LA INJERENCIA EN EL DERECHO AL SECRETO DE LAS COMUNICACIONES A TRAVÉS DE LA REGULACIÓN DE LAS MEDIDAS DE INVESTIGACIÓN TECNOLÓGICA

Carmen Rodríguez Rubio

Profesora Titular de Universidad interina de Derecho Procesal
Universidad Rey Juan Carlos

SUMARIO: I. Consideraciones generales. II. La interceptación de las comunicaciones telefónicas antes de la reforma operada por la ley de medidas de investigación tecnológica. III. La Directiva 2006/24/CE, del Parlamento Europeo y del Consejo de 15 de marzo de 2006 y su transposición a la Ley española. IV. La nueva regulación de la interceptación de las comunicaciones.

Palabras clave

Proceso penal. Derecho al secreto de las comunicaciones; Jurisprudencia; Directivas comunitarias; Tecnologías de la comunicación y de la información.

Resumen

La interceptación de las comunicaciones ha sido un instrumento utilizado con frecuencia en la investigación criminal. Con este fin, la Ley procesal penal reguló la injerencia en la correspondencia escrita y telegráfica y, tras el desarrollo de las comunicaciones en el siglo XX, introdujo la intervención de las comunicaciones telefónicas. Después de la Segunda Guerra Mundial se procede al reconocimiento del derecho al respeto de la correspondencia, dando lugar a que los tribunales de justicia declaren la falta de adecuación de la legislación española con el derecho reconocido internacionalmente. Esta circunstancia, unida a la obligación legal de la conservación de datos por los operadores de telecomunicaciones, ha sido el origen de una nueva ordenación de esta materia por medio de la Ley reguladora de las medidas de investigación tecnológica.

I. CONSIDERACIONES GENERALES

Hoy en día, el uso de los medios tecnológicos para las comunicaciones humanas ha adquirido una gran trascendencia al incrementarse los procedimientos a través de los cuales es posible lograr una comunicación. En las últimas décadas las posibilidades de relacionarse han aumentado vertiginosamente con la aparición de nuevos instrumentos en las relaciones entre personas. Así, el correo electrónico, el SMS o servicio de mensajes

cortos y en gran medida la mensajería multimedia o MMS demuestran la rapidez con la que han penetrado en la sociedad actual los nuevos medios de correspondencia entre personas[1]; se trata de instrumentos que ya no se limitan a la comunicación bidireccional sino que permiten una comunicación multidireccional, creando chats entre distintos individuos. Estos nuevos instrumentos además se caracterizan porque no solo permiten enviar mensajes de texto sino que se configuran como medios cuyo contenido es diverso, pudiendo incluir imágenes, animación, sonido o video. Asimismo, se prevé que en el futuro, y a través de la mensajería multimedia, se podrá enviar otro tipo de contenido conforme se desarrolle la nueva telefonía móvil.

La información que proporcionan los medios de comunicación telefónica y telemática puede ser muy valiosa a la hora de investigar la comisión de un hecho delictivo. No obstante, la importancia de las comunicaciones como fuente para obtener información sobre la comisión de un delito ha estado presente desde la promulgación de la Ley de Enjuiciamiento Criminal —en adelante, LECrim—; es más, en diversas Constituciones decimonónicas también se reconocía la posibilidad de su interceptación mediante resolución motivada[2]. Es cierto que en el momento presente la correspondencia postal y telegráfica no es el medio más empleado para las comunicaciones diarias, sin embargo en otros momentos de la historia el correo postal y telegráfico se constituyó como medio indispensable para la comunicación humana; así, en el siglo XIX fue muy utilizado, y como tal el legislador, previendo que en la comisión de hechos delictivos se pudieran obtener fuentes de investigación, reguló en la primera Ley procesal la detención de la correspondencia privada, postal y telegráfica del procesado.

Como se acaba de indicar, diversas Constituciones del siglo XIX recogieron la injerencia en la correspondencia escrita, en este sentido las Constituciones de 1869 y 1876 se expresaban en términos similares, prohibiendo a la autoridad gubernativa la detención y la apertura de la correspondencia postal, con la singularidad de que la Constitución de 1876 también incluía la correspondencia telegráfica. La Constitución de 1931, que vino a sustituir a la anterior, introdujo los términos de inviolabilidad y de correspondencia, comprendiendo cualquier tipo, afirmando que se garantizaba en todas sus formas, es decir, que debido al desarrollo de las comunicaciones en el siglo XX, se pretendió garantizar la correspondencia en su ámbito más amplio. En todo caso, los textos constitucionales admitían la posibilidad de la restricción de la correspondencia mediante auto motivado

[1] El correo electrónico es una de las vías más importantes en la comunicación actual, en diversas estadísticas se afirma que en el año 2010 se mandaron 294 mil millones de emails al día, lo que equivale a 2,8 millones de mensajes enviados cada segundo. M.T. Jimeno García, M.A. Caballero Velasco, C. Míguez Pérez, A.M. Matas García, E. Heredia Soler, *La biblia del Hacker,* Anaya multimedia, Madrid, 2012, p. 767.

[2] R. Hernández Hernández, «Las escuchas telefónicas: medio probatorio en el proceso penal», *Actualidad Penal*, núm. 32, 1992, p. 324.

—textos constitucionales de 1869 y 1876— y únicamente auto, de conformidad con la Constitución de 1931[3]. Como ya apuntaba Aguilera de Paz, el auto se caracteriza por ser una resolución que, no resolviendo sobre el fondo de la causa, afecta a la misma o a sus resultados. Al tratarse de una resolución que puede causar algún gravamen a las partes, es indispensable que esté fundamentado, con el objeto de que los perjudicados puedan utilizar los recursos procedentes. Por otra parte, el art. 583 LECrim, en su redacción original, exponía claramente que la detención y el registro de la correspondencia o la entrega de las copias de los telegramas precisaba de auto motivado. Si este precepto se pone en conexión con el antiguo art. 141 LECrim[4], se puede concluir que la resolución limitadora del derecho al secreto de las comunicaciones ha requerido tradicionalmente en nuestro ordenamiento jurídico la forma de auto; en oposición a la providencia que ha sido considerada una resolución de mero trámite cuyo objeto es ordenar y dirigir el procedimiento para facilitar la regularidad de la instrucción y del juicio[5].

Si esto es lo sucedido en las distintas Constituciones españolas, se hace imprescindible destacar la universalización de los derechos humanos tras la finalización de la Segunda Guerra Mundial[6]. Efectivamente, en este contexto histórico, los países europeos, tras la Declaración Universal de los Derechos Humanos, toman conciencia de la necesidad de lograr el mantenimiento de la paz en Europa mediante la protección y el desarrollo de los derechos humanos[7]. De este modo, el Consejo de Europa procederá a su reconocimiento en el Convenio Europeo para la Protección de los Derechos Humanos y Libertades fundamentales, de 4 de noviembre de 1950 —en adelante, CEDH— ratificado por España el 26 de septiembre de 1979. Con posterioridad, la Carta de Derechos Fundamentales de la Unión Europea, proclamada en Niza el 7 de diciembre de 2000 —en adelante, la Carta— ha incidido en los derechos y libertades reconocidos en el CEDH, existiendo un vínculo entre ambos textos internacionales. Dicho vínculo se manifiesta tanto en el prólogo como en el articulado de la Carta. En el primero porque se reafirman los derechos reconocidos

[3] www.congreso.es (2 de junio de 2016).

