LA LUCHA CONTRA EL DELITO EN LA RED

JOSÉ ALBERTO FERNÁNDEZ RODERA

MAGISTRADO DE LA AUDIENCIA NACIONAL

RESUMEN

La lucha contra el crimen en el proceloso mundo digital precisa de un marco jurídico adecuado, lo que obliga al legislador a una rigurosa labor de adaptación frente a los efectos del uso de las nuevas tecnologías por los delincuentes. La ley penal sustantiva ofrece respuesta a las actividades ilícitas en la red, aunque en forma dispersa, pues resultaría sumamente dificultosa una de naturaleza autónoma. Así el principio de territorialidad queda con frecuencia desdibujado, lo que hace que la cooperación internacional sea esencial.

Palabras clave: Cibedelincuencia, efecto lesivo, prueba electrónica, dirección IP

ABSTRACT

Fight against crime in the complex digital era precise an accurate legal framework, which forces the legislator to implement a strict effort of adaptation against the effects of the use of new technologies by criminals. The substantive criminal law offers new answers to the online illegal activities, but in a scattered way, as it would be extremely difficult to give an independent answer. The principle of territoriality is sometimes disfigured, which makes international cooperation an essential tool.

Key words: Cybercrime, harmful effect, electronic proof, internet protocol (IP)

1. INTRODUCCIÓN

Cuando CLAUSEWITZ hablaba de la "niebla de la guerra" no podía imaginar que en el futuro la llamada "nube" cibernética y sus proteicos aledaños conformarían un escenario cuajado de riesgos e incertidumbres. No corresponde analizar ahora la ciberguerra y los ciberataques a ella inherentes[1], pues transitaremos por el mundo de la ciberdelincuencia. Pero permítase aprovechar la expresión del prusiano, a la vista de los problemas vinculados al uso ilícito de la red, emparentando ambas metáforas. La "nube" es "niebla", un mundo de constantes y mudables incógnitas, en el que el principio de territorialidad muchas veces se difumina e incluso volatiliza o en el que el secreto de las comunicaciones queda relativizado en dispositivos sin retorno, sean monodireccionales (un terminal móvil se utiliza como detonador) o multidireccionales (ataques de denegación de servicio con difusión de "*malware*"). Botones de muestra

1 "*Empleo del ciberespacio en la guerra asimétrica*", Grupo de Trabajo nº 2, XXXIII Curso de Defensa Nacional (2013), coordinado por el autor, disponible en *www.defensa.gob.es* ; *"Ciberguerra y derecho al ius ad bellum y el ius in bello en el ciberespacio" ,* JÉRÓNIMO DOMINGUEZ BASCOY, *Revista Española de Derecho Militar* núm. 100; *"Responsabilidad penal internacional en el ciberespacio",* KAI AMBOS, *Indret, Revista para el Análisis del Derecho*, abril 2015.

de las dificultades que el ámbito considerado procura al Derecho, un espacio del que se dice que ya mueve más dinero que el narcotráfico. Intentaremos abordarlo desde una perspectiva penal, en lo sustantivo y en lo procesal.

2. EL MARCO JURÍDICO DE REFERENCIA

Las normas básicas a tener en cuenta son la Constitución (art. 18 CE), el Código Penal (CP), la Ley de Enjuiciamiento Criminal (LECrim.), con especial incidencia de la Ley Orgánica 13/2015, que la modifica, entre otros aspectos, en lo relativo a la regulación de medidas de investigación tecnológica, la Ley Orgánica de Protección de Datos (LO 15/99, de 13 de diciembre, LOPD), la Ley de Servicios de la Sociedad de la Información y Comercio Electrónico (L. 34/02, de 11 de julio), la Ley de Conservación de Datos relativos a las Comunicaciones Electrónicas (L. 25/07, de 18 de octubre) y la Ley General de Telecomunicaciones (L. 9/14, de 9 de mayo, LGT).

Las normas internacionales a considerar son el Convenio sobre la Ciberdelincuencia (Budapest, 23 de noviembre de 2001), con Instrumento de ratificación publicado en el BOE 226/10, de 17 de diciembre de 2010, y la Directiva 2002/58, relativa al correo electrónico, sin olvidar las de naturaleza más general, Declaración Universal de Derechos Humanos de 1948 (art. 12), Convenio de Roma de 1950 (art.8), Pacto Internacional de Derechos Civiles y Políticos de 1966 (art. 17) y Carta de Derechos Fundamentales de la UE respecto de la vida privada y familiar (art. 7). Al hilo de la exposición se irán trayendo a colación. La Recomendación CM/Rec (2014) 6, del Consejo de ministros a los estados miembros, se refiere a una Guía de los derechos humanos para los usuarios de internet (Consejo de ministros de 16 de abril de 2014, en la 1.197ª reunión de delegados de los ministros) y determina que nadie debe ser sometido a medidas generales de vigilancia o interceptación, así como que solo en circunstancias excepcionales definidas en la ley, como sería la investigación de un delito, se podrá quebrantar la privacidad con respecto a los datos personales.

