FACULTAD DE DERECHO

LA INTERVENCIÓN DE LAS COMUNICACIONES EN EL PANORAMA TECNOLÓGICO ACTUAL

Autor: Miguel García de Mesa

5º E-3 B

Área de Derecho Procesal

Tutora: Sara Díez Riaza

Madrid

Junio 2019

ÍNDICE DE CONTENIDOS

LISTADO DE ABREVIATURAS

AP	Audiencia Provincial
BOE	Boletín Oficial del Estado
CE	Constitución Española
CGPJ	Consejo General del Poder Judicial
Directiva 2007/65/CE	Directiva 2007/65/CE del Parlamento Europeo y del Consejo, de 11 de diciembre de 2007, por la que se modifica la Directiva 89/552/CEE del Consejo sobre la coordinación de determinadas disposiciones legales, reglamentarias y administrativas de los Estados miembros relativas al ejercicio de actividades de radiodifusión televisiva
Directiva 2010/13/UE	Directiva 2010/13/UE, de 10 de marzo de 2010, sobre coordinación de determinadas disposiciones legales, reglamentarias y administrativas de los estados miembros relativas a la prestación de servicios de comunicación audiovisual (Directiva de servicios de comunicación audiovisual).
Directiva (UE) 2018/1808	Directiva (UE) 2018/1808 del Parlamento Europeo y del Consejo, de 14 de noviembre de 2018, por la que se modifica la Directiva 2010/13/UE sobre la coordinación de determinadas disposiciones legales, reglamentarias y administrativas de los Estados miembros relativas a la prestación de servicios de comunicación audiovisual (Directiva de servicios de comunicación audiovisual), habida cuenta de la evolución de las realidades del mercado
LECrim	Ley de Enjuiciamiento Criminal
Ley 7/2010	Ley 7/2010, de 31 de marzo de 2010, General de la Comunicación Audiovisual.
LO	Ley Orgánica

LO 1/1996	Ley Orgánica 1/1996, de 15 de enero, de Protección Jurídica del Menor, de modificación parcial del Código Civil y de la Ley de Enjuiciamiento Civil.
LO 3/2018	Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
LO 13/2015	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
LO 15/1999	Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.
LOPJ	Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial
RD	Real Decreto
RGPD	Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos
TC	Tribunal Constitucional
TIC	Tecnologías de la Información y la Comunicación
TJUE	Tribunal de Justicia de la Unión Europea
TS	Tribunal Supremo

1. RESUMEN

El presente trabajo se centra en una aproximación al estudio de la regulación sobre la intervención de las comunicaciones que han surgido en el panorama tecnológico tras la reforma de 2015. El motivo de esta investigación responde a la revolución tecnológica que ha marcado los últimos años y a los numerosos avances que ha traído consigo. Todos ellos se manifiestan en la vida diaria de las personas y en el tráfico jurídico que se genera. En este sentido, la presencia clave de la industria tecnológica respecto de las comunicaciones hace necesario entrar a regular tanto los derechos como las obligaciones que se derivan para los usuarios de estas nuevas formas de comunicación digitalizadas en el ámbito procesal. Sin embargo, estos adelantos traen consigo resultados positivos y negativos, surgiendo respecto de los segundos nuevas vías para vulnerar los derechos fundamentales de las personas, como pueden ser el derecho a la intimidad y al secreto de las comunicaciones. Concretamente, se hará referencia a la desprotección que en este sentido puede afectar a los menores y a la necesidad de lograr una coordinación entre todos los participantes del medio digital, tanto en el ámbito nacional como en el europeo, a través de normativa específica con la que se pretenda garantizar su seguridad e integridad.

Palabras clave: Intimidad, secreto de las comunicaciones, revolución tecnológica, intervención de las comunicaciones, Internet, protección de datos, menores, control.

ABSTRACT

This paper focuses on an approach to the study of regulation on the intervention of communications which have emerged in the technological landscape after the 2015 reform. The reason for this research is due to the technological revolution that has marked the last few years and the numerous advances that it has brought with it. All of them are manifested in people's daily lives and in the legal traffic that is generated. In this sense, the key presence of the technological industry as for communications makes it necessary to regulate both the rights and obligations derived for the users of these new forms of digitalized communication in the procedural field. However, these advances bring with them both positive and negative results, and new ways of violating people's fundamental

rights, such as the right to privacy and the secrecy of communications, are emerging with regard to the latter. In particular, reference will be made to the lack of protection that may affect minors in this respect and to the need to achieve coordination between all those involved in the digital environment, both at national and European level, through specific regulations aimed at guaranteeing their security and integrity.

Keywords: Intimacy, communications secrecy, technological revolution, communications intervention, Internet, data protection, minors, control.

2. INTRODUCCIÓN

El objeto de estudio de este trabajo se centra en la manera en que el desarrollo de las nuevas tecnologías que han ido surgiendo desde la reforma del 2015, así como de las nuevas formas de comunicación, ha cambiado el tratamiento que recibía la cuestión en el ámbito procesal.

La aparición de nuevos aparatos de escucha y de interceptación de las comunicaciones ha llevado a cuestionar la licitud o ilicitud de los mismos a la hora de recoger pruebas o testimonios que puedan ser admitidos en la investigación criminal. Con el objetivo de lidiar con esta situación se promulgó la LO 13/2015[1]. Esta modificación pretendía esclarecer el papel que tenían los distintos medios de comunicación digital a lo largo del proceso penal. Además, se buscaba garantizar con ella el empleo de diligencias en la fase de instrucción evitando la posible injerencia en los derechos fundamentales de los que son titulares todos los ciudadanos y poder así llegar a soluciones concluyentes en cuanto al papel que jugaban los medios digitales a lo largo del proceso penal.

De igual forma, dado el creciente protagonismo de los jóvenes y menores en el uso de estos dispositivos, en el presente trabajo de investigación se llevará a cabo una pequeña aproximación sobre la manera más pertinente de proceder a su intervención en el proceso penal. A su vez, tratará de abordar también la protección que éstos merecen o que reciben hoy en día como consecuencia de la adaptación a la nueva realidad tecnológica que define la manera de vivir en el panorama actual.

El presente trabajo queda estructurado en tres partes principales. La primera de ellas se basa en una primera aproximación a las nociones que pueden considerarse básicas para continuar con las siguientes partes de la investigación, tratadas a lo largo del capítulo primero. En ella se tratan derechos como el derecho a la intimidad y el relativo al secreto de las comunicaciones. Por otro lado, se aproxima a los aspectos principales que caracterizan al tratamiento que recibe el derecho al secreto de las comunicaciones en el proceso penal después de la LO 13/2015. En esta misma parte, se lleva a cabo una

[1] 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 (BOE de 6 de octubre de 2015).

aproximación en cuanto a la intervención de las comunicaciones en algunos medios de comunicación. En la segunda parte, se investiga sobre la influencia que han tenido las nuevas tecnologías en el proceso penal en cuanto a su intervención para el esclarecimiento de los delitos y la protección de la que son merecedores los datos que entran en juego, junto con la evolución en el acceso a los mismos. En cuanto a la última parte, toda ella se enfoca desde el punto de vista de los menores. Se lleva a cabo una breve investigación sobre la intervención de los procesos en los que los menores son la figura principal, tratando tanto la exposición a la que estos se ven sometidos en las redes sociales como la protección que reciben y el alcance del control parental. Además, se tratarán algunas cuestiones relevantes, enfocadas al ámbito de los menores, sobre la Directiva (UE) 2018/1808[2]. Finalmente, se expondrán las conclusiones a las que se ha llegado en relación a cada una de las ideas fundamentales tratadas a lo largo del trabajo.

[2] Directiva (UE) 2018/1808 del Parlamento Europeo y del Consejo, de 14 de noviembre de 2018, por la que se modifica la Directiva 2010/13/UE sobre la coordinación de determinadas disposiciones legales, reglamentarias y administrativas de los Estados miembros relativas a la prestación de servicios de comunicación audiovisual (Directiva de servicios de comunicación audiovisual), habida cuenta de la evolución de las realidades del mercado.

3. CAPÍTULO 1: NOCIONES BÁSICAS

3.1. El derecho a la intimidad

El carácter privado de la información sobre la que se va a desarrollar la investigación hace que resulte pertinente una referencia, en este apartado preliminar, a la intimidad de las personas.

A la hora de referirse a la intimidad como un derecho constitucionalmente protegido, resulta necesario destacar que, tanto por su amplitud como por los diferentes matices que revisten al mismo, nuestro ordenamiento jurídico no ha sido capaz de encontrar una expresión única con la que poder definir lo que entiende por la intimidad constitucionalmente protegida. La idea de intimidad y el contenido de la misma que merece protección ha ido evolucionando con el paso del tiempo. Esta evolución ha hecho que pase de ser considerada como parte del ámbito de retiro individual de cada uno, ámbito en el cual no había cabida para intromisiones de carácter ajeno, a ser considerada como una de las preocupaciones principales en cuanto a la capacidad de control que puede y debe ejercerse sobre la misma.

Fruto de esta misma evolución, se llega a la conclusión de que la vía más adecuada con la que cuentan los individuos para garantizar su dignidad personal es la capacidad de control sobre cualquier tipo de información que tenga que ver con ellos mismos. De esta forma, se logra superar la dimensión clásica de la intimidad que se tenía (en cuanto a los ámbitos que tenían la consideración de reservados, los lugares a los que se restringía el acceso y los contenidos cuya divulgación no estaba permitida).

La dimensión informativa que se incorpora al derecho a la intimidad permite llevar a cabo un control más exhaustivo sobre todos aquellos datos o contenidos de carácter personal y que, como tales, forman parte de la dimensión privada de la vida de los individuos. Esta misma faceta informativa es la que permite que el titular del derecho a la intimidad controle la información y los datos que resultan esenciales para el desarrollo de la vida privada y que, por ello, merecen una especial labor de vigilancia y protección.

Así, acceder a datos o información que formen parte de esa esfera personal e íntima constitucionalmente protegida, ya mencionada, sin que el titular del derecho a la intimidad otorgue su consentimiento con carácter previo, constituye una forma de intromisión en el derecho a la intimidad de los individuos. Respecto de la necesidad de dicho consentimiento informado coinciden tanto la protección de derechos que recoge el artículo 18.1 de la CE[3] como la que reconoce lo establecido en el artículo 18.4 de la misma Ley. La regla general a propósito del mismo reconoce la necesidad de contar con una autorización de carácter judicial previa para poder recopilar todo ese tipo de información procedente de una fuente íntima y personal[4].

Por otro lado, tal y como ya se ha mencionado, un aspecto importante del que hablar cuando se hace referencia a las comunicaciones entre las personas a través de distintos medios es la situación en la que se encuentra el derecho a la intimidad de las personas y las posibilidades de protección que se le reconocen en el panorama actual. Con la referencia a ese panorama actual, nos referimos a la evolución que han experimentado ambos conceptos como consecuencia de la revolución tecnológica y los avances que han marcado los últimos tiempos. Así, el uso de Internet ha hecho que, hoy en día, la mayoría de los datos con los que operamos se encuentren de alguna manera digitalizados.

El tráfico de las relaciones entre los individuos ha pasado del plano material o físico al plano tecnológico. Este enorme paso informático ha hecho que lo relevante, a propósito de todos estos datos e información personal pertenecientes a la esfera más personal e íntima de los ciudadanos, deje de ser el lugar del que procedan los mismos y de dónde se obtengan. Hoy en día, poco importa el que procedan de discos duros o, por el contrario, de ficheros y archivadores físicos, pudiendo localizarse ambos tipos en lugares diferentes. Sin embargo, una práctica común en la labor de almacenamiento de datos es la de digitalizar y pasar a programas informáticos de almacenamiento de datos todos aquellos que, originariamente, se transcribían al papel. Son ventajas como el ahorro de espacio físico a la hora de almacenarlos, o la facilidad con la que cuenta la población en general para manejar este tipo de sistemas y programas las que han promovido el traslado del

[3] Constitución Española, de 27 de diciembre de 1978 (BOE 29 de diciembre de 1978).
[4] Sánchez Yllera, I., *La nueva regulación de las medidas limitativas de los derechos reconocidos en el art. 18 CE (I): Detención y apertura de correspondencia escrita y telegráfica. Disposiciones comunes. Interceptación de comunicaciones telefónicas y telemáticas*, Publicación del CENDOJ, Madrid, 2016, p. 6.

tráfico de información del papel a los ordenadores y sistemas informáticos. Tal es el impacto que ha tenido esta revolución tecnológica en el procesamiento y almacenamiento de los datos, que algunos autores sostienen que fenómenos como la digitalización y el uso de Internet de manera masiva han llegado a superar el fenómeno que supuso el surgimiento de la sociedad industrial a finales del siglo XIX y han provocado un cambio de mayores dimensiones en lo que a la población respecta[5].

Sin embargo, todo este proceso favorable de evolución está marcado por una serie de cambios menos favorables. Así como el contenido que el derecho a la intimidad protege ha evolucionado, también lo ha hecho, de forma paralela, la mayor capacidad intrusiva y de almacenamiento de datos. Son las nuevas tecnologías las que, a pesar de contribuir a la mejora de la calidad de vida de la población en general, han permitido esta evolución con connotaciones negativas.

En este sentido, resulta necesario destacar el tratamiento que la LO 13/2015 lleva a cabo en cuanto a los límites frente a los que se encuentra la posibilidad de llevar a cabo un control tecnológico de esfera de intimidad. Sin duda, esta es una de las cuestiones que más deben preocupar y preocupan con vistas a una convivencia futura.

3.2. El derecho al secreto de las comunicaciones

El artículo 18.3 CE incluye el derecho al secreto de las comunicaciones entre los derechos fundamentales que establece nuestra Carta Magna. La protección de la que gozan las distintas formas de comunicación quedó ya recogida expresamente en la Declaración de Derechos del Hombre y del Ciudadano de 1789[6]. A partir de entonces, este derecho al secreto de las comunicaciones ha adquirido una importancia clave en tanto en cuanto resulta necesario para respetar y desarrollar la personalidad del ser humano.

