EL DERECHO AL ENTORNO DIGITAL: UNA APROXIMACIÓN

Alfonso López Feria
Comandante auditor

Resumen

La aparición de las nuevas tecnologías y la utilización de las mismas en nuestro día a día ha dado origen a la proclamación de un nuevo derecho fundamental, que ha de entenderse englobado dentro del catálogo de derechos fundamentales y libertades públicas protegidos en la Constitución, recibiendo la denominación actual de «derecho del individuo al entorno digital». El objeto del presente trabajo es realizar una breve aproximación al derecho al entorno digital como derecho de nueva generación, determinando qué razones justifican su nacimiento y cuál es su ámbito de aplicación, al objeto de conceptuar tal derecho, tanto desde el punto de vista jurisprudencial como doctrinal.

Palabras clave: Intimidad, Comunicaciones, Entorno digital, Nuevas tecnologías.

Abstrac

The appearance of new technologies and the use of them in our daily lives has led to the proclamation of a new fundamental right, which must be understood within the catalogue of fundamental rights and public freedoms protected by the Constitution, which is currently called the "right of the individual to the digital environment", of which the right to data pro-

tection is part. The objective of this work is to briefly approach the right to the digital environment as a new generation right, to determine the reasons that justify its birth and what is its scope of application, in order to conceptualise such right, from both the jurisprudential and legal point of view.

Keywords: Privacy, Communications, Digital Environment, New Technologies.

Sumario

1. INTRODUCCIÓN

La aprobación 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[1], supuso la incorporación de la Ley de Enjuiciamiento Criminal

[1] Publicada en el *Boletín Oficial del Estado* n.º 239, de 6 de octubre de 2015. Entró en vigor el 6 de diciembre de 2015. El Consejo de Ministros, a propuesta del entonces ministro de Justicia, Rafael Catalá, aprobó el 5 de diciembre de 2014 el Anteproyecto de la Ley Orgánica que modificaba la Ley de Enjuiciamiento Criminal, con el que se conseguiría agilizar la justicia penal, así como regular las medidas de investigación tecnológica, que en ese momento necesitaban un marco legal adaptado a las nuevas realidades tecnológicas, al tratarse de un texto normativo aprobado en el año 1882. Este texto se remitía al borrador del Código Procesal Penal realizado por una comisión de expertos en el que se proponía un cambio radical del sistema de justicia penal, cuya implantación requería un amplio consenso. La propuesta de este nuevo Código Procesal Penal nunca llegaría al Consejo de Ministros. [Consulta: 25 de marzo de 2022]. Disponible en : https://www.mjusticia.gob.es/gl/ElMinisterio/GabineteComunicacion/Documents/1292427272299-NdP_Anteproyecto_Ley_Enjuiciamiento_Criminal.pdf

Uno de los objetivos de esa décima legislatura fue la Propuesta de texto articulado de Ley de Enjuiciamiento Criminal, elaborada por la Comisión Institucional creada por Acuerdo del Consejo de Ministros de 2 de marzo de 2012. Dicha Comisión Institucional estaba formada por un presidente, el magistrado del Tribunal Supremo Manuel Marchena

al mundo de las nuevas tecnologías. Resultaba imperioso afrontar ciertas cuestiones que no podían demorarse más y que estaban carentes de regulación, entre ellas, la regulación de las medidas de investigación tecnológica que incidían en el ámbito de los derechos a la intimidad, al secreto de las comunicaciones y a la protección de datos personales garantizados por la Constitución, y que durante muchos años fueron corregidos a través valiosas interpretaciones realizadas por el Tribunal Constitucional, el Tribunal Supremo y el Tribunal Europeo de Derechos Humanos.

Hasta la aprobación de dicha Ley Orgánica las medidas de investigación tecnológica se habían venido justificando por medio de las interpretaciones de nuestros Tribunales de Justicia sobre la base del antiguo y sobrepasado artículo 579 de la Ley de Enjuiciamiento Criminal, el cual únicamente hablaba de comunicaciones telegráficas, telefónicas y postales, medios de comunicación ordinarios entre las personas hasta la llegada de la denominada era digital, y que constituía su soporte legal, abordando, con una insuficiente regulación, la interceptación de las comunicaciones.

La regulación de la interceptación de las comunicaciones, y de la injerencia en los derechos a la intimidad y protección de datos ha adquirido una especial relevancia en los últimos años como consecuencia de la irrupción de las nuevas tecnologías en la vida de los ciudadanos, y, fundamentalmente, debido a los nuevos sistemas de comunicación utilizados. Los correos electrónicos y, muy especialmente, el advenimiento de plataformas de comunicación específica como Whatsapp, Telegram o Instagram han supuesto un aumento considerable de la interactividad de los usuarios.

La aparición de las nuevas tecnologías y la utilización de las mismas en nuestro día a día, ha dado origen a la proclamación de un nuevo derecho fundamental recibiendo la denominación actual, ya recogida por nuestro Tribunal Supremo, de «derecho del individuo al entorno digital»[2]. Se trata de un derecho fundamental de nueva generación, de carácter complejo y conectado con los anteriores, no expresamente recogido en la Constitu-

---

Gómez y por siete vocales compuestos por Jacobo López Barja de Quiroga, magistrado jefe del Gabinete Técnico del Tribunal Supremo, Antonio del Moral García, magistrado del Tribunal Supremo, Jaime Moreno Verdejo, Fiscal del Tribunal Supremo, Gabriela Bravo Sanestanislao, fiscal y vocal Portavoz del Consejo General del Poder Judicial, Luis Rodríguez Ramos, catedrático de Derecho Penal y Abogado, Nicolás González-Cuéllar Serrano, catedrático de Derecho Procesal y abogado, y por un secretario, Jaime Requena Juliani, magistrado y asesor del Gabinete del Secretario de Estado de Justicia. [Consulta: 25 de marzo de 2022]. Disponible en: https://www.mjusticia.gob.es/es/AreaTematica/ActividadLegislativa/Documents/1292430153214-Propuesta_texto_articulado_L.E.Crim.PDF

[2] La Sentencia del Tribunal Supremo 342/2013, de 17 de abril (Sala de lo Penal, Sección 1.ª), recoge por primera vez la expresión derecho al entorno digital.

ción, pero deducible de ella, a través del juego combinado de los artículos 18.1, 18.3 y 18.4 de la Carta Magna y de la normativa que desarrolla cada uno de estos derechos fundamentales, y por ello, dentro del mismo existen diversos escalones de protección jurisdiccional.

En un ordenador, en un dispositivo masivo de información o en un *smartphone,* existen diferentes tipos de datos que pueden incidir en el derecho a la intimidad del artículo 18.1, como por ejemplo los contactos, fotografías o archivos personales; en el derecho al secreto de las comunicaciones del artículo 18.3, tal podría ser el caso del contenido de los mensajes enviados por los sistemas de mensajería instantánea; y en el derecho a la protección de datos del artículo 18. 4, como determinados datos personales y de geolocalización[3].

La reforma de la Ley de Enjuiciamiento Criminal y la nueva regulación de las medidas de investigación tecnológica limitativas de los derechos reconocidos en el artículo 18 de la Constitución ha supuesto la consagración y limitación en el ámbito del proceso penal de este nuevo derecho al entorno digital, dentro del cual existen distintos niveles de protección jurisdiccional. Más allá del tratamiento constitucional fragmentado de estos tres derechos fundamentales, existe un derecho del individuo al propio entorno digital o virtual. Y, en tal derecho se integraría, sin perder su genuina manifestación de derecho constitucional de *nomen iuris propio*, toda la información contenida en formato electrónico y telemático que a través de las nuevas tecnologías van generando los usuarios y que forman parte del núcleo de estos tres derechos fundamentales.

Los nuevos instrumentos tecnológicos de comunicación y de almacenamiento contienen gran cantidad de datos y el tratamiento de cada uno de ellos de forma separada resulta insuficiente para garantizar una protección eficaz de los mismos. No se puede obviar que llevada a cabo la aprehensión física de estos dispositivos por las Fuerzas y Cuerpos de Seguridad

[3] Durán Silva, C. M. (2020). *Los medios de prueba tecnológicos como garantía de la correcta incorporación de las nuevas fuentes de prueba al juicio oral. Derecho probatorio y otros estudios procesales*. Madrid, Ediciones Jurídicas Castillo de Luna, pp. 611 y ss. En la actualidad, puede afirmarse categóricamente que el desarrollo de las nuevas tecnologías constituye un fenómeno mundial. La evolución de los sistemas tecnológicos se produce a velocidades vertiginosas que, sin duda, han sobrepasado todas las expectativas puestas en su desarrollo. Prueba de ello es el hecho de que las presentaciones de los nuevos teléfonos inteligentes se producen con un menor intervalo temporal entre el último modelo presentado por la compañía correspondiente y el siguiente. Sin embargo, no todos los ámbitos de nuestra sociedad avanzan con la misma rapidez con la que lo hace dicho sector y este es el caso, entre otros, del ámbito jurídico donde la actualización de las leyes se produce con mayor sosiego que la modernización tecnológica, con los inconvenientes que de ello se derivan, especialmente en el ámbito penal.

del Estado, por la Policía Judicial o acordada la misma en el marco de un procedimiento penal, una vez autorizado el acceso al contenido de los mismos para investigar datos que afecten, por ejemplo, únicamente al derecho a la intimidad (como podrían ser los contactos de una agenda o fotografías), pueden ser hallados datos tutelados por el derecho al secreto de las comunicaciones o datos personales y de geolocalización amparados por el derecho a la protección de datos. Y es por ello que el Legislador otorga un tratamiento unitario a los datos contenidos en los ordenadores, en los teléfonos móviles de nueva generación y en los dispositivos masivos de información, reveladores del perfil personal del investigado, configurando este derecho constitucional de nueva generación como es el derecho a la protección del propio entorno virtual.

El propio Preámbulo de la Ley Orgánica 13/2015 señala que:

> «La Ley de Enjuiciamiento Criminal no ha podido sustraerse al paso del tiempo. Renovadas formas de delincuencia ligadas al uso de las nuevas tecnologías han puesto de manifiesto la insuficiencia de un cuadro normativo concebido para tiempos bien distintos. Los flujos de información generados por los sistemas de comunicación telemática advierten de las posibilidades que se hallan al alcance del delincuente, pero también proporcionan poderosas herramientas de investigación a los poderes públicos».

Consciente de esta situación, la Ley Orgánica 13/2015 ha introducido una regulación detallada de las medidas de investigación tecnológica limitativas de los derechos reconocidos en el artículo 18 de la Constitución afectando y configurando este nuevo derecho al entorno digital.

Por tanto, el objeto del presente trabajo es realizar una breve aproximación al derecho al entorno digital como derecho de nueva generación, hasta llegar a un concepto del mismo, teniendo en cuenta los pronunciamientos doctrinales y jurisprudenciales. Para ello se hace necesario determinar qué razones justifican su nacimiento y cuál es su ámbito de aplicación, de manera que resulta forzoso abordar los diferentes derechos fundamentales que lo integran, pues es preciso una breve aproximación al contenido de tales derechos fundamentales, en la medida que este derecho del individuo al entorno virtual está integrado, por distintos niveles de protección, y, en cada caso concreto, habrá que estar al derecho fundamental afectado al objeto de determinar el tratamiento y aplicación de las medidas de investigación restrictivas de los mismos introducidas por la Ley Orgánica 13/2015 que, en su caso, van a limitar los mismos.