Conviene resaltar que la Disposición Final Segunda de la Ley 9/2014, de 9 de mayo, de Telecomunicaciones, modifica la reseñada Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico. Introduce un apartado cinco bis en la disposición adicional sexta, en el que se habilita a la autoridad de asignación para suspender cautelarmente o cancelar, de acuerdo con el correspondiente requerimiento judicial previo, los nombres de dominio mediante los cuales se esté cometiendo un delito o falta tipificado en el Código Penal, lo que también podrá hacer cuando las Fuerzas y Cuerpos de Seguridad del Estado le dirijan requerimiento de suspensión cautelar dictado como diligencia de prevención dentro de las 24 horas siguientes al conocimiento de los hechos. Se introduce también una disposición adicional octava, en la que se regula la colaboración de los registros de nombres de dominio establecidos en España en la lucha contra actividades ilícitas, y una disposición adicional novena sobre gestión de incidentes de ciberseguridad que afecten a la red de internet, estableciendo la obligación de colaboración con el CERT ("*Computer Emergency Response Team*") competente y disponiendo que la Secretaria de Estado de Telecomunicaciones y para la Sociedad de la Información garantizará un intercambio fluido de información con la Secretaria de Estado de Seguridad del Ministerio del Interior sobre incidentes, amenazas y vulnerabilidades según lo contemplado en la

Ley 8/2011, de 28 de abril, por la que se establecen medidas para la Protección de las Infraestructuras Críticas.

3. LAS PREVISIONES DEL CÓDIGO PENAL

Nuestra ley penal sustantiva no contempla una categoría específica de delitos informáticos, pero bajo diferentes rúbricas incluye conductas que responden a las que se refiere el Convenio de Budapest sobre ciberdelincuencia. Por otra parte, ha de tenerse en cuenta que tanto la Ley Orgánica 1/2015 como la Ley Orgánica 2/2015, ambas de 30 de marzo, que modifican el Código Penal, contemplan nuevas previsiones en la materia que nos ocupa.

Así, dentro de los delitos contra la libertad sexual (Título VIII del Libro II), añade la Ley Orgánica 1/2015 un artículo 183 ter, sancionando al que, a través de internet, del teléfono o de cualquier otra tecnología de la información y la comunicación contacte con un menor de 16 años y proponga concertar un encuentro a fin de cometer cualquiera de los delitos descritos en los artículos 183 y 189. El artículo 189 castiga la pornografía infantil, cualquiera sea el soporte utilizado.

También, dentro de los delitos contra la intimidad (Título X), se tipifica el descubrimiento y revelación de secretos en los apartados 1 y 2 del art. 197 (apoderamiento de mensajes de correo electrónico; apoderamiento, utilización o modificación en perjuicio de tercero de datos reservados de carácter personal o familiar de otro que se hallan registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado). La LO 5/10, de 22 de junio, modificó el precepto y contempló en su apartado 3 el acceso informático sin autorización y en el 8 la realización por grupo u organización criminal. La Ley Orgánica 1/2015 añade al Código los artículos 197 bis a 197 quinquies, con miras a reforzar la protección penal en este ámbito (acceso o facilitación, traslado a terceros, organizaciones o grupos criminales, personas jurídicas).

Dentro de los delitos contra el patrimonio (Título XIII), el hurto informático, aunque no se prevea expresamente (art.534), la sustracción de tarjeta o soporte magnético para acceder (arts. 238 y 239), la estafa informática (art. 248), la apropiación indebida informática, aunque no se contemple expresamente (arts. 252 y 253), la utilización sin autorización de equipos terminales de telecomunicación (art. 256), los daños informáticos (art. 264) y la copia ilegal de programas informáticos (arts. 270 y 271). La Ley Orgánica 1/2015 introduce los artículos 264 bis a 264 quater (interrupción grave de sistema informático, facilitación a terceros, personas jurídicas).

El art. 346, incluido en el Título XVII, (delitos contra la seguridad colectiva), sanciona los estragos que afecten a cualquier medio de comunicación. El nuevo art. 362 quater, dentro de los delitos contra la salud pública, agrava la pena para los casos en que las sustancias se ofrezcan a través de medios de difusión a gran escala.

Por otra parte, dentro de las falsedades (Título XVIII), se encuadra la simulación de tarjetas (arts. 390 y 392) y la fabricación o tenencia de programas destinados a la falsedad documental (art. 400).

Ni que decir tiene que los tipos reseñados no agotan las posibilidades de persecución de otras conductas, pues cabe derivar responsabilidad penal de contenidos

ilícitos o uso instrumental de medios telemáticos, respecto de quienes divulguen, los aprovechen o empleen[2]. Además, tras la reciente reforma de la ley penal sustantiva, en el llamado delito "de odio", del artículo 510, se sanciona el uso de todo tipo de soporte al efecto, cualificando la conducta, la utilización de internet o de tecnologías de la información (en el BOE 26/2015, de 30 de enero, se publicó el Instrumento de Ratificación del Protocolo adicional al Convenio sobre la Ciberdelincuencia relativo a la penalización de actos de índole racista y xenófoba cometidos por medio de sistemas informáticos, hecho en Estrasburgo el 28 de enero de 2003); en el art. 559, dentro de los delitos contra el orden público, se castiga la distribución o difusión pública, a través de cualquier medio, de consignas que inciten a los desórdenes públicos; y, en fin, la Ley Orgánica 2/2015, en lo que a los delitos de terrorismo respecta, incorpora novedades importantes en los arts. 573, 575, 578 y 579 (delitos informáticos, adoctrinamiento o adiestramiento a través de la red y enaltecimiento o justificación en la red, con habilitación al juez o tribunal para la destrucción o borrado de contenidos).