En relación al punto anteriormente expuesto, cabe destacar la relevancia del contenido del derecho a la intimidad, dado que la regulación que tiene el derecho al secreto de las

[5] *La nueva regulación de las medidas limitativas de los derechos reconocidos en el art. 18 CE (I): Detención y apertura de correspondencia escrita y telegráfica. Disposiciones comunes. Interceptación de comunicaciones telefónicas y telemáticas* "cit." p. 7.
[6] Declaración de los Derechos del Hombre y del Ciudadano (26 de agosto de 1789).

comunicaciones en nuestro ordenamiento jurídico se encuentra estrechamente ligada a la que recibe el derecho a la intimidad. Tal es la pertinencia del tratamiento que los relaciona, que se ha llegado a plantear la duda de si el secreto de las comunicaciones constituye una manifestación del derecho a la intimidad o si, por el contrario, no existe entre ellos ningún tipo dependencia[7]. Es, sin embargo, la segunda de las posturas de la discusión la que parecer ser más acertada a pesar de la cercanía que pueda existir respecto del contenido que ambos derechos protegen. Sobre la cuestionada vinculación entre ambos derechos se manifestó el Tribunal Constitucional en una de sus sentencias, aclarando que:

> […] la diferenciación y autonomía del ámbito de protección de los derechos fundamentales a la intimidad personal (art. 18.1 CE) y al secreto de las comunicaciones (art. 18.3 CE) que se proyecta sobre el régimen de protección constitucional de ambos derechos. Pues si «ex» art. 18.3 CE la intervención de las comunicaciones requiere siempre resolución judicial, "no existe en la Constitución reserva absoluta de previa resolución judicial" respecto del derecho a la intimidad personal, de modo que excepcionalmente hemos admitido la legitimidad constitucional de que en determinados casos y con la suficiente y precisa habilitación legal la policía judicial realice determinadas prácticas que constituyan una injerencia leve en la intimidad de las personas siempre que se hayan respetado las exigencias dimanantes del principio de proporcionalidad […].[8]

La protección que reciben las comunicaciones se basa en que es la propia comunicación que de alguna forma se entabla la que es considerada como secreta, con independencia de lo que en ellas se diga[9]. En este sentido, el hecho de considerar que la relevancia en cuanto a "lo secreto" reside en el propio medio de comunicación ha permitido que se recojan entre las protegidas una gran variedad de nuevas formas de comunicación. El origen de las mismas se encuentra en la revolución tecnológica que comenzó a finales del siglo pasado y que se ha prolongado hasta hoy. Esta nueva realidad ha llevado a que las formas de comunicación a las que se refiere expresamente la CE (la postal, la telegráfica y la telefónica) adquieran la consideración de ejemplos de entre todas las empleadas. Se ha llegado a ampliar la protección de comunicaciones que van desde las palabras que se emiten en el transcurso de una conversación, hasta las comunicaciones en las que se

[7] Noya Ferreiro, Mª L., *Derecho de defensa e intervención de las comunicaciones de los abogados*, Tirant lo Blanch, Valencia, 2018, p. 84.
[8] Sentencia del Tribunal Constitucional de 9 de octubre 281/2006 FJ 3.
[9] Jiménez Campo, J., *La garantía constitucional del secreto de las comunicaciones*, REDC, núm. 20, 1987, p. 50.

requiera la intervención de cámaras (en cuanto a la videoconferencia), o el uso de dispositivos móviles (en cuanto al WhatsApp o a las redes sociales)[10].

La norma constitucional fue redactada como garante de la impenetrabilidad que son susceptibles de sufrir las comunicaciones en general. Esta defensa se predica respecto de terceros que sean ajenos a las mismas, prohibiendo así su interceptación o el conocimiento de carácter antijurídico. Con esta protección se busca, además del contenido de la comunicación, aspectos como los relativos a la identidad de los propios interlocutores que participan en el proceso de comunicación, o de los corresponsales que en su caso medien por ellos[11].

Por otro lado, debe destacarse la distinción sobre el tipo de comunicación que efectivamente se protege con el artículo 18.3 CE, siendo estas las conversaciones de carácter privado. Quedan excluidas de dicha protección las conversaciones que adquieran la calificación de públicas. Sin embargo, dicha distinción entre ambos tipos de comunicación ha de ser establecida con carácter previo por las personas que la mantienen en cuanto a su voluntad de que permanezca en el ámbito privado. Puede verse entonces como esta consideración no viene determinada por el número de personas que en ella participen. Una conversación, por tanto, aunque se desarrolle entre varias personas puede perfectamente quedar dentro del ámbito privado en tanto en cuanto la relación que entre ellos exista así lo permita. Esta última situación puede verse claramente en el caso de los partidos políticos o de las juntas de accionistas, cuando se produce una reunión entre sus miembros, situaciones de las que puede deducirse la nota de privacidad por los intereses que comparten todos los implicados[12].

3.3. El secreto de las comunicaciones en el proceso penal antes y después del 2015

La LO 13/2015 lleva a cabo una regulación sobre dos cuestiones claves en cuanto a la intervención de las comunicaciones en el desarrollo del proceso penal. Estas son la modificación del derecho de defensa y la regulación de las medidas dirigidas a la

[10] Rodríguez Álvarez, A., Diligencia de registro de dispositivos y smartphones, en "Fodertics 5.0. *Estudios sobre nuevas tecnologías y Justicia*", 2016, p. 255.
[11] Sentencia del Tribunal Constitucional de 29 de noviembre 114/1984.
[12] *Derecho de defensa e intervención de las comunicaciones de los abogados* "cit." p. 86.

investigación de la tecnología[13]. En atención al objetivo que se persigue con el presente trabajo de investigación se tratará con mayor profundidad la segunda de las cuestiones.

Esta regulación ha dado lugar al tan esperado desarrollo legislativo sobre la adopción de medidas de intervención de las comunicaciones con fines investigadores respecto de las limitaciones que existen al derecho de las comunicaciones. No sólo hace referencia a las cuestiones en torno a las medidas de intervención telefónica, sino que regula de igual forma la intervención de otro tipo de comunicaciones que, como se ha venido adelantando, forman parte del panorama actual.

En lo que se refiere al artículo 579 LECrim, la modificación que lleva a cabo la mencionada LO procede a limitar el contenido de dicho artículo a, únicamente, la intervención de la correspondencia escrita y telegráfica. Además, introduce el artículo 579 bis, el cual recoge las condiciones y requisitos necesarios que deben darse para poder emplear la información obtenida de descubrimientos o del propio procedimiento en el que se acuerda la intervención de la comunicación en un procedimiento diferente. De esta forma, pasan a regularse los efectos que habitualmente se derivan de los descubrimientos casuales[14].

La LO 13/2015 trae consigo una modificación de la manera en la que en origen se estructuraba la LECrim. Dentro del Título VIII del Libro II de esta última ley quedan recogidas las medidas de investigación limitativas de los derechos cuyo contenido queda recogido en el artículo 18 CE, quedando todas ellas distribuidas en diez capítulos. De todos ellos, los capítulos que resultan relevantes para el objeto de esta investigación van desde el Capítulo III hasta el X, ambos dos incluidos. En los capítulos del trabajo se llevará a cabo una pequeña aproximación al contenido de algunos de ellos por la relevancia práctica y teórica de los mismos en el panorama actual.

Esta modificación hace que el artículo 579 LECrim deje de abarcar un abanico de situaciones tan amplio como, en origen, se pretendía. Con carácter previo a la promulgación de dicha LO, el objetivo había sido añadir al contenido del mencionado

[13] Rodríguez Álvarez, A., *Intervención de las comunicaciones telefónicas y telemáticas y smartphones* en "Justicia penal y nuevas formas de delincuencia", 2017, p. 149.
[14] *Derecho de defensa e intervención de las comunicaciones de los abogados* "cit." p. 101.

artículo las previsiones que regulaban las medidas de restricción del derecho al secreto de las comunicaciones por medio de dispositivos y técnicas que incorporaban numerosas innovaciones. En este sentido, los órganos jurisdiccionales debían interpretar dicho precepto de manera extensiva, excediendo así la capacidad para regular las diligencias de investigación con que contaban con carácter previo a la modificación[15]. El peligro que esta interpretación extensiva del precepto traía consigo fue planteado por el Tribunal Constitucional en una de sus sentencias, manteniendo la siguiente línea de pensamiento:

> […] analizamos una intervención de las comunicaciones absolutamente extraña al ámbito de imputación de dicha regulación. […] No estamos por lo tanto ante un defecto por insuficiencia de la ley, ante un juicio sobre la calidad de la ley, sino que se debate el efecto asociado a una ausencia total y completa de ley. Y es que el art. 579.2 LECrim se refiere de manera incontrovertible a intervenciones telefónicas, no a escuchas de otra naturaleza, ni particularmente a las que se desarrollan en calabozos policiales y entre personas sujetas a los poderes coercitivos del Estado por su detención, como las que aquí resultan controvertidas; ámbito que por su particularidad debe venir reforzado con las más plenas garantías y con la debida autonomía y singularidad normativa […][16].

Por otro lado, esta ley trajo consigo una serie de principios y bases que han tenido una importancia clave dentro del proceso de investigación penal que nuestro ordenamiento jurídico regula. Uno de ellos, se basa en la consideración del principio de proporcionalidad en el proceso penal, siendo el artículo 588 bis a) el que desarrolla el contenido legal de dicho principio. Asimismo, éste está constituido por una serie de subprincipios que definen su contenido: el de especialidad, en cuanto a la consideración de delitos concretos; el de necesidad, en cuanto a que la medida empleada tiene que ser la única solución viable para la obtención del resultado de la manera menos gravosa; el de idoneidad, en cuanto a que la medida que se decida tiene que ser útil para conseguir el fin que se persigue con ella; y el de excepcionalidad, en cuanto a que la medida en cuestión no podrá contar con la autorización necesaria para el caso de que comprometa o dificulte el desarrollo de la investigación.

En cuanto a los límites que esta ley introduce en nuestro ordenamiento cabe hacer referencia al que recoge el artículo 579.1 en relación a la intervención de las correspondencia escrita y telegráfica. Además, este artículo se aplica, en atención a lo

[15] Marchena Gómez, M., González-Cuellar Serrano, N., *La reforma de la Ley de Enjuiciamiento Criminal en 2015*, Ediciones Jurídicas Castillo de Luna, Las Palmas de Gran Canaria, 2015, p. 176.
[16] Sentencia del Tribunal Constitucional de 22 de septiembre 145/2014 FJ 7.

recogido en los artículos 588 ter a) y 588 ter b), de forma extensiva a todas las intervenciones que se llevan a cabo de las comunicaciones telefónicas, telemáticas y ambientales. Sin embargo, esta intervención es lícita únicamente en los delitos: dolosos que lleven aparejada una pena con límite máximo de, al menos, tres años de prisión; los que llevan a cabo los integrantes de un grupo u organización con fines criminales; los delitos de terrorismo; y los delitos en los que, para su comisión, resulta necesaria la utilización de instrumentos informáticos o de cualquier otro medio tecnológico o de comunicación del que pueda obtenerse información[17].

Todo ello hace pensar en la importancia que tiene el hecho de identificar correctamente aquellos datos o hechos de carácter objetivo que puedan constituir algún indicio sobre la posible existencia de un delito. También debe concretarse la conexión que pueda vincular a las personas que estén siendo objeto de investigación con dicho delito[18]. Para ello, ha de tenerse en cuenta que por indicio se entiende algo que va más allá de la mera sospecha, pero menos que lo que se exige para el procesamiento en atención a la racionalidad de los indicios[19]. La relevancia de todos estos datos que se exigen en atención al principio de proporcionalidad y que los órganos jurisdiccionales necesitan se ha incrementado como consecuencia de la modificación promovida por la LO 13/2015. En este sentido, el artículo 588 bis b) ha pasado a concretar el contenido de la solicitud policial o del Ministerio Fiscal. Este se concreta en base a los siguientes elementos:

> 1.º La descripción del hecho objeto de investigación y la identidad del investigado o de cualquier otro afectado por la medida, siempre que tales datos resulten conocidos.
> 2.º La exposición detallada de las razones que justifiquen la necesidad de la medida de acuerdo a los principios rectores establecidos en el artículo 588 bis a, así como los indicios de criminalidad que se hayan puesto de manifiesto durante la investigación previa a la solicitud de autorización del acto de injerencia.
> 3.º Los datos de identificación del investigado o encausado y, en su caso, de los medios de comunicación empleados que permitan la ejecución de la medida.
> 4.º La extensión de la medida con especificación de su contenido.
> 5.º La unidad investigadora de la Policía Judicial que se hará cargo de la intervención.
> 6.º La forma de ejecución de la medida.
> 7.º La duración de la medida que se solicita.
> 8.º El sujeto obligado que llevará a cabo la medida, en caso de conocerse[20].

[17] *Derecho de defensa e intervención de las comunicaciones de los abogados* "cit." p. 103-104.
[18] Sentencia del Tribunal Constitucional de 14 de marzo 25/2011.
[19] Sentencia del Tribunal Constitucional de 3 de julio 220/2006.
[20] Artículo 588 bis b) 2. de la 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 (BOE de 6 de octubre de 2015).

4. CAPÍTULO 2: PANORAMA EN LA LEGISLACIÓN ACTUAL EN CUANTO A LA INTERVENCIÓN DE LAS COMUNICACIONES

4.1. Intervención telefónica

La intervención de los teléfonos ha sido y es en la actualidad la medida de investigación, en el plano tecnológico, más recurrente. Este medio de comunicación ha experimentado un rápido e importante avance desde sus orígenes, en los que se intervenían los teléfonos para investigar las actividades de los grupos organizados de criminales. Frente a las comunicaciones que se mantenían entonces, todas ellas en base a la transmisión de la voz, hoy en día los dispositivos móviles disponibles en el mercado van más allá. De la voz, se ha pasado a los mensajes de texto, las fotografías y los vídeos, entre las más comunes. La posibilidad con la que ahora cuentan estos dispositivos de conectarse a Internet permite la transmisión de información de todo tipo. Dicha evolución tecnológica justifica que la medida de investigación de la intervención de los teléfonos móviles se haya ampliado a las comunicaciones telemáticas. Por tales, se entienden aquellas en las que se transmiten datos en formato digital por medio de Internet u otra red de comunicación similar. Ambos tipos de comunicación han quedado regulados en el artículo 588 ter a-i) LECrim, frente a su anterior regulación conjunta e insuficiente en el artículo 579 LECrim.