2. LA JUSTIFICACIÓN DE UN DERECHO AL ENTORNO DIGITAL

En la actualidad estamos incursos en la cuarta revolución industrial, término elaborado en el año 2016 por el fundador el Foro Económico Mundial KLAUS SCHWAB[4], y la tecnología está cambiando profundamente la vida de los individuos. Los instrumentos que nos suministran las nuevas tecnologías están cambiando la sociedad y las cosas permitiendo enormes avances en el ámbito económico, social y, en general, en todos los sectores de la vida. Esta cuarta revolución industrial ha tenido una gran incidencia en la vida de los ciudadanos, permitiendo la total accesibilidad de los individuos a las redes sociales y la comunicación instantánea a través de internet y el acceso a los más variados recursos y a todo tipo de información, sin ser conscientes de la acelerada velocidad de los cambios tecnológicos y de la necesidad de adaptación a los mismos. La era digital ha traído grandes beneficios, pero también ha supuesto un incremento de los riesgos cibernéticos como los comportamientos ilícitos que se llevan a cabo en las redes sociales y que proporcionan al delincuente importantes herramientas para la comisión de hechos que revisten caracteres de delito y que, hasta épocas bien recientes, resultaban impensables. Pensemos, por ejemplo, en el número de estafas y fraudes de todo tipo que se llevan a cabo con la utilización de las nuevas tecnologías, las amenazas y situaciones de acoso a menores de edad a través de las redes sociales, el acceso no autorizado

[4] El profesor Klaus Schwab es el fundador y presidente ejecutivo del Foro Económico Mundial, la Organización Internacional para la Cooperación Público-Privada. En el año 2016 escribió su libro *La Cuarta Revolución Industrial*, en el que lleva un análisis de las características clave de esta nueva revolución tecnológica. [Consulta: 1 de abril de 2022]. Disponible en: https://www.weforum.org/about/klaus-schwab

Señala Bueno de Mata que, actualmente, nos encontramos inmersos en la denominada «cuarta revolución industrial». Este término, acuñado por Schawb, fundador del Foro Económico Mundial, parte de la reflexión acerca del impacto que tendrá una nueva gama de tecnologías vinculada al tratamiento y manejo de datos en diferentes sectores e indica lo siguiente: «Consideremos las posibilidades ilimitadas de tener miles de millones de personas conectadas mediante dispositivos móviles, lo que da lugar a un poder de procesamiento, una capacidad de almacenamiento y un acceso al conocimiento sin precedentes. O pensemos en la impresionante confluencia de avances tecnológicos que abarca amplios campos, como la inteligencia artificial (IA), la robótica, el internet de las cosas (IoT), los vehículos autónomos, la impresión 3D, la nanotecnología, la biotecnología, la ciencia de materiales, el almacenamiento de energía y la computación cuántica, por nombrar unos pocos. Muchas de estas innovaciones están en sus albores, pero ya están llegando a un punto de inflexión en su desarrollo a medida que se construyen y amplifican mutuamente en una fusión de tecnologías a través de los mundos físico, digital y biológico». Bueno De Mata, F. (2020). *El Derecho probatorio ante la cuarta revolución industrial. Derecho probatorio y otros estudios procesales*. Madrid, Ediciones Jurídicas Castillo de Luna. pp. 299 y ss.

a nuestros ordenadores o aplicaciones informáticas, o los atentados a la integridad moral a través de estos nuevos sistemas.

El ciberespacio nos posibilita una conectividad universal y facilita el libre flujo de información. La inteligencia artificial, la robótica, el *big data*, el *blockchain* y el internet de las cosas están ya en el ámbito de las relaciones sociales y personales y el ciberespacio se ha convertido en un universo donde se entrelaza la información y la privacidad de las personas y de sus datos, siendo necesario preservar los derechos fundamentales de los ciudadanos en este novedoso ámbito, especialmente su privacidad y sus datos personales[5].

Este flujo de información masiva en el ciberespacio como consecuencia de las nuevas tecnologías ha tenido diversas incidencias en el ámbito del proceso penal. De una parte, se advierte que las nuevas tecnologías constituyen un instrumento adecuado y apto para la comisión de hechos que revisten caracteres de delito y para las renovadas formas de delincuencia ligadas a los nuevos sistemas tecnológicos y telemáticos; de otra parte, estos nuevos artificios técnicos constituyen un poderoso instrumento para las Fuerzas y Cuerpos de Seguridad del Estado, la Policía Judicial o los propios órganos judiciales en el ámbito de las investigaciones penales, que en muchas ocasiones puede suponer el acceso de manera indiscriminada al flujo masivo de datos personales que los ciudadanos poseen en este nuevo entorno y, que, sin duda, ha supuesto un cambio en la concepción e interpretación de los tradicionales derechos a la intimidad, al secreto de las comunicaciones y al derecho a la protección de datos[6].

---

[5] La Orden PCI/487/2019, de 26 de abril, por el que se publica la Estrategia Nacional de Ciberseguridad 2019, aprobada por el Consejo de Seguridad Nacional, publicada en el *Boletín Oficial del Estado* n.º 103, de 30 de abril, pp. 43437-43455, ya ha puesto de manifiesto esta nueva concepción del ciberespacio: «Es una dimensión fundamental para la estabilidad el preservar la defensa de los valores y principios constitucionales y democráticos, así como los derechos fundamentales de los ciudadanos en el ciberespacio, especialmente en la protección de sus datos personales, su privacidad, su libertad de expresión y el acceso a una información veraz y de calidad».

[6] Dice al respecto Fuentes Soriano que la «invasión tecnológica», en el contexto social, como internet, las redes sociales, la comunicación instantánea y la total accesibilidad de la ciudadanía a los más sofisticados recursos tecnológicos está condicionando el tratamiento procesal de la información que los particulares obtienen. Como factor determinante de la evolución a la que asistimos cabe destacar el flujo masivo de los datos personales que la ciudadanía cede, voluntaria e involuntariamente, con la mera suscripción y utilización de determinadas aplicaciones informáticas. Este flujo masivo de datos personales por la red, accesible para terceros a través de muy diversas y numerosas aplicaciones, está teniendo como consecuencia una importante evolución en la concepción e interpretación de tradicionales derechos fundamentales como el derecho a la intimidad o la propia extensión del derecho al secreto de las comunicaciones, así como el nacimiento de otros derechos fundamentales que, hace apenas una década, resultaban totalmente inimaginables, al menos, en

Se observa pues, como los nuevos sistemas tecnológicos y de comunicación han variado en pocos años la concepción primitiva de estos derechos fundamentales, pues en el ámbito de una investigación penal, en este nuevo entorno cibernético, pueden verse afectados, de manera conjunta o aislada, todos o alguno de los derechos reconocidos en el artículo 18 de la Constitución. Por ello, una adecuada protección de estos derechos fundamentales no puede ser efectiva mediante un tratamiento aislado de los mismos, sino que es preciso un tratamiento más amplio, por lo que se hace indispensable y resulta imperioso regular este nuevo derecho al entorno digital[7].

Entre el cúmulo de información que almacena una persona en el ciberespacio, en un ordenador personal, en un teléfono inteligente, en un dispositivo de información masivo o en cualquier otro repositorio de datos, puede haber datos sobre la vida privada de las personas en forma de documentos, tales como carpetas, fotografías, vídeos, datos médicos o contraseñas, entre otros, datos que, de ser accesibles por terceros, afectan a la esfera más íntima de la persona y al ámbito de la protección de datos. De la misma manera, al acceder a tal información se tiene conocimiento, en muchas ocasiones, de historiales de navegación por internet, acceso a foros, conversaciones a través de Whatsapp, Telegram, Instagram u otras redes sociales, realización de operaciones de comercio electrónico que los usuarios llevan a cabo a través de internet o acceso a determinadas páginas web, que, sin duda, suponen una revelación de datos acerca de la personalidad de una persona y que, por ello, afectan al núcleo más íntimo del derecho a la intimidad al recoger datos que pueden revelar la ideología, religión, creencias, orientación sexual, salud, gustos y aficiones personales

---

su actual dimensión, como es el caso del derecho a la protección de datos o, desde luego, el derecho al propio entorno virtual. Fuentes Soriano, O. (2020). *La prueba prohibida aportada por particulares, a la luz de las nuevas tecnologías. Derecho probatorio y otros estudios procesales*. Madrid, Ediciones Jurídicas Castillo de Luna, pp. 715 y ss.

[7] Como señala Sanchís Crespo, en el curso de una investigación penal pueden verse afectados los diferentes derechos a los que se refiere el artículo 18 de la Constitución. Si bien todos ellos están relacionados con el derecho a la intimidad, responden a distintos objetos de tutela y la protección que nuestra Constitución dispensa a cada uno de ellos es, consecuentemente, desigual. Tanto los derechos al honor, a la intimidad personal y familiar y a la propia imagen, como el derecho a la inviolabilidad domiciliaria y el derecho al secreto de las comunicaciones o el derecho a la protección de datos, constituyen manifestaciones de la intimidad, pero mientras que para la inviolabilidad domiciliaria y el secreto de las comunicaciones, la tutela es más intensa pues se exige autorización judicial para violentarlos, en el caso del honor, intimidad, imagen y protección de datos, esa referencia constitucional no existe. Velasco Núñez, E. y Sanchís Crespo, C. (2019). *Delincuencia informática. Tipos delictivos e investigación. Con jurisprudencia tras la reforma procesal y penal de 2015*. Valencia, Editorial Tirant lo Blanch, pp. 260 y ss.

de los individuos, o datos de geolocalización que afectan al derecho a la protección de datos. Igualmente, en muchas ocasiones, también se tiene acceso en el ciberespacio y en dichos dispositivos al contenido de correos electrónicos del usuario o las conversaciones mantenidas por el usuario en redes sociales, planteándose también su injerencia en el derecho al secreto de las comunicaciones.

Este cúmulo de información que flota en el ciberespacio y estos dispositivos que la almacenan, una vez intervenidos en el curso de una investigación judicial suponen algo más que simples piezas de convicción en el sentido que apunta la Ley de Enjuiciamiento Criminal[8], pues estos datos cibernéticos, así como los almacenados en estos dispositivos, si bien es cierto que constituyen instrumentos que recogen este gran volumen de información, también es innegable el hecho que reúnen información especialmente sensible que entra en el ámbito de los derechos reconocidos en el artículo 18 de la Constitución, de manera que suponen algo más que un mero depósito de datos. La regulación de la intromisión que supone el conocimiento del contenido de tales datos en formato electrónico que está presente en tales dispositivos o en el ciberespacio ha de realizarse de manera unitaria si se quiere llevar a cabo una protección efectiva de esos derechos más elementales del individuo y, por tanto, evitar vulneraciones de los derechos a la intimidad, secreto de las comunicaciones, y protección de datos, lo que sin duda, justifica el nacimiento de este nuevo derecho como es el derecho al entorno digital.

La adecuada protección de los derechos fundamentales de la persona consagrados en el artículo 18 de la Carta Magna, en este nuevo entorno digital, ha de realizarse de manera inseparable. Sin embargo, en determinados supuestos, tal intrusión va a suponer una incidencia parcial en el ámbito del derecho al entorno digital. Indudablemente, habrá casos en que la injerencia en este nuevo derecho al entorno virtual se va a realizar de manera completa, es decir con afectación de todos los derechos del artículo 18 y, en otras ocasiones, la invasión del derecho puede realizarse de manera parcial, pues no se puede olvidar que el derecho al entorno digital está

[8] Las piezas de convicción se encuentran reguladas en la LECrim en los artículos 334 y ss. El primero de ellos conceptúa las piezas de convicción como el conjunto de armas o efectos de cualquier clase que puedan tener relación con el delito, y se hallen en el lugar en que este se cometió, o en sus inmediaciones, o en poder del reo, o en otra parte conocida siendo la misma intervenida por el Juzgado a disposición del procedimiento judicial. Por otra parte, la LECrim denomina, en el artículo 367, a las piezas de convicción efectos judiciales y las define señalando que: «Tendrán la consideración de efectos judiciales, en el orden penal, todos aquellos bienes puestos a disposición judicial, embargados, incautados o aprehendidos en el curso de un procedimiento penal».

integrado por distintas categorías de protección, en función del derecho fundamental afectado, como, por ejemplo, los supuestos en los que únicamente sea necesario para el buen curso de la investigación penal conocer datos de tráfico que no estén asociados a un proceso de comunicación, en los que derecho integrante del entorno virtual afectado es el derecho a la protección de datos[9].

3. LA CONFIGURACIÓN DE UN DERECHO FUNDAMENTAL AL ENTORNO DIGITAL

Antes de tratar de elaborar un concepto del derecho al entorno digital, resulta necesario una breve aproximación de carácter general a los elementos que integran este nuevo derecho. Una adecuada configuración del derecho al entorno digital debe partir del análisis de los diferentes derechos que lo integran, pues es preciso identificar qué derecho fundamental ampara la protección de los diferentes datos dentro de este universo digital. Un acercamiento a cada uno de estos derechos resulta trascendental para abordar el concepto del derecho al entorno digital, pues determinar cuál es el derecho fundamental afectado en este mundo cibernético resulta de obligada resolución, pues no se puede obviar que nuestra Constitución otorga un régimen de protección diferente, según se trate de uno u otro derecho.

De esta manera, el derecho al entorno digital se muestra en su nacimiento como un derecho de nueva generación, de carácter complejo y compuesto por tres elementos: el derecho a la intimidad, el derecho al secreto de las comunicaciones y el derecho a la protección de datos.