Tan amplio elenco punitivo permite perseguir el uso de "*sniffers*", esto es, rastreadores para acceder a información ajena interceptando correo electrónico o captando datos (art. 197.1), el "*cyberpunk*" o vandalismo electrónico y el "*cracking*" o sabotaje electrónico, con o sin vulneración de claves o sistemas de protección de *software* (art. 264), el "*phising*", fraude bancario o acceso a cuentas ajenas con fines defraudatorios (art. 248.2.b y concordantes)…[3]. Queda, en principio, extramuros del Derecho Penal el "*spamming*" (envío inconsentido de publicidad), que puede ser sancionado administrativamente desde la LOPD, pero que si utiliza sistemas de monitorización previa en la red pudiera vulnerar el secreto de las comunicaciones (art. 197)[4].

Se denomina "*crimeware*" el conjunto de prácticas desarrolladas en Internet que aprovechan fragilidades en los usuarios para obtener beneficio o un propósito dañoso. Pueden incardinarse en los tipos penales reseñados y a los supuestos anteriores, sin afán de exhaustividad, añadiremos las siguientes: "*hacking*" (ataques a sistemas de información), "*pharming*" (suplantación del sistema de resolución de nombres de dominio para conducir a una *web* falsa), "*warez*" (intercambio de archivos protegidos vulnerando licencias), ataques por saturación, ciberescuchas (interceptación de correos)[5], pirateos de *web*, "*carders*" (robos informáticos de tarjetas), "*mailbombing*" (bloqueo de mensajería electrónica), "*phreaking*" (pirateo de líneas telefónicas), ataques "*DOS- Denial of Service*" (denegación de servicio, con saturación de los servicios de red y privando de accesibilidad a *webs*)…[6]. Una práctica reciente, digna

2 "*Consideraciones a propósito del Proyecto de Ley de 2009 de modificación del Código Penal*", págs. 223 a 226 y 245 a 252, Valencia, 2010; "*Comentarios a la Reforma Penal de 2010*", págs. 249 a 256, 269, 270, 277 a 281, Valencia, 2010; "*Comentarios al Código Penal*" (2ª edición), págs. 909 y sigs., en particular 969 a 971 y 1021 a 1024, Valladolid, 2010.

3 La Sentencia de la Sala Segunda del Tribunal Supremo de 2 de diciembre de 2014 se refiere a un supuesto de "*phising*", consistente en la utilización de una dirección de correo perteneciente supuestamente a una caja de ahorros para obtener las claves de cuentas corrientes, con el señuelo de una actualización.

4 "*Jornada sobre seguridad privada en la red; investigación privada y de-prueba en el marco de las nuevas tecnologías*", ABELARDO RAMOS FRADE, Barcelona, marzo 2011.

5 "*Dimensión jurídico-penal del correo electrónico*", MANUEL MARCHENA GÓMEZ, Diario *La Ley* nº 6475, 4 de mayo de 2006; "*¿Una orden judicial para ver un correo electrónico de mi propia empresa?*", XAVIER RIBAS, *xribas.com*, 2014/09/22.

6 "La investigación policial en el ámbito de la informática", F. JAVIER INDA, *Eguzkilore* nº 20, diciembre 2006.

también de mención, vendría dada por la encriptación de ordenadores, pidiendo a cambio del cese un pago en "*bitcoins*".

No puede extrañar, a la vista de cuanto hasta ahora se ha expuesto, que en una relevante Sentencia de la Audiencia Provincial de Madrid (Sección Cuarta), de febrero de 2015, al hilo de unas frases denigrantes en un foro de internet, amparadas en un "*nickname*" anónimo, se reflexione sobre el deber de investigar los delitos cometidos en la red con independencia de su gravedad, recordando que la red de redes es el más potente medio de comunicación y difusión social de nuestro tiempo, en el que se incrementa el efecto lesivo, alcanzando las conductas ilícitas una gravedad que no se puede minimizar[7].