[4] Este precepto disponía el modo de dictar las providencias, los autos y las sentencias. En particular, establecía que se denominaban autos las resoluciones «*cuando decidan incidentes o puntos esenciales que afecten de una manera directa a los procesados, acusados, particulares o actores civiles; cuando decidan la competencia del Juzgado o Tribunal, la procedencia o improcedencia de la recusación, la reposición de alguna providencia, la denegación de la reposición, la prisión y soltura, la admisión o denegación de prueba o del beneficio de pobreza, y finalmente, las demás que según las leyes deben fundarse*». Real Decreto de 14 de septiembre de 1882 por el que se aprueba la Ley de Enjuiciamiento Criminal. Htpps://boe.es/diario_boe/ (21 de junio de 2016).

[5] E. Aguilera de Paz, *Comentarios a la Ley de Enjuiciamiento Criminal*, Madrid, 1916, p. 162.

[6] A. Sáiz Arnaiz, *La apertura constitucional al Derecho internacional y europeo de los derechos humanos. El art. 10.2 de la Constitución española*, Consejo General del Poder Judicial, Madrid, 1999, p. 134.

[7] I. Flores Prada, *Manual de organización judicial*, (dir. V. Moreno Catena), Tirant lo Blanch, Valencia, 2003, p. 41. J.A. Pastor Ridruejo, *Curso de Derecho Internacional Público*, Tecnos, Madrid, 1989, p. 194.

en el CEDH, y en la jurisprudencia del Tribunal Europeo de Derechos Humanos —en adelante, TEDH— y, en el segundo, porque los derechos garantizados tienen un significado similar. Así, en ambos textos —arts. 8 y 7, respectivamente— se reconoce el derecho a la vida privada y familiar y, en particular, el derecho al respeto de la correspondencia —art. 8 CEDH—[8] y el derecho al respeto de las comunicaciones —art. 7 de la Carta—[9]. Este último texto internacional utiliza el término comunicación en lugar de correspondencia y también, en atención a su reciente redacción, reconoce el derecho a la protección de datos de carácter personal, en su art. 8[10].

Por su parte el art. 18.3 de la Constitución española —en adelante, CE— garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial. El citado precepto se ha de poner en relación con el art. 10.2 CE, al disponer que los derechos y libertades que la Constitución reconoce han de ser interpretados conforme a la Declaración Universal de los Derechos Humanos y Acuerdos internacionales sobre las mismas materias ratificados por España. En definitiva, el derecho al secreto de las comunicaciones se ha constituido en un derecho garantizado tanto a nivel interno como a nivel internacional, pero que sin duda puede verse limitado en tanto en cuanto se dicte una resolución motivada con el objeto de averiguar el delito y su autor.

II. LA INTERCEPTACIÓN DE LAS COMUNICACIONES TELEFÓNICAS ANTES DE LA REFORMA OPERADA POR LA LEY DE MEDIDAS DE INVESTIGACIÓN TECNOLÓGICA

La intervención de las comunicaciones telefónicas en la LECrim se produjo a través de Ley Orgánica 4/1988, de 25 de mayo, dando lugar a la modificación del art. 579 de

[8] Art. 8

«1. *Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia.*

2. *No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho, sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás*». www.derechoshumanos.net (27 de junio de 2016).

[9] Art. 7 «*Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de sus comunicaciones*». www.europarl.europa.eu (27 de junio de 2016).

[10] Art. 8

«1. *Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan.*

2. *Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto en la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación.*

3. *El respeto de estas normas quedará sujeto al control de una autoridad independiente*». www.europarl.europa.net (27 de junio de 2016).

este texto legal. Antes de la modificación operada, la intervención de este tipo de comunicaciones en las causas penales se llevaba a efecto en aplicación, por el Juez Instructor, del art. 18.3 CE y del art. 579 LECrim antes de su modificación. Sin embargo ante esta situación, el TEDH, en Sentencia de 30 de julio de 1998 —caso *Valenzuela c. España*— declaró que la interceptación requería además de cobertura legal, una ley de calidad, de manera que la ley interna de cada Estado miembro del Consejo de Europa, debía hacer saber a todos los individuos, de forma clara y suficiente, cuáles son las circunstancias y condiciones que han de cumplirse para que el poder público pueda adoptar esta medida restrictiva de un derecho fundamental —el TEDH ya se había pronunciado en este sentido en las Sentencias *Krusling y Huvig*, ambas de 27 de marzo de 1990—. Efectivamente, a través de este pronunciamiento el TEDH puso de manifiesto el vacío existente en esta materia, no siendo suficiente ni el precepto constitucional ni tampoco la regulación de la correspondencia en la Ley procesal antes de la incorporación de la LO 4/1988, de 25 de mayo. En esta expresiva Sentencia, el TEDH manifestó que, en atención a su jurisprudencia anterior, la ley permisiva de la injerencia había de reunir unas garantías mínimas, a saber: tipo de personas a las que se le intervienen las comunicaciones, conductas delictivas objeto de investigación, fijación de un límite de duración en la ejecución de la medida, condiciones de los atestados que consignan las conversaciones interceptadas, precauciones que se deben tomar para mantener intactas y completas las grabaciones realizadas para su control por el Juez y por las partes, y por último, cuándo se debe proceder al borrado o a la destrucción de lo grabado.

Por consiguiente, se hacía precisa una ordenación adecuada de esta materia. En atención a lo expuesto con anterioridad, la LO 4/1988, de 25 de mayo pretendía colmar el vacío existente regulando por primera vez en nuestra legislación procesal, la interceptación de las comunicaciones telefónicas como diligencia de investigación en el proceso penal. La nueva normativa, como es sabido, se ha caracterizado por su imperfección ya que dejaba sin resolver aspectos relevantes en la ejecución de la diligencia[11]. A su vez, la terminología empleada también daba lugar a dudas sobre el tipo de interceptación regulada, debido a que, conforme a la nueva redacción del art. 579 LECrim, su apartado segundo reconocía la posibilidad de que el Juez acordara la intervención de las comunicaciones telefónicas del procesado, mientras que el apartado tercero se refería a la observación de las comunicaciones de las personas sobre las que existieran indicios de responsabilidad criminal, es