3.1. El derecho a la intimidad. Sustantividad y autonomía respecto a otros derechos fundamentales

El derecho a la intimidad aparece constitucionalizado en el artículo 18.1 de nuestra Norma Suprema: «Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen». El Texto Constitucional

[9] Tal sería el caso del acceso a los datos de tráfico que no requieren autorización judicial, es decir, de datos que no aparecen vinculados a un proceso de comunicación, pero que afectan al derecho a la protección de datos del artículo 18.4 de la Constitución, entre los que el legislador ha destacado en los artículos 588 ter l) y m), de la Ley de Enjuiciamiento Criminal, la numeración IMSI e IMEI y los datos de identificación de números telefónicos o los números que corresponden a un titular.

recoge en el citado precepto tres derechos fundamentales que derivan de la dignidad humana y están dirigidos a la protección del patrimonio moral de los individuos. A pesar de su estrecha relación, como lo demuestra el hecho de su reconocimiento en el mismo apartado del artículo 18.1, tienen un contenido propio y específico[10].

Ahora bien, como se ha subrayado, el derecho a la intimidad tiene sustantividad propia, incluso en relación con los derechos que menciona el artículo 18.1. Nuestro Tribunal Constitucional[11], ha puesto de ma-

[10] Señala Torres del Moral que el reconocimiento del derecho a la intimidad personal y familiar es bien reciente y todavía escaso. Pero su idea originaria, que como dice el Tribunal Constitucional, es el respeto a la vida privada, sí se encuentra en algunos de los derechos tradicionales, como la inviolabilidad del domicilio y el secreto de la correspondencia. Gimeno Sendra, V. *et al*. (2018). *Los Derechos fundamentales y su protección jurisdiccional*. Madrid, Edisofer, S. L., pp. 152 y ss.

Por su parte, la Sentencia del Tribunal Constitucional 110/1984, de 26 de noviembre, ha señalado que: «El reconocimiento explícito en un texto constitucional del derecho a la intimidad es muy reciente y se encuentra en muy pocas Constituciones, entre ellas la española. Pero su idea originaria, que es el respecto a la vida privada, aparece ya en algunas de las libertades tradicionales. La inviolabilidad de domicilio y de la correspondencia, que son algunas de esas libertades tradicionales, tienen como finalidad principal el respeto a un ámbito de vida privada, personal y familiar, que debe quedar excluido del conocimiento ajeno y de las intromisiones de los demás, salvo autorización del interesado. Lo ocurrido es que el avance de la tecnología actual y del desarrollo de los medios de comunicación de masas ha obligado a extender esa protección más allá del aseguramiento del domicilio como espacio físico en que normalmente se desenvuelve la intimidad y del respeto a la correspondencia, que es o puede ser medio de conocimiento de aspectos de la vida privada. De aquí el reconocimiento global de un derecho a la intimidad o a la vida privada que abarque las intromisiones que por cualquier medio puedan realizarse en ese ámbito reservado de vida».

[11] Sentencia del Tribunal Constitucional 14/2003, de 28 de enero, Fundamento de Derecho Cuarto.

En el mismo sentido, Sentencia del Tribunal Supremo 692/2012, de 13 de noviembre (Sala de lo Civil, Sección 1.ª), en el Fundamento de Derecho Noveno, ha señalado que: «[...] de forma reiterada el Tribunal Constitucional, entre otras en la STC 81/2001, de 26 de marzo, ha señalado que los derechos al honor, a la intimidad personal y a la propia imagen, reconocidos en el artículo 18.1 CE , a pesar de su estrecha relación en tanto que derechos de la personalidad, derivados de la dignidad humana y dirigidos a la protección del patrimonio moral de las personas, tienen, no obstante, un contenido propio y específico. Se trata, de derechos autónomos, con propia sustantividad y la apreciación de la vulneración de uno no conlleva necesariamente la vulneración de los demás. El carácter autónomo de los derechos del artículo 18.1 CE supone que ninguno de ellos tiene respecto de los demás la consideración de derecho genérico que pueda subsumirse en los otros dos derechos fundamentales que prevé este precepto constitucional, pues el carácter específico de cada uno de estos derechos impide considerar subsumido otro en alguno de ellos. De tal manera que con aplicación al presente caso, las vulneraciones de los otros derechos que puedan ocasionarse a través de una imagen que muestre, además de los rasgos físicos que permiten la identificación de la persona, aspectos de su vida privada, partes íntimas de su cuerpo o que se la represente en una situación que pueda hacer desmerecer su buen nombre o su propia estima, permitirá en tales supuestos que junto a la apreciación de la vulneración del derecho a la

nifiesto que los derechos al honor, a la intimidad personal y a la propia imagen, todos ellos reconocidos en el artículo 18.1 de la Constitución, a pesar de su estrecha relación en tanto que derechos de la personalidad, derivados de la dignidad humana y dirigidos a la protección del patrimonio moral de las personas, tienen, no obstante, un contenido propio y específico. Se trata, dicho con otras palabras, de derechos autónomos, de modo que, al tener cada uno de ellos su propia sustantividad, la apreciación de la vulneración de uno no conlleva necesariamente la vulneración de los demás[12]. El carácter autónomo de los derechos del art. 18.1 de la Constitución supone que ninguno de ellos tiene respecto de los demás la consideración de derecho genérico que pueda subsumirse en los otros dos derechos fundamentales que prevé este precepto constitucional, pues la especificidad de cada uno de estos derechos impide considerar subsumido en alguno de ellos las vulneraciones de los otros derechos que puedan ocasionarse a través de una imagen que muestre, además de los rasgos físicos que permiten la identificación de la persona, aspectos de su vida privada, partes íntimas de su cuerpo o que se la represente en una situación que pueda hacer desmerecer su buen nombre o su propia estima. En tales supuestos la apreciación de la vulneración del derecho a la imagen no impedirá, en su caso, la apreciación de la vulneración de las eventuales lesiones del derecho a la intimidad o al honor que a través de la imagen se hayan podido causar, pues, desde la perspectiva constitucional, el desvalor de la acción no es el mismo cuando los hechos realizados solo pueden considerarse lesivos del derecho a la imagen que cuando, además, a través de la imagen puede vulnerarse también el derecho al honor o a la intimidad, o ambos derechos conjuntamente[13].

El contenido propio y específico del derecho a la intimidad personal y familiar obliga a su delimitación en relación con otros derechos fundamentales con los que aparece claramente interrelacionado. Así, respecto al derecho a la inviolabilidad del domicilio consagrado en el artículo 18.2 de la Constitución, constituye una manifestación del derecho a la intimidad del artículo 18.1, si bien, como se ha dicho,

---

imagen, la apreciación en su caso, de la vulneración de las eventuales lesiones del derecho a la intimidad o al honor que a través de la imagen se hayan podido causar».

De la misma manera, Sentencias del Tribunal Supremo (Sala de lo Civil, Sección 1.ª) 625/2012, 459/2011, 311/2010, 525/2011.

[12] Sentencias del Tribunal Constitucional 81/2001, de 26 de marzo, Fundamento de Derecho Segundo; 156/2001, de 2 de julio, Fundamento de Derecho Tercero.

[13] Sentencias del Tribunal Constitucional 81/2001, de 26 de marzo, Fundamento de Derecho Segundo; 83/2002, de 22 de abril, Fundamento de Derecho Cuarto.

ambos derechos gozan de autonomía propia. El derecho a la intimidad protege un ámbito reservado de la vida de las personas excluido del conocimiento de terceros, sean estos poderes públicos o particulares, en contra de su voluntad, en tanto que el derecho a la inviolabilidad del domicilio tiene por objeto la protección de ese ámbito especial determinado, el domicilio, es decir, aquel espacio en el que las personas ejercen su libertad más íntima, libres de cualquier sujeción a los usos y convenciones sociales, siendo el objeto de protección tanto el espacio físico en sí mismo considerado como lo que en él hay de emanación de la persona y de su esfera privada. La Sentencia del Tribunal Constitucional 10/2002, de 17 de enero, ha puesto de relieve el carácter autónomo de ambos derechos al señalar que la norma constitucional que proclama la inviolabilidad del domicilio y la interdicción de la entrada y registro domiciliario, del artículo 18.2 de la Constitución constituye una manifestación de la norma precedente, el artículo 18.1, que garantiza el derecho fundamental a la intimidad personal y familiar. De esta construcción interrelacionada resulta que la protección de la inviolabilidad domiciliaria tiene carácter instrumental respecto de la protección de la intimidad personal y familiar, si bien dicha instrumentalidad no empece a la autonomía que la Constitución reconoce a ambos derechos, distanciándose así de la regulación unitaria de los mismos que contiene el art. 8.1 del Convenio Europeo de Derechos Humanos.

El derecho a la intimidad personal y familiar tiene por objeto la protección de un ámbito reservado de la vida de las personas excluido del conocimiento de terceros, sean estos poderes públicos o particulares, en contra de su voluntad[14], mientras que el derecho a la inviolabilidad del domicilio protege un ámbito espacial determinado, el domicilio, por ser aquel en el que los individuos, libres de toda sujeción a los usos y convenciones sociales, ejercen su libertad más íntima, siendo objeto de protección de este derecho tanto el espacio físico en sí mismo considerado, como lo que en él hay de emanación de la persona y de su esfera privada[15].

También el derecho a la intimidad aparece delimitado respecto al derecho al secreto de las comunicaciones y el derecho a la protección de datos, en los términos que veremos a continuación.

[14] Sentencias del Tribunal Constitucional 144/1999, de 22 de julio, Fundamento de Derecho Octavo; 119/2001, de 24 de mayo, Fundamento de Derecho Quinto.

[15] Sentencias del Tribunal Constitucional 22/1984, de 17 de febrero, Fundamento de Derecho Quinto; 94/1999, de 31 de mayo, Fundamento de Derecho Quinto; y 119/2001, de 24 de mayo, Fundamento de Derecho Sexto.

3.2. El derecho al secreto de las comunicaciones. Sustantividad y autonomía

Los derechos fundamentales de los que son titulares los ciudadanos ostentan un doble carácter. De una parte, se trata de derechos subjetivos, es decir, derechos de los individuos no solo como derechos de los ciudadanos en sentido estricto, sino en la medida en que garantizan un status jurídico o libertad en un ámbito de la existencia; y, de otra parte, son elementos esenciales del ordenamiento jurídico en una comunidad nacional, en cuanto esta se configura como marco de la convivencia humana justa y pacífica, plasmado en la actualidad en el Estado social y democrático de Derecho, según la fórmula establecida en la Constitución, en su artículo 1.1[16].

Entre estos derechos, el derecho al secreto de las comunicaciones se encuentra reconocido en el artículo 18.3 de nuestra Norma Fundamental que consagra la libertad de las comunicaciones: «Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial».

Respecto a su naturaleza, la doctrina[17], ha puesto de manifiesto que, aunque dicho derecho se relacione con el derecho a la intimidad, no se identifica en absoluto con él, sino que posee un contenido mucho más amplio, ya que mediante el artículo 18.3 el constituyente no ha querido proteger exclusivamente el secreto de las comunicaciones íntimas, sino cualquier clase de comunicación, y ello con independencia de su contenido material

El bien constitucionalmente protegido es, pues, el derecho de los titulares a mantener el carácter reservado de una información privada, o lo que

[16] Sentencia del Tribunal Constitucional 99/2021 de 10 mayo (Pleno), Fundamento de Derecho Tercero.

[17] Dice Gimeno Sendra que la intervención de las comunicaciones, como su propio nombre indica, consiste en la restricción del derecho fundamental contenido en el artículo 18.3 de la Constitución, efectuada por una resolución judicial motivada, en cuya virtud se autoriza a la policía judicial a entrar en un procedimiento de comunicación con el objeto de conocer y, en su caso, recabar y custodiar una noticia, pensamiento, imagen penalmente relevante para su reproducción en un juicio oral, incoado por la comisión de un delito grave.

Mediante el artículo 18.3 el constituyente no ha querido proteger exclusivamente el secreto de las comunicaciones íntimas, sino cualquier clase de comunicación, y ello con independencia de su contenido material, lo que ha llevado a nuestra doctrina (Jiménez Campo, Asencio, López Fragoso) y jurisprudencia (Sentencia del Tribunal Constitucional 114/1984, de 29 de noviembre, 34/1996, de 11 de marzo, 127/1996, de 9 de julio, 58/1998, de 16 de marzo, 123/2002, de 20 de mayo, 70/2002, de 3 de abril, 56/2003, de 24 de marzo) a proclamar el carácter formal de este derecho fundamental (Circular de la Fiscalía General del Estado 1/2013, de 11 de enero). Gimeno Sendra, V. *et al.* (2018). *Los Derechos fundamentales… Op. cit.,* pp. 557 y ss.

es lo mismo, a que ningún tercero pueda intervenir en el proceso de comunicación y conocer la idea, pensamiento o noticia transmitida por el medio.