4. LA PRUEBA EN INTERNET[8]

La prueba electrónica tiene naturaleza de prueba documental (art. 26 del CP: "A los efectos de este Código se considera documento todo soporte material que exprese o incorpore datos, hechos o narraciones con eficacia probatoria o cualquier otro tipo de relevancia jurídica"). Y jurisdiccionalmente se prevé su valoración en el art. 726 LECrim. ("El Tribunal examinará por sí mismo los libros, documentos y demás piezas de convicción…"), así como la utilización de medios técnicos el art. 230 de la Ley Orgánica del Poder Judicial (LOPJ). Por su parte, los arts. 567, 573 y siguientes de la LECrim. consideran los documentos prueba de convicción, con miras al esclarecimiento de los hechos. En el campo que nos ocupa rige también, como no puede ser menos, el principio de libre valoración de la prueba por el juzgador, que la apreciará "según su conciencia" y a su "libre arbitrio" (art. 741 LECrim.), sin poder tener en cuenta la obtenida ilícitamente, con violación de derechos o libertades fundamentales (art. 11 LOPJ) y siempre bajo imperativos lógicos, máximas de experiencia o de la sana crítica. En definitiva, las pruebas obtenidas en la red deberán cumplir idénticos requisitos que las recabadas en otras áreas de investigación, pudiéndose utilizar en un proceso todos los medios técnicos de documentación y reproducción pertinentes, siempre que reúnan adecuadas garantías de autenticidad, con arreglo a lo previsto en el art. 230 LOPJ.

Ahora bien, la secuencia lógica en una metodología de investigación podría ser la que sigue: identificación del emisor, dirección electrónica del ordenador, domicilio-sistemas de almacenamiento, autor. En este escalonamiento descollará el *IP* ("*internet protocol*") como medio de prueba, en cuanto identificador de cada terminal conectado a Internet, cuya huella queda en los sitios *web* accedidos, registrada en un *log* (fichero de registro). Esa dirección *IP* es pública, pero se reputa dato personal y se deberá obtener autorización judicial para que el *ISP* ("*Internet Service Provider*", proveedor de servicios en Internet, esto es, una empresa dedicada a conectar a internet a los usuarios o las distintas redes que tengan y ofrecer el mantenimiento necesario para que el acceso funcione correctamente) facilite nombre y datos personales del usuario. Volveremos luego sobre ello.

7 "*Actualidad Diaria*", núm. 2838, 27 de febrero de 2015 (publicación de *paraprofesionales.com*)

8 "*La actuación de la policía judicial en el proceso penal*", PEDRO MARTÍN GARCÍA (dir.), en particular págs. 151 a 157, Madrid/Barcelona 2009; "*La valoración de la prueba en soportes informáticos*", ROCÍO MORA DÍAZ, noticias.jurídicas.com, junio 2004.

En lo que respecta a las resoluciones judiciales (que revestirán forma de auto) resultarán imprescindibles en una investigación tipo y afectarán a cuatro aspectos: sobre proveedor de acceso (dirección electrónica y momento de conexión), sobre proveedor de servicios (identidad del abonado), sobre interceptación de comunicaciones y sobre, finalmente, entrada y registro. Es evidente que ha de garantizarse la identidad e integridad de los datos obtenidos en la cadena de custodia, en la que tendrá papel relevante el secretario judicial, en su calidad de titular de la fe pública[9].

Problemas prácticos en estas investigaciones en la red, en lo atinente a la determinación de la autoría delictiva, se plantean habitualmente cuando el ataque informático se realiza desde un ordenador público y el establecimiento (por ejemplo, un cibercafé) no tiene registro de usuarios, también cuando el acceso a Internet se produce desde un portátil con tarjeta prepago y asimismo en los casos de "*hackers*" que atacan servidores o difunden virus destructivos, ocultando con un *software* ilegal o "*ad hoc*" su dirección *IP*. En esos casos las dificultades probatorias son evidentes, así como la circunstancia de que la mera identificación del ordenador que se ha usado no integre prueba plena, por si sola, para justificar una atribución de responsabilidad. Además, la prueba indiciaria en internet es muy complejo que determine la autoría, pues localizar un ordenador no implica identificar al usuario y se precisarían elementos probatorios complementarios.

Un importante escollo entraña el carácter a menudo internacional de los ilícitos cometidos en o a través de la red. Su posible comisión desde cualquier rincón del mundo relativiza y desvirtúa el principio de territorialidad[10]. La cooperación policial internacional resulta imprescindible, sea a través de INTERPOL, sea a través de EUROPOL (arts. 2.1 y 3.1 del Convenio sobre Europol, derivado del art. K.3 del Tratado de la UE, hecho en Bruselas el 26 de julio de 1995). El Convenio Europeo de asistencia judicial en materia penal, de 29 de mayo de 2000, establece en su art. 6.4 que, en caso de urgencia, las solicitudes de asistencia judicial podrán transmitirse por conducto de INTERPOL o de cualquier órgano competente según las disposiciones adoptadas en virtud del Tratado de la UE (EUROPOL). Esto no descarta la posible cooperación bilateral, normalmente a través de los consejeros y agregados de Interior en las legaciones diplomáticas del Reino de España. Merece la pena destacar que los "*analysis work files*" de EUROPOL integran un instrumento técnico de primerísimo nivel en la coordinación de la lucha contra la criminalidad cibernética internacional.

