IDACE, lo que normalmente demandaría a su vez, no ya el acceso a los datos conservados del último año sino, con toda seguridad, a los de años atrás si la Ley lo permitiese.

Además, es relativamente frecuente que los DACE antiguos sean la única fuente de prueba en los casos más complicados y, en muchas ocasiones, la piedra de toque a partir de la cual las investigaciones dan un espectacular vuelco que permite aventurar su éxito.

Puede decirse, en consecuencia, que se necesitan normalmente pocos datos antiguos pero que, cuando se ha de acudir a ellos, es porque se necesitan imperiosamente por no haberse encontrado vías alternativas para que la investigación progrese[1099,1100].

[1098] Sobre este asunto, en el documento de evaluación se resume estadísticamente que: *"La información cuantitativa facilitada hasta ahora por los Estados miembros en lo que respecta a la antigüedad de los datos conservados indica que, cuando los servicios con funciones coercitivas realizan la solicitud de acceso (inicial), cerca del 90 % de los datos cuentan con una antigüedad de seis meses o menos y cerca del 70 % con una de tres meses o menos".* Vid. *Informe de evaluación sobre la Directiva de conservación...doc. cit., p*to. 4.5.

[1099] Un ejemplo lo constituye el caso de la desaparición del niño Yéremi (ocurrida en las Islas Canarias en el mes de marzo de 2007) que, aunque no se ha podido esclarecer hasta el momento (año 2012), gracias a la información de los repetidores del lugar de los hechos y al análisis del tráfico llamadas entrantes y salientes se pudo descartar a multitud de sospechosos y establecer nuevas hipótesis. Asimismo, esta metodología sirvió indirectamente para identificar y detener a 12 presuntos pederastas

Sobre esto, reflejando además los problemas relacionados con el riesgo de demora y las deficiencias prácticas en materia de cooperación policial y judicial internacional[1101,1102], la conclusión del informe de evaluación de la DCD no puede ser más contundente y clarificadora:

> "*Según la mayoría de los Estados miembros, el uso de los datos conservados con una antigüedad mayor de tres e incluso seis meses es menos frecuente, pero puede ser de crucial importancia; su uso tiende a dividirse en tres categorías. En primer lugar, los datos de Internet suelen solicitarse después*

---

en el transcurso de la indagación. La investigación pone en cuestión los rígidos periodos legales de conservación de datos ya que, al alargarse las pesquisas y aparecer insospechadas vías de progresión, a veces sobre sugerentes indicios, no se pudo acudir a los DACE sobre las comunicaciones de los nuevos objetivos por haber excedido el tiempo de conservación, lo que, sin duda, hubiera permitido sostener la dinámica investigativa de confirmación-refutación imprescindible para la resolución del caso.

[1100] Otro ejemplo sería el representado por la OP. CORBETA, sobre determinadas formas de la delincuencia económica, ya que, durante la vida de este tipo de investigaciones, centradas principalmente en las defraudaciones del IVA, las actuaciones se dirigen principalmente en determinar quién es el verdadero responsable del fraude (agente económico de hecho que se aprovecha impunemente del delito) y que manipula desde la sombra a los testaferros (agentes económicos de derecho que sufren las consecuencias del delito). Por ello, es necesario comprobar las direcciones IP de acceso telemático para el cumplimiento instrumental de determinadas obligaciones fiscales, como por ejemplo las declaraciones trimestrales de IVA, o la gestión de las cuentas de banca electrónica vía Internet, todo ello para determinar quién realmente los lleva a cabo. El *modus operandi* típico de la delincuencia económica se basa, por otra parte, en la sucesiva renovación de las estructuras mercantiles fraudulentas, a activar a la finalización de los periodos anuales de regularización de las obligaciones fiscales, para evitar de esta forma la perseguibilidad de los infractores. La gestión mercantil, la de la fiscalidad y la del producto económico de la defraudación suele hacerse por vía telemática, lo que permite la identificación del verdadero autor de los fraudes, el descubrimiento de nuevas redes de testaferros y el resarcimiento final de la hacienda pública afectada mediante las acciones investigativas de afianzamiento del patrimonio evadido y de los actos de blanqueo de capitales. Persiste además la necesidad genérica de obtener los demás DACE de los actores involucrados en el delito en la escena internacional. Nótese además, en relación con al insuficiencia de los periodos de conservación de datos que, en relación al *modus operandi,* se hace imprescindible contar con un histórico de IP que permitan la determinación de las sucesivas tramas en relación con el periodo de prescripción de las obligaciones fiscales (cinco años). Este tipo de usos comunicativos responden al esquema persona a máquina.

[1101] El documento de evaluación advierte de la desconfianza nacida, tanto del riesgo de demora, como de la complejidad de los procedimientos judiciales en la escena internacional, así como de la gran inseguridad jurídica sobre su resultado y oportunidad. A ello se suma la imposibilidad jurídica de acudir a los instrumentos de intercambio de información, como la Decisión Marco 2006/960/JAI del Consejo, de 18 de diciembre de 2006, *sobre la simplificación del intercambio de información e inteligencia entre los servicios de seguridad de los Estados miembros de la Unión Europea*, por tratarse de un instrumento accesible sólo si no han mediado medidas coercitivas en la recopilación de la información, como es el caso de lo previsto en la DCD y la legislación transpuesta. Vid. *Informe de evaluación sobre la Directiva de conservación...doc. cit., p*to. 5.3.

[1102] La disparidad de la legislación transpuesta alcanza también a la cuestión de la reserva judicial, ya que, como se indica en el documento de evaluación de la DCD, *"once Estados miembros exigen una autorización judicial para cada solicitud de acceso a los datos conservados. En tres Estados miembros se requiere autorización judicial en la mayoría de los casos. Otros cuatro exigen la autorización de una autoridad de alto nivel, pero no de un Juez. En dos, la única condición es que la solicitud se presente por escrito".* Vid. *Informe de evaluación sobre la Directiva de conservación...doc. cit., p*to. 4.3.

de otras formas de prueba en el curso de las investigaciones penales. El análisis de los datos de telefonía móvil y fija genera a menudo posibles pistas que conducen a la solicitud de datos más antiguos. Por ejemplo, si durante una investigación se descubre un nombre gracias a los datos de telefonía móvil o de red fija, los investigadores pueden querer identificar la dirección del Protocolo de Internet (IP) que dicha persona ha estado utilizando y pueden querer identificar con quien ha estado en contacto durante un período de tiempo determinado utilizando esa dirección IP. En tal caso, es probable que los investigadores soliciten datos que les permitan rastrear también las comunicaciones con otras direcciones IP y la identidad de las personas que han utilizado esas direcciones IP.

En segundo lugar, las investigaciones de delitos particularmente graves, de una serie de delitos, de la delincuencia organizada y de atentados terroristas tienden a basarse en datos conservados más antiguos que reflejen el tiempo que se necesita para planificar estos delitos, a fin de identificar las pautas de comportamiento criminal y las relaciones entre los cómplices de un delito, y establecer la intencionalidad delictiva. Las actividades relacionadas con los delitos financieros complejos no se detectan a menudo hasta pasados varios meses. En tercer lugar, y excepcionalmente, los Estados miembros han solicitado datos de tráfico conservados en otro Estado miembro, que generalmente sólo pueden comunicarse previa autorización judicial en respuesta a una comisión rogatoria cursada por un Juez del Estado miembro solicitante. Este tipo de asistencia judicial puede ser un proceso muy largo, lo que explica por qué algunos datos solicitados tienen en estos casos una antigüedad superior a seis meses".

Todas estas experiencias permiten la discusión sobre la necesidad, no de la rebaja de los límites temporales objetivos sino, muy por el contrario, la de sopesar la posibilidad de, al menos, llevarlos a sus hitos superiores.

No es descartable, de otro lado, la teórica posibilidad de establecer unos límites incluso superiores a los fijados en el art. 6 DCD[1103], como lo permite, bajo determinadas circunstancias, el art. 12 DCD, para lo cual podría ser muy útil introducir criterios de especialidad criminológica que aconsejasen modular los tiempos previstos en el art. 5 LCDCE, particularmente para afrontar fenómenos graves de delincuencia o en aquellos en que se produzca un abuso criminal las TIC, tanto como elemento de concertación y apoyo del *iter criminis* o como finalidad delictiva en sí misma. De ser así, uno de los beneficios podría ser el de establecerse rangos de conservación menores para el común de los ciudadanos y más duraderos según los criterios de naturaleza criminológica planteados, atendida la proporcionalidad de esta medida según un desarrollo de *lege ferenda*.

En cuarto lugar, efectivamente, es absolutamente necesario contar con una autoridad independiente que garantice la proporcionalidad delos accesos a los datos y, dicho sea de paso, asistida por los medios necesarios para que esta tarea se adapte dinámicamente a las necesidades de las investigaciones.

Resulta incongruente invocar la necesidad de limitar las autoridades que pueden acceder a los datos pues, de la simple lectura de los listados incluidos en el informe, no se aprecia el más mínimo cuerpo extraño que deba ser excluido, por variopintos que parezcan.

El cuanto al señalamiento de tales autoridades, las legislaciones nacionales han confiado a diversos organismos o instituciones que, en el caso de España, se han centrado, en lo que se refiere al levantamiento del secreto, a la Autoridad Judicial, con tácita exclusión del Ministerio Fiscal, y en cuanto a la Autoridad de Control, a la Agencia de Protección de Datos.

Sobre la falta de habilitación legal del Fiscal como autoridad reconocida en la LCDCE, MAEZTU referencia el Acuerdo del Tribunal Supremo, adoptado el 23 de

[1103] *"Los Estados miembros están obligados a garantizar que las categorías de datos mencionados en el artículo 5 se conserven por un período de tiempo que no sea inferior a seis meses ni superior a dos años. Todo Estado miembro que «deba hacer frente a circunstancias especiales que justifiquen una ampliación limitada del período máximo de conservación» podrá ampliar el período máximo de conservación; dicha ampliación deberá notificarse a la Comisión, que podrá decidir, en el plazo de seis meses a partir de la notificación, si aprobar o rechazar la ampliación. Si bien el período de conservación máximo puede ampliarse, no hay ninguna disposición que prevea su reducción a menos de seis meses".* Vid. *Informe de evaluación sobre la Directiva de conservación...doc. cit., p*to. 4.5.

febrero de 2010, en una Sala General no Jurisdiccional, donde se establece que *"es necesaria la autorización judicial para que los operadores que prestan servicios de comunicaciones electrónicas o de redes públicas de comunicaciones cedan los datos generados o tratados por tal motivo. Por lo cual, el Ministerio Fiscal precisará de tal autorización para obtener de los operadores los datos conservados que se especifican en el art. 3 de la Ley 25/2007, de 18 de octubre".*

Estoy de acuerdo con este autor en lamentar que la Ley no haya habilitado al Ministerio Fiscal para que pueda requerir los datos objeto de la LCDCE – y que hay atribuir a la lógica de la radical ligazón que establece con el derecho al secreto de las comunicaciones y a la diáfana claridad con que se ha impuesto la reserva jurisidiccional -, y que sería necesario corregir si fuese posible vincularla de alguna forma con el derecho a la protección de datos, ya que esta injustificable omisión no se compadece con la posición que el Fiscal tiene o debiera tener en el proceso penal[1104]. No obstante, no comparto que, como modo de manifestar esta insuficiencia, el autor considere que *"se ha equiparado la Fiscalía a los agentes autorizados [o facultados, con mayor precisión jurídica]"*, pues son instituciones netamente distintas en razón de sus facultades y de su papel en el proceso penal[1105].

En mi opinión, las garantías sobre el uso restringido de las facultades de acceso a los datos conservados no se deben fundamentar en exclusiva en el papel de las anteriores autoridades, sino, de forma bien ponderada, deben extenderse a un equilibrado conjunto de medidas basadas en la proporcionalidad, en el que deben participar también los demás operadores jurídicos, la propia PJE e, incluso, los sujetos obligados, junto con la implementación accesoria de las correspondientes salvaguardas tecnológicas que faciliten el más adecuado control jurisdiccional material. En este proceso debe contemplarse además un régimen de acceso para intervenir ante situaciones críticas.

Sobre la cuestión de las salvaguardas, no obstante lo dicho sobre la aplicabilidad a la cuestión policial y judicial de la Directiva 1995/46/CE, el SEPD[1106], en

[1104] Y que, como apunta RODRÍGUEZ LAINZ, sí tuvo con la redacción del derogado art. 12 LSSI. Vid. Rodríguez Lainz, José Luis. *El principio de proporcionalidad…op. cit.*
[1105] Vid. Maeztu Lacalle, David. *La identificación del titular…op. cit.*, pág. 257.
[1106] Vid. http://europa.eu/about-eu/institutions-bodies/edps/index_es.htm.

un dictamen sobre el estado de protección de datos orientado a conseguir un marco armonizado y eficaz de protección de datos entre los países miembros de la UE, concluye en el pto. 179 que un *"un instrumento global que incluya el ámbito policial y judicial permite normas especiales que tienen debidamente en cuenta las especificidades de este sector, con arreglo a la Declaración 21 anexa al Tratado de Lisboa. Deben aplicarse salvaguardias específicas para compensar al interesado, concediéndole una protección complementaria en un ámbito en que el tratamiento de datos personales puede ser más invasivo de la intimidad"* [1107,1108].

Ello es debido a que, en su opinión, recogida en el pto. 170, *"las disposiciones relativas a la protección de datos deben ofrecer, en la medida de lo posible, un apoyo activo en lugar de obstaculizar otros intereses legítimos (como la economía europea, la seguridad de las personas y la responsabilidad de los gobiernos)".*

De ser así, las propuestas contenidas en este estudio recibirían un respaldo sensible por venir impregnadas de la necesaria proporcionalidad, sentido de la oportunidad y de ajuste a la realidad social que representa el uso de las TIC.

En quinto lugar, y con carácter general, no parece adecuado plantear una reducción de las categorías de datos a conservar sino, más bien – y sin que esto suponga una claudicación al efecto "Gran Hermano" -, mantener las que ya existen y aumentar algunas, como sería el caso de los datos de cobertura, cuya acreditada necesidad de conservación por un periodo breve de tiempo se justifica en la necesidad de ganar reactividad ante una situación crítica, como un secuestro, un atentado terrorista, una desaparición, etc., todo ello de suerte que, con independencia de las comunicaciones electrónicas que se hayan producido, exista la posibilidad de acceder a datos – y particularmente los de localización – que propicien un éxito en la resolución del caso.