A pesar de quedar reguladas en los mismos artículos de nuestro ordenamiento, se puede concretar una distinción entre ellas. Así, por telefónica puede entenderse una comunicación vía oral que se desarrolla a distancia a través de terminales telefónicos. Por telemática, sin embargo, se entiende una comunicación de tipo oral, en la que también pueden transmitirse imágenes, mensajes de texto, documentos o datos a través de dispositivos telefónicos u ordenadores o tablets con posibilidad de conectarse a una red WIFI. En este sentido, la ley ha terminado por ampliar el concepto de dispositivo de comunicación para abarcar todo el abanico de posibilidades de establecer una comunicación en la realidad actual. Lo relevante en cuanto a la intervención de este tipo de comunicación se basa en la averiguación sobre la persona que realiza la llamada, el momento en el que lo hace, el tiempo que emplea y la localización geográfica de los interlocutores durante la llamada. Para poder hacer uso de esta medida de intervención, resulta necesario que la policía o el Fiscal la soliciten de forma expresa. Dicha petición

tiene que resultar idónea y necesaria y los hechos involucrados han de suponer un cierto grado de gravedad para poder garantizar el principio de proporcionalidad. Puede acordarse respecto a los mismos tipos de delitos ya mencionados en el apartado anterior en relación al artículo 588 ter a) y su remisión al 579.1 LECrim[21].

La manera en la que tiene lugar esta intervención es a través de la grabación de las conversaciones que puedan estar vinculadas a los hechos que se investigan. En cuanto a la telemática, también es posible hacerlo grabando los mensajes o los documentos que se hubiesen transmitido, entre otros. Sin embargo, a la hora de intervención, esta se extiende a todas las comunicaciones que se hayan producido a través de un mismo dispositivo.

En cuanto a los sujetos pasivos de dicha medida de intervención, estos se concretan en todos aquellos que resulten implicados en base a los indicios existentes, sin importar que sean o no ellos los titulares de dichos dispositivos o sus usuarios habituales. El hecho de que el teléfono que resulte intervenido no esté a nombre del sospechoso no impide que se imponga la medida de intervención telefónica. Lo que sí resulta necesario es que quede de alguna forma constante que ese mismo aparato constituye el medio a través del cual las personas investigadas por el delito pueden entablar cualquier tipo de comunicación. A este respecto se pronuncia el TS en una de sus sentencias como sigue:

> […] En relación a la pretendida identidad entre el titular del terminal telefónico intervenido y su usuario, también hay que recordar […] que lo importante es la identidad del titular de la línea telefónica a intervenir, siendo indiferente para la validez de las informaciones obtenidas la identidad de la persona que haga uso de dicho terminal […] [22]

El plazo para el cual se acordará la medida de intervención no podrá superar los 3 meses desde la fecha en el que el juez la autorice y podrá prorrogarse por períodos sucesivos de 3 meses hasta alcanzar los 18 meses, tal y como recoge el artículo 588 ter g) LECrim. Para poder obtener la concesión de la prórroga, la policía será la responsable de solicitarlo de manera fundamentada aportando todo lo investigado en relación a los hechos investigados para apoyar la necesidad de mantener la medida.

[21] Richard González, M., *Investigación y prueba mediante medidas de intervención de las comunicaciones, dispositivos electrónicos y grabación de imagen y sonido*, Wolters Kluwer, Madrid, 2017, p. 137.
[22] Sentencia del Tribunal Supremo de 12 de enero 993/2016 FJ 6.

Por otro lado, el auto por medio del cual se pretende la intervención de las comunicaciones va dirigido a la empresa operadora de las comunicaciones con la que se tuviese contratado el servicio. Estas compañías quedan obligadas a colaborar con la policía en su labor de intervención acordada judicialmente, tal y como reconocen la LECrim, la Ley 9/2014 General de Telecomunicaciones[23] y la Ley 25/2007 de Conservación de Datos[24]. En este sentido, el artículo 88.1 del RD 424/2005 Reglamento de servicios de comunicaciones[25] establece lo siguiente:

> 1. Los sujetos obligados deberán facilitar al agente facultado, salvo que por las características del servicio no estén a su disposición y sin perjuicio de otros datos que puedan ser establecidos mediante real decreto, los datos indicados en la orden de interceptación legal, de entre los que se relacionan a continuación:
>
> a) Identidad o identidades -en la acepción definida en el artículo 84.i)- del sujeto objeto de la medida de la interceptación.
> b) Identidad o identidades -en la acepción definida en el artículo 84.i)- de las otras partes involucradas en la comunicación electrónica.
> c) Servicios básicos utilizados.
> d) Servicios suplementarios utilizados.
> e) Dirección de la comunicación.
> f) Indicación de respuesta.
> g) Causa de finalización.
> h) Marcas temporales.
> i) Información de localización.
> j) Información intercambiada a través del canal de control o señalización. [26]

Por último, dicho auto puede dirigirse igualmente a otra persona que conozca o participe en el transcurso de la comunicación por el motivo que fuere, quien incurriría en un delito de desobediencia en caso de no hacerlo. No podrán revelar ningún tipo de información concerniente a las actividades que las autoridades les hubiesen requerido.

A propósito de la medida de intervención telefónica cabe destacar un auto reciente de la AP de Tarragona de noviembre de 2018[27]. La cuestión de la que se deriva el procedimiento judicial seguido comienza con la investigación de un robo de una cartera

[23] Ley 9/2014, de 9 de mayo, General de Telecomunicaciones (BOE 10 de mayo de 2014).
[24] Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones (BOE 19 de octubre de 2007).
[25] Real Decreto 424/2005, de 15 de abril, por el que se aprueba el Reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios (BOE 29 de abril de 2005).
[26] Artículo 88.1 del Real Decreto 424/2005, de 15 de abril, por el que se aprueba el Reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios (BOE 29 de abril de 2005).
[27] Auto de la Audiencia Provincial de Tarragona de 23 de noviembre 647/2018.

y un móvil en el que media violencia. En este caso, el Juzgado de Instrucción número 3 de Tarragona niega la posibilidad de que la Policía Judicial accediese a los datos personales o de filiación contenidos en el dispositivo que había sido objeto del robo, ya que consideró que el robo no poseía la calificación de delito grave, necesaria para practicar dicha medida de investigación. Sin embargo, el Ministerio Fiscal recurrió dicho auto ante la AP de Tarragona.

Esta situación lleva a la AP de Tarragona a plantear una cuestión prejudicial ante el TJUE sobre el umbral concreto en base al cual se determina la mayor o menor gravedad de los delitos y que permitiría, en caso de ser suficientemente grave, llevar a cabo una injerencia en los derechos fundamentales. En el caso concreto, la injerencia se basaba en el acceso por parte de la Policía Judicial a los datos personales recogidos por los proveedores de servicios de comunicaciones electrónicas.

El TJUE[28] determinó que dicho acceso encontraba su fundamento de aplicación en la Directiva sobre la privacidad y las comunicaciones electrónicas[29]. Por otro lado, estableció en su sentencia que el hecho de poder acceder a los datos de la tarjeta SIM contenida en un dispositivo móvil robado suponía llevar a cabo una injerencia en los derechos fundamentales de los titulares de dichas tarjetas y propietarios de los datos, con independencia de la posible consideración de la misma como grave y de que la información sea o no sensible o que de la injerencia se deriven inconvenientes para el propietario de la misma. A pesar de esta concepción, la Directiva recoge a su vez los casos concretos en los que las autoridades públicas pueden acceder a esta información como una excepción a la confidencialidad por la que se caracterizan los procesos de comunicación a través de medios digitales. Sin embargo, el Tribunal puntualiza que la Directiva reconoce dichos supuestos respecto de los delitos en términos generales, sin hacer referencia exclusiva a los calificados como graves.

Así, el TJUE responde a la cuestión prejudicial planteada por la AP de Tarragona diciendo que el acceso a los datos concretos sobre los que la Policía Judicial llevo a cabo la

[28] Sentencia del Tribunal de Justicia de la Unión Europea de 2 de octubre de 2018 C-207/16.
[29] Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (BOE 31 de julio de 2002), en su versión modificada por la Directiva 2009/136/CE del Parlamento Europeo y del Consejo, de 25 de noviembre de 2009 (BOE 18 de diciembre de 2009).

solicitud no se entendería como una injerencia grave, puesto que de los mismos no cabe concluir aspectos concretos de su vida privada. Por tanto, entiende que la injerencia pretende la investigación o esclarecimiento de un delito de carácter general.

4.2. Grabación de conversaciones y colocación de aparatos de escucha

La cuestión que se aborda en el presente apartado constituye un aspecto de gran trascendencia en lo que respecta a los planteamientos acometidos por la reforma de la LECrim en 2015, desde el artículo 588 quarter a) hasta la letra e) del mismo artículo.

Queda regulada de esta forma la posibilidad de grabar la voz (aunque también se refiere a la imagen) de la persona investigada a través de dispositivos destinados al efecto con independencia del lugar en el que se proceda a hacerlo. Si bien puede que esté implícito el hecho de que se permita la grabación de las conversaciones entabladas oral y directamente con terceras personas, lo determinante es la posibilidad de que el lugar en el que se graben las mismas sea público o cerrado. De esta forma, la norma ha pasado a contemplar de alguna manera el hecho de que se pueda grabar a las personas en su domicilio personal o familiar, interfiriendo de esta manera en su intimidad. Parece necesario mencionar brevemente la manera en la que el TC entiende el concepto de domicilio. Así, concreta la definición de domicilio como un "espacio apto para desarrollar vida privada"[30], así como aquel que "entraña una estrecha vinculación con su ámbito de intimidad"[31], "el reducto último de su intimidad personal y familiar"[32].

De esta forma, se estaría limitando tanto el derecho al secreto de las comunicaciones del individuo, en el sentido en el que queda recogido en el artículo 18.3 CE, como el derecho a la inviolabilidad del domicilio contenido en el apartado anterior del mismo artículo. Esta doble limitación requiere que el juez habilite de forma expresa la entrada al lugar cerrado para poder llevar a cabo la grabación de la conversación[33].

[30] Sentencia del Tribunal Constitucional de 31 de mayo 94/1999 FJ 4.
[31] Sentencia del Tribunal Constitucional de 26 de abril 69/1999 FJ 2.
[32] Sentencia del Tribunal Constitucional de 27 de noviembre 283/2000 FJ 2.
[33] Rayón Ballesteros, Mª C., "Medidas de investigación tecnológica en el proceso penal: la nueva redacción de la Ley de Enjuiciamiento Criminal operada por la Ley Orgánica 13/2015." *Anuario Jurídico y Económico Escurialense*, n. 52, 2019, p. 196.

Además de la necesidad de que existan indicios de la situación delictiva en base a la investigación realizada, la medida que se plantea necesita, para que pueda contemplarse, que los hechos investigados sean efectivamente constitutivos de delito (los especificados en el artículo 588 quater b)2.a) LECrim) y que pueda preverse que los dispositivos empleados sean de ayuda en cuanto a la aclaración de los hechos y la identificación del autor y en cuanto a la obtención de datos que resulten esenciales para la investigación que se esté llevando a cabo (artículo 588 quater b) LECrim).

Sin embargo, esta posibilidad de grabar las conversaciones del investigado sólo está permitida para encuentros concretos, ya que, de lo contrario, se estaría autorizando el empleo indiscriminado de dispositivos de grabación respecto de cualquier tipo de comunicación que pudiese establecer el investigado. Así, será necesario que con la autorización de la medida se concrete tanto el lugar en el que se va a practicar como las situaciones concretas de la vida del investigado en las que se hará.

Tal y como recoge el artículo 588 ter i) LECrim, las partes implicadas en el proceso podrán tener acceso a las grabaciones de las conversaciones pertinentes haciéndoles entrega de una copia de las mismas o de su transcripción en caso de que se hubiese realizado. Para poder proceder a la entrega de las copias es necesario que se haya levantado el secreto de las comunicaciones y que la medida de intervención que se hubiese interpuesto anteriormente haya dejado de estar vigente. Sin embargo, en caso de que el contenido de las grabaciones hiciese referencia a aspectos relacionados con la intimidad de las personas, las copias y transcripciones que se faciliten no podrán contener estas partes. El carácter incompleto de las mismas tendrá que constar expresamente[34].
Respecto a la finalización de la medida, el tiempo durante el cual se lleve a cabo deberá ser únicamente el necesario para el objetivo de la investigación. Una vez completada la grabación de la conversación requerida, se desactivarán todos los dispositivos que fueron habilitados para ello y el juez ordenará que se eliminen todos aquellos registros que puedan figurar en los sistemas empleados, teniendo que verificar la efectiva eliminación de los mismos.

[34] "Medidas de investigación tecnológica en el proceso penal: la nueva redacción de la Ley de Enjuiciamiento Criminal operada por la Ley Orgánica 13/2015." "cit." p. 197.

4.3. Ilicitud de la prueba por vulneración del derecho al secreto de las comunicaciones

Serán declarados nulos de pleno derecho todos aquellos actos de los que se derive un incumplimiento de las normas, de carácter esencial, relativas al proceso penal y que provoque la situación de indefensión de la parte cuyas comunicaciones deban ser intervenidas. En estos supuestos, la investigación judicial será declarada nula y la prueba obtenida con dichas medidas, ilícita.

Respecto de esta indefensión, el artículo 24 CE recoge el principio de tutela judicial efectiva, en base al cual se tratará de evitar la indefensión, considerándose en caso contrario una violación de los derechos fundamentales del investigado. Asimismo, el artículo 11.1 LOPJ[35] recoge la prohibición de que de la prueba que se haya obtenido de manera ilícita se derive cualquier tipo de efecto. El mismo artículo pone al mismo nivel el hecho de que la prueba ilícita se haya obtenido de forma directa como indirecta. En base al contenido de los mencionados artículos se concreta la diferencia entre el incumplimiento de la normativa constitucional, en cuanto a la adopción y ejecución de la medida, y el incumplimiento de la normativa procesal, que recoge la aportación y práctica de la prueba. En el primer caso, se consideran nulos e ilícitos tanto los hechos como las evidencias que hayan podido obtenerse, mientras que en el segundo caso, la nulidad de la prueba afectada es relativa y el hecho en sí es lícito y susceptible de prueba en base a diferentes medios de los ya utilizados[36].

Todas aquellas pruebas para cuya obtención se hayan intervenido las comunicaciones del investigado vulnerando su derecho a la intimidad o al secreto de sus comunicaciones serán declaradas nulas de pleno derecho. Los supuestos en los que deban ser calificadas de esta manera serán aquellos en los que no se haya producido ninguna autorización por parte del juez, en los que no se haya controlado el resultado de la investigación o en los que no se haya motivado de manera suficiente las notas de necesidad y proporcionalidad que requiere la medida en cuestión para que se pueda llevar a cabo. Sin embargo, sólo podrá conseguirse dicha calificación en el caso en el que se presenten razones y

[35] Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial (BOE 2 de julio de 1985).
[36] *Investigación y prueba mediante medidas de intervención de las comunicaciones, dispositivos electrónicos y grabación de imagen y sonido*, "cit." p. 364.

evidencias acreditadas que demuestren una actuación ilícita por parte de la policía, dado que los actos de investigación llevados a cabo por sus miembros cuentan con la aceptación de su legitimidad.