En cuanto a la competencia de la jurisdicción española en relación con hechos cometidos fuera de nuestro territorio nacional, habrá de estarse, claro está, a cuanto disponen los arts. 23 y 65 LOPJ. Al respecto, resulta interesante aludir a la reciente Sentencia de la Audiencia Nacional, Sala de lo Penal, Sección 2ª, de 5 de marzo de 2015, dictada en el recurso 5/2014 (caso "*Youkioske*"), y referida a delito contra la propiedad intelectual cometido a través de una *web* alojada en servidores canadienses, pues en su momento asumió la competencia para conocer de los hechos el Juzgado Central de Instrucción núm.5, tras recurso del Ministerio Fiscal, no sólo por perjudicar a una pluralidad de afectados, también por tener una difusión nacional e internacional.

9 Ob. cit., *"Jornada sobre…".*

10 "La investigación policial en Internet: estructuras de cooperación internacional", ANTONIO LÓPEZ, Revista de Internet, Derecho y Política (UOC), número 5, 2007.

Por último, como ya apuntamos, la Ley Orgánica 13/2015, de 5 de octubre, ha introducido en la Ley de Enjuiciamiento Criminal una avanzada y detallada regulación de las medidas de investigación tecnológica. Se verifica en los Capítulos V a VII del Titulo VIII del Libro II, artículos 588 ter a a 588 quinquies c, con acomodo a la jurisprudencia del Tribunal Supremo, tal como enfatiza el Preámbulo de la norma. La regulación también sigue aguas a los principios que al respecto ha decantado el Tribunal Constitucional, con pleno respeto al de especialidad, prohibiéndose las medidas de investigación tecnológica de naturaleza prospectiva (STC 253/2006, de 11 de septiembre). La pertinente resolución judicial habilitadora se ajustará a los principios de idoneidad, excepcionalidad, necesidad y proporcionalidad, y está obligada a cumplir, lógicamente, con el deber constitucional de motivación.

Se regula la solicitud de prórroga, la duración, el secreto, el control de la medida, la afectación a terceras personas, la utilización de información en procedimiento distinto, el cese de la medida y la destrucción de registros. En cuanto a la interceptación de comunicaciones telefónicas y telemáticas, se siguen análogos criterios que los que rigen con carácter general. Las nuevas normas autorizan la intervención y registro de las comunicaciones de cualquier clase que se realicen a través del teléfono o de cualquier otro medio o sistema de comunicación telemática, lógica o virtual. La correspondiente resolución judicial habilitante deberá motivar si resulta imprescindible la interceptación de SMS, MMS o cualquier otra forma de comunicación telemática de naturaleza bidireccional. La medida tendrá un plazo máximo de tres meses, ampliable a dieciocho.

Es exigible la utilización de un sistema de sellado o firma electrónica que garantice la información volcada desde el sistema central, con la finalidad de asegurar la autenticidad e integridad de los soportes puestos a disposición judicial, al socaire de la jurisprudencia de la Sala Segunda del Tribunal Supremo. También se contempla el borrado y eliminación de las grabaciones originales, una vez concluido el procedimiento judicial. La reforma es tributaria de la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones, pues requiere autorización judicial para su cesión a los agentes facultados, siempre que se trate de datos vinculados a procesos de comunicación, siempre bajo el principio de proporcionalidad. Se ofrece un tratamiento jurídico individualizado al acceso por agentes de policía al IMSI, IMEI, dirección IP y demás elementos de identificación de tarjeta o terminal. La cesión de datos desvinculados de los procesos de comunicación relativos a la titularidad o identificación de un dispositivo electrónico también es regulada, datos a los que podrá acceder el Ministerio Fiscal o la Policía Judicial en el ejercicio de sus funciones sin necesidad de autorización judicial.

En lo atinente a la captación y grabación de comunicaciones orales mediante dispositivos electrónicos, no son posibles autorizaciones de carácter general o indiscriminadas, por lo que el dispositivo de escucha y, en su caso, las cámaras a él asociadas, deberán desactivarse tan pronto finalice la conversación cuya captación fue permitida. Asimismo, se regulan los dispositivos de técnicos de seguimiento y captación y el registro de dispositivos informáticos de almacenamiento masivo y el registro remoto de equipos informáticos. En cuanto a las diligencias de investigación tecnológica, se establece como medida de aseguramiento la orden de conservación de datos, hasta que se obtenga la autorización judicial para su cesión. La orden tendrá un plazo máximo de vigencia de noventa días prorrogable hasta que se autorice la cesión o se cumplan ciento ochenta días.

Finalmente, ha de resaltarse que la reforma regula la importante figura del agente encubierto informático, que requiere una autorización judicial para actuar en canales cerrados de comunicación y una autorización especial (en la misma resolución judicial, con motivación separada y suficiente, o en otra distinta), para intercambiar o enviar archivos ilícitos por razón de su contenido en el curso de una investigación.

5. EL ACOPIO Y LA CESIÓN DE DATOS

El art. 12 de la Ley 34/02, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico, dispuso la obligación de retener los datos de conexión y tráfico generados por las comunicaciones establecidas, durante la prestación de un servicio de la sociedad de la información, por un periodo máximo de 12 meses. Esos datos retenidos serían los necesarios para facilitar la localización del equipo terminal empleado.