El derecho al secreto de las comunicaciones constituye una plasmación singular de la dignidad de la persona y el libre desarrollo de la personalidad que son fundamento del orden político y de la paz social, en los términos expuestos en el artículo 10 de la Constitución. Las comunicaciones comprendidas en este derecho han de ser aquellas indisolublemente unidas por naturaleza a la persona, a la propia condición humana. En consecuencia, la comunicación es a efectos constitucionales el proceso de transmisión de expresiones de sentido a través de cualquier conjunto de sonidos, señales o signos. Aunque en la jurisprudencia constitucional no encontramos pronunciamientos directos sobre el ámbito objetivo del concepto constitucional de comunicación, sí existe alguna referencia indirecta al mismo derivada del uso indistinto de las expresiones comunicación y mensaje, o del uso de términos como carta o correspondencia cuando de la ejemplificación del secreto de las comunicaciones postales se trataba[18].

En relación a su contenido, dice Gimeno Sendra[19] que el objeto material a través del cual puede vulnerarse este derecho fundamental es cualquier medio de comunicación, sea escrito, oral, radioeléctrico, telemático, en soporte magnético o electrónico. Nuestra Constitución ha reservado a la autoridad judicial todo tipo de intervención de las comunicaciones, sea una carta postal, se efectúe a través del cable o del espacio radioeléctrico (telefonía digital y por satélite incluida), consista en la intervención de una cinta magnetofónica, de vídeo o DVD, de un disco duro de ordenador, de sus elementos reproductores o de la fiscalización del correo electrónico.

La doctrina del Tribunal Constitucional[20] sobre el secreto de las comunicaciones se ha venido asentando sobre tres puntos:

1. Se protege la libertad de comunicaciones. El derecho fundamental consagra la libertad de las comunicaciones, implícitamente, y, de modo expreso, su secreto, estableciendo en este último sentido la interdicción de la interceptación o del conocimiento antijurídicos de las comunicaciones ajenas. El bien constitucionalmente protegido es así, a través de la imposición a todos del secreto, la libertad de las comunicaciones.

[18] Sentencia del Tribunal Constitucional 281/2006, de 9 de octubre.

[19] Gimeno Sendra, V. *et al.* (2018). *Los derechos fundamentales… Op. cit*., p. 560.

[20] Sentencias del Tribunal Constitucional 114/1984, de 29 de noviembre, Fundamento de Derecho Séptimo; 34/1996, de 11 de marzo. Fundamento de Derecho Cuarto; y 70/2002, de 3 de abril, Fundamento de Derecho Noveno.

2. Se garantiza la impenetrabilidad de la comunicación para terceros. Sea cual sea el ámbito objetivo del concepto de comunicación, la norma constitucional se dirige inequívocamente a garantizar su impenetrabilidad por terceros, públicos o privados, pues el derecho posee eficacia erga omnes ajenos a la comunicación misma.
3. El concepto de lo secreto tiene carácter formal, en el sentido de que se predica de lo comunicado, sea cual sea su contenido y pertenezca o no el objeto de la comunicación misma al ámbito de lo personal, lo íntimo o lo reservado.

En un principio, el Tribunal Constitucional consideró que el derecho puede conculcarse tanto por la interceptación en sentido estricto (que suponga aprehensión física del soporte del mensaje, con conocimiento o no del mismo, o captación, de otra forma, del proceso de comunicación) como por el simple conocimiento antijurídico de lo comunicado (apertura de la correspondencia ajena guardada por su destinatario, por ejemplo)[21].

Sin embargo, posteriormente, el Tribunal Constitucional[22] estableció una nueva doctrina en el entendimiento del concepto de comunicación

[21] Sentencia del Tribunal Constitucional 114/1984, de 29 de noviembre, Fundamento de Derecho Séptimo. Esta sentencia, sobre la base de la Sentencia del Tribunal Europeo de Derechos Humanos, de 2 de agosto de 1984 (Caso Malone, que reconocía expresamente la posibilidad de que el art. 8 de la Convención podía resultar violado por el empleo de un artificio técnico que, como el llamado *comptage,* permite registrar cuáles hayan sido los números telefónicos marcados sobre un determinado aparato, aunque no el contenido de la comunicación misma), extendía la protección del derecho al secreto de las comunicaciones más allá del proceso de la comunicación, de manera que el derecho podía conculcarse por la simple aprehensión física del soporte del mensaje, con conocimiento o no del mismo, o captación de otra manera del proceso de comunicación.

[22] Sentencia del Tribunal Constitucional 70/2002, de 3 de abril, Fundamento de Derecho Noveno. El Tribunal Constitucional ha seguido una línea vacilante en esta materia. Así, la Sentencia del Tribunal Constitucional 123/2002, de 20 de mayo, F.4 señala al respecto que: «[…] la protección del derecho al secreto de las comunicaciones alcanza al proceso de comunicación mismo, pero finalizado el proceso en que la comunicación consiste, la protección constitucional de lo recibido se realiza en su caso a través de las normas que tutelan la intimidad u otros derechos», de modo que la protección de este derecho alcanza a las interferencias habidas o producidas en un proceso de comunicación. Dicha doctrina también fue confirmada por la Sentencia del Tribunal Constitucional 173/2011, de 7 de noviembre, F. 3, en relación con los correos electrónicos encontrados en un ordenador, situándolos en el ámbito del derecho a la intimidad: «[…] A esto debe añadirse que el ordenador es un instrumento útil para la emisión o recepción de correos electrónicos, pudiendo quedar afectado en tal caso, no solo el derecho al secreto de las comunicaciones del art. 18.3 CE, por cuanto es indudable que la utilización de este procedimiento supone un acto de comunicación, sino también el derecho a la intimidad personal (art. 18.1 CE), en la medida en que estos correos o *email*, escritos o ya leídos por su destinatario, quedan almacenados en la memoria del terminal informático utilizado. Por ello deviene necesario establecer una

como consecuencia de los avances tecnológicos que se venían produciendo en el ámbito de las telecomunicaciones y consideró que la protección del derecho al secreto de las comunicaciones alcanza al proceso de comunicación mismo, pero finalizado el proceso en que la comunicación consiste, la protección constitucional de lo recibido se realiza, en su caso, a través de las normas que tutelan la intimidad u otros derechos. De acuerdo con este nuevo concepto, la aprehensión por las Fuerzas y Cuerpos de Seguridad del Estado de una carta abierta, la cual se encontraba en una agenda y doblada en su interior, y la cual fue leída sin previa autorización judicial en el momento de la detención del investigado, no suponía vulneración del derecho al secreto de las comunicaciones, pues tal intervención no interfería en el proceso de comunicación, sino que el citado proceso ya había finalizado, lo que justificaba el tratamiento del documento como tal (como efectos del delincuente que se examinan y se ponen a disposición judicial) y no en el marco del secreto de las comunicaciones.

Una y otra postura constitucional han tenido abundante apoyo a través de numerosas sentencias del Tribunal Constitucional y del Tribunal Supremo lo que constituye una manifestación de la dificultad de delimitar el concepto de comunicación. No obstante, tanto el Tribunal Supremo[23], como

---

serie de garantías frente a los riesgos que existen para los derechos y libertades públicas, en particular la intimidad personal, a causa del uso indebido de la informática, así como de las nuevas tecnologías de la información».

En contra de dicha postura se han pronunciado las Sentencias del Tribunal Constitucional 281/2006, de 9 de octubre, Fundamento de Derecho Cuarto; 230/ 2007 , de 5 de noviembre, Fundamento de Derecho Segundo; 142/2012, de 2 de julio, Fundamento de Derecho Tercero, y 241/2012, de 17 de diciembre, 115/2013, que recogen la siguiente doctrina: El derecho al secreto de las comunicaciones (artículo 18.3 de la Constitución) consagra tanto la interdicción de la interceptación como el conocimiento antijurídico de las comunicaciones ajenas, por lo que dicho derecho puede resultar vulnerado no solo por la interceptación en sentido estricto –aprehensión física del soporte del mensaje, con conocimiento o no del mismo, o captación, de otra forma, del proceso de comunicación– sino también por el conocimiento antijurídico de lo comunicado, como puede suceder, sin ánimo de exhaustividad, en los casos de apertura de la correspondencia ajena guardada por su destinatario o de un mensaje emitido por correo electrónico o a través de telefonía móvil.

[23] Sentencia del Tribunal Supremo 264/2018, de 31 de mayo, (Sala de lo Penal, Sección 1.ª), Fundamento de Derecho Cuarto, con cita en Sentencia del Tribunal Constitucional 70/2002, de 3 de abril (supuestos de acceso por la policía a una carta abierta que el detenido llevaba consigo en el momento de la detención); Sentencia del Tribunal Supremo de 3 de marzo de 2000 (examen por la policía de la pantalla de un teléfono fijo para identificar una llamada entrante o comprobación de la memoria del aparato; Sentencias del Tribunal Supremo de 27 de junio de 2002, y 30 de noviembre de 2005 (examen de los mensajes SMS registrados en un teléfono móvil intervenido; Sentencias del Tribunal Supremo de 25 de septiembre de 2003, 25 de julio de 2003 y 30 de noviembre de 2005; Sentencia del Tribunal Constitucional 56/2003, de 24 de marzo (examen del registro de llamadas de un teléfono móvil).

nuestros Tribunales de Justicia[24] parecen acogerse a esta segunda postura en sus últimos pronunciamientos reconociendo que no existe intromisión en el derecho al secreto de las comunicaciones (sino intervención en el derecho a la intimidad) en los supuestos de acceso por la Policía a una carta abierta que el detenido llevaba consigo en el momento de la detención, examen por la Policía de la pantalla de un teléfono fijo para identificar una llamada entrante o comprobación de la memoria del aparato, examen de los mensajes SMS registrados en un teléfono móvil intervenido o examen del registro de llamadas de un teléfono móvil.

En su origen, la Ley de Enjuiciamiento Criminal regulaba en los artículos 579 a 588 las intervenciones postales y telegráficas. Posteriormente, la Ley Orgánica 4/1988, de 25 de mayo, de reforma de la Ley de Enjuiciamiento Criminal en materia de delitos relacionados con la actividad de bandas armadas o de elementos terroristas o rebeldes, modificó el artículo 579 incluyendo en los párrafos segundo a cuarto la intervención de las comunicaciones telefónicas y la observación de las comunicaciones postales, telegráficas y telefónicas. En la actualidad y tras la modificación efectuada por la Ley Orgánica 13/2015, de 5 de octubre, la Ley de Enjuiciamiento Criminal regula en capítulo aparte, en los artículos 579 a 588 la detención y apertura de la correspondencia escrita y telegráfica, regulando en un capítulo específico, el Capítulo V, del Título VIII, en los artículos 588 ter a) a 588 ter m) la interceptación de las comunicaciones telefónicas y telemáticas.

La injerencia en el derecho al secreto de las comunicaciones exige, también, perfilar el concepto de intervención. La doctrina[25] ha puesto de manifiesto que, aunque no existe una definición legal de tales interven-

[24] Auto 67/2020, de 5 de febrero, de la Audiencia Provincial de Cádiz (Sección 3ª), Fundamento de Derecho Primero: «Esta cuestión es tratada en la reciente STS 2408/2018 de 31 de mayo de 2018, Ponente Sr. Del Moral García, en cuyo FD cuarto se dice: "[...] los datos obtenidos en el volcado y a los que se refiere el oficio (tanto la agenda telefónica como el contenido de los mensajes) no afectan al secreto de las comunicaciones del investigado, sino al derecho a su intimidad, sin que fuera preciso, en tales supuestos y en todo caso, la previa autorización judicial". La STS 41/2010, de 26 de enero, explica como "la jurisprudencia ha venido considerando que no existe intromisión en el derecho al secreto de las comunicaciones (sino intervención en el derecho a la intimidad) en los supuestos de acceso por la Policía a una carta abierta que el detenido llevaba consigo en el momento de la detención (STC 70/2002, de 3 de abril); examen por la Policía de la pantalla de un teléfono fijo para identificar una llamada entrante o comprobación de la memoria del aparato (STS 3 de marzo de 2000); examen de los mensajes SMS registrados en un teléfono móvil intervenido (SSTS 27 de junio de 2002, 30 de noviembre de 2005); examen del registro de llamadas de un teléfono móvil (SSTS 25 de septiembre de 2003, 25 de julio de 2003 y 30 de noviembre de 2005; STC 56/2003, de 24 de marzo)"».

[25] Gimeno Sendra, V. *et al.* (2018). *Los derechos fundamentales… Op.cit*, p. 561.

ciones y que por intervención telefónica o electrónica, puede entenderse todo acto de investigación, limitativo del derecho fundamental al secreto de las comunicaciones, por el que el Juez de Instrucción, en relación con un hecho punible de especial gravedad y en el curso de un procedimiento penal, decide, mediante auto especialmente motivado que, por la policía judicial, se proceda al registro de llamadas, correos electrónicos o datos de tráfico y/o a efectuar la grabación magnetofónica o electrónica de las conversaciones telefónicas o correos electrónicos del imputado durante el tiempo imprescindible para poder preconstituir la prueba del hecho punible y la participación de su autor.