Aunque exista autorización por parte del juez, todas aquellas actuaciones que se hayan producido sin las garantías legales pertinentes serán radicalmente nulas. Así, el hecho de que el auto en sí mismo no sea lícito hace nulos el resto de los autos en los que se hayan podido autorizar prórrogas, no pudiendo sanarse la nulidad que se dio desde antes del inicio de las actuaciones.

En caso de que la prueba se haya obtenido ilícitamente en base a la vulneración de alguno de los derechos recogidos como fundamentales, dicha prueba se excluirá tanto si se obtuvo por parte de las fuerzas del orden público como si la obtuvieron particulares. La distinción entre ambos tipos se encuentra en que, mientras que en el caso de los particulares serán susceptibles de valoración en tanto que hayan sido fruto de una actuación espontánea con la que no se pretendiese preconstituir un prueba frente al acusado; en el caso de las obtenidas por las fuerzas del Estado, estas serán declaradas ilícitas de manera casi absoluta.

5. CAPÍTULO 3: INFLUENCIA DE LAS NUEVAS TECNOLOGÍAS

5.1. Intervención de conversaciones de WhatsApp

La aplicación móvil de WhatsApp representa a día de hoy un porcentaje de descargas casi absoluto. Esto se debe a que, en relativamente poco tiempo, las personas han cambiado el hecho de pulsar el botón de llamada de sus teléfonos por el de tener que aceptar unas condiciones de uso que resultan obligatorias para poder comenzar a usar WhatsApp. De esta forma, el tráfico de información y centro neurálgico de los procesos de comunicación de las personas se ha desplazado a esta aplicación móvil, entrando todos sus usuarios a formar parte de una comunidad digital en la que se genera contenido y se comparte información de todo tipo (tanto mensajes de texto como notas de voz y audios). Sin embargo, para transmitir todos estos contenidos la aplicación requiere que el usuario en cuestión no active los mecanismos que dejarían sin efecto estas formas de consentimiento en cuanto a la información que se comparte. En conclusión, esto lleva definitivamente a un cambio en las reglas del juego, cambio que provoca que la persona pase a un segundo plano, siendo de alguna forma la propia aplicación de WhatsApp la que "tome el control" del dispositivo.

Respecto de WhatsApp, el proveedor del servicio únicamente facilita el proceso de comunicación. Cuenta con el apoyo de una serie de medidas y protocolos que garantizan la seguridad de las mismas en base al cifrado de la información que se transmite. Podríamos entender que permite un cierto margen de actuación en cuanto a la manera en la que se puede acceder a la información conservada, dado que conservan lo mandado a través de mensajería instantánea hasta que el usuario al que le hubiese sido enviado dicho contenido se conectase y accediese a la aplicación.

Sin embargo, el continuo proceso de actualización en el que se encuentran inmersas las aplicaciones web impide que WhatsApp se quede rezagada ante lo que, si se dejan a un lado la gran cantidad de problemas que se derivan de este mismo proceso de actualización tecnológica, podría entenderse como una continua búsqueda por mejorar la calidad de vida de la sociedad. En este sentido, tanto las aplicaciones de última generación como las clásicas, gracias a una actualización de estas últimas, se muestran como inmunes a la

intromisión de figuras ajenas a aquellas a quienes se enviaron los mensajes. Además, el tratamiento que se hace de dicha información garantiza su privacidad, no sólo ante las personas ajenas a las que nos referimos, sino también ante los encargados de la prestación del servicio de mensajería de WhatsApp.

Para el caso de WhatsApp, puede comprobarse cómo se da una situación algo diferente frente a las que se plantearán en los siguientes apartados. Esto se debe a que la clave que se necesita para poder acceder a toda la información contenida en dicha aplicación no tiene que ver con una clave en la aplicación (si bien es cierto que existen otras aplicaciones diferentes destinadas precisamente a establecer contraseñas para las propias aplicaciones), sino que la clave que alguien ajeno necesita para acceder al WhatsApp es la clave del dispositivo móvil en el que se encuentre descargado. Así, a diferencia de lo que se verá a propósito de las redes sociales o del correo electrónico, el WhatsApp se encuentra ligado y depende del móvil en el que se hubiese hecho la descarga. A su vez "la clave del usuario suele interrelacionarse con una clave de dispositivo; y ambas con claves criptográficas que son creadas por un generador de números aleatorio, que se activa cada vez que se inicia el dispositivo" [37].

En base a todo lo expuesto, una orden que pretendiese interceptar los contenidos de una conversación concreta puede no ser suficiente para poder examinarlos directamente, ya que los datos que se obtendrían figurarían en un lenguaje incomprensible para las personas. Lo que sí que podría garantizar es el acceso a los datos del tráfico para, a su vez, poder reenviar la señal que fuese susceptible de interceptación al centro que estuviese encargado de su recepción.

Esta situación hace que resulte difícil someter las comunicaciones entabladas a través de aplicaciones como WhatsApp a medidas de injerencia discreta. Incluso, seguiría siendo una cuestión difícil aunque el prestador del servicio de mensajería se mostrase dispuesto a colaborar.

Por tanto, la única manera de sobreponerse a estas elaboradas estrategias de protección es por medio de la utilización de herramientas propias creadas para desencriptar los

[37] Rodríguez Lainz, J. L., "Retos jurídicos de la interceptación de comunicaciones a través de prestadores de servicios de Internet", Publicación del CENDOJ, 2017, p. 25.

mensajes. También deben diseñarse otras herramientas con las que se puedan forzar las claves de acceso que dan protección en los propios dispositivos de los que parte o a los que llega la información. Además, el uso de estas herramientas no sólo se pretende de la información ya almacenada (enviada o recibida), sino también de toda aquella que se capte en tránsito. Sin embargo, igual mención como solución para tratar de regular esta realidad merece la consecución de protocolos en los que se acuerde la colaboración con las operados en aras de proporcionar la mayor cantidad de datos e información posible, pero garantizando una actuación conforme a la legislación y evitando cualquier vulneración de derechos de las partes.

5.2. Intervención de las redes sociales

A la hora de hablar de las redes sociales, hemos de hacer referencia a aquellas que cuentan con una mayor notoriedad o popularidad entre los usuarios del mundo tecnológico y digitalizado en el que vivimos en la actualidad. Así, cabe destacar Instagram, Facebook, Twitter o Google+ de entre todas ellas. Estas nuevas vías para establecer cualquier tipo de comunicación entre los usuarios de Internet de manera casi inmediata se caracterizan fundamentalmente por constituir las mayores fuentes de datos que dominan nuestra realidad tecnológica. Toda esta información procede de los propios usuarios de las mismas, quienes, a través de sus publicaciones, generan y aportan contenido en el tráfico de información. En cuanto a la posibilidad de acceder a la misma, pueden hacerlo tanto los usuarios que componen la comunidad digital relativa a cada una de estas redes como grupos concretos, en base a una serie de filtros que permiten la posibilidad de aceptar o rechazar el acceso a dicha información por parte de terceros ajenos.

La cuestión merecedora de especial protección por parte de los diferentes sistemas jurídicos tiene que ver con toda esa información que los usuarios de las redes publican en sus perfiles. Al contrario de lo que pueda llegar a pensarse, ésta puede recuperarse, dado que no se destruye necesariamente, incluso tiempo después de que los propios usuarios la hayan eliminado de sus perfiles o se hayan borrado la cuenta por completo. Este situación responde a que las operadoras de las redes sociales guardan copias de seguridad de toda la información que van almacenando en su base de datos desde el momento en el que el usuario crea su perfil de contacto.

El motivo de dicha conservación se deriva de la obligación legal a la que las operadoras se ven sometidas con arreglo a la normativa vigente. Así, las operadoras sostienen que esta es una medida necesaria para el mantenimiento del servicio en caso de que el sistema se caiga o pase a funcionar de manera anormal. De esta forma, lo que se consigue es evitar que se pierda toda la información. Por otro lado, el hecho de conservar la información constituye una manera garantizar a los usuarios que puntualmente se den de baja la posibilidad de volver sin tener que empezar desde el principio y pudiendo recuperar lo que en su día publicaron. Resulta igualmente posible recuperar la información que se hubiese intercambiado, y no sólo la propia[38].

El proceso de comunicación tiene lugar, por tanto, a partir de una identidad electrónica basada en un nombre de usuario y la clave que da acceso al perfil en cuestión. Así, cada acceso o intercambio de información a través de estas redes tendrá sus propias huellas, generando un tráfico de datos en el medio digital, susceptibles todos ellos de una posible injerencia en los mismos. Sin embargo, todo este tráfico no se refiere únicamente a la publicación del contenido, sino que además cuentan las redes sociales con aplicaciones de mensajería instantánea (respecto a chats privados) que se canalizan a través de las mismas o de manera independiente a través de otra aplicación diferente a la que gestiona el perfil del usuario.

Dado que, como decimos, toda esta información es conservada por el propio prestador del servicio, no reviste una gran complejidad la posibilidad de llevar a cabo una injerencia en las comunicaciones y la información personal de los usuarios de las redes. Por tanto, la protección que nuestro ordenamiento destina a todo este tipo de información trata de garantizar un grado de certeza suficiente sobre la imposibilidad de alterar la información transmitida e intervenida en base a la orden de interceptación de las comunicaciones y sobre la negación de manipulación o eliminación de información[39].

Respecto de todos los datos que se encuentran automatizados por parte de los prestadores de servicios, el artículo 588 ter j) LECrim reconoce que sólo serán susceptibles de

[38] "Retos jurídicos de la interceptación de comunicaciones a través de prestadores de servicios de Internet" "cit." p. 23.
[39] "Retos jurídicos de la interceptación de comunicaciones a través de prestadores de servicios de Internet" "cit." p. 24.

incorporación al proceso penal si se cuenta con una autorización por parte del juez que lo permita. Más concretamente, el segundo párrafo de dicho artículo recoge la solicitud que puede hacerse al juez competente del asunto de una autorización para poder recabar información al respecto cuando sea indispensable conocer todos esos datos para continuar con la investigación[40].

5.3. Intervención de correspondencia

En cuanto a la intervención de la correspondencia, este apartado se centrará en la correspondencia digital derivada del tráfico de mensajería a través de Internet, esto es, el correo electrónico.

Algunas de las direcciones de correo electrónico más populares y conocidas por los usuarios de Internet son Outlook, Gmail y Hotmail. A través de estos servicios, es posible conectarse a las bases de datos en las que se almacenan los correos que se vayan a recibir y en las que puede obtenerse información en tiempo real sobre todos aquellos que les lleguen nuevos, pudiendo revisarlos y volver a ellos en cualquier momento.

Como en todas las plataformas que permiten interaccionar a las personas a través de Internet, para poder operar en el correo electrónico (ya sea con el objetivo de acceder a los nuevos correos como para examinar o eliminar los ya recibidos) es necesario que se acceda a dicha dirección en la que se almacena toda la información del propietario de la cuenta. La cuestión que hace que se entienda que el correo electrónico impide, en cierta forma, a cada uno tener un control absoluto sobre lo que manda o recibe es el hecho de que no se conserva en la memoria del dispositivo electrónico o medio desde el cual se reciben o se envían, sino que todos ellos se almacenan en la base de datos externa del prestador del servicio. Así, el dispositivo por medio del cual se accede a la cuenta y que permite enviar y recibir los correos constituye una vía para poder acceder y no una fuente de conservación de mensajes[41].

[40] "Medidas de investigación tecnológica en el proceso penal: la nueva redacción de la Ley de Enjuiciamiento Criminal operada por la Ley Orgánica 13/2015." "cit." p. 193.
[41] "Retos jurídicos de la interceptación de comunicaciones a través de prestadores de servicios de Internet" "cit." p. 25.

En esta línea, para poder recuperar un mensaje que se hubiese eliminado de manera definitiva será necesario atender a lo dispuesto en la política de conservación de datos en base a la que cada operadora de correo funcione.

5.4. Incorporación de los datos obtenidos con la interceptación

De la misma forma que resulta de gran importancia el hecho de que la fuente de la que proceda la información interceptada no sea manipulada o destruida, es importante también que se garantice su llegada al juzgado de forma íntegra y sea fiel a lo que, efectivamente, se pudo obtener del dispositivo mediante el que se comunicaron las partes. Así, deben cumplirse lo dispuesto en el artículo 588 ter f) LECrim en cuanto a las exigencias del acto, en función de la medida de interceptación que se hubiese puesto en marcha.

Para poder incorporar dichos datos, es necesario que se garantice la autenticidad de los mismos a través del sellado y que el traslado de esta información hasta los centros de recepción pertinentes (pudiendo ser tanto policiales como judiciales) se lleve a cabo a través de canales seguros. Igualmente, debe poder garantizarse que la información mantiene el formato con el que contaba en origen ya que así podrá ser empleada para llevar a cabo comparaciones en aquellos casos en los que alguna parte pueda dudar sobre la autenticidad e integridad de los datos con los que cuentan los jueces. La necesidad de que se encuentre en su formato original responde a que, de esta forma, podrán ser sometidas a pruebas posteriormente realizadas por los peritos[42].

La importancia de la seguridad que ha de revestir toda esta situación puede llevar a que se exija que se acredite dicha seguridad en relación con la gestión que se haya hecho de las comunicaciones y con el deber de conservación que hubiese sometido a algún prestador.

[42] "Retos jurídicos de la interceptación de comunicaciones a través de prestadores de servicios de Internet" "cit." p. 27.