[1107] *Dictamen del Supervisor Europeo de Protección de Datos sobre la Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones — «Un enfoque global de la protección de los datos personales en la Unión Europea» (2011/C 181/01),* de 14 de enero de 2011.

[1108] En el pto. 180, se dice que *"el nuevo marco jurídico debe ser, en la medida de lo posible, claro, simple y coherente. Debe evitarse la proliferación de diferentes regímenes que se aplican, por ejemplo, a Europol, Eurojust, a los sistemas SIS y de la Declaración Prüm. El SEPD entiende que la tarea de alinear las normas de los distintos sistemas debe llevarse a cabo de manera cuidadosa y gradual".*

En igual medida, una revisión de la Ley debe contemplar la extensión de la obligación de conservar datos a los ISP lo que supondría, sin duda, un sensible aumento de las categorías de datos y, naturalmente, de las necesidades logísticas asociadas a la implentación material de estos nuevos imperativos jurídicos[1109].

En sexto lugar, conviene no confundir las "búsquedas aleatorias" o la "minería de datos", cuya naturaleza prospectiva es perfectamente rechazable en cualquier ámbito democrático, con la necesidad de obtener inteligencia sobre comunicaciones electrónicas ya que, dado el complejo escenario criminal favorecido por las TIC, se hace necesario proponer algunas formas admisibles en derecho con vocación de tenerse por proporcionadas.

En definitiva, todas estas opciones, planteadas desde una perspectiva general, han de tener su acomodo en concretas propuestas de reforma de la legislación actualmente vigente, siempre y cuando su contenido quede revestido de la necesaria razonabilidad y en el entendimiento de que la Ley es un ente vivo y abierto a una nueva hermenéutica que sea capaz de adecuarse a la realidad social de los tiempos.

f) Impacto social de la DCD

No parece, en general, que haya cundido entre la sociedad alarma o inquietud sobre esta decisión adoptada en el seno de los países de la más honda tradición democrática. Todo indica que los europeos no perciben las obligaciones de conservación de los DACE como un abuso o una amenaza a su libertad, lo que puede atribuirse, precísamente, a una perfectamente identificable necesidad social de controlar el delito, a la calidad de la Ley y a la forma que, en general, se ha legislado sobre el secreto o, al menos, sobre una forma consolidadamente democrática de acceder a los repositorios restringidos de datos.

Los ciudadanos, a mi parecer, sienten seguros sus datos al contar con unas normas más o menos afortunadas pero que, sin duda, sabrán tratar también cualquier desviación de su legítima intención – la remisión a los regímenes sancionadores y a

[1109] Véase más adelante el apartado que contiene las propuestas de *lege ferenda* al respecto.

determinados tipos penales es la prueba de esta afirmación -, siendo plenamente conscientes de que sólo se accederá a tan controvertidos datos por aquellas personas y en aquellos casos en que sea estrictamente necesario y legítimo y, siempre, bajo unas salvaguardas y medidas de control adoptadas por una autoridad independiente.

Es evidente también que, en su mayoría, lo admitirán como un necesario sacrificio orientado a su protección – que se extiende de la vida física a la virtual, necesitada de la perentoria intervención del Estado de Derecho -, bien que haya sido ponderada, en cualquier caso, la proporción en que ha de verificarse.

Además, y esto es un suponer, muchos de ellos se habrán visto ya beneficiados en estos años de vigencia por tan controvertida directiva cuando hayan sido rescatados de un secuestro, se haya probado el homicidio de un ser querido, se haya evitado un atentado terrorista o, simplemente, se les haya encontrado tras sufrir una desorientación en el monte, a veces, en precarias condiciones para su integridad. En suma, ver cómo sus policías y jueces actúan con diligencia gracias a las facultades legales que se les otorgan.

Cabe esperarse de un miembro de la PJE, por tanto, una decidida apuesta por extremar el rigor en materia de conservación de DACE sin reparar en demasía en el sacrificio de los derechos fundamentales que conlleve. No es así. Examinada la casuística y la experiencia práctica y tomando en consideración las expectativas de la sociedad democrática a la que sirve, un ejercicio de mesura exige precisar y limitar el acceso a esta fuente de prueba que, en cualquier caso y aún siendo criticable, *ex* art. 1.1 LCDCE es potestad exclusiva de la Autoridad Judicial pero, al mismo tiempo, es también preciso proclamar que quien accede no es cualquier ciudadano, sino una PJE facultada bajo su dependencia funcional y regida mediante una exigente regulación jurídica que impediría cualquier abuso.

3. El Convenio de Ciberdelincuencia como referente

Junto a lo relativo al insuficiente y parcial ámbito objetivo descrito en la DCD y la LCDCE, que se ha presentado en los apartados anteriores, y en referencia ahora a las

posibilidades de acceso del Estado de Derecho al contenido material y formal de las comunicaciones electrónicas (según el concepto amplio que se ha propuesto en este trabajo), es necesario incorporar al ámbito objetivo de aplicación de las obligaciones de conservación a los servicios de comunicaciones electrónicas proporcionados por los proveedores de servicios de la sociedad de la información, incomprensiblemente excluidos de la obligación de conservación de los DACE originados por el empleo masivo y extraterritorial de la telemática en los usos comunicativos sociales actuales.

En efecto, la telemática, como compendio de las inmensas posibilidades que resultan de la suma de las telecomunicaciones y la informática, ofrece a los internautas diverso *software* de uso muy común que permite el envío, por medio de las redes de comunicaciones electrónicas, reguladas técnicamente en el territorio español por la LGT, de los paquetes de datos preparados por los diversos programas informáticos, bien bajo complejos protocolos previos de codificación en origen y descodificación en destino, bien con ausencia de ellos en abierto, según corresponda al uso de determinados programas facilitados por los ISP, incluidos los ***servicios subyacentes*** contemplados en el art. 1.d CCib.

Reflejando el concepto amplio de comunicaciones electrónicas que de modo efectivo impera en la sociedad de la información, el *Convenio del Consejo de Europa sobre la Ciberdelincuencia*[1110], de 23 de noviembre de 2001, hace constar en su preámbulo que su objeto *es "dotar de mayor eficacia las investigaciones y los procedimientos penales relativos a los delitos relacionados con los sistemas y datos informáticos, así como facilitar la obtención de pruebas electrónicas de los delitos"*, algo que difícilmente se consigue sin contar con una legislación procesal adecuada y con una Policía Judicial legalmente habilitada al efecto.

[1110] Este convenio es una referencia para los posteriores desarrollos de la comunidad internacional como lo son los mencionados en el documento de la UIT sobre el que venimos trabajando. En los artículos 2 al 13, el Convenio de Ciberdelincuencia ya adelantó sus propias tipologías en materia de derecho penal sustantivo, y entre los arts. 14 y 22, las de derecho procesal. No obstante, y en referencia al plano procesal, es necesario anotar que las utilísimas medidas de cooperación internacional que propician la rápida y efectiva congelación, conservación y cesión de datos informáticos lo son en tiempo real, es decir, a partir desde el momento en que gana eficiencia técnica una petición formal acogida al convenio, no imponiendo obligaciones respecto de la conservación de datos en la forma que exigen las directivas de UE que motivaron la transposición de la LCDCE, por lo que su capacidad real para la investigación de hechos ya pasados es nula, por no haber impuesto similares obligaciones de conservación.

En este sentido, en el art. 16.1 se dice que *"cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para permitir a sus autoridades competentes ordenar o imponer de otra manera la conservación rápida de determinados datos electrónicos, incluidos los datos sobre el tráfico, almacenados por medio de un sistema informático"*, lo que aporta una definición bastante amplia del concepto *"dato electrónico*" como para salvar cualquier deficiencia de técnica legislativa que suponga una restricción injustificada de las categorías de datos a incluir en el texto de la Ley.

Pero, para precisar el ámbito de esta forma singular de comunicarse, es necesario acudir a las definiciones del art. 1 CCib para comprender qué facetas devienen jurídica y materialmente controvertidas en relación con su perseguibilidad, según los estándares aceptados para la intervención de las comunicaciones en un Estado de Derecho:

Artículo 1 - Definiciones

A los efectos del presente Convenio:

a) por "sistema informático" se entenderá todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, siempre que uno o varios de ellos permitan el tratamiento automatizado de datos en ejecución de un programa;

b) por "datos informáticos" se entenderá cualquier representación de hechos, información o conceptos de una forma que permita el tratamiento informático, incluido un programa diseñado para que un sistema informático ejecute una

c) por "proveedor de servicios" se entenderá:

i) toda entidad pública o privada que ofrezca a los usuarios de sus servicios la posibilidad de comunicar por medio de un sistema informático, y

ii) cualquier otra entidad que procese o almacene datos informáticos para dicho servicio de comunicación o para los usuarios de ese servicio;

d) por "datos sobre el tráfico" se entenderá cualesquiera datos informáticos relativos a una comunicación por medio de un sistema informático, generados por un sistema informático como elemento de la cadena de comunicación, que indiquen el origen, destino, ruta, hora, fecha, tamaño y duración de la comunicación o el tipo de servicio subyacente".

Es, por tanto, en el apartado d) donde se halla la definición del ámbito de intervención que centra el interés de este trabajo, a sumar a lo que se ha dicho con análogo propósito sobre la telefonía fija o móvil, en un intento de ofrecer una visión de conjunto (un concepto amplio de comunicación electrónica) sobre la problemática común asociada: *"…cualesquiera datos informáticos relativos a una comunicación por medio de un sistema informático, generados por un sistema informático como elemento de la cadena de comunicación".*

Es, por ello, muy interesante profundizar en la posibilidad que el usuario de este tipo de comunicaciones tiene de codificar el contenido material, listo para viajar por las redes de comunicación electrónica sin posibilidad de descodificación por terceros, aspecto que no resulta precisamente baladí, pues no existen normas en el derecho interno que obliguen a depositar los protocolos específicos a disposición del Estado y, mucho menos, cuando el propietario del código trabaje desde entidades extraterritoriales, circunstancia que añade un plus de dificultad en el tratamiento técnico y jurídico de los diversos problemas detectados.

Pero lo verdaderamente notable a los efectos de la codificación es que, no sólo los ISP radicados en el extranjero, sino los situados en España bajo los presupuestos de los arts. 2 al 5 LSSI, tienen obligación jurídica alguna de facilitar la intervención de sus contenidos bajo imperativos similares a los incluidos en el art. 33 LGT ni aunque circulen en abierto, aún dando por hecho que los emitan a través de los correspondientes operadores de redes de comunicaciones electrónicas a los que sí les afectará, pero sin posibilidad, por su estatus jurídico, de acceso a tales contenidos, ni

aún en el caso de que concurra en ellos la condición jurídica de operadores de redes de comunicaciones electrónicas[1111].

Sobre la intervención de los ISP en la conformación del contenido material de los mensajes telemáticos, el CCib reconoce explícitamente que, junto a este, existen datos, cuyas categorías no precisa en el art. 1.d con mucha exactitud[1112], que son útiles para la investigación en la escena internacional y que deben intervenirse en tiempo real[1113], obligándose los países ratificantes del Convenio *ex* art. 16.1 a *"ordenar o imponer de otra manera la conservación rápida de determinados datos electrónicos, incluidos los datos sobre el tráfico, almacenados por medio de un sistema informático"*, *ex* art. 16.2 *"…hasta un máximo de noventa días"*, *ex* art. 19.1 a "*registrar o a tener acceso de una forma similar…a un sistema informático…o a un medio de almacenamiento informático"* y, *ex* art. 21.1, a *"obtener y grabar…en tiempo real los datos sobre el contenido de determinadas comunicaciones en su territorio, transmitidas por medio de un sistema informático".*

Las anteriores obligaciones anuncian la posibilidad técnica y jurídica del Estado de efectuar todas las operaciones necesarias frente a los ISP para satisfacer recíprocamente los fines acordados en el CCib por lo que, reflexivamente, los países se deben colocar en evidente posición de satisfacerlas respecto de sus propios objetivos internos.

Pues bien, habiendo sido esto acordado así para facilitar el acceso a los contenidos y para preservar los datos de tráfico en tiempo real, nada debe obstar para que también se impongan en este ámbito a los ISP (es decir, a los proveedores de servicios contemplados en el art. 1.c) CCib), regidos en el derecho interno por la LSSI y con las modificaciones que en la normativa legal sea procedente introducir, unas obligaciones análogas de conservación de datos a las impuestas por la DCD y LCDCE a

[1111] En cuyo caso se necesitará de la interposición de una sonda ADSL que, de alguna manera, alcance los efectos en el orden práctico de adquisición de los contenidos con análoga eficacia a la que se obtendría de la intervención de una línea de telefonía fija o móvil.

[1112] Es evidente que las categorías genéricas del art. 1.d CCib, que adolecen de la necesaria determinación jurídica, deberían ser precisadas mediante normas de desarrollo por parte de los países que han ratificado el Convenio *ex* arts. 14.1, 16.1 y 18 CCib.

[1113] Nótese que el CCib habla de requerimientos de preservación sobre los datos de determiandos objetivos y, en nigún caso, de conservación generalizada de datos, lo que lo diferencia sustancialmente de la DCD.

las operadoras de telecomunicaciones sobre los servicios de comunicaciones electrónicas que presten bajo la regulación de la LGT pero, eso sí, precisando de *lege ferenda* el marco jurídico en que todo esto debe hacerse. Dicho de otra forma, sería necesario imponerles obligaciones de conservación de los *logs* producidos como consecuencia de las operaciones telemáticas en que hayan intervenido como tales prestadores de servicios de la sociedad de la información.

De alcanzarse, por tanto, un régimen jurídico equivalente de conservación de datos como el que se propugna y el oportuno grado de acceso técnico a sus fuentes, así como un ágil y seguro intercambio de datos entre los países obligados por CCib – siempre, *ex* art. 15.2 CCib, bajo *"la supervisión judicial u otra forma de supervisión independiente"* -, se lograría, sin duda alguna, una altísima eficiencia, seguridad y carácter de mínima intervención procesal sobre la aplicación universal de las posibilidades de intervención de las comunicaciones de todo tipo lo que, además, permitiría el establecimiento de acciones conjuntas de exigencia de obligaciones recíprocas frente a los países terceros no participantes en el CCib y, desde luego, frente a la acción perturbadora de los paraísos informáticos.