En la actualidad, debemos extender el concepto de interceptación a las comunicaciones telefónicas y telemáticas. La distinción entre ambas clases de comunicación resulta hoy en día ciertamente difusa. El legislador, en lugar de regular la interceptación de telecomunicaciones, que incluiría toda transmisión, emisión o recepción de signos, señales, escritos, imágenes, sonidos o informaciones de cualquier naturaleza por hilo, radioelectricidad, medios ópticos u otros sistemas electromagnéticos (apartado 39 del Anexo II de la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones) ha optado por la limitación de la previsión legal a las comunicaciones que se realizan a través de dos medios concretos, que es a lo que alude la diferenciación establecida en la ley.

Si bien el concepto de comunicación telefónica no plantea muchos problemas, no ocurre lo mismo con las comunicaciones telemáticas. La telemática, según la Real Academia Española, es la «aplicación de las técnicas de la telecomunicación y de la informática a la transmisión de información computerizada»; en consecuencia, pueden definirse las comunicaciones telemáticas como aquellas que emplean la informática para la transmisión de información. Ahora bien, la mera intervención de un equipo o sistema informático en el proceso de transmisión de una comunicación no puede resultar suficiente para catalogar esta como telemática, ya que, hoy en día, todas las comunicaciones telefónicas utilizan tecnologías digitales, manejadas por sistemas informáticos, para su transmisión y gestión técnica. En consecuencia, el criterio distintivo debe residir en el medio empleado para llevar a cabo la comunicación: telefónica cuando se utilice un teléfono para generar el mensaje que se comunica, y telemática cuando se utilice un sistema informático, aunque nuevamente aquí se encontraría una zona de duda en las comunicaciones generadas a través de los modernos *smartphones* o teléfonos inteligentes, que mezclan en un mismo dispositivo las capacidades de un teléfono y de un ordenador y que podrían ser catalogadas como comunicaciones mixtas.

En cualquier caso, al gozar ambos tipos de comunicación de una misma regulación, el problema de su distinción únicamente se proyecta sobre aquellas normas de comunicación que no tuvieran cabida en ninguna de estas dos, a las que les faltaría la previsión legal que posibilitara su intervención, lo que hoy en día no resulta imaginable, aunque sí se plantea como una posibilidad de futuro[26].

3.3. El derecho a la protección de datos. Sustantividad y autonomía respecto a otros derechos fundamentales

El derecho a la protección de datos aparece constitucionalizado en el artículo 18.4 de la Norma Suprema: «La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos»[27].

Este derecho está protegido también a nivel europeo. Bajo los auspicios del Consejo de Europa, ya en 1981 se celebró un Convenio sobre Protección de Datos Personales. Y aunque el Convenio Europeo de Derechos Humanos, dada la fecha de su elaboración, no consagra expresamente este derecho, la protección de datos se considera incluida dentro de la noción de vida privada de su art. 8. Por lo que se refiere a la Unión Europea, el derecho a la protección de datos de carácter personal está consagrado en el art. 8 de la Carta de Derechos Fundamentales de la Unión Europea, un precepto distinto del relativo al derecho a la vida privada. Además, existe derecho derivado de la Unión Europea, donde se encuentra actualmente la regulación general de esta materia: el Reglamento (UE) 2016/679, que sustituye a la antigua Directiva 95/46/CE. La legislación española se halla en la Ley Orgánica 3/2018, de Protección de Datos Personales, y adap-

[26] Circular 2/2019, de la Fiscalía General del Estado sobre interceptación de comunicaciones telefónicas y Telemáticas, publicada en el *Boletín Oficial del Estado* n.º 70, de 22 de marzo de 2019, pp. 30093 y 30094.

[27] Díez-Picazo, L. M. (2021). *Los derechos de la vida privada. Sistema de derechos fundamentales.* Valencia, Editorial Tirant lo Blanch, p. 311. La redacción de este precepto no es afortunada, ya que limitar el uso de la informática es, además de poco factible, escasamente deseable. No tiene sentido oponerse al progreso tecnológico. Cosa distinta, que es lo que sin duda el constituyente quiso decir, es poner coto a los eventuales abusos en el empleo de nuevas tecnologías. Y a nadie se le escapa que la revolución de los ordenadores y el advenimiento de la sociedad de la información han abierto un escenario cualitativamente distinto, donde las posibilidades (públicas y privadas) de control de los individuos se han multiplicado de manera exponencial. Por todo ello, la expresión asentada hoy en día es «protección de datos».

ta el derecho español a las exigencias del mencionado Reglamento (UE) 2016/679[28].

Igualmente, en el ámbito de la Unión Europea cabe destacar la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo, de 27 de noviembre de 2008, relativa a la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal, que había sido superada por varias razones. Dicha Directiva ha sido transpuesta al ordenamiento jurídico español por la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales.

El artículo 18.4 de la Constitución incorpora una garantía constitucional para responder a una nueva forma de amenaza concreta a la dignidad y a los derechos de la persona. Tanto el Tribunal Constitucional[29] como el Tribunal Supremo[30], han venido sosteniendo que el derecho a la protección de los datos consagra en sí mismo un derecho o libertad fundamental que excede el ámbito propio del derecho fundamental a la intimidad (artículo 18.1 de la Constitución), y que se traduce en un derecho de control sobre los datos relativos a la propia persona. La llamada libertad informática es así el derecho a controlar el uso de los mismos datos insertos en un programa informático (*habeas data*) y comprende, entre otros aspectos, la oposición del ciudadano a que determinados datos personales sean utilizados para fines distintos de aquel legítimo que justificó su obtención.

Como dice nuestro Tribunal Supremo[31], la llamada libertad informática significa el derecho a controlar el uso de los datos de carácter personal y familiar que pueden recogerse y tratarse informáticamente (*habeas*

[28] Díez-Picazo, L. M. (2021). *Los derechos de la vida privada… Op. cit.,* p. 311.

[29] Sentencias del Tribunal Constitucional 96/2012, de 7 de mayo, 254/2000, de 30 de noviembre, y 292/2000, de 30 de noviembre.

[30] Sentencia del Tribunal Supremo 438/2018, de 3 de octubre (Sala de lo Penal, Sección 1.ª).

[31] Sentencia del Tribunal Supremo 634/2019, de 19 de diciembre (Sala de lo Penal, Sección 1.ª), Fundamento de Derecho Décimo.

data); en particular, como señala la doctrina, entre otros aspectos, la capacidad del ciudadano para oponerse a que determinados datos personales sean utilizados para fines distintos de aquel legítimo que justificó su obtención.

También ha perfilado las singularidades del derecho a la protección de datos indicando expresamente que su objeto es más amplio que el del derecho a la intimidad puesto que el derecho fundamental a la protección de datos amplía la garantía constitucional a aquellos de esos datos que sean relevantes para o tengan incidencia en el ejercicio de cualesquiera derechos de la persona, sean o no derechos constitucionales y sean o no relativos al honor, la ideología, la intimidad personal y familiar a cualquier otro bien constitucionalmente amparado. En consecuencia, el objeto de protección del derecho fundamental a la protección de datos que se deriva del artículo 18.4 de la Constitución no se reduce solo a los datos íntimos de la persona, sino a cualquier tipo de dato personal, sea o no íntimo, cuyo conocimiento o empleo por terceros pueda afectar a sus derechos, sean o no fundamentales, porque su objeto no es solo la intimidad individual, que para ello está la protección que el artículo 18.1 de la Constitución otorga, sino los datos de carácter personal. Por consiguiente, también alcanza a aquellos datos personales públicos que, por el hecho de serlo, de ser accesibles al conocimiento de cualquiera, no escapan al poder de disposición del afectado porque así lo garantiza su derecho a la protección de datos.

Dice Díez- Picazo[32] que, en cuanto derecho fundamental, la protección de datos tiene dos facetas: negativamente, impone topes a la recogida de datos por los poderes públicos; y positivamente, permite que el interesado acceda a esos datos y, en su caso, se oponga a su utilización abusiva. En su faceta positiva, la protección de datos comporta, ante todo una facultad de acceso a los datos relativos a uno mismo. Así, haciendo un parangón con la venerable garantía de la libertad personal, se habla de habeas data. La protección de datos implica también una facultad de instar la corrección de aquellos que sean falsos o erróneos, así como la cancelación de aquellos cuya conservación ya no esté legalmente justificada. Y entraña, asimismo, una facultad de oponerse a cualquier utilización abusiva de datos, entendiendo por «abusiva» la utilización para fines distintos de los que justifican la recogida y archivo de la información.

[32] Díez-Picazo, L. M. (2021). *Los derechos de la vida privada… Op. cit.,* pp. 312-313.

4. LOS DERECHOS FUNDAMENTALES DEL ARTÍCULO 18 EN EL ENTORNO DIGITAL

4.1. El derecho a la intimidad en el entorno virtual

Señala Corral Maraver[33] que en los últimos tiempos el desarrollo vertiginoso de las tecnologías de la información y la comunicación ha supuesto un cambio en la configuración del derecho a la intimidad. El entorno digital en el que las personas nos movemos y nos relacionamos en la actualidad ha conseguido derribar los antiguos límites de la intimidad personal y así, por ejemplo, las redes sociales han generado nuevas formas de sociabilización que conllevan hacer públicos datos y hechos de nuestra vida íntima, poniéndolos a disposición de conocidos y extraños. Basta observar cómo las personas interactuamos en las redes sociales, Facebook, Twitter, Instagram…, y compartimos en ellas información, experiencias y múltiples datos personales, ya sea a través de fotos, videos, *gifs*, textos escritos, etc. De esa forma nos relacionamos, alimentamos la propia autoestima y vamos conformado también nuestra identidad, especialmente las personas más jóvenes. La información que se comparte puede ser de diversa índole, pero es frecuente que tenga un carácter íntimo, perteneciente a la vida privada o a la vida cotidiana. Esto se lleva a cabo con total normalidad a menudo a través de perfiles públicos y con acceso libre por cualquier persona que forme parte de la red social correspondiente. De esta forma, lo que antes quedaba relegado a la vida privada y era parte de nuestra intimidad personal ahora es compartido en plataformas con usuarios anónimos y desconocidos.

Dice la autora citada[34] que al margen de las cuestiones sociológicas y psicológicas que estos cambios sociales puedan suscitar, estos provocan numerosas consecuencias en el ámbito jurídico y la más destacada es quizá la proliferación de nuevos riesgos para la intimidad como consecuencia de la generalización del mundo digital y de nuestra sobreexposición al mismo.

Martín Ríos[35] ha dicho que no se prevé en nuestro ordenamiento un derecho fundamental a la intimidad informática que se contemple de manera

[33] Corral Maraver, N. (2020). *Intimidad personal, nuevas tecnologías y derecho penal: viejos conceptos y nuevos problemas*. *Era digital, sociedad y derecho*. Editorial Tirant lo Blanch, p. 139.

[34] Corral Maraver, N. (2020). *Intimidad personal, nuevas tecnologías y derecho penal: viejos conceptos y nuevos problemas... Op. cit*., p. 140.

[35] Martín Ríos, P. (2020). *El alcance del derecho al propio entorno virtual… Op. cit.,* p. 1260.

autónoma y diferenciada. Resulta llamativo que otras manifestaciones concretas de la intimidad, igual de singulares y diferenciadas que esta, como el derecho al secreto de las comunicaciones y el derecho a la inviolabilidad del domicilio, sí cuenten, por el contrario, con tal previsión.

Dentro de este entorno virtual surge la imperiosa necesidad de armonizar la protección jurisdiccional del derecho a la intimidad en el marco de las investigaciones judiciales con la exigencia del ejercicio de la acción penal ante determinados hechos que revisten caracteres de delito, pues, como hemos dicho, el derecho a la intimidad protege un ámbito reservado de la vida de las personas excluido del conocimiento de terceros, sean estos poderes públicos o particulares.

Desde ese punto de vista, se hace necesario delimitar el contenido del derecho a la intimidad dentro de este nuevo entorno virtual, pues como ha señalado el Tribunal Constitucional, en Sentencia 64/2019, de 9 de mayo[36]:

> […] el contenido del derecho a la intimidad no está predeterminado: el art. 18.1 CE «no garantiza una 'intimidad' determinada, sino el derecho a poseerla, a tener vida privada, disponiendo de un poder de control sobre la publicidad de la información relativa a la persona y su familia, con independencia del contenido de aquello que se desea mantener al abrigo del conocimiento público» […].