6. CAPÍTULO 4: PROTECCIÓN DE LOS DATOS Y EVOLUCIÓN EN EL ACCESO A LOS MISMOS

6.1. Cuestiones introductorias relativas a la protección de los datos

En cuanto al derecho que toda persona tiene a que sus datos gocen de la protección jurídica adecuada, el TC se pronunció en su Sentencia 39/2016[43]. La situación necesitada de la intervención de dicho tribunal se refería a un supuesto en el que se había colocado una cámara de vídeo destinada a vigilar las actuaciones llevadas a cabo por la trabajadora de una tienda en la caja de la misma, de quien se sospechaba una apropiación indebida del dinero contenido en la caja. Así, el TC se apoyó en una sentencia anterior en el tiempo y dictada por la misma Sala; la Sentencia 292/2000. En uno de los fundamentos jurídicos de esta última sentencia declaró lo siguiente:

> […] El contenido del derecho fundamental a la protección de datos consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso. Estos poderes de disposición y control […] se concretan jurídicamente en la facultad de consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles, por un tercero, sea el Estado o un particular. Y ese derecho a consentir el conocimiento y el tratamiento, informático o no, de los datos personales, requiere como complementos indispensables, por un lado, la facultad de saber en todo momento quién dispone de esos datos personales y a qué uso los está sometiendo, y, por otro lado, el poder oponerse a esa posesión y usos […].[44]

En este sentido, y tal y como destaca el TC en su Sentencia 39/2016, todo el sistema de protección de datos de carácter personal queda definido en torno al consentimiento que ha de otorgar el afectado a que se recopilen y utilicen sus datos y a tener conocimiento de ello; esto es, el derecho del propietario de esos datos a ser informado debidamente[45].

Así, la LO 15/1999[46] limita la posibilidad de tratar con datos de carácter personal a aquellos supuestos en los que se cuente con el consentimiento de los titulares de esos

[43] Sentencia del Tribunal Constitucional de 3 de marzo 39/2016.
[44] Sentencia del Tribunal Constitucional de 30 de noviembre 292/2000 FJ 7.
[45] Granados Pérez, C., "La utilización de mecanismos de geolocalización, la captación de imagen y sonido en la lucha contra la delincuencia", *Cuadernos Digitales de Formación*, n. 43, 2016, p. 31.
[46] Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (BOE 14 de diciembre de 1999).

datos. Sin embargo, en la misma línea, reconoce la posibilidad de que esos mismos datos no requieran del consentimiento en aquellos supuestos en los que se cuente con habilitación legal. Dicha situación queda recogida en el artículo 6.1 LO 15/1999, cuyo contenido especifica la necesidad de contar con el consentimiento inequívoco de la persona afectada salvo que la ley hubiese dispuesto otra manera de proceder respecto a la situación concreta de que se trate. Por el contrario, el siguiente apartado del mismo artículo especifica aquellos casos en los cuales no resulta necesario el consentimiento del propietario de los datos. Así, la LO 15/1999 recoge lo siguiente:

> No será preciso el consentimiento cuando los datos de carácter personal se recojan para el ejercicio de las funciones propias de las Administraciones públicas en el ámbito de sus competencias; cuando se refieran a las partes de un contrato o precontrato de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento; cuando el tratamiento de los datos tenga por finalidad proteger un interés vital del interesado en los términos del artículo 7, apartado 6, de la presente Ley, o cuando los datos figuren en fuentes accesibles al público y su tratamiento sea necesario para la satisfacción del interés legítimo perseguido por el responsable del fichero o por el del tercero a quien se comuniquen los datos, siempre que no se vulneren los derechos y libertades fundamentales del interesado[47].

En línea con lo que se ha venido tratando en apartados anteriores respecto a la calificación de los datos propiamente dicha, resulta necesario destacar el principio de calidad de los datos que recoge el artículo 4 LO 15/1999. El primer apartado de dicho artículo especifica, de entre las condiciones que los datos deben cumplir, que los datos han de ser adecuados, pertinentes y no excesivos y que el motivo de su tratamiento y obtención persiga una serie de finalidades determinadas, explícitas y de carácter legítimo.

En caso de no solicitar el consentimiento del propietario de los datos o de no informársele previamente estaríamos ante una vulneración del derecho fundamental a la protección de los datos. Esta vulneración habrá de ser ponderada en base a la proporcionalidad de la medida que se ponga en marcha para la obtención de los datos y que suponga una restricción de los derechos fundamentales. Por ello, se entiende que este derecho no goza de una protección ilimitada y encuentra sus límites en los demás derechos fundamentales y bienes que gocen de protección a nivel constitucional[48].

[47] Artículo 6.2 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (BOE 14 de diciembre de 1999).
[48] "La utilización de mecanismos de geolocalización, la captación de imagen y sonido en la lucha contra la delincuencia" "cit." p. 33.

Con respecto al supuesto concreto sobre el que el TC tuvo que manifestarse, en base a lo ya expuesto, el Tribunal consideró que la colocación de las cámaras de videovigilancia en el puesto de trabajo estaba justificada ya que cumplía con los requisitos que hacían que fuese proporcional. Por un lado, existían sospechas razonables sobre la apropiación indebida por parte de la trabajadora; por otro, se trataba de una solución idónea para poder descubrir la autoría de la apropiación y para poder aplicar las medidas disciplinarias correspondientes; era necesaria gracias a su validez probatoria; y, dado que el área de grabación se limitó al puesto de trabajo concreto, se trataba igualmente de una medida equilibrada. En base a este análisis, el Tribunal determinó que "[…] debe descartarse que se haya producido lesión alguna del derecho a la intimidad personal consagrado en el art. 18.1 CE"[49].

6.2. Cambios derivados de la modificación de la Ley de Protección de Datos

En el presente apartado, se hará una breve aproximación a los cambios producidos en la legislación española a consecuencia de la nueva LO 3/2018[50].

Con esta nueva LO se pretende transponer al ordenamiento jurídico español el RGPD[51], cuya entrada en vigor tuvo lugar el 25 de mayo de 2018. Por otro lado, se busca complementar dicha norma y velar por la protección de los que han pasado a ser denominados como derechos digitales. El retraso en la transposición del Reglamento llevó a la inmediata entrada en vigor de la nueva LO, el día siguiente a su publicación en el BOE tal y como se dispuso en el contenido de la misma[52].

La primera de las novedades se refiere a las bases para la legitimación de las Administraciones Públicas para poder proceder al uso y cesión de los datos personales que en cada caso correspondan. Así, el artículo 6 del RGPD concreta que se dará en aquellos supuestos en los cuales la ley expresamente obligue al tratamiento de los datos

[49] Sentencia del Tribunal Constitucional de 3 de marzo 39/2016 "cit." FJ 5.
[50] Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (BOE 6 de diciembre de 2018).
[51] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos) (DOUEL núm. 119 de 4 de mayo de 2016).
[52] Minero Alejandre, G., "Nuevas tendencias en materia de protección de datos personales. La nueva Ley Orgánica y la jurisprudencia más reciente" *Anuario Jurídico y Económico Escurialense*, L. II, 2019, pp. 127-139.

y cuando hacerlo sea necesario para proteger el interés público o se lleve a cabo en el ejercicio de poderes públicos. Por otro lado, la nueva LO incorpora un nuevo artículo 8 en el que especifica que dicho tratamiento en base a una obligación legal ha de responder a una previsión del mismo en una norma de Derecho de la Unión Europea o norma que posea rango de ley.

A su vez, la nueva LO añade otros supuestos en los que se debe nombrar a un Delegado de Protección de Datos. Respecto de este último, especifica la necesidad de que cuente con un título universitario con el que demuestre que cuenta con conocimientos especializados tanto en el área de Derecho como en todas las cuestiones relativas a la protección de datos. Por último, establece que los afectados por cuestiones de esta índole podrán dirigirse al Delegado de la entidad contra la que pretendan interponer cualquier tipo de reclamación antes de presentarla ante el órgano competente para resolverla.

A consecuencia del casi inabarcable tráfico de información que se mueve a través de los nuevos medios digitales, tal y como se ha expuesto en apartados anteriores, no resulta extraño que esta nueva LO haya incluido en su artículo 94 todas las cuestiones relativas al Derecho al olvido en materia de redes sociales y otros servicios relacionados con el mundo digital y el medio de Internet. Este derecho permite que las personas afectadas puedan solicitar que se supriman todos aquellos datos de carácter personal que hubiesen sido facilitados por ellas mismas o por terceros. Para ello, estos datos deben ser "inadecuados, inexactos, no pertinentes, no actualizados o excesivos o hubieren devenido como tales por el transcurso del tiempo, teniendo en cuenta los fines para los que se recogieron o trataron, el tiempo transcurrido y la naturaleza e interés público de la información"[53].

Respecto de las personas que hubiesen fallecido, la LO 3/2018 recoge en su artículo 3 que serán aquellas que presenten una vinculación de tipo familiar o de hecho con el difunto o sus herederos los que deban solicitar el acceso a los datos del fallecido, así como la rectificación o supresión de los mismos que en su caso sea necesaria. Sin embargo, la ley recoge la posibilidad de que o bien sea el difunto quien hubiese prohibido dichas acciones, o bien estas estuviesen prohibidas por disposición legal. Respecto de los datos

[53] Artículo 94.2 Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (BOE 6 de diciembre de 2018).

de consideración patrimonial del fallecido la excepción no impedirá que los herederos puedan acceder a los mismos.

En cuanto a la regulación de las relaciones laborales, la nueva LO trae consigo la modificación del Estatuto de los Trabajadores[54] y de la Ley del Estatuto Básico del Empleado Público[55]. Ambos reconocen el derecho a la intimidad del que gozan los trabajadores respecto al empleo que puedan hacer de los dispositivos digitales que se les faciliten. A su vez, reconocen su derecho a la intimidad en relación al conflicto que existe con el empleo en los puestos de trabajo de aparatos destinados a la vigilancia de sus actividades y su derecho a la desconexión respecto de dichos dispositivos.

Sin embargo, no sólo trae consigo la modificación de la normativa mencionada en el párrafo anterior, sino que con la LO 3/2018 se modifican a su vez las siguientes normas:

- En materia sanitaria: Ley General de Sanidad[56]; Ley básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica[57].
- En materia de educación: Ley Orgánica de Educación[58]; Ley Orgánica de las Universidades[59].
- En materia electoral: Ley Orgánica del Régimen Electoral General[60]. A propósito de dicha Ley, la novedad que ha suscitado mayor controversia ha sido la relativa al artículo 25 bis, el cual recoge la utilización de los medios tecnológicos y de los datos personales en las actividad que se llevan a cabo en el ámbito electoral. El motivo reside en que esta modificación habilita la recopilación de datos sobre opiniones y posturas políticas por parte de los diferentes partidos políticos.
- En materia de Derecho Procesal Civil: Ley de Enjuiciamiento Civil[61].

[54] Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores (BOE 24 de octubre de 2015).
[55] Real Decreto Legislativo 5/2015, de 30 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto Básico del Empleado Público (BOE 31 de octubre de 2015).
[56] Ley 14/1986, de 25 de abril, General de Sanidad (BOE 29 de abril de 1986).
[57] Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica (BOE 15 de noviembre de 2002).
[58] Ley Orgánica 2/2006, de 3 de mayo, de Educación (BOE 4 de mayo de 2006).
[59] Ley Orgánica 6/2001, de 21 de diciembre, de Universidades (BOE 24 de diciembre de 2001).
[60] Ley Orgánica 5/1985, de 19 de junio, del Régimen Electoral General (BOE 20 de junio de 1985).
[61] Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil (BOE 8 de enero de 2000).

- En materia de Derecho Administrativo: Ley del Procedimiento Administrativo Común[62]; Ley Reguladora de la Jurisdicción Contencioso-Administrativa[63].
- Otras materias: LOPJ; Ley de transparencia, acceso a la información pública y buen gobierno[64].

[62] Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (BOE 2 de octubre de 2015).
[63] Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-administrativa (BOE 14 de julio de 1998).
[64] Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno (BOE 10 de diciembre de 2013).

7. CAPÍTULO 5: INTERVENCIÓN DE LOS MENORES

7.1. Exposición de los menores en el plano tecnológico

En la actualidad, cada vez resulta más común el hecho de que en los colegios se les faciliten dispositivos electrónicos como Ipads o Tablets a los estudiantes con los que puedan interactuar de manera más eficaz, tecnológicamente hablando. El progreso informático y tecnológico pasa así a formar parte de la realidad de un gran número de centros educativos, promoviendo nuevas formas y técnicas de aprendizaje y desarrollo; esto es lo que ha pasado a denominarse como la "educación 2.0" o las pantallas educativas[65]. Sin embargo, este progreso conlleva una gran responsabilidad, no sólo para los menores, sino también para los padres, profesores y la propia dirección del centro educativo en cuestión. Es por este motivo por el cual todos ellos deben disponer de unas guías o pautas relativas al conjunto de derechos y obligaciones que pasan a asumir en esta nueva realidad que rodea a los dispositivos de aprendizaje electrónicos.

Tanto el conocimiento como la existencia efectiva de garantías a propósito de las situaciones que impliquen la utilización de dispositivos tecnológicos resulta imprescindible, dado que de ellas se derivan las consiguientes responsabilidades de diferentes grados. Así, continuando en el plano educativo, los centros deben dar a conocer a todos los involucrados en el mismo tanto las normas de convivencia como el régimen sancionador que sería de aplicación en los supuestos en los que se estuviese llevando a cabo un uso fraudulento de dichos dispositivos, pudiendo poner en riesgo a los menores de edad.

Sin embargo, como ya se ha mencionado, la importancia de las nuevas tecnologías hace que toda esta implicación en la protección del menor resulte insuficiente dado que la realidad lleva a que el control sobre la protección del menor resulte cada vez más complicado al desarrollarse en ámbitos en los que es más difícil de identificar o seguir. Toda esta situación constituye el germen de lo que hoy se conoce como ciberbullying[66].

[65] Santos Pascual, E., "Protección de menores y TIC", ICEF Consultores, 2018, p. 1.
[66] Do Nascimento, L., Lastras Alejandre, C., "Guía de Actuación: Menores y el bullying" , Universidad Carlos III de Madrid, 2018, p. 5.

Este subtipo de bullying encuentra su razón de ser en la creciente utilización que hoy en día se lleva a cabo de las TIC, las cuales se encuentran cada vez más al alcance de menores y adolescentes. De esta forma, junto con la apertura al progreso, se esta abriendo una nueva vía para que los agresores (bullies) puedan agredir o acosar a sus víctimas a través de, por ejemplo: páginas web que creen con el fin de dañar a su víctima de alguna forma; la usurpación de la clave del correo electrónico para que el menor no pueda acceder a su sesión y poder violar la intimidad de sus mensajes; la publicación de comentarios en foros que busquen dañar su imagen u ofenderlo; la participación en chats suplantando la identidad del menor para provocar reacciones que sean perjudiciales para el menor.

En este sentido, cabe subrayar que todas estas conductas a través de los medios digitales se deben tanto a la temprana edad a la que los menores pasan a ser usuarios y víctimas del mundo virtual, como a las carencias de información y formación con las que cuentan en el momento en el que pasan a formar parte. Así, sería necesario que contasen con conceptos y nociones adecuadas sobre lo que verdaderamente es la información y la utilidad que pueden llegar a tener todos los datos que pueden obtenerse del mundo de Internet.