[11] J. Montero Aroca, *La intervención de las comunicaciones telefónicas en el proceso penal (un estudio jurisprudencial),* Tirant lo Blanch, Valencia, 1999, p. 19. A. Montón Redondo, «Las interceptaciones telefónicas constitucionalmente correctas», *La Ley,* tomo IV, 1995, pp. 1042-1052. J.V. Gimeno Sendra, «Las intervenciones telefónicas en la jurisprudencia del Tribunal Constitucional y del Tribunal Supremo», *La Ley*, año XVII, 1996, pp. 1617-1624.

decir, se utilizaban dos términos diferentes para referirse a la interceptación, por un lado la intervención y, de otro, la observación; incluso también se refería al procesado, y al que apareciera como responsable por la existencia de indicios de criminalidad; en palabras de Montón Redondo y, también de Ortells Ramos, se trataría de dos medidas diferentes; mientras que la intervención consistiría en conocer el contenido total de las conversaciones telefónicas, la observación sería una injerencia de menor intensidad que supondría la constatación de las llamadas efectuadas o recibidas sin conocer su contenido. Incluso se podría entender, como opinaba Ortells Ramos, que la observación sería una medida propia de los delitos de menor gravedad y la única que podía ser ordenada sin autorización judicial previa[12]. La existencia de esta normativa defectuosa se puso de manifiesto por el TEDH en Sentencia de 18 de febrero de 2003 —caso *Prado Bugallo c. España*— al entender que las garantías introducidas por la Ley Orgánica de 25 de mayo de 1988 no respondían a todas las condiciones exigidas en su jurisprudencia. De modo que la nueva Ley no determinaba los delitos que permitían las escuchas; tampoco un límite temporal en la duración de la diligencia, debido a que la reforma legislativa apuntaba un plazo de tres meses prorrogable por iguales períodos, pero sin establecer un límite máximo; tampoco regulaba las condiciones que debían cumplirse para asegurar la regularidad de las escuchas ni las precauciones a tomar para conservar intactas y completas las comunicaciones interceptadas.

En relación con las deficiencias expresadas, estas también han sido puestas de manifiesto por el Tribunal Constitucional —en adelante, TC—. De esta manera, en Sentencia 104/2006, de 3 de abril, declaró que le correspondía al legislador, a través de un juicio de proporcionalidad, delimitar la naturaleza y la gravedad de los hechos que podían ser investigados a través de la intervención de las comunicaciones; no obstante, hasta que el legislador actuara, le correspondía suplir las deficiencias al propio Tribunal —véase Sentencia 184/2000, de 23 de octubre—. En este sentido, cuando se aborda la gravedad del delito, como requisito para la adopción de esta medida restrictiva, se ha de tener en consideración que no sólo habrá que apreciar la pena atribuida al delito, sino que también son elementos a valorar el bien jurídico protegido y la relevancia social del mismo, sin olvidar que junto a estas condiciones también el uso de las tecnologías en su comisión debe ponderarse, porque facilita la perpetración del delito y dificulta su persecución —STC 104/2006, de 3 de abril—. Este Tribunal también ha manifestado la importancia de que la intervención esté fundamentada, tanto en el aspecto fáctico como en el jurídico, porque de este modo se posibilita el derecho a la defensa y se puede valorar la proporcionalidad

[12] A. Montón Redondo, «Las interceptaciones telefónicas…», *cit.*, pp. 1042-1052. M. Ortells Ramos, *Derecho Jurisdiccional III. Proceso Penal*, obra colectiva, J.M. Bosch, Barcelona, 1994, p. 193.

entre la restricción del derecho y la causa que provoca tal limitación —STC 37/1989, de 15 de febrero y STC 85/1994, de 14 de marzo—.

Es conveniente no olvidar que la comunicación humana proporciona al investigador información diversa que adquiere una gran importancia en la averiguación del delito y en el descubrimiento del autor y de sus circunstancias. Este tipo de información puede ser de distinta entidad: desde quién es el titular de la línea, el usuario, también información sobre el tráfico de llamadas, es decir, quién es el emisor, el receptor, duración de la llamada o ubicación del terminal, hasta el contenido de la conversación. Hay cierta información que puede ser conocida directamente por el investigador; sin embargo, al tratarse de una materia que incide directamente en un derecho fundamental, como se ha apuntado en líneas anteriores, la injerencia precisa de autorización judicial[13]. En relación con la necesidad de motivar la resolución que dispone la intervención de las comunicaciones, es preciso que el auto recoja los hechos o datos objetivos que puedan indicar la existencia de un delito y su relación con la persona o personas investigadas —SSTC 253/2006 de 11 de septiembre y 136/2006, de 8 de mayo— además del teléfono que debe ser intervenido y el delito investigado —SSTC 165/2005, de 20 de junio y 26/2006, de 30 de enero—. Las decisiones del TC se han fundamentado en el criterio mantenido por el TEDH, ya que exige la concurrencia «*de buenas razones o fuertes presunciones*» de que el delito está a punto de cometerse —Sentencia de 6 de septiembre de 1978, caso *Klass,* y Sentencia de 15 de junio de 1999, caso *Lüdi*—.

Con anterioridad a la autorización de la medida, es frecuente que previamente a la solicitud policial se hayan realizado ciertos actos de investigación que permitirán a la policía razonar su solicitud ante la autoridad judicial. De esta manera, habrá que determinar la gravedad del delito, lo que se pretende con la intervención y los indicios existentes, es decir, aquellas circunstancias que sirvan de base para justificar la interceptación de las comunicaciones[14]. En relación con los motivos que recoge la solicitud policial y la fundamentación del auto que ordena la intervención, el TC, en Sentencia de 5 de abril de 1999, declaró que ante una autorización judicial que asumía las razones manifestadas por los agentes de policía en su solicitud, haciendo suyos los motivos de la petición y no expresando las razones de la solicitud sino por remisión a las que fueron aducidas por la policía, atenta contra el derecho al secreto de las comunicaciones, entendiendo que los motivos expuestos en la solicitud policial y valorados por el Juez eran insuficientes, ya que se basaban en sospechas y en conjeturas sobre el delito y los que habían participado en él. A partir de esta Sentencia, el TC empezó a clarificar los requisitos que había de reunir la resolución

[13] A. González Clavero, *Monográfico de metodología y técnicas de investigación criminal*, Sociedad Española de Criminología y Ciencias Forenses, 2013, libro electrónico.

[14] A. González Clavero, *Monográfico de metodología… cit.,* libro electrónico.

autorizante. De este modo, declaró que el Juez de Instrucción ha de expresar los hechos o datos objetivos que se consideren indicios de la existencia de un delito grave, así como su relación con los sujetos afectados por la intervención. Esta expresión de los hechos podrá realizarse en el auto, que es lo deseable a juicio del Tribunal, o por remisión a la solicitud policial —STC 239/2006, de 17 de julio—. En el auto, que podrá remitir a la solicitud policial, se harán constar: las personas y hechos delictivos determinados, líneas telefónicas que se han de intervenir, plazo prefijado y la ejecución de la medida por la policía, medida que se llevará a cabo según lo determinado en el auto —STC 104/2006, de 3 de abril—.