Posteriormente, la Ley 25/07, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones, deroga ese precepto, entre otros, de la Ley 34/02, y establece la obligación de conservar datos (art. 4) y el período de conservación de esos datos (art. 5) por parte de los sujetos obligados, los operadores que presten servicios de comunicaciones electrónicas disponibles al público o exploten redes públicas de comunicaciones (art. 2). Concreta los datos a acopiar (art.3), el plazo de la obligación se fija en 12 meses, salvo excepciones (art. 5) y, lo que es de notoria relevancia, determina que los datos conservados sólo podrán ser cedidos de acuerdo con lo que dispone la Ley para los fines que se determinan y previa autorización judicial (art. 6). El apartado 2 del art. 6 explicita cuales son los agentes facultados para la cesión de información (miembros de las distintas Fuerzas de Seguridad, en funciones de policía judicial, funcionarios de la Dirección Adjunta de Vigilancia Aduanera, en funciones de policía judicial, y personal del CNI en el curso de investigaciones de su incumbencia). Los arts. 7 y 8 regulan, respectivamente, el procedimiento de cesión de datos y la protección y la seguridad de los datos.

Concordante con la anterior Ley es la Ley General de Telecomunicaciones. 9/14, de 9 de mayo, que establece un marco normativo también aplicable en la materia: art. 41 (protección de los datos de carácter personal) y 42 (conservación y cesión de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones). Su art. 42 se remite a la Ley 25/07 y reitera que la conservación y cesión se hará a los agentes facultados a través de la correspondiente autorización judicial.

Cuestión de interés supone que si la Ley 25/07 invoca en su Preámbulo la Directiva 2006/24/CE, del Parlamento y del Consejo, de 12 de julio, e indica que su transposición a nuestro ordenamiento jurídico es el objeto principal de la Ley, resulta que la Sentencia del Tribunal de Justicia de la Unión Europea de 8 de abril de 2014 ha invalidado la Directiva sobre la conservación de datos, afirmando que la conservación de datos que impone no puede vulnerar el contenido esencial de los derechos fundamentales al respeto de la vida privada y a la protección de datos de carácter personal. Añade que el legislador de la Unión sobrepasó los límites que exige el respeto del principio de proporcionalidad, al no establecer ninguna diferenciación, limitación o excepción en función del objetivo de lucha contra los delitos graves. La Sentencia también cuestiona la regulación del período de conservación de los datos, por no precisar los criterios objetivos con arreglo a los que debe determinarse el período de conservación para

garantizar que se limite a lo estrictamente necesario, así como advierte de la ausencia de garantías suficientes contra el riesgo de abuso y que la Directiva no obliga a que los datos se conserven en el territorio de la Unión.

¿En qué situación queda la Ley 25/07 tras la meritada Sentencia? Sin perjuicio de hipotético pronunciamiento del Tribunal Constitucional sobre afectación de derechos fundamentales o rango de la norma, lo cierto es que si confrontamos la argumentación del Tribunal de Luxemburgo con la Ley 25/07 resulta que ésta, entre otras cautelas, ciñe su aplicación a los delitos graves (art. 1), determina cuales son los datos objeto de conservación en forma exhaustiva (art. 3), establece la obligación de adoptar medidas necesarias para garantizar la adecuada conservación (art. 4), modula el período de conservación (art. 5.1), exige autorización judicial (arts. 6.1 y 7.2), subraya la aplicabilidad del régimen jurídico de protección de datos (arts. 5.2, 8 y 9.2), limita la cesión de información a los agentes facultados a la "que resulte imprescindible" (art. 6.2) y proclama los principios de necesidad y proporcionalidad (art. 7.2), conformando un marco jurídico nacional sobre conservación y cesión de datos inspirado en criterios razonablemente garantistas y que, "*prima facie*", parecen dar respuesta proporcionada a cuantas exigencias parecían incumplidas por la Directiva, salvo en lo relativo a la conservación de los datos en el territorio de la Unión, siquiera explícitamente.

En cualquier caso, en lo que afecte a investigaciones de naturaleza judicial, permítase dar por reproducido cuanto reseñábamos en el ordinal precedente sobre la regulación que ofrece la Ley Orgánica 13/2015 en lo que atañe a la cesión y conservación de datos.

6. CRITERIOS JURISPRUDENCIALES. EL DESLINDE ENTRE RASTREO DE DATOS, DERECHO A LA INTIMIDAD Y DERECHO AL SECRETO DE LAS COMUNICACIONES

Nuestro Tribunal Supremo, en Sentencia de su Sala Segunda de 9 de mayo de 2008 (Recurso de casación 1797/07, Sentencia 236/08), expresó que 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 CE) sino en el marco del derecho a la intimidad personal (art. 18.1 CE) con la salvaguardia que puede dispensar la LOPD y su Reglamento, sin despreciar la LGT y su Reglamento, en los que parece desprenderse que sin el consentimiento de unos datos reservados, contenidos en archivos informáticos, no pueden facilitarse a nadie, salvo en 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. Pero la Sentencia, en relación con rastreos verificados por el equipo de Delitos Telemáticos de la Guardia Civil en Internet, orientados a desenmascarar la identidad críptica de los IPS ("*Internet protocols*") que habían accedido a unos "*hash*" que contenían pornografía infantil, afirma que no se precisa autorización judicial para conseguir lo que es público y el propio usuario de la red es quien lo ha introducido en la misma (la huella de la entrada queda siempre registrada y eso lo sabe el usuario). Y si muchos de los datos se convierten en públicos para los usuarios de Internet estos no se hallan protegidos ni por el art. 18.1 ni por el 18.2 CE. Otra cosa es, agrega la Sentencia, que fuera precisa autorización judicial para desvelar la identidad de la terminal, teléfono o titular del contrato de un determinado IP, en salvaguardia del derecho a la intimidad personal ("*habeas data*"). Abunda en estos criterios la Sentencia 292/08, de 28 de mayo.