En España, el número de casos en los que los menores han sido víctimas de este ciberbullying se han incrementado en los últimos años. Concretamente, un informe publicado por la Organización Mundial de la Salud en marzo de 2016 mostró a España como uno de los países en los que existía una mayor tasa de ciberacoso hacia los menores, en relación con otros estados de América del Norte y países de la Unión Europa. Por otro lado, un grupo de investigación de la Universidad del País Vasco, conocido como EU Kids Online, llegó a la conclusión de que el ciberacoso se produce con un 35% de probabilidad respecto de las chicas y con un 29% respecto de los chicos. De igual forma, en el estudio se concretó que es a partir de los 15 años cuando la probabilidad de ser víctima de estos comportamientos se reduce en un 6% de media[67].

7.2. Protección que reciben los menores

[67] "Guía de Actuación: Menores y el bullying" "cit." p. 7.

En cuanto a la manera en la que los menores pueden hacer valer los derechos y deberes que se derivan del uso que hacen de las tecnologías de la información, la LO 1/1996[68] recoge una serie de aclaraciones. La misma establece que los menores obtendrán información, asistencia, protección y defensa, solicitándola ante la entidad pública competente, y podrán comunicarse con el Ministerio Fiscal y plantear quejas ante la autoridad que en su caso resulte competente, o incluso interponer las denuncias necesarias ante el Comité de Derecho del Niño[69].

Además, en lo que respecta a los centros educativos, los profesores y directores detentan potestad de tipo correctora y disciplinaria, pudiendo por ello imponer sanciones disciplinarias a los menores. Sin embargo, la cuestión que suscita mayor interés es la nueva manera en la que han de afrontarse estas realidades en un panorama dominado por el uso de las tecnologías.

Aunque existan ciertos casos en los que la intromisión en la intimidad de los menores de edad pueda resultar conforme a la legalidad, de otros tantos pueden derivarse consecuencias jurídicas con motivo de las limitaciones y restricciones que existen para evitar intromisiones hechas de manera indiscriminada[70].

Una primera reacción ante los riesgos derivados de una exposición cada vez más controvertida a Internet puede llevarnos a justificar mentalmente un control sin límites respecto de la actividad de las personas en este medio. Concretamente, la obligación legal de los padres de proteger a sus hijos menores y procurar su seguridad e integridad ha llevado a que aplicaciones que permitan a los padres controlar la actividad de sus hijos en Internet o, directamente, el acceso a las cuentas de estos, sean consideradas adecuadas. Sin embargo, y contrariamente a lo que un padre considere adecuado reconocer, este tipo de conductas puede no sólo suponer una vulneración de derechos de los menores, sino estar recogida como un supuesto de actuación delictiva.

[68] Ley Orgánica 1/1996, de 15 de enero, de Protección Jurídica del Menor, de modificación parcial del Código Civil y de la Ley de Enjuiciamiento Civil (BOE 17 de enero de 1996).
[69] "Protección de menores y TIC" "cit." p. 2.
[70] Davara Fernández de Marcos, L., *Menores en Internet y Redes Sociales: Derecho Aplicable y Deberes de los Padres y Centros Educativos: Breve referencia al fenómeno Pokémon Go.* Agencia Española de Protección de Datos, Madrid, 2016, p.18.

A pesar de que, en un principio, no sea la consideración compartida con carácter general en un ámbito fuera de lo jurídico, la vigilancia de la actividad en las redes sociales que lleven a cabo los progenitores respecto de los hijos menores no es libre.

Sin embargo, tanto en el panorama jurídico nacional como en el internacional, las respuestas que dan los tribunales de las distintas instancias siguen siendo hoy bastante heterogéneas, dada la complejidad del asunto y las consideraciones que en cada caso resulta necesario entrar a valorar. En este sentido, mientras que un Juzgado de lo Penal de Pamplona[71] dictaba una sentencia favorable en relación a la absolución de la acusada de un delito de revelación de secretos, el Tribunal Cameral de Berlín[72] dictaba una sentencia desfavorable en cuanto a la vulneración del derecho a la intimidad.

En el primer caso, se acusaba a una mujer de revelar secretos como consecuencia de haber instalado en el móvil de su hija menor de edad una aplicación que le permitía grabar las conversaciones telefónicas que su propietaria mantuviese. Esta pretendía grabar las conversaciones que la niña tuviera, más concretamente, con su padre, para tratar de encontrar pruebas sobre la existencia de algún delito del que la menor fuera el centro, ya que sospechaba dicha situación. Aunque procedió sin el consentimiento de la menor, la decisión del Juzgado de absolverla se basó, por un lado, en que la edad de la menor (11 años) no daba a lugar a pensar que esta fuera suficientemente madura como para que su consentimiento constituyese un requisito esencial. Por otro lado, también se basó en que el comportamiento que el padre de la menor tenía con ella hizo necesaria la intervención de un psicólogo que tratara a la menor, dado que no se correspondía legalmente con el propio de un progenitor. Por tanto, la conducta de la madre estuvo guiada en todo momento por la obligación que tienen los padres de velar por la protección e intereses de sus hijos menores de edad.

Respecto del segundo caso mencionado, el Tribunal Cameral de Berlín mantenía la prohibición de acceso a la cuenta de Facebook de una menor fallecida por parte de sus progenitores. La fundamentación jurídica se basaba en la vulneración que, entendían, suponía para el derecho a la intimidad, no sólo de la menor, sino también de todos aquellos terceros que en algún momento se hubieran comunicado con ella. Aunque de

[71] Sentencia del Juzgado de lo Penal Nº. 1 de Pamplona de 29 de mayo 145/2017.
[72] Sentencia del *Kammergericht* (Tribunal Cameral) de Berlín de 31 de mayo de 2017 21 U 9/16.

esta situación pudiera deducirse un derecho de los padres sobre la cuenta de su hija fallecida, el Tribunal antepuso el derecho a la intimidad de los ya mencionados[73].

A pesar de distinguirse en términos de edad, la protección que de su derecho a la intimidad tienen reconocida los menores es igual a la que merecen los adultos. El *quid* de la cuestión, sin embargo, reside en el necesario equilibrio que debe existir en relación a la obligación de los padres de procurar la seguridad de sus hijos. Una valoración sobre el sacrificio de uno de estos dos derechos en favor del otro es la que llevará a determinar, en cada caso concreto, si estamos ante una intromisión legítima o ilegítima.

En vista del presente conflicto y de la dificultad para sentar las bases de un equilibrio entre ambas partes que sirva de criterio de aplicación universal, una de las mejores formas de buscar la protección de los menores es tratar de atajar el problema desde su educación. Así, la gran mayoría de los profesionales califican la educación como una de las mejores iniciativas para lograr la protección de los menores por medio de sistemas de supervisión o la materialización de dichas iniciativas en reglas y límites que guíen el destino de sus actuaciones. A modo de ejemplificación, el hecho de destinar una serie de espacios al uso de dichos dispositivos dentro de hogar familiar, así como de establecer horarios para un uso comedido y responsable de los mismos constituyen dos buenas prácticas. Además, el Grupo de Redes de la Policía Nacional y el Instituto Nacional de Ciberseguridad aconsejan que los menores faciliten a sus progenitores las claves de acceso a sus redes sociales para el caso en que resulte necesario su intervención.

En este sentido, resulta necesario analizar hasta qué punto debe anteponerse ese derecho a la intimidad de los menores y de qué manera tendría que cambiar, o no, el alcance del mismo en función de la edad del menor. En primer lugar, el artículo 4 de la LO 1/1996 recoge el derecho que tienen los menores a su intimidad, a la inviolabilidad de su correspondencia y al secreto de sus comunicaciones. Tal y como ya se ha expuesto, en el caso de los menores el tema que adquiere una especial relevancia tiene que ver con la lucha de poderes que existe entre la posibilidad de ejercer sus derechos de manera plena y el grado de madurez que se considere que tienen y que les permitiría llevar a cabo ese ejercicio pleno de derechos adecuadamente. Así, se establece comúnmente el criterio de

[73] Santos Morón, Mª. J., "La denominada "herencia digital": ¿Necesidad de regulación? Estudio de Derecho Español y Comparado", *Cuadernos de Derecho Transnacional*, vol. 10, n. 1, 2018, pp. 413-438.

que conforme crece el menor en edad y madurez, disminuirá la capacidad de controlarlos que tienen los progenitores respecto a este tipo de cuestiones. Es a partir de la edad de 14 años, en base a la normativa sobre protección de datos, cuando se entiende que puede presumirse que el menor cuenta con la madurez suficiente para llevar a cabo un ejercicio responsable y adecuado de sus derechos y cuando se requiere de su consentimiento para proceder a la injerencia en sus redes sociales. Dicho consentimiento otorgado por el menor será válido a excepción de los supuestos en los que sea necesario el consentimiento de aquellos que ejerzan la patria potestad sobre los menores. En cuanto a los menores de 14 años, por el contrario, se requiere el consentimiento explícito de los progenitores o tutores[74].

Aunque llegar a una única solución aplicable con carácter general resulta casi imposible, estas previsiones son fundamentales para evitar una intromisión sin límites y sin consentimiento previo en la vida del menor. No se consideraría una intromisión ilícita en la intimidad del menor de edad cuando los progenitores no tuviesen otra alternativa para protegerlos. La intromisión ha de ser, por tanto, esencial y necesaria.

Nuevamente se planteó la cuestión objeto de estudio ante la AP de Tarragona[75]. En este caso, al acusado le fueron imputados un delito de abusos sexuales a menores y cinco de exhibicionismo. La clave para poder arrojar luz sobre la autoría de estos delitos se basó en la prudente actuación de la madre de una de las menores que había sido víctima, al acceder y aportar las conversaciones que el agresor había entablado con la menor por medio de la red social Facebook.

El problema en este sentido se planteó en tanto en cuanto la madre no contó con el consentimiento expreso de su hija para poder hacerlo. Los motivos en los que el acusado trató de fundamentar la nulidad de las pruebas ante el TS fueron que la madre ni había respetado su derecho a la intimidad y al secreto de las comunicaciones, ni contó previamente con el consentimiento de ninguna de las partes implicadas. Así, el TS concretó[76] los factores en los que encontraría su legitimidad el hecho de acceder al perfil personal de Facebook de un menor sin que este lo haya consentido con carácter previo.

[74] "Guía de Actuación: Menores y el bullying" "cit." p. 5.
[75] Sentencia de la Audiencia Provincial de Tarragona de 8 de abril 135/2015.
[76] Sentencia del Tribunal Supremo de 10 de diciembre 864/2015.

Por un lado, el Tribunal sostuvo la legitimidad del acto de la madre porque ella misma ya contaba con las claves de acceso de su hija, por lo que no tuvo que investigar para obtenerlas. Por otro, existía una suficiente evidencia de la posición de su hija como víctima para poder comenzar a sospechar sobre el delito. Esta posición del Tribunal legitima claramente el acceso de los padres a las cuentas personales de los menores en las redes sociales cuando lo que busquen con dichas intervenciones sea salvaguardarlos.

7.3. Control parental

En la actualidad, uno de los principales temas de debate, a propósito de la revolución y avance que han experimentado las redes sociales, se centra en la fiscalización que los padres llevan a cabo de las conversaciones y mensajes que sus hijos menores de edad emiten vía WhatsApp.

Por otro lado, en cuanto a la regulación legal que encuentran las aplicaciones web que permiten un control por parte de los padres de los dispositivos y las cuentas resulta necesario llevar a cabo una distinción. En primer lugar, pueden encontrarse aquéllas que tienen como propósito limitar tanto la duración del acceso como el acceso a determinados contenidos, y las que buscan un control más exhaustivo de toda la actividad de los menores. Mientras que las que pertenecen a la consideración del primer grupo, que tienen en cuenta la edad de los menores, se basan en un control que responde a la labor educativa y de dirección de sus progenitores; las del segundo grupo, se basan en la potencial intromisión en la intimidad del menor y su derecho a la misma.

El artículo 4.1 de la LO 1/1996 recoge el derecho al honor, la intimidad personal y familiar y a la propia imagen que tienen todos los menores. Al hilo del presente trabajo de investigación, este mismo artículo recoge su derecho a la inviolabilidad del domicilio familiar, de la correspondencia y su derecho al secreto de las comunicaciones. El apartado quinto del mismo artículo establece la obligación de respeto y protección de los mencionados derechos a la que quedan sujetos padres, tutores y poderes públicos. Por tanto, puede concluirse que la minoría de edad no resulta contraria al derecho a la intimidad ni a su protección. Igualmente, respecto de los padres resulta necesario concluir ciertos aspectos que condicionan su capacidad de intervención en los dispositivos

electrónicos privados de sus hijos y, con ello, en sus conversaciones de mensajería, o en la manera en la gestionan las redes sociales.

En este sentido, la consideración que la cuestión merece cambia significativamente dependiendo del supuesto de que se trate. Por un lado, podemos referimos únicamente al control y vigilancia sin mayor profundidad de la actividad de los menores. Por otro, podemos hacer referencia también a la vigilancia y control que estos pretenden llevar a cabo en caso de que exista un cierto grado de sospecha del que pueda llegar a entenderse que el menor se encuentra en riesgo[77].

Uno de los autos más recientes que han surgido al respecto ha sido dictado por la AP de Pontevedra[78]. En él, el Tribunal entraba a valorar la legitimidad que un padre tenía para poder analizar las conversaciones que su hija de 9 años había mantenido a través de su teléfono móvil. La madre de la menor fue la que denunció estas actuaciones llevadas a cabo por el padre. Sin embargo, la revisión de las mencionadas conversaciones se llevó a cabo en presencia de la menor y con su consentimiento tácito. Además, el dispositivo móvil contaba con una contraseña que protegía el acceso al mismo.