III. LA DIRECTIVA 2006/24/CE, DEL PARLAMENTO EUROPEO Y DEL CONSEJO DE 15 DE MARZO DE 2006 Y SU TRANSPOSICIÓN A LA LEY ESPAÑOLA

La restricción en el derecho al secreto de las comunicaciones también ha sido objeto de regulación en las directivas europeas. Así, la Directiva 2006/24/CE, del Parlamento Europeo y del Consejo de 15 de marzo, establece la obligación de los operadores de telecomunicaciones de retener los datos que se generen a través de una comunicación y ponerlos a disposición de los agentes facultados previa autorización judicial[15]. Los motivos por los que la Directiva justifica esta medida son diversos: de una parte, la existencia de diversa legislación en los Estados miembros relativa a la conservación de datos para descubrir o enjuiciar un delito; de otra, las conclusiones del Consejo de Justicia e Interior de 19 de diciembre de 2002, la Declaración sobre la lucha contra el terrorismo, de 25 de marzo de 2004 y la Declaración de 13 de julio de 2005 condenando los atentados terroristas de Londres. Estas razones han sido esenciales a la hora de ordenar la retención de los datos derivados de una comunicación, estableciéndose en el Consejo Europeo como prioridad la lucha contra el terrorismo. La transposición de la Directiva comunitaria a la ley española ha tenido lugar a través de la Ley 25/2007, de 18 de octubre, de Conservación de Datos relativos a las Comunicaciones Electrónicas y a las Redes Públicas de Comunicación. De conformidad con la norma interna, los datos generados por una comunicación se han de proporcionar a la autoridad competente, en el marco de una investigación criminal. La información obtenida será cedida a los agentes facultados, previa resolución judicial. Estos agentes son los miembros de las Fuerzas y Cuerpos de Seguridad, como auxiliares de los Juzgados, Tribunales y del Ministerio Fiscal, en el descubrimiento del delito. Los datos que se han de proporcionar a la autoridad judicial abarcan: los necesarios para identificar

[15] Además de esta Directiva existen otras anteriores, Directivas 95/46/CE y 2002/58/CE, que también han regulado el tratamiento de los datos personales generados por el uso de las comunicaciones.

el origen de la comunicación, su destino, fecha, hora, duración, tipo de comunicación, el equipo utilizado y su localización, nunca el contenido de la comunicación[16].

La Directiva mencionada ha sido objeto de varias cuestiones prejudiciales interpuestas ante el Tribunal de Justicia de la Unión Europea —en adelante, TJUE— por el Tribunal Superior de Irlanda y el Tribunal Constitucional de Austria[17]. Estos dos últimos Tribunales han solicitado al TJUE que examine la validez de la Directiva, a la luz de dos derechos fundamentales de la Carta de los Derechos Fundamentales de la Unión Europea: el derecho al respeto de la vida privada y el derecho a la protección de datos de carácter personal. Al respecto, el TJUE[18] ha declarado que la conservación de datos puede proporcionar indicaciones muy precisas sobre la vida privada de las personas, sus hábitos, lugares de residencia, desplazamientos y actos sociales. El TJUE entiende que la conservación de datos se inmiscuye de manera especialmente grave en los dos derechos antes citados, y considera que el legislador de la Unión ha sobrepasado los límites que exige el principio de proporcionalidad. Es cierto que, según el TJUE, la conservación de datos puede considerarse adecuada para lograr el fin que persigue, esto es, la seguridad pública, pero por diversas razones la injerencia no está lo suficientemente regulada para lograr que tal restricción se limite a lo necesario. Así, abarca de manera generalizada a todas las personas, medios de comunicación electrónica y datos relativos al tráfico sin ninguna diferenciación; además no garantiza que las autoridades nacionales competentes únicamente tengan acceso a los datos; tampoco define los delitos graves en los que se podrá utilizar la información obtenida, dejándolo en manos de los ordenamientos de cada Estado miembro; tampoco establece las condiciones materiales y procesales en las que las autoridades nacionales pueden tener acceso a los datos y utilizarlos con posterioridad; no fija los criterios a seguir para determinar el período de conservación de datos, oscilando entre los seis y veinticuatro meses; no garantiza una protección eficaz contra la utilización ilícita de los datos; tampoco su destrucción después del período de conservación y, por último, la norma comunitaria no obliga a que los datos se conserven dentro del territorio de la Unión. De esta manera, la Directiva no garantiza plenamente el cumplimiento de los requisitos de protección y de seguridad por una autoridad independiente, tal y como exige la Carta.

---

16 La Ley Orgánica 13/2015 de modificación de la Ley de Enjuiciamiento Criminal ha introducido la incorporación al proceso de datos electrónicos de tráfico o asociados, tras la redacción del nuevo art. 588 ter j. En este precepto se establece la necesidad de que se dicte autorización judicial para recabar la información que conserven los prestadores de servicios de comunicación, incluida la búsqueda entrecruzada o inteligente de datos.

17 http://curia.europa.eu (15 de junio de 2016).

18 Sentencia en los asuntos acumulados C-293/12 y C-594/12 *Digital Rights Ireland y Seitlinger y otros*. http://curia,europa.eu (27 de junio de 2016).

Antes de pasar a analizar el pronunciamiento del TJUE se hace preciso distinguir la medida de conservación de datos impuesta a los operadores de telecomunicaciones, de la injerencia que en numerosas ocasiones se produce en el derecho al secreto de las comunicaciones cuando se ha iniciado un proceso penal y se autoriza la intervención para el descubrimiento del delito y de su autor. Esta última intervención únicamente tiene lugar una vez incoado el proceso penal como modo de averiguación del delito, pudiéndose conocer los datos asociados a las comunicaciones o incluso el contenido de la comunicación, si fuera necesario para el descubrimiento del hecho delictivo y de su autor. En cambio, en la medida que prevé la norma comunitaria, la conservación de datos existe antes de la autorización judicial, porque su conservación tiene lugar por imperativo legal. Es con posterioridad a la retención de la información cuando el Juez dicta auto para que a través de la entrega de la información requerida, el Instructor pueda tener conocimiento de los datos precisos para conocer la identidad subjetiva de los interlocutores, lugar, fecha y duración de la comunicación.