El grado de automatización de la intervención de las comunicaciones electrónicas con el que el Estado de Derecho debiera contar, en lo que afecte al papel de los ISP es, hoy por hoy, de una absoluta e injustificada inferioridad a los que garantizan su derecho de injerencia en las comunicaciones electrónicas a través la telefonía fija o móvil, siendo esencialmente idénticos, pudiéndose calificar los medios actuales para injerirse en aquellos como meros parches técnicos y jurídicos, de reducidísimas posibilidades reales y de una gran inseguridad y precaria utilidad para el proceso penal, sólo compensada por la acreditada eficiencia técnica alternativa que la PJE actual está en condiciones de aportar.

En este sentido, determinados ISP participan, con una inmensa variedad de prestaciones, en la conformación del mensaje (el contenido material) que es transmitido por las redes públicas de comunicaciones (generando los correspondientes DACE). Consecuentemente, en lo que hace referencia a la intervención de las comunicaciones, esta aportación singular de los ISP – perfectamente integrable en el

concepto amplio de comunicaciones electrónicas que se ha propuesto - debe quedar hábil y accesible para el ejercicio del derecho de injerencia del Estado.

Por ello, considerando que, de acuerdo con la definición del art. 1 d) CCib de "dato de tráfico" y la contenida art. 1 b) CCib sobre "dato informático", es necesario precisar y definir qué DACE (*logs*) de los generados por los ISP son de necesaria conservación según un enfoque análogo al de la LCDCE y LGT.

Esta materia, urgida de un desarrollo legislativo específico, junto con los previsto en la LCDCE y las reformas que la mejoraran, completaría y unificaría el tratamiento jurídico del derecho de injerencia del Estado en las comunicaciones electrónicas mediante la integración de todos sus elementos relevantes, por lo que, consecuentemente, debe quedar definido específicamente en la Ley el contenido de los datos técnicos o *log* que sería necesario conservar a tales fines, materia que se tratará en el apartado siguiente.

VI. CONCLUSIONES

1. El estado evolutivo de las TIC, su alta penetración en una sociedad intensamente globalizada, la transferencia al mundo virtual de partes sensibles de la vida física de las personas y la modificación que, por su influjo, se produce sobre determinados factores de orden criminológico, desbordan el espacio jurídico actual y evidencian la necesidad de mejorar la intervención del Derecho.

2. Existe una anomia real en la regulación de la actividad humana en el ámbito de las TIC que provoca importantes lagunas legales, así como una anomia aparente en cuanto a la percepción de algunas personas de hallarse interactuando en un espacio alegal.

3. Desde un punto de vista criminológico, se detecta en la interactuación a través de Internet un efecto disociativo entre el autor y la víctima y/o los objetos del delito, que puede resolver desfavorablemente el conflicto del paso al acto, con posibles secuelas de reforzamiento y despersonalización de la conducta criminal, atenuación o desaparición de los sentimientos de morbidez y de producción de una elevada cifra negra, incluyendo sensibles efectos de victimización secundaria.

4. El uso criminal de las TIC presenta una faceta relacionada con la concertación criminal en un sentido clásico, esto es, como medio de comunicación entre personas, y otra, no menos importante, que tiene como finalidad en sí misma el desarrollo de nuevos *modus operandi* delictivos, donde el uso de las comunicaciones electrónicas deviene meramente instrumental.

5. En todas las comunicaciones se produce una protección acrítica, según la percepción jurídica actual, del derecho al secreto de las comunicaciones del art. 18.3 CE (como concepto jurídico-formal y sustantivo), de superior importancia a la que corresponde a su naturaleza íntima (de contenido ético-psíquico o material).

6. El uso criminal de las TIC no propicia la aparición de nuevos tipos penales, sino un dimensionamiento nuevo de los ya conocidos mediante la

instauración de nuevos *modus operandi*. Por ello, se descarta la existencia de lo que vienen denominándose "delitos informáticos".

7. El uso proporcionado de los medios técnicos de investigación y la adquisición de la evidencia digital suponen, frente a la mayoría de los métodos clásicos de investigación, un saldo de menor intrusión en los derechos fundamentales de los investigados, ya que permiten la discriminación de las facetas de su vida privada que tengan un eventual interés para el proceso penal de las que no lo tienen.

8. La utilización de alguno de los medios técnicos empleados en la investigación criminal queda reservado a la decisión judicial y, en todos los casos, facilitan el ejercicio seguro de su control jurisdiccional contando con el apoyo, además, de sus propias prestaciones tecnológicas, circunstancias todas ellas que alejan los vicios de nulidad que pudieran atribuírseles.

9. El uso de las tecnologías de la investigación policial no suponen un vaciamiento de las funciones jurisdiccionales, ni un desplazamiento de la instrucción judicial hacia la PJE. Antes bien, aportan seguridad jurídica al desempeño de las labores del juzgador y al ejercicio de los derechos fundamentales de los justiciables a la tutela judicial efectiva, a la defensa y a un proceso con todas las garantías que están reconocidos en el art. 24 CE.

10. La PJ, en cumplimiento de las funciones conferidas por el art. 126 CE – de distinta naturaleza jurídica que las atribuidas por el art. 104 CE a la policía de seguridad -, interviene con objetividad y sujeción al principio de legalidad en el cumplimiento de las finalidades del proceso penal, actuando imparcialmente con inmediatez a los Jueces y Fiscales, de quienes depende funcionalmente, y con un completo grado de autonomía respecto de sus dependencias orgánica y técnica. A lo anterior, se une su exigente formación técnica y científica y la estricta perspectiva ética y deontológica con que desarrollan las investigaciones criminales.

11. La actividad de la PJE y el recurso a los elementos de salvaguarda y certificación que la tecnología aporta como contraste objetivo, otorgan la

debida seguridad jurídica en la limitación de los derechos fundamentales y facilita su control jurisdiccional.

12. La insuficiencia del derecho positivo español en materia procesal, el *quantum* de indeterminación jurídica que contiene el principio de proporcionalidad, el grado de discrecionalidad con que el actor jurisdiccional puede interpretarlo, la convivencia de resoluciones valorativas contradictorias sobre la apreciación de este principio y, en definitiva, la incertidumbre asociada a su ejercicio, dificultan la función de la PJE, además de suponer un riesgo jurídico inaceptable para el investigador.

13. El concepto jurídico de gravedad ha devenido insuficiente para valorar la proporcionalidad de determinadas medidas ablativas de derechos fundamentales, al desbordarse las percepciones que lo atan coyunturalmente a aspectos relacionados con la mera retribución penológica cuantitativa por el concreto delito cometido, siendo necesario también apreciar la trascendencia social de las conductas, la importancia del bien jurídico protegido y el ámbito tecnológico de la intervención.

14. Se propone un concepto jurídico amplio de comunicación electrónica que tome en consideración que, en la conformación del mensaje, se produce la intervención singular de un elemento que excede a los propios usuarios y a los dispositivos e infraestructuras de transmisión y que se refiere a los servicios telemáticos que, como suma de la informática y las telecomunicaciones, son puestos a disposición de los ciudadanos por los proveedores de servicios de la sociedad de la información regulados por la LSSI, intervención que, con toda lógica, interesa al proceso penal con análoga fuerza imperativa que la relativa a las redes e infraestructuras públicas de comunicaciones y a los correspondientes servicios de comunicaciones electrónicas regulados *ex* LGT.

15. En atención al concepto amplio de comunicaciones electrónicas que se ha propuesto, las obligaciones de conservación de datos que actualmente sólo afectan a los operadores regidos por la LGT, deberían extenderse también a los producidos por los proveedores de servicios de la sociedad de la

información, regulados por la LSSI, por su participación en la conformación de los servicios telemáticos accedidos por los usuarios cuando se preordenen a su circulación por las redes públicas de comunicaciones electrónicas. Particularmente, es necesario imponer a los ISP obligaciones de conservación de los *logs* análogas a los DACE regulados por la LCDCE.

16. Debe contemplarse también un concepto amplio de datos asociados a las comunicaciones electrónicas, según una caracterización no exhaustiva, que permita entender como tales a aquellos, distintos del contenido material del mensaje transmitido, que hayan sido producidos por cualquier dispositivo técnico apto para materializar una comunicación electrónica, aun cuando no se vinculen a un acto de comunicación en concreto.

17. En refuerzo de una visión amplia de los DACE, la evolución de las TIC ha evidenciado la existencia de datos que no se relacionan con concretas comunicaciones electrónicas, sino que se generan por la puesta a disposición de la red pública de comunicaciones electrónicas a los diversos dispositivos de comunicaciones de los usuarios (Datos de cobertura de BTS, la identificación del IMSI o el IMEI, la obtención de datos de GPS en régimen de valor añadido o el seguimiento de los *hash* de determinados archivos informáticos). La obtención de estos datos puede hacerse mediante el análisis del espectro radioeléctrico por la PJE con total independencia de los actos de comunicación que eventualmente puedan producirse.

18. No todas las comunicaciones consisten en mensajes inteligibles para los interlocutores, estos no tienen por qué ser personas, ni dirigirse a un número finito e identificable de receptores, ya que existen actos de comunicación técnica distintos de la transmisión de voz o texto entre personas.

19. Frente a la percepción jurisprudencial dominante, que otorga idéntica protección al contenido material de las comunicaciones que al formal, existen razonadas posiciones jurisprudenciales, anteriores a la entrada en vigor de la LCDCE que, descartando la afectación al derecho al secreto de las comunicaciones, vinculan el acceso a los DACE conservados únicamente con

el derecho a la protección de datos recogido en los arts. 18.1 CE o 18.4 CE. Según esta doctrina, el acceso a los DACE se podría considerar una faceta relacionada con las funciones de indagación propias de la PJE, cuya obligada y precisa incorporación al proceso penal se materializa *ex* arts. 549.1.a) LOPJ, 11.2.d) LOPD, 22.2 LOPD y 1, 2 y 4 RDPJ.

20. Una eventual reforma de la LCDCE debiera contemplar un régimen excepcional de cesión de los DACE en aquellos casos justificados de urgencia vital o riesgo catastrófico para que la PJE, de propia autoridad y en evitación de un peligro de demora de cualquier naturaleza, pudiese recabar directamente de los sujetos obligados (incluidos los ISP) los que precisase para resolver eficazmente la incidencia.

21. Es necesario, con carácter general, ampliar los DACE objeto de conservación *ex* art. 3.1 LCDCE a los datos de cobertura, por un periodo de tiempo mínimo de 72 horas y en referencia a la localización de la BTS principal en la que se haya registrado el dispositivo de comunicaciones (con expresión de sus datos de CGI), todo ello para atender reactivamente las justificadas necesidades urgentes de intervención policial. Alternativamente, se propone un requerimiento de preservación de datos por el que se habilite a la PJE para ordenar a los sujetos obligados la conservación de los que interese, haciéndose efectiva la cesión a la presentación del correspondiente mandato judicial.

22. Resulta preciso instaurar la conservación de los DACE referidos a las conexiones a Internet a través de las BTS de los *smartphones* u otros dispositivos análogos de comunicaciones electrónicas.

23. Se propone una nueva visión de la prueba pericial de inteligencia, bajo la denominación de prueba de inteligencia policial, que será aquella que, habiendo sido incorporada al proceso penal a través del atestado policial, contenga juicios policiales de inferencia estrictamente fundamentados, tanto en los estudios periciales practicados, como en referencia a las pruebas directas e indirectas o indiciarias que hayan sido del conocimiento de la PJE durante la fase de investigación que, a su vez, hayan sido

realizadas bajo la dependencia funcional de Jueces y Fiscales y legítimamente admitidas para su contradicción y valoración en el acto de juicio oral.

24. La rigurosa percepción jurídica que vincula la cesión de los DACE conservados (como contenido formal de las comunicaciones) a los derechos reconocidos en el art. 18.3 CE, como efecto inmediato del carácter formal del secreto, impide el discernimiento jurídico entre comunicaciones personales (de carácter humano e íntimo) e instrumentales (de carácter técnico y no íntimo) en el sentido de estar todas ellas indistintamente protegidas por este precepto de superior y amplia protección constitucional. De identificarse el derecho concernido como el de protección de datos, cuya tutela se residencia en los arts. 18.1 CE o 18.4 CE, podría obtenerse una IDACE acorde con la moderna casuística criminal relacionada con las TIC, de elevado potencial lesivo en la escena internacional, en que el uso técnico instrumental de las comunicaciones electrónicas desborda y desdibuja por completo su uso clásico como medio de comunicación personal digno, por su parte, de la más estricta protección.

25. La habilitación judicial de la PJE para la obtención de IDACE debe adaptarse a las circunstancias impuestas por la realidad social del uso de las TIC, su potencial lesivo, el carácter transnacional de las maquinaciones, la ingente, compleja y variada producción de datos y, finalmente, la propia naturaleza del medio donde ha de intervenir. Todo ello ha de hacer posible que el mandato judicial habilite a la PJE para la realización de tareas complejas de obtención de IDACE, según lo exija la dinámica de la investigación y la ponderación de los derechos fundamentales puestos en juego.

26. La necesidad de obtener IDACE para los propósitos del proceso penal en el exigente ámbito de las comunicaciones electrónicas, cuando exista limitación de derechos fundamentales, en ningún momento ha de ser prospectiva, aleatoria, genérica o abierta, sino resultado de la valoración de su proporcionalidad por la Autoridad Judicial. Caso de estimarse su

procedencia, podría ejecutarse bajo la dirección de la PJE, con apoyo de las salvaguardas jurídicas y tecnológicas que se han planteado y con el eventual nombramiento de un auxilio jurisdiccional a determinados técnicos adscritos a las operadoras e ISP, cuya intervención en el proceso penal sería de naturaleza pericial.

27. Se aprecia una clara insuficiencia en materia de cooperación policial y judicial internacional, condicionada por la fragilidad de los instrumentos jurídicos de cooperación, algunos de los cuales no pueden invocarse cuando la información se haya obtenido por medios coercitivos, así como por las demoras judiciales, la disparidad de las legislaciones procesales o penales, la falta de armonización, etc. Es necesario dotarse de los instrumentos jurídicos que la permitan bajo el principio de reconocimiento mútuo de las resoluciones judiciales, allí donde sean de aplicación los acuerdos internacionales específicos.