Dada la mayor complejidad y peligrosidad que se deriva de estos nuevos usos de Internet, los padres tienen la obligación de proteger la intimidad de los menores a través de un uso responsable de este tipo de servicios. Sin embargo, no debemos olvidar que el manejo de Internet a través de las diversas aplicaciones y redes sociales que existen está sujeto a restricciones relativas a la edad mínima que deben tener los usuarios de las mismas. En este caso, la niña tenía únicamente 9 años, edad que se encuentra por debajo del mínimo requerido en las condiciones de uso de WhatsApp. El contenido que queda recogido en sus términos y condiciones de uso especifica lo siguiente:

> Debes tener por lo menos 13 años de edad para poder usar nuestros Servicios (o la edad mínima requerida en tu país para tener autorización para usar nuestros Servicios sin aprobación de tus padres). Además de tener la edad mínima requerida para usar nuestros Servicios en virtud de la ley aplicable, si no tienes la edad suficiente para poder aceptar nuestros Términos en tu país, tu padre, madre o tutor deben aceptar nuestros Términos en tu nombre.[79]

[77] *Menores en Internet y Redes Sociales: Derecho Aplicable y Deberes de los Padres y Centros Educativos: Breve referencia al fenómeno Pokémon Go.* "cit." p.71.
[78] Auto de la Audiencia Provincial de Pontevedra de 25 de octubre 893/2017.
[79] Normativa WhatsApp Inc. sobre Condiciones del Servicio y Política de Privacidad (Última modificación: 15 de mayo de 2018).

Por tanto, dado que se trata de una menor que no llega al mínimo legal requerido para el empleo de la aplicación de mensajería instantánea, necesitaría del consentimiento parental para poder hacerlo.

Sin embargo, en caso de que se sospechase sobre el potencial peligro del menor (por un delito de acoso o cualquier otro de mayor gravedad), no tendría cabida más consideración que la de anteponer el deber de tutela del menor a su derecho a la intimidad. Por tanto, estaría permitida la intervención de sus comunicaciones cuando ello permitiese a los progenitores esclarecer la situación en la que se encontrase el menor en cuestión.

En relación con la idea expuesta en el párrafo anterior, puede de nuevo traerse a colación la situación que se llegó a plantear ante el TS en relación a la existencia de un supuesto acoso en la red social Facebook, sobre la cual ya se han comentado algunas cuestiones en el apartado anterior. Sobre dicha sentencia, dictada por la Sala Segunda de este Tribunal en 2015[80], resulta necesario retomar la decisión del Tribunal, el cual determinó que los datos que esta madre obtuvo de la cuenta de Facebook de su hija, quien se la había dejado abierta, eran válidos como prueba constitutiva del delito de abuso sexual del que estaba siendo víctima la menor.

Al entrar algo más en profundidad, por el contenido tratado en este apartado de la investigación, pueden apreciarse los motivos sobre los que el Tribunal apoyo su decisión de admitir la licitud de la actuación de la madre, siendo estos:

- La sospecha de la potencial situación de peligro por un delito de ciberacoso en la que se encontraba la niña;
- El hecho de que fuese concretamente la madre (quien ejercía la patria potestad sobre la niña), y no otra persona, la que accedió a la cuenta de la menor;
- Y el hecho de que para dicho conocimiento no se sirvió de técnicas frente a las que la menor se mostrase contraria.

La conclusión a la que se llegó fue, por tanto, que en determinados casos resulta incompatible el deber de los padres de velar por sus hijos menores de edad con la privación total del control que pueden ejercer sobre los mismos. Puede verse, en cuanto

[80] Sentencia del Tribunal Supremo de 10 de diciembre 864/2015.

a esta incompatibilidad, cómo se trata de una confrontación clara entre el derecho de los menores a su intimidad, y la obligación que los padres tienen respecto de los mismos de velar por su defensa y protección. Resulta necesario alcanzar un equilibrio entre ambos derechos enfrentados que permita a los padres procurar la seguridad de los hijos sin entrometerse injustificadamente en la esfera de intimidad del menor, declarando así la legitimidad o ilegitimidad de cada caso en concreto. Sin embargo, tal y como puede derivarse de las sentencias mencionadas hasta este punto, se trata aún hoy de un tipo de casos respecto de los que no se puede establecer una respuesta directa ya que entra en juego la consideración sobre el grado de madurez del menor y aquel que determina la suficiencia de la misma para poder ejercer su derecho a la intimidad plenamente y sin necesidad de tutela parental.

7.4. Cuestiones relativas a la Directiva (UE) 2018/1808, del Parlamento Europeo y del Consejo, de 14 de noviembre de 2018. Especial referencia a los menores

Aunque la realidad que rodea a esta Directiva (UE) 2018/1808[81] constituye un terreno aún sin explorar en profundidad, en el presente apartado se pretenderá destacar los aspectos más relevantes acerca de la prestación de servicios de comunicación audiovisual. Respecto de esa necesidad de investigación sobre el tema, el 13 de junio de 2019 la Universidad Pontificia de Comillas albergará una jornada sobre "Derecho de acceso a la información de los niños, niñas y adolescentes". El contenido de la misma se centrará en la transposición al ordenamiento jurídico español de dicha Directiva y en la modificación que requiere la Ley 7/2010[82] como consecuencia del impacto que ha tenido en los últimos años el rápido desarrollo de Internet. Esta modificación de la Ley deberá llevarse a cabo con carácter especial respecto de los menores de edad.

En relación con la materia de los menores, es el artículo 7 de la Ley 7/2010 el que regula de forma amplia el contenido de la protección de los menores en relación con la comunicación audiovisual. De entre todos los apartados que componen dicho artículo,

[81] Directiva (UE) 2018/1808 del Parlamento Europeo y del Consejo, de 14 de noviembre de 2018, por la que se modifica la Directiva 2010/13/UE, de 10 de marzo de 2010, sobre la coordinación de determinadas disposiciones legales, reglamentarias y administrativas de los Estados miembros relativas a la prestación de servicios de comunicación audiovisual (Directiva de servicios de comunicación audiovisual), habida cuenta de la evolución de las realidades del mercado. (DO L 303 de 28 de noviembre de 2018).
[82] Ley 7/2010, de 31 de marzo, General de la Comunicación Audiovisual (BOE 1 de abril de 2010).

pueden destacarse algunos por la relevancia de su contenido. Por ejemplo, el apartado segundo hace referencia de manera particular a la prohibición de emisión de contenidos pornográficos o en los que puedan apreciarse situaciones de maltrato, violencia de género o violencia gratuita. En este mismo apartado, se hace también referencia a los programas sobre juegos de azar y apuestas o los relacionados con el esoterismo y las paraciencias, los cuales sólo podrán ser emitidos en franjas horarias concretas con el fin de proteger a los menores. Respecto del apartado tercero, se establece la necesidad de evitar que las comunicaciones de tipo comercial perjudiquen al menor a nivel moral o físico, estableciéndose respecto de las mismas una enumeración de limitaciones que se recogen en el mismo apartado.

Es importante destacar, por otro lado, que esta misma Ley ya en su momento tuvo por objeto la unificación de toda la normativa que había dispersa sobre materia de protección audiovisual y también implicó la transposición de la Directiva 2007/65/CE[83].

La aparición del fenómeno relativo a la tecnología digital, que provoca la aparición de nuevas vías para acceder a los medios audiovisuales y un efecto multiplicador de las audiencias, ha hecho que la industria audiovisual haya ido adquiriendo una importancia vital en los últimos tiempos. Es por ello por lo que, en esta misma línea, la actual Directiva (UE) 2018/1808 se superpone sobre la Directiva 2010/13/UE[84], la cual es anterior en el tiempo sobre la misma materia. Este hecho encuentra su razón de ser en su carácter necesario a la vista de la evolución que Internet había venido experimentando, y que sigue experimentando en la actualidad.

Así, el uso que se está haciendo de Internet y de los diferentes dispositivos electrónicos que aparecen en el panorama digital es diferente al que en un primer momento tanto el legislador como la Unión Europea llegaron a contemplar. A consecuencia de esta falta de previsión, que por otro lado resulta lógica dado que las novedades respecto al mundo

[83] Directiva 2007/65/CE del Parlamento Europeo y del Consejo, de 11 de diciembre de 2007, por la que se modifica la Directiva 89/552/CEE del Consejo sobre la coordinación de determinadas disposiciones legales, reglamentarias y administrativas de los Estados miembros relativas al ejercicio de actividades de radiodifusión televisiva (DO L 332 de 18 de diciembre de 2007).

[84] Directiva 2010/13/UE del Parlamento Europeo y del Consejo, de 10 de marzo de 2010, sobre coordinación de determinadas disposiciones legales, reglamentarias y administrativas de los estados miembros relativas a la prestación de servicios de comunicación audiovisual (Directiva de servicios de comunicación audiovisual) (DO L 95 de 15 de abril de 2010).

tecnológico son resultado de un progreso continuo y constante, puede dar lugar a una desprotección de los menores; "de los niños y de las niñas", tal y como se refiere la ya mencionada jornada.

La Directiva que nos ocupa, como ya se ha mencionado, llevó a que se modificase la Directiva 2010/13/UE ante los continuos cambios que se estaban produciendo en el mercado. Dicha modificación reconoce la importancia los códigos de conducta que han de establecerse entre todos los operadores del medio digital para lograr la autorregulación y corregulación de los supuestos normativos. Es por ello por lo que la creación de organismos dedicados a procurar estos fines resulta imprescindible, creándose un Grupo de Entidades Reguladoras Europeas para los Servicios de Comunicación Audiovisual con los representantes nacionales para supervisar dicha labor[85].

Además, queda establecido que los contenidos que sean susceptibles de emitirse no podrán vulnerar la dignidad de las personas, ni llamar al odio, la violencia o la comisión de actos terroristas. En esta línea, quedarán prohibidos los contenidos comerciales de publicidad que inciten al consumo de tabaco, al consumo de alcohol por parte de los menores, a llevar a cabo actuaciones que resulten contrarias a la salud y al medio ambiente, así como aquellas llamadas al consumo de alimentos perjudiciales para la salud por parte de los menores.

La Asociación de Usuarios de la Comunicación mantiene una doble postura respecto a la Directiva (UE) 2018/1808. Por un lado, reconoce que esta ha introducido novedades de gran relevancia, como son la intención de lograr la autorregulación y corregulación ya mencionadas y la inclusión de las plataformas en las que se lleva a cabo el intercambio de vídeos dentro de su ámbito de aplicación. Sin embargo, manifiesta de igual forma que la Directiva ha dotado de una gran ambigüedad a la protección que se lleva a cabo de los menores de edad en cuanto a asuntos de gran trascendencia como la prohibición de la violencia gratuita, la emisión de pornografía en abierto y el etiquetado de programas por sus contenidos en función de la edad[86].

[85] Balaguer Callejón, Mª. L., "Crónica de la legislación europea", *ReDCE*, n. 30, 2018.
[86] Perales, A., "La Asociación de Usuarios de la Comunicación valora positivamente la nueva Directiva Audiovisual, pero critica algunos aspectos relacionados con la protección de los menores y la saturación publicitaria", *Asociación de Usuarios de la Comunicación*, 5 de diciembre de 2018 (disponible en

Volviendo a la comprensible falta de previsión de los que en su momento regularon dichas materias, la desprotección que pueden sufrir los menores puede darse respecto de la comunicación audiovisual en los diferentes aspectos que la misma contiene. Es por este motivo por el que la UE ha decidido volver a intervenir en la regulación de los estados miembros con el fin de que adapten su legislación a unos criterios muchos más dirigidos a la protección de los menores en los aspectos a los que se refiere la Directiva (UE) 2018/1808 en sus considerandos 19, 20 y 21, entre otros.

A lo que obedece esta normativa es a que el mercado de acceso a Internet y de uso de dispositivos ha evolucionado, como ya se ha mencionado, y en consecuencia es necesario regularlo. Sin embargo, no sólo debe regularse, sino que también debe buscar proteger al consumidor (más concretamente a los menores) como consecuencia de esta evolución. En este sentido, en el primer considerando de la Directiva (UE) 2018/1808 se hace referencia a los vídeos cortos o contenido que generan los propios consumidores en relación a la forma en la que compartimos vídeos grabados por nosotros mismos a través de plataformas y aplicaciones como YouTube o Instagram y que se cuelgan en Internet.

Respecto al considerando 19 de la Directiva que nos ocupa, puede apreciarse que la Unión Europea exige que resulta necesario establecer facilidades a los espectadores, incluidos los padres y menores de edad, para que tengan conocimiento del contenido de lo que van a ver. Estas facilidades se centran en que los prestadores de los servicios de comunicación informen sobre los contenidos con el fin de que los espectadores puedan decidir por ellos mismos si lo ven o no.

En el considerando número 20 se establece que las medidas de protección de los menores que se habían venido contemplando para los servicios de radiodifusión televisiva (a través de la televisión y de la radio) deberían ser aplicables también a los servicios de comunicación audiovisual para aquellos casos en los que se solicitase dicha aplicación. Estos últimos pueden ser servicios a través de Internet dado que, en la actualidad, a través de los medios de comunicación audiovisual puede llegarse a tener acceso a todo tipo de información. Dicha solicitud ha de procurar la protección de los menores.

http://www.auc.es/Paginas/download.php?type=comunica&year=2018&file=dic01.pdf; última consulta 07/06/2019).

Por último, en materia de menores, resulta igualmente destacable el considerando 21. Sin embargo, el contenido del mismo se refiere más bien a los propios datos personales de los menores y no a la comunicación audiovisual que estos puedan recibir. En la gran mayoría de los casos, para poder tener acceso a los distintos servicios de Internet es necesario que el menor facilite sus datos relativos a la fecha de nacimiento o dirección de correo electrónico, entre otros. Por tanto, toda esa información sobre el menor debe gozar de la protección adecuada, no pudiendo utilizarse con fines comerciales respecto de los menores.

8. CONCLUSIONES

- La revolución tecnológica en el ámbito del Derecho no sólo ha llevado al surgimiento de nuevas formas de investigación de los delitos, que permiten una mayor concreción y profundidad, sino también a la aparición de delitos que, por su carácter tecnológico, no habían sido contemplados hasta el momento. De ahí la importancia de que se redactase la LO 13/2015, cuyo fin era el de modificar aspectos de la normativa en cuanto al ámbito de las nuevas medidas de investigación tecnológica. La LO ha dotado de una mayor importancia a todos los requisitos que la ley exige con respecto al principio de proporcionalidad.

- La sociedad y el Derecho no evolucionan al mismo ritmo. Así, el progreso tecnológico deja atrás, en la mayoría de las ocasiones, la normativa legal que regula los llamados "derechos digitales". Sin embargo, aunque parezca una falta de previsión por parte del legislador, puede entenderse como una situación lógica, dado que a través del Derecho se pretende buscar soluciones a los problemas de la sociedad y estos van surgiendo en base a distintos fenómenos y acontecimientos. De esta forma, serán los jueces los que tengan que resolver sobre las controversias que en cada caso se planteen atendiendo a las distintas circunstancias que concurran.