Como apunta el TJUE, a través de la conservación de esta información se puede obtener información muy precisa sobre la vida privada de las personas. Por otra parte, y como también señala este Tribunal, la medida puede resultar adecuada para lograr la seguridad pública; no hay que olvidar que la finalidad es luchar contra el terrorismo y el crimen organizado; sin embargo a juicio del TJUE, la medida no es proporcionada y la norma comunitaria no está lo suficientemente regulada para que se pueda afirmar que la injerencia se limite a lo necesario. Se ha de tener presente que la propia Directiva reconoce, en virtud del art. 8 del CEDH, el derecho de toda persona al respeto de su vida privada y de su correspondencia y entiende, a su vez, que la conservación de datos en tanto en cuanto cumple con los requisitos del CEDH es una medida necesaria. Los datos solo podrán proporcionarse a las autoridades nacionales competentes, en los casos y de conformidad con la legislación del Estado miembro. Por consiguiente, a cada Estado le corresponde definir el procedimiento y las condiciones que han de seguirse para tener acceso a los datos, de conformidad con los principios de necesidad y de proporcionalidad; así como las disposiciones del CEDH y su interpretación por el TEDH. En palabras del Tribunal, la Directiva no está lo suficientemente regulada y la medida no se adecua al principio de proporcionalidad. Este pronunciamiento tiene un carácter que, en cierto modo, se corresponde en su significado al que el TEDH ha venido apuntando en relación con la insuficiencia de la ley española en orden a la intervención de las comunicaciones. El TEDH en diversas sentencias dejó constancia de los defectos en que incurría la legislación española. De esta manera, afirmó que el derecho interno de cada Estado debía hacer saber a todos claramente en qué circunstancias y en qué condiciones podía tener lugar la injerencia, las personas que podían verse afectadas por la intervención, así como las infracciones penales que podían justificar la vigilancia de las comunicaciones y el borrado o destrucción de la información obtenida, entre otras circunstancias —STEDH de 30 de julio de 1998—.

Y tras la Sentencia de 18 de febrero de 2003, El TEDH reiteró la insuficiencia de la ley española por no establecer el tipo de infracciones que podían dar lugar a las escuchas, ni la duración de la ejecución de la intervención, tampoco las condiciones de las actas, ni las precauciones a tomar para que las grabaciones permanecieran intactas y completas. De este modo el TJUE, al igual que el TEDH en sus diferentes pronunciamientos interpretadores del art. 8 CEDH, pone de manifiesto la insuficiencia de la Directiva.

En relación con la Sentencia del TJUE, su pronunciamiento ha dado lugar a que se esté realizando una reflexión sobre el alcance de la norma comunitaria[19]. No obstante, la Ley 25/2007, de 18 de octubre, sigue siendo de aplicación, y junto con la reforma operada en la LECrim y lo previsto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal —en adelante, LOPD—, se puede obtener una visión más próxima a las condiciones que requiere la conservación de datos. En este sentido, la reforma operada en la Ley procesal, y que se expondrá en líneas posteriores, trata de solventar las deficiencias del antiguo art. 579 LECrim, realizando una ordenación de la materia más exhaustiva. Así, en el momento presente la Ley procesal determina qué tipo de personas se pueden ver afectadas por la injerencia; qué tipo de medios de comunicación pueden ser intervenidos y las modalidades de la injerencia. También, y esta circunstancia es de gran relevancia, ya que el legislador no lo había previsto ni tan siquiera en la Ley de transposición de la Directiva, determina los delitos que pueden ser investigados a través de la interceptación de las comunicaciones. Además, al remitir la Ley 25/2007, de 18 de octubre a la Ley procesal penal, tras la reforma ya se recoge el contenido del auto que habilita la injerencia, y el significado y contenido de los principios de necesidad y de proporcionalidad. Por otra parte y, en relación con los datos conservados, los operadores de telecomunicaciones, en virtud de la LOPD, han de adoptar las medidas necesarias para garantizar su tratamiento adecuado, evitando su uso para fines distintos de los comprendidos en la ley. Igualmente, aquellos que intervengan en el tratamiento de datos están obligados al secreto de los mismos y al deber de guardarlos incluso cuando la relación con el operador haya concluido; esta obligación legal, tras la reforma que ha tenido lugar recientemente, adquiere mayor importancia porque resalta la necesidad de colaboración de los prestadores de servicios de telecomunicaciones, de tal forma que si incumplieran el deber de guardar secreto, podrían incurrir en delito de desobediencia. Asimismo, se prevé la anulación de los datos conservados cuando dejen de ser necesarios para el fin con el que se hubieran recabado, procediéndose a su cancelación una vez concluido el tiempo legalmente establecido. Por otra parte, y en lo que concierne al tratamiento sancionador,

[19] *«La Sentencia del TJUE no tiene efectos directos en la Ley española, pero es posible que desde los Juzgados se planteen incidentes de nulidad de acciones que en la práctica puedan anular instrucciones de procesos donde haya habido recopilación de comunicaciones por mandato del juez»*. www.legaltoday.com (7 de junio de 2016).

las infracciones y sanciones aparecen recogidas legamente, siendo de aplicación el régimen establecido en la Ley 32/2003, de 3 de noviembre, General de Comunicaciones, y atribuyendo la competencia sancionadora al Secretario de Estado de Telecomunicaciones y para la Sociedad de la Información; así como a la Agencia Española de Protección de Datos en lo que se refiera al incumplimiento de las obligaciones de protección y de seguridad de la información personal[20]. Por último, los arts. 33 y 34 de la LOPD regulan el movimiento internacional de datos, disponiendo las garantías a cumplir cuando la información de carácter personal se transfiera a otros países.

IV. LA NUEVA REGULACIÓN DE LA INTERCEPTACIÓN DE LAS COMUNICACIONES

En los últimos años se ha planteado en el seno del Ministerio de Justicia la elaboración de una Ley procesal penal como texto único que sustituya a la actual Ley de Enjuiciamiento Criminal[21]. Este propósito aún no ha culminado, encontrándose la nueva ley sometida a información pública y a debate; no obstante, mientras llega la tan ansiada Ley procesal, el legislador ha optado por incorporar en la actual Ley nuevas medidas de investigación tecnológica que afectan irremediablemente al derecho a la intimidad, al secreto de las comunicaciones y al derecho a la protección de los datos personales garantizados por la Constitución[22]. Como apunta la Exposición de Motivos de la nueva Ley, la LECrim no ha podido sustraerse al paso del tiempo. Es cierto que en la materia referida a la investigación criminal la LECrim ha sido modificada en numerosas ocasiones, no solo en lo relacionado con la intervención telefónica, sino también en lo referido a la actuación de agentes encubiertos, a la circulación vigilada de drogas o a la obtención de muestras biológicas para la determinación del ADN, todo ello debido a los adelantos e innovaciones en el campo de la investigación del delito y de su autor. Sin embargo, la LECrim carece de unidad en la ordenación del proceso, por lo que se hace imprescindible la elaboración de una nueva Ley procesal penal conforme a los principios que lo informan. En la materia que aquí interesa, la interceptación de las comunicaciones, se produjo una modificación en los años ochenta; sin embargo, como se ha puesto de manifiesto, ha sido insuficiente y los tribunales han tenido que colmar el vacío que esta legislación presentaba.

[20] La Agencia Española de Protección de Datos se constituye como un órgano con plena independencia de las Administraciones públicas en el ejercicio de sus funciones (art. 35 LOPD).