28. Los tiempos de conservación de datos, excesivamente cortos, no facilitan la accesibilidad a la inteligencia sobre delincuencia compleja, con tendencia a crear infraestructuras criminales estables, resistentes a la persecución penal, duraderas en el tiempo y con fácil ocultación o destrucción del rastro tecnológico, lo que debiera ser precisamente la finalidad última de una Ley claramente dirigida a proteger la vida, la libertad y la seguridad de los ciudadanos. Podrían establecerse plazos de conservación adecuados a las características criminológicas de las nuevas tipologías.

VII. PROPUESTAS DE LEGE FERENDA

Si se pretendiese introducir reformas en la legislación de modo que acogiesen las propuestas contenidas en la parte expositiva de este estudio, caso de ser política y jurídicamente posible, sería necesario operarlas en cuerpos jurídicos muy complejos, tanto en la escena internacional (CCib, DCD y demás directivas estudiadas, etc.), como en la nacional (CP, LCRIM, LOPD, LOPJ, LGT, LSSI, etc.).

Sin embargo, sin olvidar lo anterior, puede hacerse una aproximación, a modo de ejercicio complementario a lo aportado en este estudio, sobre aquellas modificaciones cuya introducción fuese posible en la LCDCE[1114].

En consecuencia, se proponen las siguientes reformas de *lege ferenda:*

Art. 1.1 LCDCE[1115]:

[1114] A título meramente complementario, se incluye una de las enmiendas al anteproyecto de la LCDCE por la que se consideraba necesario extender las obligaciones de conservación a los *logs* introduciendo el párrafo siguiente entre los numerales 1 y 2 del art. 3 LCDCE:
"Los datos que deben conservarse por los Prestadores de Servicio de la Sociedad de la Información especificados en el art. 2 de esta ley, con respecto a los servicios por Internet, son los siguientes:
i) El número de teléfono, fecha y hora de la conexión y desconexión, y datos de identificación del abonado o del usuario registrado al que se le ha asignado una dirección de Protocolo de Internet (IP), por un Prestador de Servicio de Acceso a Internet.
ii) La dirección de Protocolo de Internet (IP) del usuario que establece la comunicación, con expresión de la fecha y hora de la comunicación por la que hace uso del servicio ofrecido por el Prestador de Servicios de la Sociedad de la Información, basada en un determinado huso horario. Se excluyen las comunicaciones a servicios implementados sobre protocolo web que no creen, modifiquen o borren contenidos (*NOTA:* Esto excluye la conservación de datos sobre meras consultas *web*, donde no se produce interacción con el prestador de servicios. Sería tan imposible como excesivo obligar a guardar este tipo de transacciones).
iii) Los datos de registro facilitados por un usuario a un Prestador de Servicios para hacer uso de un servicio (nick o sobrenombre, e-mail, filiación...).
iv) Los datos de perfil de cliente que almacena el Prestador de Servicios de la Sociedad de la Información, con ocasión de la prestación de un servicio (contactos mensajería instantánea, canales de preferencia de redes IRC, etc.).
v) Los datos de identificación del equipo y de la aplicación informática utilizada para la comunicación, obtenidos por el Prestador de Servicios de la Sociedad de la Información con ocasión de la prestación de un servicio (cookies y datos identificadores de los programas navegadores del cliente).
vi) La identificación de usuario, el número de teléfono asignado y el número de teléfono del destinatario o de los destinatarios, de toda comunicación que acceda a la red pública de telefonía haciendo uso del servicio de telefonía por Internet.
vii) El número de teléfono de origen en caso de acceso mediante marcado de números al servicio de telefonía por Internet".
Para elaboración de las propuestas de este apartado se han tomado en consideración, en general, las *Enmiendas al Proyecto de Ley 25/2007 - 121/000128.* 2007. 128-6, Madrid: Boletín Oficial de las Cortes Generales - Congreso de los Diputados - VIII Legislatura, 7 de mayo de 2007, págs. 17-49.

[1115] Redacción vigente del art. 1.1 LCDCE*: "Esta Ley tiene por objeto la regulación de la obligación de los operadores de conservar los datos generados o tratados en el marco de la prestación de servicios de comunicaciones electrónicas o de redes públicas de comunicación, así como el deber de cesión de dichos*

> *"Esta Ley tiene por objeto la regulación de la obligación de los operadores del Mercado de las Telecomunicaciones de conservar los datos generados o tratados en el marco de la prestación de servicios de comunicaciones electrónicas o de redes públicas de comunicación y de los prestadores de servicios de la sociedad de la información en lo referente a los datos de registro de acceso a sus servidores, así como el deber de cesión de dichos datos a los agentes facultados siempre que les sean requeridos a través de la correspondiente autorización judicial o requerimiento del Ministerio Fiscal con fines de detección, investigación y enjuiciamiento de delitos graves contemplados en el Código Penal o en las leyes penales especiales o en aquellos casos en que lo exija la relevancia social del hecho o del bien jurídico protegido y la potencialidad lesiva del uso de instrumentos informáticos para la comisión del delito".*

La propuesta se justifica en la necesidad de precisar que el ámbito objetivo de aplicación de las obligaciones de conservación de DACE de los operadores del Mercado de las Telecomunicaciones regulados por la LGT, debe extenderse también a los prestadores de servicios de la sociedad de la información regulados por la LSSI, con la explicación adicional de que debe referirse a los datos de acceso de los usuarios a los servicios telemáticos que les presten. Esto último, obligaría a la conservación de los correspondientes *logs ex* art. 3.1 LCDCE en tanto representasen un acceso a los servicios de formación telemática de un mensaje preordenado a su circulación por las redes públicas de comunicaciones electrónicas.

Aunque he considerado al Ministerio Fiscal como facultado en la Ley al modo en que originariamente lo está la Autoridad Judicial, esto no sería posible debido a la configuración jurídica actual de la LCDCE, firmemente ligada al art. 18.3 CE por haber atado el legislador esta Ley al derecho al secreto de las comunicaciones, lo que le excluiría del ejercicio de esta función. Consecuentemente, la inclusión del Ministerio Fiscal sólo sería posible mediante un cambio en la invocación jurídica de los derechos

---

datos a los agentes facultados siempre que les sean requeridos a través de la correspondiente autorización judicial con fines de detección, investigación y enjuiciamiento de delitos graves contemplados en el Código Penal o en las leyes penales especiales".

concernidos por el acceso a los DACE mediante su derivación a los contenidos en los arts. 18.1 CE o 18.4 CE, según procediese, relacionándolos con la protección de datos y no con el secreto de las comunicaciones.

Finalmente, la propuesta contiene una referencia al concepto amplio de gravedad que se ha propuesto y que aleja la reserva exclusiva de intervención de la LCDCE de los delitos graves, según el concepto retributivo penológico fijado en el CP, para extenderla al necesario tratamiento de la casuística real relacionada con el uso criminal de las TIC.

Introducción del art. 1 bis LCDCE:

" Los agentes facultados podrán de propia autoridad recabar los datos a que se refiere esta Ley en aquellos casos de urgencia en los que existiese peligro de demora, dando inmediata cuenta a la Autoridad Judicial en los términos previstos en la Ley".

La propuesta se justifica en la evidente necesidad de que la PJE intervenga eficientemente para afrontar las situaciones de urgencia vital o riesgo catastrófico en las que un acreditado peligro de demora pudiese ocasionar una inaceptable pérdida de eficiencia. La invocación de estas facultades excepcionales de los agentes estaría sujeta a las obligaciones contenidas en los arts. 549.1.a) LOPJ, 11.2.d) LOPD, 22.2 LOPD y 1, 2 y 4 RDPJ y a un control posterior de jurisdiccionalidad.

Art. 1.2 LCDCE[1116]:

"Esta Ley se aplicará a los datos de tráfico y de localización de los dispositivos de comunicaciones electrónicas, a los registros de sucesos o logs contenidos en los

[1116] Redacción vigente del art. 1.2 LCDCE: *"Esta Ley se aplicará a los datos de tráfico y de localización sobre personas físicas y jurídicas y a los datos relacionados necesarios para identificar al abonado o usuario registrado"*.

servidores de los prestadores de servicios de la sociedad de la información y a los datos relacionados necesarios para identificar al abonado o usuario registrado".

Esta propuesta contiene una precisión de evidentes consecuencias jurídicas al aclarar que los datos de localización son referidos a los dispositivos de comunicaciones electrónicas y nunca a las personas físicas o jurídicas, por más que sea común la coincidencia espacio-temporal de unos y otros. En este sentido, existen numerosas clases de dispositivos de comunicaciones electrónicas que no son de uso personal, por lo que es necesario introducir la redacción alternativa propuesta.

En igual medida, la nueva redacción, manteniendo su referencia a los datos afines, contiene la acreditadamente necesaria inclusión de los registros de sucesos o *logs* propios de las comunicaciones mediadas por los prestadores de servicios de la sociedad de la información.

Introducción del art. 1.4 LCDCE:

> *"Se excluyen del ámbito de aplicación de esta Ley los datos que se hallen asociados a los usos técnicos instrumentales de las comunicaciones electrónicas, pudiendo los agentes facultados obtenerlos de propia autoridad en los términos previstos en la Ley".*

Este propósito, de más que dificultoso encaje en la configuración actual de la LCDCE, supondría la aceptación de la existencia de un ámbito no personal de las comunicaciones que contrariaría el carácter formal del derecho al secreto de las comunicaciones, por más que su injerencia no supusiese penetración alguna, ni en el contenido material de las comunicaciones, ni una limitación del derecho a la intimidad de personas identificadas o identificables. Con toda evidencia, esto sólo sería posible si la LCDCE se vinculase a los efectos con el derecho a la protección de datos y no al secreto de las comunicaciones.

En relación con la reserva jurisdiccional para la injerencia de la PJE en los DACE de estas sugerentes formas de uso de las TIC, que en la propuesta introducida se omite, en realidad, nada empece a que sea previa y en toda su extensión aunque, eso

sí, con una habilitación en su operatividad sensiblemente mayor a la que se logra cuando se produce bajo los paradigmas del secreto de las comunicaciones.

Introducción del art. 3.1.g:

"Los datos de cobertura de la antena principal de telefonía móvil, con expresión de su localización, la identificación de la celda y la dirección angular de cobertura, todo ello con referencia temporal al momento de la conexión y al de la desconexión del terminal[1117]*".*

Esta categoría se introduce *ex novo* por ser necesaria para atender los casos de urgencia vital o riesgo catastrófico, por un periodo breve de tiempo en que se justifica la necesidad de conservación de los DACE, según las características criminológicas de la casuística que se pretende tratar. Supone que el agente facultado, en atención al régimen excepcional de intervención de urgencia que también se ha propuesto, podrá acceder a estos datos sin que hayan sido cancelados por los sujetos obligados.

Alternativamente, podrían ser objeto de una orden de preservación como la que se ha descrito en el apartado correspondiente.

Introducción del art. 3.1.h:

La LCDCE limita actualmente la conservación de datos a los siguientes[1118]:

- Telefonía de red fija.
- Telefonía móvil.
- Acceso a Internet[1119].
- Correo electrónico por Internet.

[1117] Obviamente, los datos cuya conservación se propone son los de CGI.
[1118] Sobre la redacción de la Ley planea alguna imprecisión, como sucede en el art. 1.2, al no mencionar específicamente al destinatario de las comunicaciones. Un buen final de este párrafo debiera incluir la frase "*…y del destinatario de la comunicación"* para no dejar lugar a la duda.
[1119] Nótese la terminología: *"acceso a Internet"* y no *"servicios prestados a través de Internet"*.

- Telefonía por Internet.

Esquemáticamente, el art. 3 de la LCDCE se refiere a los siguientes datos en relación a las comunicaciones:

1. *Datos que deben conservarse :*
    a) *Datos sobre el origen.*
    b) *Datos sobre el destino.*
    c) *Datos para determinar la fecha, hora y duración.*
    d) *Datos para determinar el tipo.*
    e) *Datos para identificar el equipo.*
    f) *Datos para identificar la localización del equipo de comunicación móvil.*
2. *No deberá conservarse ningún dato que revele el contenido de la comunicación.*

Esta clasificación muestra claramente la limitación de servicios objeto del interés de la LCDCE, que ya se ha estudiado con anterioridad, y que nace de la misma redacción de aquellos párrafos del art. 3 de sentido limitativo en los que se dice que los datos a que refiere la Ley son *"con respecto al acceso a Internet, correo electrónico por Internet y telefonía por Internet"*, cuando de una manera más extensiva y representativa de la necesidad de la que surge la Ley debiera decirse *"con respecto a los servicios por Internet"*, dando así cabida a cualquier uso de las comunicaciones que pueda generar algún interés para la Justicia.

Para introducir la conservación de los datos que interesan sobre este tipo de servicios, se propondría la siguiente redacción del nuevo art. 3.1.h LCDCE:

"Los logs de registro de los accesos a los servicios facilitados por los prestadores de servicios de la sociedad de la información, incluidos los relativos servicios subyacentes y, en particular, los siguientes:

1. *Identificación de la línea telefónica asociada.*

2. *Dirección IP y del puerto de acceso*[1120] *de los dispositivos telemáticos conectados.*
3. *Fecha, hora y huso horario*[1121].
4. *Dirección MAC*[1122] *del dispositivo telemático.*
5. *Historial de acceso IP a los servicios telemáticos subyacentes con expresión de los demás datos relacionados en este artículo.*

La utilidad de conservar datos del puerto[1123] es imprescindible, pues señala el canal preciso por el que la comunicación telemática discurre y cuya numeración va del 1 al 65535 (que corresponde a 2^{16}).

Por ejemplo, en un *router ADSL* común de los que se instalan en un domicilio particular, y que se conecta con Internet a través de una IP Pública, podrían conectarse simultáneamente a su vez diversos dispositivos telemáticos que se identificarían con una IP Privada (como un ordenador, un *smartphone*, un dispositivo de alarma, etc.).

Pues bien, cada uno de ellos sería atendido mediante la asignación de un puerto concreto que pondría en relación IP Privada con la IP Pública, con el propósito de diferenciar y distinguir su tráfico comunicativo respecto del originado por los demás dispositivos conectados simultáneamente.

Posteriormente, los paquetes de datos que compongan la comunicación saldrá del ordenador hacia el *router* y, de este, a Internet a través de la red pública de comunicaciones electrónicas, todo ello mediante la asignación, a su vez, de la referida IP Pública por el operador del mercado de las telecomunicaciones (cuya identificación es la que tiene la obligación de conservar *ex* art. 3.1 LCDCE, que no por el ISP, con independencia de que el operador la haya asignado como estática o dinámica).