Siguiendo la doctrina del Tribunal Constitucional y la jurisprudencia del Tribunal Supremo, podemos describir casuísticamente una serie de supuestos que se consideran una injerencia en el ámbito de la vida privada de las personas, desde el punto de vista del derecho al entorno digital, pudiendo distinguirse los siguientes:

- La información que se almacena en un ordenador personal, tal como documentos, carpetas, fotografías o videos. La Sentencia del Tribunal Supremo 463/2019, de 14 de octubre[37] declara que:

> […] el cúmulo de la información que se almacena por su titular en un ordenador personal, entre otros datos sobre su vida privada y profesional (en forma de documentos, carpetas, fotografías, vídeos, etc.), con funciones equiparadas a las de una agenda electrónica, no solo forma parte de este mismo

[36] Sentencia del Tribunal Constitucional 64/2019, de 9 de mayo, Fundamento de Derecho Tercero.

[37] Sentencia del Tribunal Supremo 463/2019, de 14 de octubre (Sala de lo Penal, Sección 1.ª), Fundamento de Derecho Sexto.

ámbito, sino que además a través de su observación por los demás pueden descubrirse aspectos de la esfera más íntima del ser humano […].

Sin embargo, el propio Tribunal Supremo, en la referida sentencia, con cita en la Sentencia 426/2016, de 19 de mayo[38], ha declarado y matizado, en relación al contenido informático encontrado en un despacho perteneciente a un organismo público:

> […] que se trata de un despacho perteneciente a un organismo público, por lo que quienes trabajan en ellos y los utilizan por razón de su trabajo, no pueden tener una pretensión de privacidad que el lugar no les puede proporcionar. Si bien

[38] Sentencia del Tribunal Supremo 426/2016, de 19 de mayo (Sala de lo Penal, Sección 1.ª), Fundamento de Derecho Séptimo: «...Si no hay duda de que los datos personales relativos a una persona individualmente considerados, a que se ha hecho referencia anteriormente, están dentro del ámbito de la intimidad constitucionalmente protegido, menos aún pueda haberla de que el cúmulo de la información que se almacena por su titular en un ordenador personal, entre otros datos sobre su vida privada y profesional (en forma de documentos, carpetas, fotografías, vídeos, etc.) –por lo que sus funciones podrían equipararse a los de una agenda electrónica–, no solo forma parte de este mismo ámbito, sino que además a través de su observación por los demás pueden descubrirse aspectos de la esfera más íntima del ser humano. Es evidente que cuando su titular navega por Internet, participa en foros de conversación o redes sociales, descarga archivos o documentos, realiza operaciones de comercio electrónico, forma parte de grupos de noticias, entre otras posibilidades, está revelando datos acerca de su personalidad, que pueden afectar al núcleo más profundo de su intimidad por referirse a ideologías, creencias religiosas, aficiones personales, información sobre la salud, orientaciones sexuales, etc. Quizás, estos datos que se reflejan en un ordenador personal puedan tacharse de irrelevantes o livianos si se consideran aisladamente, pero si se analizan en su conjunto, una vez convenientemente entremezclados, no cabe duda que configuran todos ellos un perfil altamente descriptivo de la personalidad de su titular, que es preciso proteger frente a la intromisión de terceros o de los poderes públicos, por cuanto atañen, en definitiva, a la misma peculiaridad o individualidad de la persona. A esto debe añadirse que el ordenador es un instrumento útil para la emisión o recepción de correos electrónicos, pudiendo quedar afectado en tal caso, no solo el derecho al secreto de las comunicaciones del art. 18.3 CE (por cuanto es indudable que la utilización de este procedimiento supone un acto de comunicación), sino también el derecho a la intimidad personal (art. 18.1 CE), en la medida en que estos correos o *email*, escritos o ya leídos por su destinatario, quedan almacenados en la memoria del terminal informático utilizado. Por ello deviene necesario establecer una serie de garantías frente a los riesgos que existen para los derechos y libertades públicas, en particular la intimidad personal, a causa del uso indebido de la informática, así como de las nuevas tecnologías de la información [...].

[...] No obstante lo anterior en el caso presente no se trata de despachos, ni ordenadores privados del recurrente sino de los existentes en un organismo público como es la Jefatura Provincial de Tráfico, que no ampara la intimidad que protege el domicilio y quienes trabajan en ellos y los utilizan por razón de su trabajo, no tienen una pretensión de privacidad que el lugar no les puede proporcionar...».

el despacho en un edificio público puede estar restringido a la utilización personal y, en ocasiones, exclusiva de un empleado público, el propio interés público al que está vinculado el inmueble en último término, veta que pueda construirse una expectativa razonable y fundada de absoluta y permanente exclusión de terceros de un lugar cuya cesión es temporal y sujeta a criterios de funcionalidad del servicio.

- Los datos contenidos en una agenda telefónica, el visionado de la pantalla de un teléfono para identificar una llamada entrante, la comprobación de la memoria de un teléfono móvil o el registro de llamadas. La Sentencia del Tribunal Supremo 264/2018, de 31 de mayo[39], con cita en la Sentencia 41/2010, de 26 de enero, ha declarado que existe intervención en el derecho a la intimidad en los supuestos de examen de una agenda telefónica, examen por la policía de la pantalla de un teléfono fijo para identificar una llamada entrante o comprobación de la memoria del aparato. De la misma manera, la Sentencia del Tribunal Constitucional 115/2013, de 9 de mayo, ya había declarado que los datos contenidos en la agenda de un teléfono móvil, es decir, el archivo elaborado por

[39] La sentencia del Tribunal Supremo 264/2018, de 31 de mayo, señala al respecto lo siguiente: «... Una razón más justifica la desestimación del reproche. De acuerdo con la jurisprudencia imperante al tiempo en que se produjo el volcado del teléfono (que, insistimos, se llevó a cabo a presencia de la autoridad judicial, del usuario entonces detenido y de su defensa letrada) los datos obtenidos en el volcado y a los que se refiere el oficio (tanto la agenda telefónica como el contenido de los mensajes) no afectan al secreto de las comunicaciones del investigado, sino al derecho a su intimidad, sin que fuera preciso, en tales supuestos y en todo caso, la previa autorización judicial. La STS 41/2010, de 26 de enero, explica como «la jurisprudencia ha venido considerando que no existe intromisión en el derecho al secreto de las comunicaciones (sino intervención en el derecho a la intimidad) en los supuestos de acceso por la Policía a una carta abierta que el detenido llevaba consigo en el momento de la detención (STC 70/2002, de 3 de abril); examen por la Policía de la pantalla de un teléfono fijo para identificar una llamada entrante o comprobación de la memoria del aparato (STS 3 de marzo de 2000); examen de los mensajes SMS registrados en un teléfono móvil intervenido (SSTS 27 de junio de 2002, 30de noviembre de 2005); examen del registro de llamadas de un teléfono móvil (SSTS 25 de septiembre de 2003, 25 de julio de 2003 y 30 de noviembre de 2005; STC 56/2003, de 24 de marzo).

[...] A todo ello tan solo cabe añadir que la actuación policial se produjo en el contexto de una investigación policial que tenía por objeto la averiguación de un delito de especial gravedad, como es un delito contra la salud pública, que el examen de los teléfonos era una diligencia imprescindible para su esclarecimiento y corroboración de las declaraciones efectuadas, con lo que era necesaria y proporcionada para el lícito fin perseguido, y se encontraba además habilitada legalmente, conforme a los arts. 282 LECr., 11.1 LOFCS, 14 LO 1/1992, de Protección de la Seguridad Ciudadana (Cfr. SSTS de 27 de junio de 2002, 25 de septiembre de 2003 o 30 de noviembre de 2005)...».

el titular de dicho teléfono que recoge una relación de números telefónicos identificados normalmente mediante un nombre, ofrece información que pertenece al ámbito privado de su titular, y, por tanto, entra dentro del ámbito del derecho a la intimidad constitucionalmente protegido en el artículo 18. De manera que el acceso policial a tales datos recogidos en el archivo electrónico o agenda de contactos telefónicos de un terminal móvil constituye una injerencia en el derecho a la intimidad personal, al igual que la apertura de una agenda en soporte de papel y la lectura de los papeles encontrados en ella[40].

- Los dispositivos de almacenamiento masivo. La sentencia del Tribunal Supremo 349/2020, de 4 de junio, ha declarado que, salvo autorización de su titular, el acceso a los dispositivos de almacenamiento masivo de información digital, no solo precisa de una específica autorización judicial habilitante, sino que requiere de una justificación específica que pondere el singular riesgo de afectación del derecho a la intimidad. Y, de la misma manera la Sentencia 311/2020, de 15 de junio, considera que dichos dispositivos son algo más que una pieza de convicción y que el contenido de los mismos contienen datos susceptibles de protección constitucional en el ámbito del derecho a la intimidad.

[40] La Sentencia del Tribunal Constitucional 70/2002, de 3 de abril, resolvió el recurso de amparo contra la Sentencia de la Sala de lo Penal del Tribunal Supremo 835/2001, de 12 de mayo, por la que se condenaba al recurrente de amparo como autor de un delito contra la salud pública. En el curso de una investigación por un delito de tráfico de estupefacientes por parte de las Fuerzas y Cuerpos de Seguridad del Estado, en el momento de la detención del recurrente se le intervinieron junto a otros efectos una agenda que la Guardia Civil leyó e incorporó a la causa. El recurrente de amparo alegó vulneración del derecho a la intimidad en relación con el derecho al secreto de las comunicaciones postales al considerar que la carta intervenida en el momento de su detención en el interior de una agenda fue abierta (desdoblada) y leída por la Guardia Civil sin la pertinente autorización judicial, considerando que se trataba de una comunicación interna y privada, que iba doblada y en el interior de una agenda y que, por ello, su contenido era ajeno a terceros.

El Tribunal Constitucional consideró que la lectura de dicha carta no entraba en el ámbito del derecho al secreto de las comunicaciones, debido a su apariencia externa, ya que no se trataba de una carta sino de unas hojas de papel dobladas en el interior de una agenda. Sin embargo, sí consideró que estábamos en el ámbito del derecho a la intimidad, puesto que lo intervenido en el momento de la detención formaba parte del derecho a la intimidad. Una agenda que el recurrente llevaba consigo y un documento, que no tenía sobre, pero que se encontraba en el interior de la agenda, son objetos pertenecientes al ámbito propio y reservado frente a la acción y el conocimiento de los demás, tanto desde un punto de vista objetivo (atendiendo al contenido de lo intervenido), como desde un punto de vista subjetivo (la protección otorgada al objeto por su titular, en cuanto a la preservación frente a terceros).

Como pone de manifiesto Martín Ríos[41] la exigencia de un auto judicial en que expresamente se autorice para el acceso a dispositivos de almacenamiento masivo pone de manifiesto que se presta una atención especial, distinta, al registro en estos respecto del que se pueda realizar en el resto de objetos presentes en un domicilio. Esta importancia que se atribuye a estos particulares «continentes» también se identifica en la tesis que sostiene que abrir un teléfono móvil para consultar la agenda no es igual que abrir una agenda de papel, dada la amplitud de contenido que aquel puede albergar, pues reflejo de gran parte de nuestra vida privada se encuentra en estos dispositivos, que usamos más como mini ordenadores que como teléfonos tradicionales. En esos aspectos, ciertamente, se aprecia que existe una diferente concepción del valor que ha de darse a los datos contenidos en bienes del «universo digital» frente al que merece aquella información susceptible de albergarse en el «mundo analógico». En definitiva, la importancia que, legal y jurisprudencialmente, se reconoce al propio entorno virtual y a su correlativa protección, los sitúa en un plano superior de reconocimiento frente a la clásica noción del derecho a la intimidad.

- El acceso a las claves de un ordenador o las claves de acceso a las redes sociales. Nuestro Tribunal Supremo, en Sentencia 97/2015, de 24 de febrero, Sala de lo Penal, Sección 1.ª, afirma que un ordenador es un medio idóneo para el ejercicio de la intimidad personal, de manera que para el acceso a su contenido es necesario el consentimiento de su titular o que se den los presupuestos que legalmente habilitan la intromisión. En estos supuestos, el consentimiento inequívoco del acusado facilitando las claves de acceso actúa como verdadera fuente de legitimación y permite la injerencia en el derecho a la intimidad. De la misma manera, cabe citar el Auto del Tribunal Supremo 124/2021, de 18 de febrero[42], por el que se inadmite el recurso de casación formalizado por el recurrente contra la sentencia dictada por la Sala de lo Civil y penal del Tribunal Superior de Justicia de Murcia, y en el que se condenaba al recurrente, entre otros, por un delito de descubrimiento y revelación de secretos. Por la representación del recurrente se

[41] Martín Ríos, P. (2020). *El alcance del derecho al propio entorno virtual… Op. cit.,* pp. 1266 y ss.