[21] Véase: Anteproyecto de Ley de Enjuiciamiento Criminal —año 2011—; Anteproyecto de Ley Orgánica de desarrollo de los derechos fundamentales vinculados al proceso penal y, por último, Propuesta de texto articulado de Ley de Enjuiciamiento Criminal, elaborada por la Comisión Institucional creada por Acuerdo de Consejo de Ministros de 12 de marzo de 2012. Ministerio de Justicia-Secretaría General Técnica.

[22] Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica.

El legislador conocedor de esta situación, ha optado por introducir una nueva regulación teniendo presente la jurisprudencia proveniente de los diferentes tribunales de justicia.

Para la ordenación de esta materia se ha optado por distinguir, por un lado, la detención y apertura de la correspondencia escrita y telegráfica y, por otro, la interceptación de las comunicaciones telefónicas y telemáticas junto con los demás medios de investigación tecnológica. El art. 579 LECrim recibe una nueva redacción, regulando únicamente —como ya hacía la antigua redacción del precepto— la interceptación de la correspondencia escrita y telegráfica. El precepto regula la detención de la correspondencia privada, postal y telegráfica, incluidos faxes, burofaxes, giros del investigado —como emisor o como receptor—, la apertura y la observación de las comunicaciones, no requiriéndose la presencia del afectado o de su representante si el Juez hubiera acordado su examen, a diferencia del antiguo art. 585 LECrim que sí lo expresaba, aunque la realización del acto se podía llevar a cabo en todo caso. Este tipo de interceptación solamente tendrá lugar cuando hubiera indicios de obtener por este medio el descubrimiento o la comprobación de algún hecho o circunstancia relevante para la causa y siempre que se investigue alguno de los siguientes delitos: delitos dolosos castigados con pena con límite máximo de, al menos, tres años de prisión, crimen organizado y delitos de terrorismo[23]. La adopción de esta medida requiere resolución motivada, pudiéndose acordar por un plazo de hasta tres meses, prorrogable por iguales o inferiores períodos hasta un máximo de dieciocho meses[24]. En determinados casos no es necesaria la autorización judicial; así no lo será: cuando se trate de envíos postales que sirvan al tráfico y transporte de mercancías o en cuyo exterior se haga constar su contenido; envíos postales bajo el formato legal de comunicación abierta y cuando la inspección se lleve a cabo conforme a la normativa aduanera o proceda conforme a las normas postales que resulten de aplicación. Por último, señalar que se crea un nuevo art. 579 bis que regula un supuesto de hecho que con anterioridad no se preveía en la LECrim; se trata de la utilización de la información obtenida en un procedimiento distinto y de los descubrimientos casuales. El precepto afirma que la información obtenida podrá utilizarse como medio de investigación y como medio probatorio en otro proceso penal. Para este

[23] La nueva redacción del art. 579, en su apartado quinto, dispone que tanto la medida solicitada como los actos posteriores se sustanciarán en pieza separada y secreta, sin necesidad de que se dicte expresamente el secreto de la causa. Esta previsión legal también se recoge en las disposiciones comunes de las medidas de investigación tecnológica,

[24] Como en la legislación anterior, se permite, en caso de urgencia cuando la investigación esté dirigida a la averiguación de bandas armadas o elementos terroristas, que la medida la ordene el Ministro del Interior o el Secretario de Estado de Seguridad; lo que se comunicará inmediatamente al Juez competente en un plazo máximo de veinticuatro horas para que revoque o confirme motivadamente la actuación en un plazo máximo de setenta y dos horas desde que se ordenó. Esta previsión legal también se recoge para la interceptación de las comunicaciones telefónicas y telemáticas.

fin, es preciso que consten todos los antecedentes que dieron lugar a la injerencia, así como las prórrogas que se decretaron en el procedimiento de origen. Su continuación requerirá autorización del órgano jurisdiccional competente que comprobará los requisitos previstos legalmente, así como la declaración de secreto.

Por lo que respecta a los medios de investigación tecnológica, se ha optado por introducir una serie de disposiciones generales que afectan a todas las nuevas diligencias de investigación, para posteriormente, regular de manera independiente la interceptación de las comunicaciones telefónicas y telemáticas. En relación con las disposiciones comunes, en primer lugar se recogen los principios rectores que informan la adopción de una medida tecnológica de investigación; en este sentido se ha de tener presente que la jurisprudencia ha defendido la existencia de unos principios a la hora de valorar que se decrete una medida restrictiva de un derecho fundamental. De este modo y, de conformidad con la nueva norma, cuando se dicte la autorización judicial, esta se sustentará en los principios de especialidad, excepcionalidad, idoneidad, necesidad y proporcionalidad. La especialidad viene referida a que la medida se debe decretar para la investigación de un delito en particular, estando prohibidas las investigaciones prospectivas sobre una persona o grupo de personas[25]. En cuanto a la idoneidad, servirá para fijar el ámbito objetivo y subjetivo de la medida, así como su duración, en virtud de su utilidad. Los principios de excepcionalidad y necesidad implican, por una parte, la inexistencia de otras medidas menos gravosas para los derechos fundamentales del investigado —o encausado— e igualmente útiles para averiguar el hecho delictivo y, de otra, la grave dificultad existente, si no se decretase la medida, para averiguar el hecho, su autor, conocer su paradero o para localizar los efectos del delito. Por último, la proporcionalidad de la medida significa que el Juez, tomando en consideración todas las circunstancias del caso, deberá tener presente que el sacrificio al derecho de las comunicaciones no sea superior al beneficio que reporta la adopción de la medida en aras del interés público; la gravedad del hecho, su trascendencia social o el ámbito tecnológico de producción; la intensidad de los indicios y el resultado perseguido con la restricción del derecho serán los aspectos que el Juez ponderará en aras del citado interés público —art. 588 bis a LECrim—.

La adopción de la medida, al igual que la de cualquier otra de naturaleza tecnológica, le corresponde decretarla al Juez, ya sea de oficio, ya sea a instancia del Ministerio Fiscal o de la Policía judicial. Es importante destacar que se ha optado por restringir la solicitud de este tipo de medidas, de manera que ni el ofendido por el delito ni el acusador popular podrán solicitarlas. La solicitud ha de recoger una serie de requisitos, a saber: hechos objetivos, identificación del investigado o de cualquier otro afectado —siempre

[25] Literalmente, el precepto 588 bis a, apartado 2.º, dispone que «*No podrán autorizarse medidas de investigación tecnológica que tengan por objeto prevenir o descubrir delitos o despejar sospechas sin base objetiva*».