[1120] Conocer el puerto es necesario porque el sistema de direccionamiento IPV4 puede asignar una misma IP a varios equipos, por lo que la individualización se debe hacer mediante la identificación por el ISP del puerto de acceso que haya adjudicado a la sesión.

[1121] Es evidente la necesidad contar con el huso horario de cada una de las veinticuatro áreas en que se divide la esfera terráquea. De no conocerse, no existiría una vinculación de los datos al tiempo en que se producen, esto es, la hora de inicio y cierre de la transacción, perdiendo por completo sus cualidades identificativas.

[1122] La dirección *MAC* individualiza el equipo o dispositivo físico, pero su conocimiento tiene la desventaja de que puede ser modificada en su configuración de fábrica mediante una sencilla y legítima manipulación de usuario. No obstante, puede tener un capital interés para la investigación, lo que justifica la necesidad de que se conserve a disposición de los agentes facultados.

[1123] También llamada NAT (acrónimo del inglés *network address translation*).

Consecuentemente, cuando el usuario acceda a un servicio de la sociedad de la información, la operadora conservará únicamente los datos de IP Pública de acceso que se han mencionado (de interés bastante pobre para la investigación, pues serán unos datos genéricos de conexión a Internet, pero de escaso valor identificativo por representar indistintamente el conjunto de los accesos a la red hechos a través de la línea telefónica que soporte, a su vez, la ADSL). Estos datos de IP Pública nada reflejarán sobre el contenido formal de cada transacción telemática correspondiente a cada IP Privada, por lo que se hace necesario el contar además con un reflejo de los *logs* en que haya consistido, por ser esta información la que contiene los datos de direccionamiento IP, tiempo, duración, puerto, etc.

Pero los *logs* no son conocidos por las operadoras del mercado de las telecomunicaciones[1124], sino por los ISP, por ser estos quienes los gestionan como parte de la prestación de sus servicios de comunicaciones electrónicas, por lo que la obligación de conservarlos, de proceder jurídicamente, les correspondería.

Todo lo anterior justifica la necesidad de conocer el DACE que representa el puerto para individualizar el dispositivo y la transacción que tengan interés para la investigación.

Por último, es necesario añadir a título meramente informativo que, con el saturamiento mundial actual de las direcciones IP del protocolo IPV4[1125], se están asignando direcciones IP idénticas para las transacciones telemáticas diversas por lo que, hasta tanto se implemente el protocolo IPV6, es necesario discriminarlas mediante la asignación de puertos diferentes para cada dispositivo. Por tanto, se trata de un dato necesario tan sólo coyunturalmente.

[1124] Si bien es cierto que hay reflejo sucesivo de las IP en el SITEL de tercera generación, incluyendo la de los servicios subyacentes. Si hay intervención en tiempo real, se ve el contenido tal y como lo vio el sujeto, salvo que se trate de contenidos codificados que no hayan entregado el código. En lo que se refiere a la conservación de datos, se verían perfectamente todas las IP pero, con la LCDCE, sólo se conservaría la de la conexión a la red pública de comunicaciones, pero no la de los servicios de la sociedad de la información conectados, incluidos los subyacentes.

[1125] Las direcciones IPv4 se configuran mediante un número binario de 32 bits, lo que permite un número total de 4.294.967.296 (2^{32}) de direcciones posibles (una dirección IP consiste en un código numérico cuyos dígitos responden a la ordenación XXX.XXX.XXX.XXX. Actualmente, dado que esta desorbitada cantidad de direcciones se ha agotado, la red Internet está migrando a la versión IPv6 que permitirá la inabarcable cifra de 2^{128} posibles direcciones o, lo que es lo mismo, 340 sextillones de direcciones.

Otro de los efectos negativos para el cumplimiento del espíritu que se contiene en la LCDCE es el relativo a la omisión de la conservación de los DACE relacionados con la activación de servicios de Internet a través de una BTS o red telefónica desde una tarjeta 3G o GPRS o desde una red WIFI (*smartphone* u ordenador), cuyo único e insuficiente rastro que puede ser requerido de las operadoras es el de la IP Pública[1126].

Art. 4.1 LCDCE[1127]:

> *"Los sujetos obligados adoptarán las medidas necesarias para garantizar que los datos especificados en el artículo 3 de esta Ley se conserven de conformidad con lo dispuesto en ella, en la medida en que sean generados o tratados por aquéllos en el marco de la prestación de los servicios de comunicaciones o de la sociedad de la información de que se trate".*

Esta nueva redacción sólo alcanza a reiterar la inclusión en el ámbito objetivo de aplicación de la LCDCE de los prestadores de servicios de la sociedad de la información.

Art. 5.1 LCDCE[1128]:

[1126] Problema que debiera quedar resulto con la migración del sistema IPV4 al IPV6.

[1127] Redacción vigente: *"Los sujetos obligados adoptarán las medidas necesarias para garantizar que los datos especificados en el artículo 3 de esta Ley se conserven de conformidad con lo dispuesto en ella, en la medida en que sean generados o tratados por aquéllos en el marco de la prestación de los servicios de comunicaciones de que se trate.*
En ningún caso, los sujetos obligados podrán aprovechar o utilizar los registros generados, fuera de los supuestos de autorización fijados en el artículo 38 de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones".

[1128] Redacción vigente: *"La obligación de conservación de datos impuesta cesa a los doce meses computados desde la fecha en que se haya producido la comunicación. Reglamentariamente, previa consulta a los operadores, se podrá ampliar o reducir el plazo de conservación para determinados datos o una categoría de datos hasta un máximo de dos años o un mínimo de seis meses, tomando en consideración el coste del almacenamiento y conservación de los datos, así como el interés de los mismos para los fines de investigación, detección y enjuiciamiento de un delito grave, previa consulta a los operadores".*

"La obligación de conservación de datos impuesta cesa a los doce meses computados desde la fecha en que se haya producido la comunicación, exceptuándose los datos de cobertura, que será de 72 horas. Reglamentariamente, previa consulta a los operadores, se podrá ampliar o reducir el plazo de conservación para determinados datos o una categoría de datos hasta un máximo de dos años o un mínimo de seis meses, tomando en consideración el coste del almacenamiento y conservación de los datos, así como el interés de los mismos para los fines establecidos en el artículo 1 de esta Ley, previa consulta a los operadores".

Aunque sería deseable contar con criterios de especialidad criminológica para determinar la duración de los periodos de tiempo de conservación, haciendo posible que el común de los ciudadanos soportasen periodos más breves que los actualmente establecidos, las modificación contribuye a la necesidad de acceder con las más amplias facultades a los datos de cobertura, debiendo alcanzarse el límite objetivo superior permitido por la LCDCE en vía reglamentaria para la conservación de los demás DACE, tal y como previene la redacción original de este artículo.

En este sentido, el periodo de conservación de los datos de cobertura se ha propuesto de modo que se tengan en cuenta sus especiales características técnicas, su utilidad inmediata para resolver situaciones en las que se necesita acceder con urgencia a datos recientes y el hecho de la sobrecarga que se impone a los sujetos obligados.

Igualmente, se abren las posibilidades de acceso a los datos aún cuando no se trate de hechos graves, según el concepto amplio que se ha introducido con la redacción alternativa propuesta para el art. 1.1 LCDCE.

Art. 7.1 LCDCE[1129]:

[1129] Redacción vigente: *"Los operadores estarán obligados a ceder al agente facultado los datos conservados a los que se refiere el artículo 3 de esta Ley concernientes a comunicaciones que identifiquen a personas, sin perjuicio de la resolución judicial prevista en el apartado siguiente"*.

"Los sujetos obligados estarán obligados a ceder al agente facultado los datos conservados a los que se refiere el artículo 3 de esta Ley concernientes a comunicaciones que identifiquen a personas, sin perjuicio de la resolución judicial prevista en el apartado siguiente".

Introducción del art. 7 bis:

"No será necesaria la previa resolución judicial en los casos siguientes:

1º Cuando el usuario del teléfono fijo o móvil o del sistema informático por el que se establece una comunicación electrónica de carácter privado consienta expresamente en que los datos conservados referentes a dicha comunicación se cedan a los agentes facultados, en el seno de un investigación para la prevención o esclarecimiento de una infracción penal.

2º Cuando se transmita públicamente cualquier dato, imagen o información de cualquier tipo a través de los sistemas de comunicaciones electrónicas, si para acceder a lo transmitido no es necesaria la utilización de clave u otro modo de identificación como usuario reconocido.

3º Cuando la intervención de los agentes facultados se acoja al régimen excepcional de urgencia establecido en el art. 1 bis".

Debe hacerse mención también de aquellos casos en que las comunicaciones que se investigan no sean privadas, es decir, que se hayan hecho por voluntad de los comunicadores en canal abierto, como sería el caso de de los chats o los foros, por ejemplo, mediante los que los usuarios publican sus comentarios o intercambian abiertamente sus archivos electrónicos a la vista de cualquier persona que esté accediendo a la red.

VIII. BIBLIOGRAFÍA

Alexy, Robert. *Teoría de los derechos fundamentales.* Madrid: Centro de Estudios Constitucionales, 1993.

Alonso Pérez, Francisco. *Intervención de las comunicaciones postales, telegráficas y telefónicas*. La protección de datos en la cooperación policial y judicial. Madrid: Dykinson S.L., 2001.

Alonso Pérez, Francisco. *La Policía Judicial. Legislación, comentarios, jurisprudencia y formularios.* 3ª Ed. Madrid: Dykinson, 1998.

Álvarez Rodríguez, José Ramón y Ríus Diego, Francisco José. *La entrada y registro en lugar cerrado: consideraciones procesales, jurisprudenciales y policiales.* Madrid: Editorial Tecnos, 2009.

Álvarez Rodríguez, José Ramón. *El atestado policial completo.* Madrid: Tecnos, 2007.

Andrés Ibáñez, Perfecto y Movilla Álvarez, Claudio. *El Poder Judicial.* Temas claves de la Constitución Española. Madrid, 1986.

Aprile, E. Spiezia, F. *Le intercettazioni telefoniche ed ambientali. Innovazioni tecnologiche e nuove questioni giuridiche.* Milano: Giuffrè Editore, 2004.

Arenas Ramiro, Mónica. *El derecho fundamental a la protección de datos personales en Europa.* Valencia: Tirant lo blanch, 2006.

Ávila Gómez, Enrique. *Derecho Penal del Enemigo. Un análisis comparado en los sistemas penales de EEUU y España*. 2ª Edición. Ed. Lulu.com, 2010.

Ballesteros Moffa, Luis Ángel. *La privacidad electrónica.* Valencia: Tirant lo blanch, 2005.

Barcelona Llop, J. *El régimen jurídico de la policía de seguridad*, Instituto Vasco de Administración Pública. Oñate, 1988.

Barcelona Llop, Javier. *Escuchas telefónicas y acción de la policía de seguridad (a partir*

de la Sentencia del TEDH sobre el Caso Malone). Revista de Administración Pública núm. 112. 1987, págs. 61-105.

Barcelona Llop, Javier. *Policía y Constitución.* Madrid: Tecnos S.A., 1997.

Barcelona Llop, Javier. *Principios básicos de actuación de las fuerzas policiales*. *Policía y seguridad: Análisis jurídico-público.* Oñate, 1990, págs. 45-76.

Barnés Vázquez, Javier. *El principio de proporcionalidad.* Cuadernos de Derecho Público, núm. 5, 1998.

Barnés Vázquez, Javier. *Introducción al principio de proporcionalidad en el Derecho comparado y comunitario.* Revista de Administración Pública núm. 135, págs. 485 y ss, 1994.

Bello Janeiro, Domingo, y otros. *El derecho a la intimidad y a la privacidad y las administarciones públicas.* Santiago de Compostela: Escola Galega de Administración Pública, 1999.

Beltrán, Francisco y Molina, Ignacio. *Retos y transformaciones actuales del Estado.* Barcelona: Universitat Oberta de Catalunya, 2010.

Bernal Pulido, Carlos. *El principio de proporcionalidad y los derechos fundamentales.* Madrid: 2006, págs. 251-486.

Blázquez González, Félix. *La Policía Judicial.* Madrid: Tecnos, 1998.

Boix Reig, Francisco Javier. *Policía y Administración de Justicia,* en el I Seminario de colaboración institucional entre la Universidad Internacional Menéndez Pelayo y la Dirección General de la Policía, *Policía y Sociedad.* Dirección General de la Policía. Santander, 1989.

Brenner, Susan W. *Organized crime? How cybercrime may affect the structure of criminal relationships.* North Carolina Journal of Law and Technology. 2002.

Camon, A. *L'acquisizione dei dati sul traffico elle comunicazioni".* Rivista italiana di

Diritto e Procedura Penale, Fasc. 2. Aprile-Giugno 2005, págs. 594-650.

Choo, Kim-Kwang Raymond. *Organised crime groups in cyberspace: a typology*. Trends in Organized crime, Vol. 11, págs. 270-295, 2008.

Cobo del Rosal, Manuel y Vives Antón, Tomás Salvador. *Derecho Penal. Parte General.* Valencia, 1987.

Conde-Pumpido Ferreiro, Cándido. *La Policía Judicial: Sus relaciones con el Ministerio Fiscal.* Cuadernos de la Guardia Civil. Madrid, 1990.

Corral Escáriz, Vicente. *Problemática de la Policía Judicial: composición, dependencia y funciones.* Madrid, 2010 (En imprenta).

Corripio Gil-Delgado, María de los Reyes y Marroig Pol, Lorenzo. *El tratamiento de los datos de carácter personal y la protección de la intimidad en el sector de las telecomunicaciones.* Madrid: Agencia de Protección de Datos, 2001.

Crump, C. *Data retention: Privacy, Anonymity, and Accountability Online*. Stanford Law Review, nº. 1, volume 56, october 2003.

Davara Rodríguez, Miguel Angel, y otros. *XVII Encuentros sobre Informática y derecho.* Madrid: Universidad Pontifica de Comillas, 2002-2003.

Davara Rodríguez, Miguel Angel. *Análisis del Real Decreto 1720/2007: El reglamento de la LOPD.* Madrid: Editorial DaFeMa, 2008.

Davara Rodríguez, Miguel Angel. *Código de Internet.* Colección de códigos profesionales. 3ª Edición. Cízur Menor (Navarra): Editorial Thomson Aranzadi SA, 2007.