En Pleno no jurisdiccional de la Sala Segunda se aprobó, el 23 de febrero de 2010, el siguiente acuerdo: "Es necesaria la autorización judicial para que los operadores que prestan servicios de comunicaciones electrónicas o de redes públicas de comunicación cedan los datos generados o tratados con tal motivo". Añade que "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 25/07, de 18 de octubre". Esta doctrina se refleja en la STS 247/10, de 18 de marzo, en la que, recordando la STC 123/02, de 20 de mayo y la STEDH de 2 de agosto de 1982 ("*caso Malone*"), se llega a la conclusión de que los datos identificativos de un titular o de un terminal deben ser encuadrados no dentro del derecho al secreto de las comunicaciones (art. 18.3 CE), sino en el marco del derecho a la intimidad personal (art. 18.1). El Supremo aclara que la absoluta equiparación de todo tipo de datos de tráfico o externos o la inclusión de todos ellos dentro del derecho al secreto de las comunicaciones comportaría un auténtico desenfoque, en cuanto 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 de autodeterminación informática del art. 18.4 CE. El corolario, puede añadirse, es que se abre la puerta a la aplicación, en los supuestos que no afectan al secreto de las comunicaciones, del régimen jurídico de protección de datos (art. 11.2d LOPD, que permite la cesión, con determinados requisitos, de datos personales al Ministerio Fiscal, entre otras instituciones)[11]. Pero el caso es que, tras el reseñado pleno no jurisdiccional, tal régimen jurídico sólo sería aplicable a hechos anteriores a la Ley 25/07, pues respecto de los posteriores se exige siempre la autorización judicial.

La Sentencia de la misma Sala de 16 de junio de 2014 (recurso de casación 2229/13) recuerda que resultará siempre necesaria la autorización e intervención judicial, en el ámbito del procedimiento penal, la intervención de las comunicaciones protegidas por el derecho consagrado en el art. 18.3 de la Constitución, pero matiza que esa exigencia operará tan sólo respecto a lo que estrictamente constituye ese "secreto de las comunicaciones", es decir, con exclusión de los denominados "datos de tráfico" o incluso de la posible utilización del equipo informático para acceder a otros servicios de la red, como páginas *web*, etc., de los mensajes que, una vez recibidos y abiertos por su destinatario, no forman ya parte de la comunicación propiamente dicha, respecto de los que rigen normas diferentes, como las relativas a la protección y conservación de datos (art.18.4 CE) o a la intimidad documental en sentido genérico y sin la exigencia absoluta de la intervención judicial (art. 18.1 CE).

En esa línea ha de traerse a colación, habida cuenta de la duplicidad de uso (datos y modos de comunicación) que facilitan los "*smartphones*"), la STC 115/13, de 9 de mayo, en la que se indica que la agenda de contactos telefónicos de un móvil es susceptible de control policial sin previa autorización judicial, pues no forma parte del proceso de comunicación, no estando en juego el secreto de las comunicaciones del 18.3 CE. Aunque la agenda de contactos está protegida por el derecho a la intimidad (art. 18.1 CE), no se vulnera ese derecho por el hecho de haber accedido a ella la policía sin consentimiento del titular del terminal y sin autorización judicial, pues ello constituye una afectación leve en la intimidad; la policía actúa persiguiendo un interés constitucionalmente legítimo -el esclarecimiento de un delito grave-, la urgencia del caso –se trataba de un delito flagrante- y existe una habilitación legal.

11 "La dirección IP. Problemas que plantea", EDUARD CHAVELI DONET, en "Fraude electrónico en entidades financieras y usuarios de banca: problemas y soluciones", Pamplona, 2011.

Por su parte –seguimos valorando el interés de una resolución por la existencia y uso profuso de "*smartphones*"-, la STS (Sala 2ª), de 29 de julio de 2013 (recurso de casación 1944/12), reitera doctrina sobre la no necesidad de autorización judicial previa por parte de la policía para obtener el *IMSI* ("*International Mobile Subscriber Identity*" o identidad internacional del abonado a un teléfono móvil) y que una vez obtenido sí será precisa la autorización judicial para que la operadora ceda los datos que obren en sus ficheros, con los que se podrá conocer el concreto número del terminal telefónico para el que se va a solicitar la intervención. En otras palabras, 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 obren en los ficheros de la operadora, sí impondrá el control judicial de su procedencia.