que sean conocidos—, razones que justifican la medida —según los principios expuestos con anterioridad—, medios que permitan la ejecución de la medida, quién la ejecutará, cómo se ejecutará y qué duración tendrá. Existe otro requisito que está relacionado con la modalidad de interceptación de las comunicaciones, ya que como se ha apuntado en líneas anteriores, las modalidades de interceptación pueden ser de mayor o menor intensidad. Este requisito es el de la extensión de la medida que, en virtud del art. 588 ter d, podrá consistir en el registro y grabación de la comunicación, indicando a qué tipo de comunicaciones afecta —habrá que indicar si se trata de las comunicaciones telefónicas, SMS, correo electrónico o mensajería multimedia—; también podrá consistir en conocer el origen o destino de la comunicación, la localización geográfica del origen o destino de la comunicación y, en último lugar, se podrá solicitar la medida para obtener otro tipo de información asociada o no al tráfico de llamadas, en cuyo caso se especificarán los datos que se pretenden conocer[26]. Ante la solicitud, el Juez de Instrucción, oído el Ministerio Fiscal, deberá decidir sobre la adopción de la medida en un plazo máximo de 24 horas desde que se solicitó; dicho plazo podrá interrumpirse si se necesitara una ampliación o aclaración de alguno de los requisitos referidos. La diligencia de investigación se decretará ante la existencia de alguno de los delitos citados en la detención y apertura de la correspondencia escrita y telegráfica, además de poderse ordenar cuando el delito se haya cometido a través de los nuevos instrumentos informáticos de la información y de la comunicación. La resolución judicial habilitante contendrá al menos lo siguiente: hecho delictivo investigado, su calificación jurídica e indicios en los que se funda la medida; identidad del investigado y de cualquier otro afectado —si fuera conocido—; modalidad de la intervención -expresando su alcance-; motivación, de acuerdo con los principios establecidos con anterioridad; quién ejecutará la medida[27] —unidad de la policía judicial—; su duración, forma y periodicidad para informar al Juez sobre sus resultados y finalidad de la medida. Desde la solicitud de la diligencia, todas las actuaciones se sustanciarán en pieza separada y secreta, sin necesidad de acordar el secreto de la instrucción. Respeto al ámbito de la intervención telefónica y telemática, la injerencia se producirá en los sistemas

[26] Además de estos requisitos, la solicitud contendrá: identificación del número de abonado, del terminal o de la etiqueta técnica, la identificación de la conexión o los datos necesarios para identificar el medio de telecomunicación. Po otro lado, el art. 588 ter b, apartado 2.º, establece que la intervención podrá suponer la intervención del contenido de la comunicación o acceso a datos electrónicos de tráfico o asociados y a los datos que se obtengan por llamadas infructuosas, en las que el investigado sea el emisor o el receptor, ya sea su titular o usuario. También, y este supuesto no se contemplaba en el proyecto de ley, se podrán intervenir los terminales o medios de comunicación de la víctima cuando se prevea un grave riesgo para su vida o integridad.

[27] El art. 588 bis c), apartado 3.º h), establece que si se conociera el sujeto obligado a realizar la medida, se mencionará expresamente el deber de colaboración y de guardar secreto, bajo apercibimiento de incurrir en un delito de desobediencia.

de comunicación que ocasional o habitualmente utilice el investigado, aunque también se permite la intervención de terminales o medios de comunicación de una tercera persona cuando haya constancia de que el investigado los utiliza para transmitir o recibir información, o su titular colabora con el investigado en el hecho delictivo o se beneficia de su actividad. Finalmente, también se podrá autorizar la intervención cuando el dispositivo sea utilizado maliciosamente por un sujeto sin conocimiento de su titular.

Como se ha apuntado en líneas precedentes, el auto contendrá entre otros requisitos, la duración de la medida. Atendiendo a la regla general recogida en la nueva Ley, la injerencia no podrá exceder del tiempo imprescindible para el esclarecimiento de los hechos; en particular, la restricción de las comunicaciones tendrá una duración máxima inicial de tres meses, prorrogables por iguales períodos sucesivos de igual duración hasta un plazo máximo de dieciocho meses[28]. La prórroga precisa también de autorización judicial que dictará el Juez de oficio o a instancia razonada del solicitante, siempre que subsistan las causas que lo motivaron. Además, en la solicitud de prórroga se contendrá un informe detallado del resultado de la medida, y la Policía Judicial aportará, en su caso, la transcripción de los pasajes de las conversaciones de donde se deduzcan las informaciones que justifiquen la continuación de la injerencia. El Juez antes de resolver podrá solicitar algún tipo de aclaración o mayor información sobre el contenido completo de las conversaciones intervenidas.

En relación con el cese de la medida, esta finalizará cuando desaparezcan los motivos que dieron lugar a su adopción o cuando se haga evidente que su utilización no reporta los resultados pretendidos y, en todo caso, cuando haya transcurrido el plazo que la haya autorizado. Durante el transcurso de la medida, la Policía Judicial ha de informar al Juez de Instrucción de sus resultados en la forma y en el tiempo que se haya determinado en el auto judicial y siempre, en todo caso, cuando se ponga fin a la misma. Con esta finalidad pondrá a disposición judicial, en soportes digitales distintos: la transcripción de los pasajes que considere de interés y las grabaciones íntegras realizadas; se indicará el origen y el destino de cada una de ellas y se asegurará mediante los procedimientos adecuados la autenticidad de la información volcada desde el ordenador hasta los soportes digitales entregados. El borrado y eliminación de los registros originales tendrá lugar cuando se termine el procedimiento mediante resolución firme; aun así se conservará una copia bajo la custodia del Secretario Judicial. Las copias conservadas se destruirán cuando hayan transcurrido cinco años desde que la pena se haya ejecutado o cuando el delito o la pena hayan prescrito, también cuando se haya decretado el sobreseimiento libre o haya recaído sentencia absolutoria firme respecto del investigado, a no ser que fuera precisa

[28] La medida finalizará a todos los efectos si no se hubiese prorrogado o hubiese finalizado su prórroga —art. 588 bis e) apartado 3.º—.

su conservación a juicio del Tribunal. Para la destrucción de los originales y de las copias conservadas, los tribunales dictarán las órdenes oportunas a la Policía Judicial. Como comentario a esto último, indicar que efectivamente el precepto recoge la destrucción de las grabaciones pero no determina qué Tribunal en particular lo ordenará, lo que podría dar lugar a que se demorara la destrucción de la información obtenida. Tras la finalización de la injerencia y alzado el secreto de las actuaciones, se prevé la entrega a las partes de una copia de las grabaciones y de las transcripciones que se hayan realizado; se trata de una disposición (art. 588 ter i LECrim) que recoge un supuesto que con anterioridad no estaba previsto legalmente; de este modo se podrá conocer la información que se haya obtenido con la intervención, aunque los datos que afecten a la vida íntima de las personas no se entregarán, lo que se hará constar de modo expreso. Las partes, una vez examinadas las grabaciones y en el plazo establecido judicialmente, podrán solicitar la incorporación en las copias de la información que consideren relevante y que no haya sido incluida, lo que decidirá el Juez de Instrucción después de examinar las comunicaciones. Por último, el precepto citado añade que el Juez de Instrucción notificará la intervención a los sujetos afectados, salvo que sea imposible, exija un esfuerzo desproporcionado o pueda afectar a futuras investigaciones. Si la persona notificada lo solicita se le entregará una copia de la grabación o de la transcripción, salvo que afecte al derecho de la intimidad de otras personas o sea contrario a los fines del proceso en el que se hubiese decretado la medida.