Davara Rodríguez, Miguel Angel. *La seguridad en las transacciones electrónicas: La firma electrónica.* Madrid: Universidad Pontifica de Comillas ICAI-ICADE, 2005.

Davara Rodríguez, Miguel Angel. *Manual de derecho informático.* 9ª Edición. Cízur Menor (Navarra): Editorial Aranzadi SA, 2007.

de la Oliva Santos, Andrés, Gascón Inchausti, Fernando y Aguilera Morales, Marién (Coordinadores). *E-Justicia en la Unión Europea.* Cízur Menor: Aranzadi, 2012. ISBN 9788499039824.

de la Oliva Santos, Andrés, y otros. *Derecho procesal penal.* Madrid: Editorial Universitaria Ramón Areces, 2007.

de la Oliva Santos, Andrés. *Jueces imparciales, Fiscales investigadores, y nueva reforma para la vieja crisis de la Justicia Penal.* Barcelona: Ed. Promociones y Publicaciones Universitarias, 1988.

de Llera Suárez-Bárcena, Emilio. *Derecho procesal Penal (Manual para Criminólogos y Policías).* 2ª Edición. Valencia: Tirant lo Blanch, 1997.

del Castillo Vázquez, Isabel-Cecilia. *Protección de datos: Cuestiones constitucionales y administrativas.* Cízur Menor (Navarra): Thomson Civitas, 2007.

del Moral Torres, Anselmo. *Cooperación policial en la Unión Europea. Planteamiento de un Modelo Europeo de Inteligencia Criminal. Tesis Doctoral.* Madrid: UNED, 2010.

Delgado Martín, Joaquín. *Criminalidad organizada.* Barcelona: J. M. Bosch, 2001.

Díaz Bermejo, Guillermo. *SITEL. La gran oreja del Gobierno no tiene suficientes garantías jurídicas.* Noticias Jurídicas, octubre de 2009.

Díaz Martínez, Manuel. *La dudosa constitucionalidad de la regulación legal de las medidas limitativas de derechos fundamentales del deudor en el proceso concursal*, en Estudios de Deusto, Vol. 59/2, Julio/Diciembre 2011, págs. 259-276.ISSN: 0423-4847.

Díez-Picazo y Ponce De León, Luis. *La doctrina de los actos propios: un estudio crítico sobre la jurisprudencia del Tribunal Supremo*. Barcelona: Bosch, 1963.

Dolz Lago, Manuel-Jesús. *La aportación científico-policial al proceso penal*. Universidad Internacional Menéndez Pelayo. Seminario sobre la policía

científica del siglo XXI en el marco europeo, 2008.

Donini, Massimo. *Derecho penal de lucha. Lo que el debate sobre el derecho penal del enemigo no debe limitarse a exorcizar* en Cancio Meliá, Manuel y Pozuelo Pérez, Laura. *Política criminal en vanguardia. Inmigración clandestina, terrorismo, criminalidad organizada.* Cízur Menor (Navarra): Aranzadi S.A., 2008, págs. 29-76.

Enmiendas al Proyecto de Ley 25/2007 - 121/000128. 2007. 128-6, Madrid: Boletín Oficial de las Cortes Generales - Congreso de los Diputados - VIII Legislatura, 7 de mayo de 2007, págs. 17-49.

Esteban Navarro, Miguel Angel. *Glosario de Ingeligencia.* Ministerio de Defensa.

Etxeberría Guridi, José Francisco. *La protección de los datos de carácter personal en el ámbito de la investigación penal.* Madrid: Agencia de Protección de Datos, 1998.

Falcone, Giovanni y Padovani, Marcelle. *Mafia.* Barcelona: Ediciones B, S.A., 1992.

Fernández de Palma, Rosa. *Análisis de la Ley 25/2007, de 18 octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones,* en *La protección de datos en la cooperación policial y judicial.* Madrid: Aranzadi S.A., 2008, págs. 175-176.

Fernández Esteban, M.L. *Nuevas tecnologías, Internet y derechos fundamentales.* Madrid: MacGraw-Hill, 1998.

Fernández Nieto, J. Principio *de proporcionalidad y derechos fundamentales: una perspectiva desde el derecho común europeo*. Madrid: Dykinson, 2008.

Fernández Rodríguez, J.J. *La intervención de las comunicaciones digitales: a propósito del sistema SITEL.* AAVV. *Cuestiones de inteligencia en la sociedad contemporánea*. Seminario de Estudios de Seguridad y Defensa USC-CESEDEN. Centro Nacional de Inteligencia. Ministerio de Defensa, 2011, págs. 61-76.

Fernández Rodríguez, J.J. *Secreto e intervención de las comunicaciones en Internet,* Madrid, 2004.

Fernández Teruelo, Javier Gustavo. *Cibercrimen. Los Delitos cometidos a través de Internet.* Madrid: Constitutio Criminalis Carolina, 2007.

Fernández Villazala, Tomás y García Borrego, José Antonio. 2010. *Derecho procesal penal para la policía judicial.* Madrid: Editorial Dykinson S.L., 2010.

Ferrajoli, Luigi. *Derecho y razón. Teoría del garantismo penal (1989).* Madrid: Trotta, 1995.

Ferrajoli, Luigi. *La legalitá violenta*. Cuadernos de Política Criminal. Madrid, 1990, págs. 305-319.

Finkelhor, David, Mitchell, Kimberley J. y Wolak, Janis. *Child Pornography Possessors Arrested in Internet-Related Crime: Findings From the National Juvenile Online Victimization Study.* Alexandria Va. : National Center for Missing and Exploited Children, 2005.

Forgione, Francesco. *'Ndrangheta. La mafia menos conocidad y más peligrosa del planeta.* Barcelona: Ediciones Destino S.A., 2009.

Fundación Telefónica. *Las TIC en la justicia del futuro.* Madrid: Airel, 2009.

García de Enterría, E. y de la Quadra Salcedo, T. (coordinadores). *Comentarios a la Ley General de Telecomunicaciones. Ley 11/1998, de 24 de abril*. Madrid: Civitas, 1999.

García-Pablos de Molina, Pablo. *Los retos de la moderna criminología empírica.* [aut. libro] J.C. Carbonell Mateu, y otros. *Constitución, derechos fundamentales y sistema penal.* Valencia: Tirant lo Blanch, 2009, págs. 693-716.

Gascón Abellán, Mariana. *La teoría general del garantismo, a propósito de la obra de L. Ferrajoli "Derecho y razón"*. Anuario del Departamento de Derecho de la

Universidad Iberoamericana, número 31, Sección de Previa, 2001.

Gimeno Sendra, Vicente, y otros. *Los derechos fundamentales y su protección jurisdiccional.* Madrid: Colex, 2007.

Gimeno Sendra, Vicente. *El Juez imparcial en la doctrina del Tribunal Constitucional*. Poder Judicial. Núm. Especial VI. Volumen 6. Madrid, 1989, págs. 267-281.

Gimeno Sendra, Vicente. *Propuestas para una nueva Ley de Enjuiciamiento Criminal. La reforma de la LECRIM y la posición del MF en la investigación penal*. Revista del Poder Judicial. Madrid, 2006.

Gimento Sendra, Vicente. *Derecho procesal.* AAVV, Madrid, 1999.

Gimento Sendra, Vicente. *La intervención de las comunicaciones* en *Manual de lucha contra la droga.* ISBN: 978-84-9903-003-6. Cízur Menor (Navarra): Aranzadi. 1ª Edición, 2011.

Gómez Bermúdez, Javier. *No destruirán nuestra libertad.* Madrid: Ediciones Planeta Madrid S.A., 2010.

Gómez de Liaño Fonseca-Herrera, Marta. *Criminalidad organizada y medios extraordinarios de investigación.* Madrid: COLEX, 2004.

Gómez Gómez, Juan de Dios. *Localización de terminales móviles de comunicaciones, nuevos desafíos para la investigación criminal.* Trabajo de investigación fin de CACES. Academia de Oficiales de la Guardia Civil. Aranjuez, 2012.

Gómez Rodríguez, Serafín Rafael. *Los agentes policiales antidroga: Riesgos penales de su actuación en España.* Tesis doctoral. Madrid: Universidad Complutense, 2004.

González Beilfuss, Markus. *Últimas tendencias en la interpretación del principio de proporcionalidad por parte del Tribunal Constitucional Español*. Cuadernos Aranzadi del Tribunal Constitucional núm. 11, 2003.

González López, Juan José. *Comentarios a la ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.* Revista General de Derecho procesal. 16 de octubre de 2008.

González López, Juan José. *Intervención de las comunicaciones: nuevos desafíos, nuevos límites,* en *El Proceso Penal en la Sociedad de la Información. Las nuevas tecnologías para investigar y probar el delito*. Coordinador: Pérez Gil, Julio. VVAA. Ed. La Ley. 2012, págs. 109-172.

González López, Juan José. *Los datos de tráfico de las comunicaciones electrónicas en el proceso penal.* Móstoles (Madrid): La Ley, 2007.

González Montes, José Luis. *Instituciones de Derecho procesal. Parte General.* Granada, 1990.

González Navarro, B.A., *Criptología y libertades públicas,* en Internet y Derecho Penal, Madrid, 2001, págs. 147 y ss.

González-Cuéllar Serrano, Nicolás. *Garantías constitucionales de la persecución penal en el entorno digital.* Prueba y proceso penal. ISBN 978-84-987-6007-1. Valencia: Tirant lo Blanch, 2008.

González-Cuéllar Serrano, Nicolás. *La reforma de la ley de enjuiciamiento criminal: necesidad de su reforma y examen de las sucesivas reformas parciales.* El proceso en el siglo XXI y soluciones alternativas, 2006, ISBN 84-8355-035-0, págs. 69-84.

González-Cuéllar Serrano, Nicolás. *Proporcionalidad y derechos fundamentales en el proceso penal.* Madrid: Colex, 1990.

Gordillo Álvarez-Valdés, Ignacio. *El atestado policial*. Revista de documentación. Madrid, 1996.

Guerrero Palomares, Salvador. *La denominada "prueba de inteligencia policial" o*

"pericial de inteligencia". Revista de Derecho y proceso penal, Núm. 25, 2011.

Häberle, Peter. *Derecho Constitucional común europeo*. Revista de Estudios Políticos, núm. 79, 1993.

Hadnagy, Christopher. *Ingeniería social. El arte del hacking personal.* Ed. Madrid: Anaya, 2011.

Hernández Guerrero, F. J. y Álvarez de los Ríos, J. L. *Medios informáticos y proceso penal.*

Hernández Guerrero, Francisco. Entrevista con el autor mantenida el 22 de noviembre de 2011.

Hernández Guerrero, Francisco. *La intervención de las comunicaciones electrónicas.* Estudios Jurídicos del Ministerio Fiscal, III-2001.

Jar Couselo, Gonzalo. *Jueces-Policías: problemas de relación entre Poderes Judicial y Ejecutivo,* en Rechea Alberola, Cristina (dir.) et al. *La criminología aplicada II.* Consejo General del Poder Judicial. Madrid 1999.

Jiménez Campo, Javier. *La garantía constitucional del secreto de las comunicaciones.* REDC, núm. 20, 1987.

Jiménez Villarejo, José. *La Policía Judicial: Una necesidad, no un problema.* Poder Judicial. Número Especial II, Justicia Penal. Madrid, 1988, págs. 175-188.

Lanzarote Martínez, Pablo. *Intervención de las comunicaciones,* en Rives Seva, Antonio Pablo, y otros. *La Prueba en el proceso penal. Doctrina de la Sala Segunda del Tribunal Supremo.* 4ª Edición. Pamplona: Thomsom - Aranzadi, 2008.

Larenz, Karl. *Derecho justo. Fundamento de ética jurídica*. Cívitas, Madrid, 1985.

Llamas Fernández, Manuel y Gordillo Luque, José Miguel. *Medios técnicos de vigilancia.* [ed.] Consejo General del Poder Judicial. *Los nuevos medios de investigación en el proceso penal. Especial referencia a la tecnovigilancia.*

Madrid, 2007, Vol. II, págs. 207-249.

Llaneza González, P. *Internet y comunicaciones digitales*. Barcelona: Bosch, 2000.

López Barja de Quiroga, Jacobo. *Tratado de Derecho procesal Penal.* Madrid: Aranzadi S.A., 2004.

López González, José. *El principio general de proporcionalidad en Derecho Administrativo.* Sevilla: Instituto García Oviedo, 1988.

López Ortega, J. J. *La admisibilidad de los medios de investigación basados en registros informáticos,* en *Delincuencia informática. Problemas de responsabilidad*. Madrid: Consejo General del Poder Judicial, 2002, págs. 77-111.

López-Barajas Perea, Inmaculada. *La intervención de las comunicaciones electrónicas*. La Ley. Grupo Wolters Kluwer, 2011. ISBN 978-84-8126-816-4.

López-Fragoso Álvarez, Tomás. *Las intervenciones telefónicas en el proceso penal*. Madrid, 1991.

Lupsha, P. *Transnational organized crime versus the nation-state.* Transnational Organized Crime. 1: 21-48, 1996.

Maeztu Lacalle, David. *La identificación del titular del una dirección IP. Problemática en apliación de la Ley 25/2007, de conservación de datos* en *El Proceso Penal en la Sociedad de la Información. Las nuevas tecnologías para investigar y probar el delito.* Coordinador: Pérez Gil, Julio. VVAA. Ed. La Ley. 2012, págs. 241-266.

Marchal Escalona, Nicolás (Director). *Manual de lucha contra la droga.* ISBN: 978-84-9903-003-6. Cízur Menor (Navarra): Aranzadi. 1ª Edición, 2011.

Marchal Escalona, Nicolás. *El atestado. Inicio del proceso penal.* 8ª Edición. Pamplona: Thomson Aranzadi, 2010.

Marchal Escalona, Nicolás. *Policía Judicial y limitación de derechos fundamentales en*

el proceso penal. Tesis Doctoral. Madrid: Universidad Nacional de Educación a Distancia, 2010.

Marchena Gómez, Manuel. *La intervención jurisdiccional del mensaje corto de telefonía móvil (SMS)*. CYBEX The digital forensic company E-newsletter, 2009, págs. 3-7.

Martín Ancín, Francisco y Álvarez Rodríguez, José Ramón. *Metodología del atestado policial. Aspectos procesales y jurisprudenciales.* Madrid: Tecnos, 1999.