[42] Auto del Tribunal Supremo 124/2021, de 18 de febrero (Sala de lo Penal, Sección 1.ª), Fundamento de Derecho Primero.

denunciaba vulneración del derecho a la intimidad con base en el artículo 588 *sexies* a) de la Ley de Enjuiciamiento Criminal, relativo al registro de dispositivos de almacenamiento masivo de información, argumentando el Tribunal Supremo que no había

> […] quiebra alguna de sus derechos fundamentales determinante de la ilicitud de la prueba que se propugna, ni siquiera en relación con la invocada limitación de su consentimiento, puesto que cuando este comunicó sus claves de acceso y autorizó el examen del material informático intervenido se encontraba debidamente asistido de abogado, con lo que se debe descartar que se prestase en un contexto coactivo […] (STS 311/2020, de 15 de junio).

4.2. El derecho al secreto de las comunicaciones en el entorno virtual

En su origen, la Ley de Enjuiciamiento Criminal regulaba en los artículos 579 a 588 las intervenciones postales y telegráficas. Posteriormente, la Ley Orgánica 4/1988, de 25 de mayo, de reforma de la Ley de Enjuiciamiento Criminal en materia de delitos relacionados con la actividad de bandas armadas o de elementos terroristas o rebeldes, modificó el artículo 579 incluyendo en los párrafos segundo a cuarto la intervención de las comunicaciones telefónicas y la observación de las comunicaciones postales, telegráficas y telefónicas. En la actualidad y tras la modificación efectuada por la Ley Orgánica 13/2015, de 5 de octubre, la Ley de Enjuiciamiento Criminal regula en capítulo aparte, en los artículos 579 a 588 la detención y apertura de la correspondencia escrita y telegráfica, regulando en un capítulo específico, el Capítulo V, del Título VIII, en los artículos 588 ter a) a 588 ter m) la interceptación de las comunicaciones telefónicas y telemáticas.

En el curso de las investigaciones judiciales se ha vuelto frecuente la aprehensión física de los dispositivos telefónicos (*smartphone*) o telemáticos (ordenadores) así como como el acceso a su contenido previa resolución judicial motivada. Desde el punto de vista del derecho al secreto de las comunicaciones como integrante del derecho al entorno digital y en relación a los nuevos sistemas de comunicación utilizados, una vez que se ha producido la aprehensión de tales dispositivos en el ámbito de un procedimiento penal, se plantea la determinación de la naturaleza que tiene el contenido de los mensajes de los correos electrónicos, de los sistemas de mensajería instantánea como el SMS (*short message service*, por sus siglas

en inglés), los MMS (*Multimedia Messaging System*), y muy especialmente, de los mensajes enviados por plataformas de comunicación específica como Whatsapp, Telegram o Instagram, al objeto de determinar si forman parte del derecho al secreto de las comunicaciones.

Nuestro Tribunal Supremo ha seguido una línea vacilante en esta materia. Así, la Sentencia 884/2012, de 8 de noviembre catalogaba los mensajes SMS como un correo electrónico y consideraba que entraba de lleno en el contenido de la inviolabilidad de las comunicaciones y participando de la misma naturaleza el MMS (*Multimedia Messaging System*).

Por su parte, la Sentencia del Tribunal Supremo 342/2013, de 17 de abril, aborda directamente la naturaleza del contenido de los mensajes, cuando estos ya han sido abiertos, considerando que los mensajes de correo electrónico, una vez descargados desde el servidor, leídos por el destinatario y almacenados en alguna de las bandejas del programa de gestión, dejan de integrarse en el ámbito propio de la inviolabilidad de las comunicaciones. En este caso, la comunicación ya ha culminado su ciclo y la información contenida en el mensaje es a partir de entonces susceptible de protección por su relación con el ámbito reservado al derecho a la intimidad protegida en el artículo 18.1 de nuestra Constitución, cuya tutela constitucional es evidente, aunque de una intensidad distinta a la reservada para el derecho a la inviolabilidad del domicilio.

Como se ha dicho anteriormente, tanto el Tribunal Supremo como nuestros Tribunales de Justicia, parecen acogerse en los últimos tiempos a la postura de que el examen de los mensajes SMS registrados en un teléfono móvil intervenido entran dentro del ámbito del derecho a la intimidad y no del derecho al secreto de las comunicaciones.

La cuestión tiene gran relevancia jurídica y práctica, pues si consideramos que el contenido de los sistemas de mensajería instantánea afecta al derecho al secreto de las comunicaciones, su interceptación e intervención deberá regirse por la regulación contenida en los artículos 588 ter a) y siguientes de la Ley de Enjuiciamiento Criminal, relativa a la interceptación de las comunicaciones telefónicas y telemáticas. Si, por el contrario, entendemos que el contenido de los sistemas de mensajería instantánea afecta al derecho a la intimidad del artículo 18.1 de la Constitución, la regulación aplicable es la contenida en los artículos 588 *sexies* a) y siguientes, relativos al registro de dispositivos masivos de información.

Ahora bien, lo que sí resulta relevante, es que una vez se ha producido la aprehensión física de uno de estos dispositivos telefónicos o telemáticos, en los mismos pueden existir correos electrónicos o mensajes, en el caso de las plataformas específicas de comunicación, leídos o escuchados, pero

también, se podrían encontrar contenidos no leídos o escuchados. Por ello, en estos casos, la resolución judicial que autorice la medida, no solo ha de recoger los criterios necesarios para el registro de los dispositivos masivos de información contenida en los artículos 588 *sexies* a y ss. (en relación a los correos electrónicos o mensajes leídos u oídos), sino también los criterios necesarios para la interceptación de las comunicaciones (en relación a los registros no leídos u oídos) contenida en los artículos 588 ter a y ss. De esta manera, los derechos afectados serían no solo el derecho a la intimidad, sino, también, el derecho al secreto de las comunicaciones, en ambos casos como integrantes del derecho al entorno digital.

4.3. El derecho a la protección de datos en el entorno virtual

Calaza López[43] ha puesto de manifiesto que la utilización masiva de las nuevas tecnologías de la información y la comunicación conlleva la paralela investigación, inspección y control, de aquellas relaciones donde se presume suficientemente la comisión de ilicitudes, merecedoras de reproche, merced a la prueba tecnológica, prueba especialmente intrusiva, expansiva y silenciosa, que habrá de ser, a su vez sometida a controles estrictos. El acceso, la obtención y la intervención judicial de la información contenida en equipos o dispositivos, sean fijos o móviles, pero en todo caso, pertenecientes al investigado presenta la posible vulneración de sus más elementales derechos fundamentales al honor, intimidad e imagen, libre desarrollo de la personalidad, secreto de las comunicaciones o, en su caso, inviolabilidad de domicilio electrónico, entre otros, de no realizarse con una previa y motivada autorización judicial. La autorización judicial motivada, previa y expresa constituye, pues, una razonable *conditio sine qua non* de la licitud de cualquier aprehensión, acceso o intervención de equipos, dispositivos o instrumentos, fijos o móviles, donde se encuentren datos personales propios de la persona investigada, salvo que medie su consentimiento, toda vez que la invasión en su intimidad y, acaso, en su dignidad es evidente. Ha de tenerse en cuenta, además, que esta motivación judicial debiera ser especialmente intensa cuando su ámbito de actuación sea el informático y/o electrónico, con frecuencia denominado entorno digital, por su alcance global, toda vez que la inspección de los datos contenidos en los equipos

[43] Calaza López, S. (2020). *Tres verdades (material, formal y virtual) y una sola realidad: la prueba electrónica. Derecho probatorio y otros estudios procesales*. Madrid, Ediciones Jurídicas Castillo de Luna, pp. 372 y ss.

y dispositivos de última generación conlleva no solo la entrada en una comunicación o incluso una localización determinadas, así como en su caso, la fiscalización y eventual aprehensión de unas concretas fuentes de prueba tecnológicas, sino toda una intromisión, invasión o intrusión, a la velocidad de la luz, en una indiscriminada y mayúscula cantidad de datos sensibles de las personas.

Considera la autora citada[44] que, sin perjuicio de la preceptiva autorización judicial, previa, motivada y expresa para cualquier invasión en el núcleo duro del derecho al secreto de las comunicaciones telefónicas y telemáticas, han surgido nuevas tesis entorno a aquellos otros datos que se generan, fluyen o afloran en el proceso de las comunicaciones, y pese a su apariencia de neutralidad, resultan muy relevantes, por sí solos o interrelacionados, para avanzar en la investigación de los delitos. Estos novedosos «datos de tráfico o asociados» conceptuados en la Ley de Enjuiciamiento Criminal como aquellos que se generan como consecuencia de la conducción de la comunicación a través de una red de comunicaciones electrónicas, de su puesta a disposición del usuario, así como la prestación de un servicio de la sociedad de información o comunicación telemática de naturaleza análoga, que nos permiten atestiguar, en el marco de una comunicación, extremos tan diversos, heterogéneos y variados como son, entre otros, la localización, la identidad de los interlocutores, la identificación del sistema operativo, el registro o la misma duración de la llamada, inciden, de manera directa en el derechos fundamentales tales como el derecho a la inviolabilidad de las comunicaciones y el derecho a la intimidad, en su dimensión de derecho a la protección de datos o derecho a la autodeterminación informativa.

La dificultad de delimitar, continúa señalando la autora citada, con cierta precisión, cuáles de esos datos están comprendidos en el núcleo del secreto y cuáles en el de la intimidad, ha impulsado a la jurisprudencia a acometer una gráfica distinción entre datos dinámicos, como aquellos originados e interferidos en el desarrollo de una conversación bidireccional interceptada y los datos estáticos como aquellos otros que, aún generados en el proceso de comunicación, quedan incorporados a una base que hace posible su tratamiento automatizado. Se integran en este segundo bloque, según esta misma jurisprudencia, los datos referidos a la identidad de los usuarios y a la identificación de los sistemas, como la información indispensable para la prestación del servicio y, en definitiva, para la facturación.

[44] Calaza López, S. (2020). *Tres verdades (material, formal y virtual) y una sola realidad… Op. cit*., pp. 376 y ss.

En un principio, la doctrina del Tribunal Constitucional y la jurisprudencia del Tribunal Supremo, en una concepción en la actualidad ya superada, partiendo de la Sentencia del Tribunal Europeo de Derechos Humanos de 2 de agosto de 1984 (Caso Malone)[45], situaba la información obtenida a partir de estos datos electrónicos en el ámbito del derecho al secreto de las comunicaciones[46]. La jurisprudencia más reciente, de manera acertada, ha aplicado un criterio restrictivo a la hora de definir el contenido material del derecho al secreto de las comunicaciones proclamado en el artículo 18.3 de la Constitución, situando la información ofrecida por esos datos asociados en el entorno que sería más propio del derecho a la intimidad, en su dimensión del derecho a la protección de datos del artículo 18.4. Así, la Sentencia del Tribunal Supremo 249/2008, de 20 de mayo[47], señala al respecto que:

> «[…] el concepto de datos externos manejado por el TEDH en la tantas veces invocada sentencia del Caso Malone, ha sido *absolutamente desbordado por una noción más amplia, definida por la locución* «datos de tráfico», en cuyo ámbito se incluyen elementos de una naturaleza y funcionalidad bien heterogénea. Y todo apunta a que la mecánica importación del régimen jurídico de aquellos datos a estos otros, puede conducir a un verdadero desenfoque del problema, incluyendo en el ámbito de la protección constitucional del derecho al secreto de las comunicaciones datos que merecen un tratamiento jurídico diferenciado, en la medida en que formarían parte, en su caso, del derecho a la protección de datos o, con la terminología de algún sector doctrinal, del derecho a la autodeterminación informativa (art. 18.4 CE)».

De manera más reciente, la Sentencia del Tribunal Supremo 740/2017, de 16 de noviembre[48], también trata de estos datos de tráfico señalando que:

> «Es cierto que los datos de localización asociados a una llamada telefónica, la identidad de los interlocutores y la duración de la lla-

[45] Sentencia del Tribunal Europeo de Derechos Humanos de 2 de agosto de 1984. Caso Malone contra Reino Unido.

[46] Sentencias del Tribunal Constitucional 114/1984, de 29 de noviembre; 123/2002, de 20 de mayo; 137/2002, de 3 de junio; 281/2006, 9 de octubre. Sentencias del Tribunal Supremo 1231/2003, 25 de septiembre y 1219/2004, 10 de diciembre.

[47] Sentencia del Tribunal Supremo 249/2008, de 20 de mayo (Sala de lo Penal, Sección 1.ª), Fundamento de Derecho Cuarto. En el mismo sentido, Sentencia 55/2007, de 23 de enero (Sala de lo Penal, Sección 1.ª), y 940/2008, de 18 de diciembre (Sala de lo Penal, Sección 1.ª).