En otro orden de cosas, la nueva Ley dedica una sección específica al acceso de los datos necesarios para la identificación de usuarios, terminales y dispositivos de conectividad. El primer artículo de esta sección —588 ter k— regula la identificación mediante número IP —Protocolo de Internet—, estableciendo que cuando la Policía Judicial, en sus funciones de prevención y descubrimiento de los delitos cometidos a través de Internet, conociera la dirección de IP utilizada y desconociera la identificación del dispositivo —computadora, tableta, portátil, Smartphone— y del usuario, solicitará al Juez que requiera a los prestadores de telecomunicaciones la cesión de la información necesaria para la identificación del dispositivo y del sospechoso. En lo que concierne a esta materia, se ha de tener presente que siempre que un dispositivo se conecta a una red debe tener asignada una dirección IP, que puede ser fija o dinámica; de esta manera cuando se utiliza un aparato con conexión a Internet, este inserta la dirección de origen y de destino. Esta información puede resultar muy valiosa para conocer la identidad del sospechoso; no obstante, también es importante tener en consideración que la Policía Judicial puede, a través de los recursos que hoy en día le proporcionan las nuevas tecnologías, tener conocimiento directamente de direcciones IP y de nombres de dominio[29], pero si desconociera la

[29] M.A. Jimeno García, M.A. Caballero Velasco, C. Míguez Pérez, A.M. Matas García, E. Heredia Soler, *La biblia del Hacker… cit.,* pp. 77-85.

identificación del aparato y del usuario, por medio de auto judicial podrá obtener la información que precise para averiguar el delito y su autor. Por otra parte, la nueva regulación de la intervención de las comunicaciones telemáticas autoriza a la Policía judicial —art. 588 ter i— en el marco de una investigación criminal, a utilizar los artificios técnicos que permitan acceder a los códigos IMEI[30] o IMSI[31] o a cualquier otro medio que permita la identificación del equipo utilizado, si en sus investigaciones necesitara conocer el número de abonado y no hubiera logrado obtener dicha información. En este sentido, es posible que el investigador directamente llegue a conocer el número de abonado a través de datos de carácter público, pero en caso contrario podrá utilizar los artificios técnicos que le permitan obtener dichos datos. Una vez conocidos, podrá solicitar al Juez competente la intervención de las comunicaciones, lo que autorizará o denegará de manera motivada. La consecución de esta información difiere de lo establecido en la Directiva 2006/24/CE y en la Ley 25/2007, ya que en esta última normativa se establece que, en la investigación de delitos graves, si la Policía Judicial precisara de la información necesaria para identificar el equipo de comunicación utilizado, necesitará de autorización judicial y de la cesión de datos por los agentes facultados. Dicha información será cedida por los operadores de telecomunicaciones debido a la obligación legal existente de conservar los datos asociados a una comunicación. En definitiva, la nueva regulación se separa de lo dispuesto en la Directiva 2006/24/CE y en la Ley 25/2007, estableciéndose una regulación divergente en esta materia. Asimismo, el último precepto que la nueva Ley dedica a la intervención de las comunicaciones telefónicas y telemáticas —art. 588 ter m— dispone que en el ejercicio de sus funciones, es decir, en la investigación del delito y de su autor, el Ministerio Fiscal o la Policía Judicial cuando necesiten conocer la titularidad de un número de teléfono o de cualquier otro medio de comunicación, o a la inversa, necesiten conocer un número de teléfono o los datos identificativos de cualquier medio de comunicación, lo que podría incluir el número IMEI ya que este código identifica de forma unívoca cualquier terminal móvil[32], se podrán dirigir a los prestadores de servicios de comunicaciones, estando estos obligados a prestar esa información, ya que en caso contrario podrán incurrir en un delito de desobediencia. Esta prestación de información también difiere de la cesión amparada por la Directiva 2006/24/CE y por la Ley 25/2007, porque la puede solicitar tanto el Ministerio Fiscal como los agentes de policía, mientras que en virtud de la Ley 25/2007 únicamente pueden obtener información de carácter personal los agentes facultados previa autorización judicial. En cuanto a la información requerida no parece haber duda

30 www.imei.com (23 de junio de 2016).
31 www.redyc.com (23 de junio de 2016).
32 www.imei.com (23 de junio de 2016).

de que se trata de datos de carácter personal[33], información que, en virtud del art. 18.4 CE[34], queda garantizada como derecho fundamental, y siendo la LOPD la que protege el citado derecho[35]. En este sentido la LOPD permite ceder los datos a un tercero sin su consentimiento cuando la cesión esté autorizada por la ley y cuando los destinatarios de la información sean: el Ministerio Fiscal, Jueces y Tribunales —art. 11—, no mencionando expresamente a la Policía judicial, aunque la cesión a los agentes sí podría enmarcarse en el precepto al ser una norma la que autoriza la entrega a esta autoridad, sin perjuicio de que la Ley 25/2007 requiera previa resolución judicial.

TITLE

THE INVASION OF PRIVACY IN ELECTRONIC COMMUNICATION VIA REGULATION OF TECHNOLOGICAL INVESTIGATION MEASURES

SUMMARY

I. Overview. II. Interception of telephone communication prior to the reform resulting from the technological investigation law. III. Directive 2006/24/CE, from the European Parliament and Council on 15 march 2006 and its incorporation into spanish law. IV. The new regulation on electronic communications interception.

KEYWORDS

Criminal procedure; Electronic communications right to privacy; Jurisprudence; EU Directives; Communication and information technology.

ABSTRACT

The interception of electronic communication is a tool that has frequently been used in criminal investigation. To this end, criminal procedure law regulated interception of written and telegraphic communications and, following the advance of communication technology in the 20th century, introduced regulations on telephone communication privacy invasion. After World War II, the right to secrecy of correspondence was recognized, resulting in the courts of justice's declaration of a lack of compliance in Spanish legislation in relation with internationally recognized legislation. This circumstance, together with the legal obligation of data storage and conservation, has been the basis for new norms and regulations on this matter through technological investigation regulatory law.

Fecha de recepción: 27/06/2016 Fecha de aceptación: 28/07/2016

33 «*Un dato de carácter personal es cualquier información que permita identificarte o hacerte identificable*». www.agpd.es (26 de junio de 2016).

34 Art. 18.4 CE: «*La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos*». www.congreso.es (26 de junio de 2016).

35 «*El derecho fundamental a la protección de datos reconoce al ciudadano la facultad de controlar sus datos personales y la capacidad para disponer y decidir sobre los mismos*». www.agpd.es (26 de junio de 2016).