Martín Pallín, José Antonio. *El equilibrio entre la conservación de datos y el secreto de las comunicaciones: implicaciones en el proceso penal.* [ed.] Agencia Española de Protección de Datos. *La protección de datos en la cooperación policial y judicial.* Madrid: Aranzadi S.A., 2008, págs. 153-162.

Martínez Pérez, Roberto. *Policía Judicial y Constitución.* [ed.] Ministerio del Interior. Elcano (Navarra): Aranzadi, 2001.

Maza Martín, J.M. *La intervención judicial de las comunicaciones a través de Internet. Internet y Derecho Penal*. Cuadernos de Derecho Judicial núm. 10, 2001, págs. 633–643.

Mena Álvarez, José María. *La Policía Judicial. Los comunistas y la reforma de la Administración de Justicia.* Madrid, 1981, págs. 35-44.

Méndez Alanís, R. *La Policía. Estudio científico-jurídico de la función, órgano y elementos de acción de la policía de derecho o de seguridad.* Tres tomos. Madrid: 1913, 1925 y 1917.

Mir Puig, Santiago. *Introducción a las bases del Derecho Penal. Derecho Penal. Parte General.* Barcelona, 1976.

Mitchison, Neil y Urry, Robin. *Crime and abuse in e-business.* [ed.] IPTS Report. 2001, págs. 19-24. Vol. 57.

Montero Aroca, Juan, y otros. *Derecho jurisdiccional III.* Valencia: Tirant lo blanch,

2007.

Moreno Catena, Víctor. *Dependencia orgánica y funcional de la Policía Judicial.* Poder Judicial. Núm. Especial VIII. Madrid, 1988.

Moreno Catena, Víctor. *Ley de conservación de datos y garantías procesales.* [ed.] Agencia Española de Protección de Datos. *La protección de datos en la cooperación policial y judicial.* Madrid: Aranzadi S.A., 2008, págs. 163-172.

Moreno Chamarro, Ismael. *El proceso penal. Ley de Enjuiciamiento Criminal comentada.* Barcelona: Deusto, 2005.

Morillas Cueva, Lorenzo, y otros. *La intervención de las comunicaciones electrónicas. Posibilidades técnicas y límites jurídicos.* Madrid, 2005.

Navarro Bonilla, Diego. *El ciclo de inteligencia y sus límites.* Cuadernos constitucionales de la Cátedra Fadrique Furió Ceriol ISSN 1135-0679, núm. 48, 2004, págs. 51-66.

Nieto Martín, Adán. *Análisis de la Ley 25/2007, de 18 octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones,* en *La protección de datos en la cooperación policial y judicial.* Madrid: Aranzadi S.A., 2008, págs. 178-181.

Noya Ferreiro, María Lourdes. *La intervención de las comunicaciones orales directas en el proceso penal.* Valencia: Tirant lo Blanch, 2000.

Oliván, A. *De la Administración Pública con relación a España.* Madrid, 1954.

Oliver Lalana, D. *Autorregulación, normas jurídicas y tecnologías de privacidad. El lado virtual del derecho a la protección de datos*, en VVAA, XVII Encuentros sobre Informática y Derecho 2002-2003, Universidad Pontificia Comillas. Madrid 2003.

Oliver Lalana, D. *El derecho fundamental «virtual» a la protección de datos. Tecnología transparente y normas privadas*, *Diario La Ley*, núm. 5592, 22 de

julio de 2002.

Ortíz Pradillo, Juan Carlos. *El registro "on line" de equipos informáticos como medida de investigación del terrorismo (online durchsuchung)* en Serrano-Piedecasas Fernández, José Ramón y Demetrio Crespo, Eduardo (Directores) y AAVV. *Terrorismo y Estado de Derecho*. Madrid: Iustel. Portal de Derecho, 2010, págs. 457-477.

Ortíz Pradillo, Juan Carlos. *Hacking legal al servicio de la investigación criminal: nuevos instrumentos para la investigación y prueba de la delincuencia informática.* Proyecto de Investigación I+D DER2008-03378. *Problemas procesales de la ciberdelincuencia y de la ciberresponsabilidad*, págs. 67-92.

Ortíz Pradillo, Juan Carlos. *Tecnología versus Proporcionalidad en la Investigación Penal: La nulidad de la ley alemana de conservación de los datos de tráfico de las comunicaciones electrónicas.* La Ley Penal, Nº 75, Octubre 2010, Editorial LA LEY.

Pardo Falcón, Francisco Javier. *Los derechos del artículo 18 de la CE en la jurisprudencia del Tribunal Constitucional*. REDC, núm. 34, 1992.

Peces-Barba Martínez, Gregorio. *Los valores superiores.* Madrid, 1986.

Pedraz Penalva, Ernesto y Ortega Benito, Victoria. *El principio de proporcionalidad y su configuración en la jurisprudencia dle Tribunal Constitucional y literatura espacializada alemanas.* El Poder Judicial núm. 17, págs. 69-89. 1990.

Pedraz Penalva, Ernesto. *Notas sobre policía y justicia penal*. Revista Jurídica de Castilla y León. 2008.

Pedraz Penalva, Ernesto. *Sobre la crisis de la justicia.* en *Constitución, jurisdicción y proceso*, Akal, Madrid 1990, p.267.

Perelló Doménech, Isabel. *El principio de proporcionalidad y la jurisprudencia constitucional.* Jueces para la democracia, ISSN 1133-0627, Nº 28, 1997, págs.

69-75.

Pérez Gil, Julio. *Brecha digital en el proceso español: empeños normativos frente a la realidad. INCLUSÃO DIGITAL E GOVERNO ELETRÔNICO.* Lefis series. Zaragoza: Prensas universitarias, 2008, Vol. 3, 3, págs. 53-74.

Pérez Gil, Julio. *El nuevo papel de la telefónia móivl en el proceso penal: ubicación y perfiles de desplazamiento,* en *El Proceso Penal en la Sociedad de la Información. Las nuevas tecnologías para investigar y probar el delito.* Coordinador: Pérez Gil, Julio. VVAA. Ed. La Ley. 2012, págs. 173-218.

Pérez Gil, Julio. *Entre los hechos y la prueba: Reflexiones acerca de la adquisición probatoria en el proceso penal*. León, Revista jurídica de Castilla y León núm. 14, enero de 2008.

Pérez Gil, Julio. *Investigación penal y nuevas tecnologías: Algunos retos pendientes*. León, Revista jurídica de Castilla y León. 2005, Vol. 7.

Pérez Sánchez, Martín. *Posición del sector de telecomunicaciones ante la nueva regulación de protección de datos: Retos y dudas*. [ed.] Agencia Española de Protección de Datos. *La protección de datos en la cooperación policial y judicial.* Madrid: Aranzadi S.A., 2008, págs. 125-132.

Pérez-Cruz Martín, Agustín Jesús y Rodríguez García, Nicolás. *Guía bibliográfica de derecho procesal.* Santiago de Compostela: Tórculo Edicións, 2005.

Prieto Castro y Gutiérrez de Cabiedes, Eduardo. *Derecho Procesal Penal.* Madrid, 1987.

Prieto Navarro, Evaristo. *Excepción y normalidad como categorías de lo político* en Cancio Meliá, Manuel y Pozuelo Pérez, Laura. *Política criminal en vanguardia. Inmigración clandestina, terrorismo, criminalidad organizada.* Cízur menor (Navarra): Editorial Aranzadi S.A., 2008, págs. 77-136.

Prieto Sanchís, L. *Tribunal Constitucional y positivismo jurídico*. Doxa, nº 23, 2000.

Queralt Jiménez, Joan Josep. *El policía y la ley.* Barcelona, 1986.

Queralt Jiménez, Joan Josep. *Introducción a la Policía Judicial.* 3ª Ed. Barcelona: J.M. Bosch Editor, 1999.

Queralt Jiménez, Joan Josep. *Oportunidad, necesidad y legalidad en la actuación policial.* Policía y sociedad. Madrid: s.n., 1990, págs. 162-165.

Requena Espada, Laura. *Delincuencia Organizada: Perfil criminológico de una muestra de miembros activos en organizaciones criminales que han actuado en España entre 1999 y 2010.* Tesis Doctoral. Facultad de Psicología. UAM. Madrid, 2011.

Rico, J. M. y Sala, L. *Inseguridad ciudadana y policía*. Tecnos, Madrid, 1988.

Rifá Soler, José María, Valls Gombau, José F. y Richard González, Manuel. *El proceso penal práctico.* Madrid: La Ley, 2005.

Rives Seva, Antonio Pablo, y otros. *La Prueba en el proceso penal. Doctrina de la Sala Segunda del Tribunal Supremo.* 4ª Edición. Pamplona: Thomsom - Aranzadi, 2008.

Rives Seva, Antonio Pablo. *El testimonio de referencia en la jurisprudencia penal.* Noticias Jurídicas, 2000.

Rodríguez Fernández, Ricardo. *Derechos fundamentales y garantías individuales en el proceso penal.* Granada: Comares, 2000.

Rodríguez Lainz, José Luis. *Dirección IP, IMSI e intervención judicial de las comunicaciones electrónicas.* Córdoba, 2008.

Rodríguez Lainz, José Luis. *El principio de proporcionalidad en la nueva Ley de conservación de datos relativos a las comunicaciones.* Diario La Ley, 7062/2007, Nº 6860, Sección Doctrina, 14 Ene. 2008, Año XXIX, Ref. D-10, Editorial LA LEY.

Rodríguez Lainz, José Luis. *Hacia un nuevo entendimiento del concepto de gravedad*

del delito en la Ley de Conservación de Datos relativos a las Comunicaciones Electrónicas. Diario La Ley, 143/2012, Nº 7789, Sección Doctrina, 2 Feb. 2012, Año XXXIII, Editorial LA LEY.

Rodríguez Lainz, José Luis. *La intervención de las comunicaciones telefónicas.* Barcelona: Bosch S.A., 2002.

Rodríguez Lainz, José Luis. *Los Dispositivos electrónicos de posicionamiento global (GPS) en el proceso penal*. Diario La Ley, Nº 7945, Sección Doctrina, 17 Oct. 2012.

Rodríguez Lainz, José Luis. *Peculiaridades de la intervención judicial de comunicaciones electrónicas.* Diario La Ley, 2009.

Rojas Amandi, Víctor Manuel. *El concepto de derecho de Ronald Dworkin.* Revista de la Facultad de Derecho de México, núm. 246, Sección de Artículos. 2006.

Ruiz Rodríguez, Luis Ramón y González Agudelo, Gloria. *El factor tecnológico en la expansión del crimen organizado. ¿Menores en riesgo?* [aut. libro] Luz María Puente Aba, Mónica Zapico Barbeito y Luis Rodríguez Moro. *Criminalidad organizada, terrorismo e inmigración. Retos contemporáneos de la política criminal.* Granada: Comares S.L., 2008, págs. 1-40.

Ruiz Ruiz, Ramón y de la Torre Martínez, Lourdes. *Algunas aplicaciones e implicaciones del principio de proporcionalidad*. Revista Telemática de Filosofía del Derecho, nº 14, 2011, págs. 27-44 D.L. M-32727-1998 ISSN 1575-7382.

Ruiz Ruiz, Ramón. *La ponderación en la resolución de colisiones de derechos fundamentales. Especial referencia a la jurisprudencia constitucional española.* Revista Telemática de Filosofía del Derecho, nº 10, 2006/2007, ISSN 1575-7382, págs. 53-77.

Ruiz Vadillo, Enrique. *Comentario al Art. 126. La Policía Judicial. Comentarios a las Leyes Políticas, dirigidas por Oscar Alzaga Villamil.* Tomo IX. Madrid, 1987,

págs. 621-635.

Ruiz Vadillo, Enrique. *El proceso penal en el estado social y democrático de derecho*. Cuadernos de la Guardia Civil. Madrid, 1993.

Sacristán París, Francisco. *La inteligencia en el tratamiento de fuentes* en *Manual de lucha contra la droga.* ISBN: 978-84-9903-003-6. Cízur Menor (Navarra): Aranzadi. 1ª Edición, 2011, págs. 681-736.

Sadowsky, George, Zambrano, Raúl y Dandjinou, Pierre. *Internet governance: A discussion document.* United Nations Task Force, 2004.

Sala i Donado, Cristina. *La Policía Judicial.* Aravaca (Madrid): McGraw Hill, 1999.

Salom Clotet, Juan. *Delito informático y su investigación. Delitos contra y a través de las nuevas tecnologías. ¿Cómo reducir su impunidad?* Madrid: Consejo General del Poder Judicial, 2006, Vol. III, págs. 93-129.

Salom Clotet, Juan. *Incidencias de la nueva regulación en la investigación de los delitos cometidos a través de medios informáticos*. [ed.] Agencia Española de Protección de Datos. *La protección de datos en la cooperación policial y judicial.* Madrid: Aranzadi S.A., 2008, págs. 133-152.

Sánchez García de Paz, Isabel. *Problemas de legitimidad de una respuesta excepcional frente a las organizaciones criminales* en Cancio Meliá, Manuel y Pozuelo Pérez, Laura. *Política criminal en vanguardia. Inmigración clandestina, terrorismo, criminalidad organizada.* Cízur Menor (Navarra): Aranzadi S.A., 2008, págs. 451-494.

Sancho Villa, Diana. *Transferencia internacional de datos personales.* Madrid: Agencia de Protección de Datos, 2003.

Sansó-Rubert Pascual, Daniel. *Criminalidad organizada transnacional y seguridad internacional.* [aut. libro] José Julio Fernández Rodríguez, Javier Jordán Enamorado y Daniel Sansó-Rubert Pascual. *Seguridad y defensa hoy.*

Construyendo el futuro. Madrid: Plaza y Valdés Editores, 2008, págs. 207-240.

Saviano, Roberto. *Gomorra.* Barcelona: Debate. Random House Mondadori S.A., 2007.

Scharpf, Fritz W. *Apuntes para una teoría del gobierno multinivel de Europa*. [aut. libro] Agustí Cerrillo i Martínez (Coordinador). *La gobernanza hoy: 10 textos de referencia*: Instituto Internacional del Governabilitat de Catalunya. Estudios Goberna. Ministerio de Administraciones Públicas, 2005.