- La sociedad de la información en la que nos encontramos y el papel que en ella juegan los dispositivos electrónicos y los prestadores de servicios de estas nuevas formas de comunicación hace que se incremente el grado en el que nuestra propia privacidad se encuentra expuesta al conocimiento de otras personas ajenas. Así, puede observarse un cambio de tendencia, por ejemplo, mediante la comprobación de la factura del teléfono móvil. En ellas, las llamadas telefónicas han quedado relegadas a un papel secundario, pasando a ser casi inexistentes, respecto al consumo de los "megas" que permiten el acceso a Internet.

- El desarrollo de una gran variedad de dispositivos inteligentes ha relegado el factor humano a un segundo plano, quedando la huella de los distintos procesos de comunicación de las personas registrada en el medio digital. Además, en cuanto

a la intervención de dichos procesos, lo relevante es la existencia de nuevas formas en las que puede concretarse la comunicación, a través de fotos, videos y mensajes instantáneos, entre otros. Debe requerirse respecto de todos ellos la misma protección jurídica que se ha venido ofreciendo a los medios y formas de comunicación tradicionales, ya que su surgimiento responde tanto al desarrollo de la sociedad como a la intención de mejorar su calidad de vida. El problema reside en que la injerencia en las nuevas formas de comunicación requiere procesos complicados para desencriptar los datos que se generan en el plano digital y tecnológico para que sean comprensibles por las personas.

- Respecto a la intimidad, ha podido comprobarse cómo el hecho de concretar un concepto que la defina reviste de una gran dificultad, dada la evolución que ha experimentado en los últimos años la idea de intimidad y la protección que se estima que merece. Frente a una situación anterior en la que no se daban intromisiones en la misma, los avances tecnológicos en el plano de las comunicaciones han centrado el foco de atención en la necesidad de adquirir una capacidad de control suficiente que permita a las personas garantizar su dignidad personal. En este sentido, cualquier intromisión en la dimensión privada de sus vidas sin contar con el consentimiento previo para ello supone una violación de su derecho a la intimidad. De ello se deduce la importancia clave del derecho fundamental al secreto de las comunicaciones en tanto que sirve para garantizar el respeto y desarrollo de la personalidad.

- Es importante concretar el tipo de comunicación de que se trate, el medio empleado para ello y las circunstancias espaciotemporales en las que se vaya a llevar a cabo la intervención de las mismas. Con ello se pretende evitar un ejercicio desproporcionado e indiscriminado de las medidas de intervención, teniendo que ser necesarias y proporcionales al delito cometido. Igualmente importante resulta la correcta calificación del delito (en cuanto a su mayor o menor gravedad), dado que el proceso penal que se seguirá para la investigación del mismo y la licitud de la medida empleada dependerá de dicha calificación.

- Lo relevante es que la consideración de sujeto pasivo encuentra su fundamento en los indicios derivados de la investigación y no en la titularidad o habitualidad de

uso de los dispositivos susceptibles de intervención. Con ello puede entenderse que se estaría permitiendo un espectro mucho más abierto de investigación, dado que se podría intervenir un teléfono, por ejemplo, aunque no estuviese a nombre del sospechoso. Sin embargo, tiene que quedar claro que es necesario que sea el dispositivo a través del cual se mantuvo la conversación objeto de investigación. En esta línea, las operadoras de este tipo de servicios quedan obligadas a colaborar en la investigación, siendo para ello de vital importancia la fijación de pautas de actuación y colaboración para esclarecer los delitos tecnológicos.

- Por medio de la aceptación de unas condiciones de uso, pasamos a formar parte de una comunidad digital cada vez más amplia y que pasaría a "tomar el control" de nuestro dispositivo al permitir el acceso a determinados contenidos del mismo. Sin embargo, somos nosotros mismos los que generamos el contenido que se comparte. Por otro lado, aunque pueda ser útil el hecho de que los nuevos medios de comunicación permitan que la información se pueda recuperar, el peligro aquí precisamente está en que la información no llega a destruirse y, por tanto, debe evitarse su manipulación.

- Respecto a los menores, estos se encuentran cada vez más expuestos a los peligros derivados del uso de estas nuevas vías de comunicación, como es el empleo de sus datos personales para fines que le sean perjudiciales. Debe concretarse que la responsabilidad que se requiere se predica no sólo de éstos, sino de todos los que participen en la realidad digital. De ahí la importancia de desarrollar guías y pautas de actuación y de establecer la normativa respecto de los derechos y obligaciones que se derivan del uso para proteger a los menores. Pero cada vez resulta más complicado, ya que el menor comienza a usar estos dispositivos y formas de comunicación a una edad muy temprana y sin contar con la información y formación que necesitaría para llevar a cabo un uso responsable. Por ello, la educación de los menores en este sentido constituye una solución adecuada para tratar de reducir la tasa de delitos de ciberacoso que sufren por este desconocimiento y falta de concienciación.

- Por último, ha de destacarse la importancia de la transposición de la Directiva (UE) 2018/1808 al ordenamiento jurídico español y la modificación que requiere

la Ley 7/2010 como consecuencia del impacto provocado por el rápido desarrollo de Internet y los cambios producidos en el mercado. Es necesario no sólo regular los cambios, sino también la protección que debe darse a los consumidores. La UE decide volver a intervenir para que los estados miembros adapten su legislación a criterios mucho más dirigidos a la protección de los menores respecto de la prestación de servicios de comunicación audiovisual.

9. BIBLIOGRAFÍA Y DOCUMENTACIÓN CONSULTADA PARA LA ELABORACIÓN DEL TRABAJO

LEGISLACIÓN

- Declaración de los Derechos del Hombre y del Ciudadano (26 de agosto de 1789).

- Constitución Española, de 27 de diciembre de 1978 (BOE 29 de diciembre de 1978)

- Ley Orgánica 5/1985, de 19 de junio, del Régimen Electoral General (BOE 20 de junio de 1985).

- Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial (BOE 2 de julio de 1985).

- Ley 14/1986, de 25 de abril, General de Sanidad (BOE 29 de abril de 1986).

- Ley Orgánica 1/1996, de 15 de enero, de Protección Jurídica del Menor, de modificación parcial del Código Civil y de la Ley de Enjuiciamiento Civil (BOE 17 de enero de 1996).

- Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-administrativa (BOE 14 de julio de 1998).

- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (BOE 14 de diciembre de 1999).

- Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil (BOE 8 de enero de 2000).

- Ley Orgánica 6/2001, de 21 de diciembre, de Universidades (BOE 24 de diciembre de 2001).

- Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica (BOE 15 de noviembre de 2002).

- Real Decreto 424/2005, de 15 de abril, por el que se aprueba el Reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios (BOE 29 de abril de 2005).

- Ley Orgánica 2/2006, de 3 de mayo, de Educación (BOE 4 de mayo de 2006).

- Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones (BOE 19 de octubre de 2007).

- Directiva 2007/65/CE del Parlamento Europeo y del Consejo, de 11 de diciembre de 2007, por la que se modifica la Directiva 89/552/CEE del Consejo sobre la coordinación de determinadas disposiciones legales, reglamentarias y administrativas de los Estados miembros relativas al ejercicio de actividades de radiodifusión televisiva (DO L 332 de 18 de diciembre de 2007).

- Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (BOE 31 de julio de 2002), en su versión modificada por la Directiva 2009/136/CE del Parlamento Europeo y del Consejo, de 25 de noviembre de 2009 (BOE 18 de diciembre de 2009).

- Ley 7/2010, de 31 de marzo, General de la Comunicación Audiovisual (BOE 1 de abril de 2010).

- Directiva 2010/13/UE del Parlamento Europeo y del Consejo, de 10 de marzo de 2010, sobre coordinación de determinadas disposiciones legales, reglamentarias y administrativas de los estados miembros relativas a la prestación de servicios de

comunicación audiovisual (Directiva de servicios de comunicación audiovisual) (DO L 95 de 15 de abril de 2010).

- Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno (BOE 10 de diciembre de 2013).

- Ley 9/2014, de 9 de mayo, General de Telecomunicaciones (BOE 10 de mayo de 2014).

- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (BOE 2 de octubre de 2015).

- 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 (BOE de 6 de octubre de 2015).

- Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores (BOE 24 de octubre de 2015).

- Real Decreto Legislativo 5/2015, de 30 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto Básico del Empleado Público (BOE 31 de octubre de 2015).

- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos) (DOUEL núm. 119 de 4 de mayo de 2016).

- Directiva (UE) 2018/1808 del Parlamento Europeo y del Consejo, de 14 de noviembre de 2018, por la que se modifica la Directiva 2010/13/UE, de 10 de marzo de 2010, sobre la coordinación de determinadas disposiciones legales, reglamentarias y administrativas de los Estados miembros relativas a la prestación

de servicios de comunicación audiovisual (Directiva de servicios de comunicación audiovisual), habida cuenta de la evolución de las realidades del mercado (DO L 303 de 28 de noviembre de 2018).

- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (BOE 6 de diciembre de 2018).

JURISPRUDENCIA

Tribunales Internacionales

- Sentencia del *Kammergericht* (Tribunal Cameral) de Berlín de 31 de mayo de 2017 21 U 9/16.

Tribunal De Justicia De La Unión Europea

- Sentencia del Tribunal de Justicia de la Unión Europea de 2 de octubre de 2018 C-207/16.

Tribunal Constitucional

- Sentencia del Tribunal Constitucional de 29 de noviembre 114/1984.

- Sentencia del Tribunal Constitucional de 26 de abril 69/1999.

- Sentencia del Tribunal Constitucional de 31 de mayo 94/1999.

- Sentencia del Tribunal Constitucional de 27 de noviembre 283/2000.

- Sentencia del Tribunal Constitucional de 3 de julio 220/2006.

- Sentencia del Tribunal Constitucional de 9 de octubre 281/2006.

- Sentencia del Tribunal Constitucional de 14 de marzo 25/2011.

- Sentencia del Tribunal Constitucional de 22 de septiembre 145/2014.

- Sentencia del Tribunal Constitucional de 3 de marzo 39/2016.

Tribunal Supremo

- Sentencia del Tribunal Supremo de 10 de diciembre 864/2015.

- Sentencia del Tribunal Supremo de 12 de enero 993/2016 FJ 6.

Audiencias Provinciales

- Sentencia de la Audiencia Provincial de Tarragona de 8 de abril 135/2015.

- Auto de la Audiencia Provincial de Pontevedra de 25 de octubre 893/2017.

- Auto de la Audiencia Provincial de Tarragona de 23 de noviembre 647/2018.

Juzgados De Lo Penal

- Sentencia del Juzgado de lo Penal Nº. 1 de Pamplona de 29 de mayo 145/2017.

OBRAS DOCTRINALES

Balaguer Callejón, Mª. L., "Crónica de la legislación europea", *ReDCE*, n. 30, 2018.

Davara Fernández de Marcos, L., *Menores en Internet y Redes Sociales: Derecho Aplicable y Deberes de los Padres y Centros Educativos: Breve referencia al fenómeno Pokémon Go.* Agencia Española de Protección de Datos, Madrid, 2016, pp.18-71.

Do Nascimento, L., Lastras Alejandre, C., "Guía de Actuación: Menores y el bullying" , Universidad Carlos III de Madrid, 2018, pp. 5-7.

Granados Pérez, C., "La utilización de mecanismos de geolocalización, la captación de imagen y sonido en la lucha contra la delincuencia", *Cuadernos Digitales de Formación*, n. 43, 2016, pp. 31-33.

Jiménez Campo, J., *La garantía constitucional del secreto de las comunicaciones*, REDC, núm. 20, 1987, p. 50.

Marchena Gómez, M., González-Cuellar Serrano, N., *La reforma de la Ley de Enjuiciamiento Criminal en 2015*, Ediciones Jurídicas Castillo de Luna, Las Palmas de Gran Canaria, 2015, p. 176.

Minero Alejandre, G., "Nuevas tendencias en materia de protección de datos personales. La nueva Ley Orgánica y la jurisprudencia más reciente" *Anuario Jurídico y Económico Escurialense*, L. II, 2019, pp. 127-139.

Noya Ferreiro, Mª L., *Derecho de defensa e intervención de las comunicaciones de los abogados*, Tirant lo Blanch, Valencia, 2018, pp. 84-104.

Perales, A., "La Asociación de Usuarios de la Comunicación valora positivamente la nueva Directiva Audiovisual, pero critica algunos aspectos relacionados con la protección de los menores y la saturación publicitaria", *Asociación de Usuarios de la Comunicación*, 5 de diciembre de 2018 (disponible en http://www.auc.es/Paginas/download.php?type=comunica&year=2018&file=dic01.pdf; última consulta 07/06/2019).

Rayón Ballesteros, Mª C., "Medidas de investigación tecnológica en el proceso penal: la nueva redacción de la Ley de Enjuiciamiento Criminal operada por la Ley Orgánica 13/2015." *Anuario Jurídico y Económico Escurialense,* n. 52, 2019, pp. 179-204.

Richard González, M., *Investigación y prueba mediante medidas de intervención de las comunicaciones, dispositivos electrónicos y grabación de imagen y sonido*, Wolters Kluwer, Madrid, 2017, pp. 137-364.

Rodríguez Álvarez, A., Diligencia de registro de dispositivos y smartphones, en "Fodertics 5.0. *Estudios sobre nuevas tecnologías y Justicia*", 2016, p. 255.

Rodríguez Álvarez, A., *Intervención de las comunicaciones telefónicas y telemáticas y smartphones* en "Justicia penal y nuevas formas de delincuencia", 2017, p. 149.

Rodríguez Lainz, J. L., "Retos jurídicos de la interceptación de comunicaciones a través de prestadores de servicios de Internet", Publicación del CENDOJ, 2017, pp. 23-27.

Sánchez Yllera, I., *La nueva regulación de las medidas limitativas de los derechos reconocidos en el art. 18 CE (I): Detención y apertura de correspondencia escrita y telegráfica. Disposiciones comunes. Interceptación de comunicaciones telefónicas y telemáticas*, Publicación del CENDOJ, Madrid, 2016, pp. 6-7.

Santos Morón, Mª. J., "La denominada "herencia digital": ¿Necesidad de regulación? Estudio de Derecho Español y Comparado", *Cuadernos de Derecho Transnacional*, vol. 10, n. 1, 2018, p. 413-438.

Santos Pascual, E., "Protección de menores y TIC", ICEF Consultores, 2018, pp. 1-2.

OTRA DOCUMENTACIÓN

- Normativa WhatsApp Inc. sobre Condiciones del Servicio y Política de Privacidad (Última modificación: 15 de mayo de 2018).