En STS (Sala 2ª) de 26 de diciembre de 2013 (recurso de casación 784/13) se señala que los archivos de un ordenador que no forman parte de un proceso de comunicación son susceptibles de registro policial sin previa intervención policial, sin que, por tanto, la ausencia de intervención del secretario judicial en la recogida de esos archivos, no integrantes de un proceso de comunicación, pueda producir nulidad probatoria alguna. Se reitera la necesidad, en la actuación policial, de motivos de urgencia, de perseguir un interés constitucionalmente legítimo como es el esclarecimiento de un delito y de habilitación legal. La misma Sala, en Sentencia de 26 de noviembre de 2014 (recurso de casación 10.269/14), abordó el caso de los padres de una joven fallecida por sobredosis tras ser inducida a la prostitución a cambio de drogas, que utilizaron el teléfono móvil de la menor para averiguar la identidad de uno de los traficantes. El Tribunal considera prueba lícita los mensajes SMS aportados por los progenitores de la joven (lo que podemos trasladar a los *whatsapp* de un *smartphone*), que consiguieron una vez fallecida, en cuanto asimila las copias de los mensajes con la correspondencia, sin que se hubiera vulnerado el derecho a la intimidad ni el secreto de las comunicaciones y afirma que los sucesores legítimos pueden acceder de forma proporcionada a la documentación en la medida en que fuera necesario para defender sus intereses, incluyendo el ejercicio de las acciones oportunas para reparar los daños causados a la fallecida en los ámbitos civil y penal. La Sala Segunda advierte de la necesidad de que el legislador "subsane con la máxima urgencia" la ausencia de una regulación legal expresa para la intervención de las comunicaciones telemáticas.

Por último, merece la pena traer a colación una Sentencia de la Audiencia Provincial de Granada, Sección 2ª, de 26 de abril de 2013 (apelación 182/12), en la que, en relación con un delito de injurias graves con publicidad a través de Internet, se estima recurso de apelación contra Sentencia de Juzgado de lo Penal, revocando condena como consecuencia de la nulidad de todos los actos de investigación practicados en el proceso de averiguación de la identidad del usuario de Internet que remitió el comentario a un diario digital, por vulnerar la resolución judicial que autorizó la injerencia los derechos a la intimidad y al secreto de las comunicaciones del remitente ya que, no habiendo reconocido el acusado la autoría del mensaje en cuestión, la presunción de inocencia habría de prevalecer. Se indica que la resolución judicial autorizante de la injerencia incumplió abiertamente los fines previstos en el art. 1 de la Ley 25/07, orientada a la detección, investigación y enjuiciamiento de delitos graves, lo que obliga al juicio de proporcionalidad que toda injerencia en los derechos de las personas debe sopesar la resolución judicial autorizante.

7. CONCLUSIONES

- La lucha contra el crimen en el proceloso mundo digital precisa de un marco jurídico adecuado. Obliga al legislador a una rigurosa labor de adaptación frente a los efectos del uso de las nuevas tecnologías por los delincuentes. Normas claras y seguridad jurídica[12]. La reciente Ley Orgánica 13 /2015 constituye una más que loable aportación a ese objetivo.
- La ley penal sustantiva ofrece respuesta a las actividades ilícitas en la red, si bien en forma dispersa, aunque está justificada la tipificación separada en diferentes ilícitos, pues resultaría sumamente dificultosa una de naturaleza autónoma.
- La obtención de pruebas en internet y su valoración se rige por los principios generales, aunque se trata de un ámbito en el que la utilización de medios muy técnicos de investigación resulta lógicamente imprescindible. Es notorio que la prueba se caracteriza por una gran complejidad, tanto que la indiciaria es difícil sea determinante en la inmensa mayoría de los casos.
- El principio de territorialidad queda con frecuencia desdibujado en esta forma de delincuencia. La cooperación internacional es esencial.
- La Ley 25/07, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones, obliga a la previa autorización judicial para la cesión de datos conservados por los operadores. A salvo de hipotético criterio del TC en contra, satisface razonablemente el principio de proporcionalidad.
- El rastreo de datos por las Fuerzas y Cuerpos de Seguridad, en principio, no precisa de autorización judicial, siempre que esté orientada a la obtención de datos de naturaleza pública o que hayan adquirido esa categoría, aun siendo privados en origen.
- Ha de deslindarse el derecho al secreto de las comunicaciones del derecho a la intimidad, mas lo cierto es que, tras el pleno no jurisdiccional del TS de 23 de febrero de 2010 y con acomodo a la Ley 25/07, la autorización judicial deviene en inexcusable.
- Ese criterio es modulado por la jurisprudencia: datos de tráfico, acceso a mensajes ya abiertos, obtención del *IMSI*… Esos casos no requieren, con carácter absoluto, de autorización judicial. La Ley Orgánica 13/2015, de 5 de octubre, supone una positiva clarificación del régimen jurídico de referencia.

Fecha de recepción: 25/06/2014. Fecha de aceptación: 20/07/2015

12 “Jueces y Fiscales reclaman leyes <aptas> para el mundo digital”, reseña de la II Jornada sobre Internet y su problemática jurídica publicada en El Economista, 29 de noviembre de 2014.