Schjølberg, Stein y Ghernaouti-Hélie, Solange. *A Global Protocol on Cybersecurity and Cybercrime. An initiative for peace and security in cyberespace.* Oslo: E-dit, 2009.

Serrano Maíllo, Alfonso. *Introducción a la criminología.* Madrid: Dykinson, 2005.

Sieira Mucientes, Sara. *El principio de proporcionalidad como juicio de necesidad y la debida intensidad de control en su aplicación al Legislador.* La Reforma del Tribunal Constitucional: actas del V Congreso de la Asociación de Constitucionalistas de España. Valencia, 2007.

Solís Navarro, Pascual, y otros. *Actuaciones de la Policía Judicial para el proceso penal.* 3ª Ed. Madrid: Academia de Oficiales de la Guardia Civil - Ministerio del Interior, 2007.

Urrea Corres, Mariola. *La cooperación reforzada en la Unión Europea: Concepto, naturaleza y régimen jurídico.* Colex, 2002.

Vallés Causada, Luis. *Análisis crítico de los instrumentos procesales para la lucha contra la criminalidad organizada. Especial referencia a la figura del Agente Encubierto.* Madrid, 2009.

Vallés Causada, Luis. *Apoyo técnico a la investigación. Cuestiones de actualidad*, en *Manual de lucha contra la droga.* ISBN: 978-84-9903-003-6. Cízur Menor (Navarra): Aranzadi. 1ª Edición, 2011.

Vallés Causada, Luis. *Aspectos policiales en la aplicación de la Orden Europea de*

Detención y Entrega. Madrid: UNED, 2009.

Vallés Causada, Luis. *La conservación y cesión de datos sobre telecomunicaciones a la Policía Judicial a la luz de la Ley 25/2007.* Madrid: UNED, 2009.

Vallés Causada, Luis. *Memoria para la obtención del Diploma de Estudios Avanzados*. Madrid: UNED, 2011.

Vallés Causada, Luis. *Problemas procesales para la obtención de inteligencia sobre comunicaciones de telefonía móvil por la Policía Judicial*. Madrid: UNED, 2009.

Vallés Causada, Luis. *Usos delictivos no comunicativos de la telefonía móvil: ¿Una excepción a la protección del art. 18.3 CE?* en *El Proceso Penal en la Sociedad de la Información. Las nuevas tecnologías para investigar y probar el delito*. Coordinador: Pérez Gil, Julio. VVAA. Ed. La Ley. 2012, págs. 219-239.

Vegas Torres, Jaime. *Obtención de pruebas en ordenadores personales y derechos fundamentales en el ámbito de la empresa.* Madrid: Universidad Rey Juan Carlos. Cátedra de investigación financiera y forense KPMG-URJC, 2011.

Velasco Núñez, Eloy. *ADSL y troyanos: Intervención de sus datos y telecomunicaciones en la investigación penal*. La Ley Penal núm. 82: La Ley, 2011

Velasco Núñez, Eloy. *Aspectos procesales de la investigación y de la defensa en los delitos informáticos.* Diario La Ley. Año XXVII. Número 6506. Viernes, 16 de junio de 2006.

Velasco Núñez, Eloy. *Crimen organizado, Internet y nuevas tecnologías*. Conferencia impartida en la Escuela de Especialización de la Guardia Civil. Madrid, 2010.

Velasco Núñez, Eloy. *Delitos cometidos a través de Internet. Cuestiones procesales.* Tesis doctoral. Las Rozas (Madrid): La Ley, 2010.

Velasco Núñez, Eloy. *El confidente.* Madrid: La Ley, 1993, págs. 823-830.

Vidal Fueyo, Camino. *El principio de proporcionalidad como parámetro de*

constitucionalidad de la actividad del Juez. Instituto de Investigaciones Jurídicas de la UNAM. Anuario de Derecho Constitucional Latinoamericano, Núm. 20052, Sección de Previa, 2005.

Vieitez Pérez, Begoña. *El Tratado de Lisboa: Una aproximación al espacio de libertad, seguridad y justicia.* Madrid: Centro de Análisis y Prospectiva de la Guardia Civil, 2009.

IX. DOCUMENTOS

ABOGACÍA DEL ESTADO	*Documento de referencia A. G. Entes Públicos 182/08*	29/12/2008
AEPD	*Solicitudes de datos efectuadas por la Policía Judicial sin mandamiento judicial o requerimiento previo del Ministerio Fiscal*	1999-0000
AEPD	*Carácter de dato personal de la dirección IP*	2003-0327
AEPD	*Cesión de la dirección IP a las Fuerzas y Cuerpos de Seguridad*	2004-0213
AEPD	*Cesión de datos de abonados a la Policía Judicial*	2005-0297
AEPD	*Cesión de datos en procedimiento judicial sin consentimiento del afectado*	2005-0479
AEPD	*Informe jurídico sobre cesión de datos a la Policía Judicial sin Mandato Judicial*	2008-0133
AEPD	*Informe Jurídico sobre la aplicación de la Ley 25/2007 a las personas jurídicas*	2008-0420
CONSEJO DE EUROPA	*Conclusiones del Consejo relativas a un Plan de Acción para establecer una estrategia común para combatir el cibercrimen*	26/04/2010
ESTADOS UNIDOS	*"National Security Strategy"*	01/05/2010
FORO ECONÓMICO MUNDIAL	*Global Risks 2011*	01/01/2011
FORO ECONÓMICO MUNDICAL	*Global Risks 2012*	01/01/2012
FUNDACIÓN ORANGE	*eEspaña 2012. Informe sobre el desarrollo de la sociedad de la información en España de la Fundación Orange*	00/00/2012
G-8	*Meeting of Justice and Interior Ministers of The Eight*	10/12/1997

	December 9-10, 1997. Communiqué. Washington, D.C.	
G-8	*"G-8 Leaders Statement on Countering Terrorism".*	26/06/2010
IEEE	*Documento de análisis del IEEE 15/2010 sobre el Resultado de la Cumbre de la OTAN de Lisboa de noviembre de 2010*	22/11/2010
MICROSOFT	*Security Intelligence Report. Volume 9, January through june 2010.*	01/06/2010
MINISTERIO DE DEFENSA	*"Nuevo concepto estratégico".*	01/01/2010
MINISTERIO DE INDUSTRIA	*Propuesta de Agenda Digital para España*	25/07/2012
MINISTERIOS DE INTERIOR E INDUSTRIA	*Convenio Marco de Colaboración en materia de ciberseguridad entre la Secretaría de Estado de Seguridad del Ministerio del Interior y la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información del Ministerio de Industria, Energía y Turismo*	04/10/2012
ONU	*Carta de las Naciones Unidas*	26/06/1945
ONU	*Declaración Universal de los Derecho Humanos.*	10/12/1948
ONU	*Convención de las Naciones Unidas contra la delincuencia organizada transnacional (Convención de Palermo).*	15/11/2000
ONU	*Asamblea General: Declaración de Viena sobre la delincuencia y la justicia.*	04/12/2000
ONU	*Consejo Económico y Jurídico: "Instrumentos jurídicos internacionales, recomendaciones y otros documentos existentes que tratan de la corrupción".*	02/04/2001
ONU	*Convención de las Naciones Unidas contra la*	31/10/2003

	corrupción.	
ONU	*Internet Governance: A Discussion Document. Prepared for the United Nations ICT Task Force*	15/03/2004
ONU	*Convención de las naciones unidas contra la delincuencia organizada transnacional y sus protocolos (Convención de Nueva York).*	01/11/2004
ONU	*"Un mundo más seguro: la responsabilidad que compartimos". Documento del Quincuagésimo noveno período de sesiones. Tema 55 del programa. Seguimiento de los resultados de la Cumbre del Milenio. A/59/565.*	02/12/2004
ONU	*Declaración de Bangkok: Sinergias y respuestas: alianzas estratégicas en materia de prevención del delito y justicia penal*	25/04/2005
ONU	*12º Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal. Novedades recientes en el uso de la ciencia y la tecnología por los delincuentes y por las autoridades competentes en la lucha contra la delincuencia, incluido el delito cibernético. A/CONF.213/9*	22/01/2010
ONU	*Declaración de Salvador sobre estrategias amplias ante problemas globales: los sistemas de prevención del delito y justicia penal y su desarrollo en un mundo en evolución*	19/04/2010
ONU	*The Globalization of Crime: A Transnational Organized Crime Threat Assessment (TOCTA).*	01/06/2010
ONU	*"The Globalization of Crime: A Transnational Organized Crime Threat Assessment".*	01/06/2010
ONU	*Conferencia de las Partes en la Convención de las Naciones Unidas contra la delincuencia organizada Transnacional.*	04/08/2010

	"Actividades de la Oficina de las Naciones Unidas contra la Droga y el Delito para hacer frente a las formas nuevas de delincuencia". (CTOC/COP/2010/3).	
OTAN	*"NATO 2020: Assured security; dynamic engagement. Analysis and recommendations of the group of experts on a new strategic concept for NATO" (Informe Albright).*	17/05/2010
REINO UNIDO	*"A Strong Britain in an Age of Uncertainty: The National Security Strategy"*	01/10/2010
SYMANTEC	*W32.Stuxnet Dossier. Versión 1.3.*	01/11/2010
UE	*Grupo del artículo 29: "Documento de trabajo. Privacidad en Internet: Enfoque comunitario integrado de la protección de datos en línea"*	21/11/2000
UE	*Comunicación al Consejo, al Parlamento Europeo, al Comité Económico y Social y al Comité de las Regiones, sobre la Creación de una sociedad de la información más segura mediante la mejora de la seguridad de las infraestructuras de información y la lucha contra los delitos informáticos. COM(2000) 890 final.*	26/01/2001
UE	*Decisión del Consejo relativa a la celebración, en nombre de la Comunidad Europea, de la Convención de las Naciones Unidas contra la delincuencia organizada Transnacional. (2004/579/CE).*	29/04/2004
UE	Comunicación de la Comisión sobre el "*Espacio de Libertad, Seguridad y Justicia: balance del programa de Tampere y futuras Orientaciones*", COM (2004) 401 final)	02/06/2004
UE	Programa de La Haya: *"Diez prioridades para los próximos cinco años. Una asociación para la*	10/05/2005

	renovación europea en el ámbito de la libertad, la seguridad y la justicia”, COM(2005) 184 final	
UE	*Convenio relativo a la profundización de la Cooperación transfronteriza, en particular en materia de lucha contra el terrorismo, la delincuencia transfronteriza y la migración ilegal, (Tratado de Prüm)*	27/05/2005
UE	*Comunicación de la Comisión al Consejo y al Parlamento Europeo sobre "Desarrollo de un concepto estratégico para hacer frente a la DO" COM(2005) 232 final,*	02/06/2005
UE	*Dictamen 3/2006 del Grupo de Trabajo del Artículo 29 sobre protección de datos (WP119); Informe 01/2010.*	25/03/2006
UE	*Comunicación de la Comisión al Consejo y al Parlamento Europeo sobre el papel de Eurojust y la Red Judicial Europea en el marco de la lucha contra la delincuencia organizada y contra el terrorismo en la Unión Europea COM(2007) 644 final*	23/10/2007
UE	Dictamen del Grupo de Trabajo del Artículo 29 sobre cuestiones de protección de datos relacionadas con los motores de búsqueda.	04/04/2008
UE	*Hacia una estrategia europea en materia de e-Justicia (Justicia en línea). COM(2008) 329 final.*	30/05/2008
UE	*Decisión Marco 2008/841/JAI del Consejo de 24 de octubre de 2008, relativa a la lucha contra la DO.*	24/10/2008
UE	*Decisión del Consejo sobre la creación de un Comité Permanente de Seguridad Interior.*	27/11/2009
UE	*Programa de Estocolmo – Una Europa abierta y segura que sirva y proteja al ciudadano*	03/03/2010
UE	*Estrategia de Seguridad Interior de la Unión*	26/03/2010

	Europea: "Hacia un modelo europeo de seguridad".	
UE	*Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. Garantizar el espacio de libertad, seguridad y justicia para los ciudadanos europeos. Plan de acción por el que se aplica el programa de Estocolmo. COM(2010) 171 final.*	20/04/2010
UE	*Propuesta de Directiva del Parlamento Europeo y del Consejo sobre la Orden Europea de Investigación en asuntos criminales.*	03/06/2010
UE	*Comunicación de la Comisión al Consejo y al Parlamento Europeo. Panorama general de la gestión de la información en el espacio de libertad, seguridad y justicia. COM(2010)385 final.*	20/07/2010
UE	*"Comunicación de la Comisión al Consejo y al Parlamento Europeo Panorama general de la gestión de la información en el espacio de libertad, seguridad y justicia".*	26/07/2010
UE	*Propuesta de Directiva del Parlamento Europeo y el Consejo sobre los ataques a los sistemas de información y modificando la Decisión Marco del Consejo 2005/222/JHA*	30/09/2010
UE	*Lista de control de los Derechos Fundamentales de la Comisión control para todas las propuestas legislativas. Estrategia para la aplicación efectiva de la Carta de los Derechos Fundamentales por la Unión Europea* COM (2010) 573/4.	20/10/2010
UE	*Conferencia "Taking on the Data Retention Directive" Discurso del Supervisor Europeo de Datos, Sr. Peter Hustinx sobre "The moment of truth for the Data*	03/12/2010

	Retention Directive".	
UE	*Dictamen del Supervisor Europeo de Protección de Datos sobre la Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones — «Un enfoque global de la protección de los datos personales en la Unión Europea» (2011/C 181/01).*	14/01/2011
UE	*Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones sobre la protección de infraestructuras críticas de Información «logros y próximas etapas: hacia la ciberseguridad global» COM(2011) 163 final*	31/03/2011
UE	*Informe de la Comisión al Consejo y Parlamento Europeo. Informe de evaluación sobre la Directiva de conservación de datos (Directiva 2006/24/CE), COM(2011) 225 final.*	18/04/2011
UE	*Propuesta de Directiva del Parlamento Europeo y del Consejo relativa a los ataques contra los sistemas de información, por la que se sustituye la Decisión marco 2005/222/JAI del Consejo, de 30 de mayo de 2011.*	30/05/2011
UE	*Special Eurobarometer 371, Wave EB75.4 TNS Opinion & Social de la Comisión Europea*	01/11/2011
UE	*Combatiendo el cibercrimen y protegiendo la privacidad en la nube.*	01/10/2012
UIT	*El ciberdelito: guía para los países en desarrollo.*	01/04/2009