[48] Sentencia del Tribunal Supremo 740/2017, de 16 de noviembre (Sala de lo Penal, Sección 1.ª), Fundamento de Derecho Primero.

> mada, no son ajenos a la protección constitucional. Se ha dicho que los formatos digitalizados han traído consigo la generación de datos que, bajo su aparente neutralidad técnica, encierran una más que valiosa información. Y esos datos que afloran durante la comunicación y son susceptibles de registro ulterior permiten, por sí solos o mediante su tratamiento interrelacionado, un conocimiento añadido de aspectos que no son, desde luego, ajenos a la privacidad de los comunicantes. Son datos cuyo interés para la investigación penal puede llegar a ser decisivo. Y pese a no afectar al contenido propiamente dicho de la conversación, proporcionan elementos de juicio de gran utilidad para el conocimiento e investigación de cualquier delito».

Esta última sentencia pone de manifiesto que hay ocasiones en que esa línea entre el espacio abarcado por el derecho al secreto de las comunicaciones y por el derecho a la protección de datos, cuyos respectivos mecanismos de defensa constitucional no son, desde luego, idénticos, no puede definirse con la nitidez deseable, poniendo como ejemplo, el caso en que la información que interesa a la investigación no es la información ya generada por llamadas anteriores, y como tal grabada en archivos automatizados, sino la que se está originando durante el desarrollo de una llamada interceptada en ese mismo momento. Y es aquí, donde la referida sentencia Tribunal Supremo, con cita en la Sentencia 7/2014, de 22 de enero, establece la distinción entre los datos estáticos y los datos dinámicos, señalando lo siguiente: «Este matiz ha sido ya dibujado en algunos precedentes de esta Sala (cfr. STS 7/2014, 22 de enero), referidos a la necesidad de dispensar un tratamiento constitucional diferenciado a los datos estáticos y datos dinámicos, necesidad que parece impuesta por el empleo de la locución…» que se encuentren vinculados a procesos de comunicación, utilizada por el art. 588 ter j) para delimitar los supuestos de exigencia de autorización judicial. A la primera categoría pertenecerían aquellos datos que son generados e interferidos durante el desarrollo de una comunicación bidireccional. En la segunda categoría –datos estáticos– se incluirían aquellos otros que, aun generados a partir de un proceso de comunicación, su interés para la investigación surge cuando esa comunicación ya ha concluido y el dato se ha incorporado a una base que hace posible su tratamiento automatizado. También se integrarían en este segundo bloque sistemático aquellos datos que están referidos a la identidad de los usuarios y a la identificación de los sistemas, como información indispensable para la prestación del servicio y, en definitiva, para la facturación».

Por su parte, la Sentencia del Tribunal Supremo 462/2019, de 14 de octubre[49], a la hora de hablar del derecho al entorno virtual como derecho de nueva generación, dentro del derecho a la protección de datos habla de determinados datos personales y de geolocalización, sin precisar más, por lo que se hace necesario determinar cuáles son estos datos que ahora aparecen protegidos dentro del entorno virtual de individuo y que la doctrina y la jurisprudencia ya han denominado como datos de tráfico.

La Ley de Enjuiciamiento Criminal trata de esos datos en el Capítulo V, del Título V, del Libro II, dentro de la regulación de la interceptación de las comunicaciones telefónicas y telemáticas, en el artículo 588 ter b), al tratar del ámbito de la intervención de las comunicaciones, señalando en el apartado 2 que: «La intervención judicialmente acordada podrá autorizar el acceso al contenido de las comunicaciones y a los datos electrónicos de tráfico o asociados al proceso de comunicación, así como a los que se produzcan con independencia del establecimiento o no de una concreta comunicación…».

Este capítulo finaliza con dos secciones que regulan la incorporación al proceso de datos de tráfico o asociados que se encuentren vinculados al proceso de comunicación, que requerirán siempre autorización judicial, artículo 588 ter j), y los artículos 588 ter k) a 588 ter m) que regulan el acceso a determinados datos de identificación de usuarios o dispositivos que no requieren autorización judicial.

La Ley de Enjuiciamiento Criminal permite diferenciar dos grandes grupos de datos:

1. Los datos electrónicos conservados por los prestadores de servicios o personas que faciliten la comunicación en cumplimiento de la legislación sobre retención de datos[50].

   Los datos que pueden conservarse por estos operadores, al amparo de lo dispuesto en el artículo 3 de la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones se agrupan en seis categorías: datos necesarios para rastrear e identificar el origen

[49] Sentencia del Tribunal Supremo, 462/2019, de 14 de octubre (Sala de lo Penal, Sección 1.ª), Fundamento de Derecho Primero.

[50] Los datos electrónicos conservados por los prestadores de servicios o personas que faciliten la comunicación en cumplimiento de la legislación sobre retención de datos relativos a las comunicaciones electrónicas vienen delimitados e identificados en la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.

de una comunicación; datos necesarios para identificar el destino de una comunicación; datos necesarios para determinar la fecha, hora y duración de una comunicación; datos necesarios para identificar del tipo de comunicación; datos necesarios para identificar el equipo de comunicación de los usuarios o lo que se considera ser el equipo de comunicación; y datos necesarios para identificar la localización del equipo de comunicación

Dentro de estos datos electrónicos podemos, a su vez, hacer las siguientes clasificaciones, partiendo de la regulación contenida en la Ley de Enjuiciamiento Criminal:

- En primer lugar, los datos de tráfico o asociados que están vinculados a la restricción del derecho fundamental al secreto de las comunicaciones. A ellos se refiere el artículo 588 ter b) de la Ley de Enjuiciamiento Criminal cuando señala que «la intervención judicialmente acordada podrá autorizar el acceso al contenido de las comunicaciones y a los datos de tráfico o asociados al proceso de comunicación, así como a los que se produzcan con independencia del establecimiento o no de una concreta comunicación». Es decir, en el marco de una investigación en el que el juez de Instrucción hubiese acordado la interceptación de las comunicaciones, también podrá acordar el acceso a estos datos, de manera que la investigación ha de versar sobre alguno de los delitos a que hace referencia el artículo 588 ter a), en relación con el artículo 579.1 de la Ley de Enjuiciamiento Criminal (delitos dolosos castigados con pena con límite máximo de, al menos, tres años de prisión; delitos cometidos en el seno de un grupo u organización criminal; delitos de terrorismo; o delitos cometidos a través de instrumentos informáticos o de cualquier otra tecnología de la información o la comunicación o servicio de comunicación). En este caso, la resolución judicial ha de pronunciarse sobre la sujeción a los principios de especialidad, idoneidad, excepcionalidad, necesidad y proporcionalidad, no solo de la injerencia en el derecho al secreto de las comunicaciones, sino también de la injerencia en el derecho a la protección de datos.
- En segundo lugar, los datos no vinculados expresamente a una interceptación de las comunicaciones telefónicas y telemáticas, que requieren autorización judicial para su incorporación al proceso judicial. A ellos se refiere el artículo 588 ter j) cuando señala que:
  1. «Los datos electrónicos conservados por los prestadores de servicios o personas que faciliten la comunicación en cum-

plimiento de la legislación sobre retención de datos relativos a las comunicaciones electrónicas o por propia iniciativa por motivos comerciales o de otra índole y que se encuentren vinculados a procesos de comunicación, solo podrán ser cedidos para su incorporación al proceso con autorización judicial. 2. Cuando el conocimiento de esos datos resulte indispensable para la investigación, se solicitará del juez competente autorización para recabar la información que conste en los archivos automatizados de los prestadores de servicios, incluida la búsqueda entrecruzada o inteligente de datos, siempre que se precisen la naturaleza de los datos que hayan de ser conocidos y las razones que justifican la cesión».

Desde esta perspectiva, el acceso a tales datos para su incorporación al proceso judicial no está condicionado a los delitos a los que hace referencia el artículo 588 ter a), en relación con el artículo 579.1 de la Ley de Enjuiciamiento Criminal. La injerencia, en este caso, ha de ajustarse a los requisitos que han ido perfilando tanto el Tribunal Constitucional[51] como la jurisprudencia del Tribunal Supremo, esto es, la existencia de un fin constitucionalmente legítimo, que la medida limitativa del derecho esté prevista en la ley, esto es, el principio de legalidad, que como regla general se acuerde mediante resolución judicial, y finalmente, la estricta observancia del principio de proporcionalidad.

- Finalmente, nos encontramos con un tercer grupo de datos que no requieren autorización judicial, es decir, de datos que no aparecen vinculados a un proceso de comunicación, pero que afectan al derecho a la protección de datos del artículo 18.4 de la Constitución, es decir, el resto de datos de tráfico, no vinculados a procesos de comunicación, entre los que el legislador ha destacado en los artículos 588 ter l) y m), la numeración IMSI e IMEI y los datos de identificación de números telefónicos o los números que corresponden a un titular. El acceso a tales datos por la policía judicial ha de ajustarse a los parámetros establecidos por el Tribunal Supremo y el Tribunal Constitucional, siendo en este caso, en mi opinión aplicable, *mutatis mutandis*, la doctrina del Tribunal Constitucional y la jurisprudencia del Tribunal Supre-

[51] Sentencias del Tribunal Constitucional 173/2011, de 7 de noviembre; y 702/2002, de 3 de abril.

mo relativa a los límites al derecho la intimidad, de manera que la intromisión en el derecho a la protección de datos es legítima en los casos de actuaciones de las Fuerzas y Cuerpos de Seguridad del Estado en el marco de investigaciones que tienen por objeto la averiguación de delitos «graves», y que dicha actuación sea proporcionada, es decir, que dichas intromisiones sean imprescindibles para el esclarecimiento de los delitos, debiendo tener dicha injerencia una habilitación legal[52].

2. Datos conservados por cualquier persona o entidad que pueda poseer estos datos por motivos comerciales o de otra índole.

   Respecto a los otros datos a los que hace referencia el artículo 588 ter j), los conservados por cualquier persona o entidad que pueda poseer estos datos por motivos comerciales o de otra índole, como dice la Circular 2/2019, de la Fiscalía General del Estado, sobre interceptación de comunicaciones telefónicas y telemáticas[53], se incluirían aquí, por ejemplo, los

[52] Siguiendo la Sentencia del Tribunal Constitucional 115/2013, de 9 de mayo, en relación a los datos contenidos en la agenda de contactos de un teléfono móvil, no queda afectado el derecho a la intimidad cuando se dan los siguientes requisitos: 1.º Existencia de un fin constitucionalmente legítimo. Dicho fin existe en los supuestos de interés público propio de la investigación de un delito y descubrimiento del delincuente. A través de este bien se defienden otros tales como la paz social y la seguridad ciudadana (artículo 10.1 y 104 de la Constitución); 2.º Existencia de cobertura legal. Tiene lugar cuando los agentes actúan con el apoyo legal del artículo 282 de la Ley de Enjuiciamiento Criminal, artículo 11.1 de la Ley Orgánica 2/1986, de 13 de marzo, de Fuerzas y Cuerpos de Seguridad del Estado y artículo 14 de la Ley Orgánica 4/2015, de 30 de marzo, de Protección de la Seguridad Ciudadana, que conforman una habilitación legal específica que faculta a las Fuerzas y Cuerpos de Seguridad del Estado para recoger los efectos, instrumentos y pruebas del delito y ponerlos a disposición judicial y para practicar las diligencias necesarias para la averiguación del delito y el descubrimiento del delincuente. Entre estas diligencias se encuentra la de examinar o acceder al contenido de esos instrumentos o efectos, así como a los documentos o papeles que se le ocupen al detenido, realizando un primer análisis de los mismos, siempre que ello sea necesario de acuerdo con una estricta observancia de los requisitos dimanantes del principio de proporcionalidad; 3.º Necesidad de la intervención policial para la averiguación del delito, el descubrimiento de los delincuentes o la obtención de pruebas incriminatorias, siempre que se respete el principio de proporcionalidad. Estas razones de urgencia y necesidad vienen avaladas por la flagrancia del delito, circunstancia que refuerza la necesidad de intervención inmediata de la Policía; 4.º Existencia de proporcionalidad. Es decir, que permita la detención del delincuente, que no exista otra medida más moderada, y que se deriven de dicha medida más beneficios y ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto, dada la naturaleza y gravedad del delito investigado y la leve injerencia que comporta en el derecho a la intimidad del recurrente el examen de la agenda de contactos de su teléfono móvil (juicio de proporcionalidad en sentido estricto).

[53] Circular 2/2019, de la Fiscalía General del Estado, sobre interceptación de comunicaciones telefónicas y telemáticas, publicada en el *Boletín Oficial del Estado* n.º 70, de 22 de marzo de 2019, pp. 30113 y 30114.

> *log* o registros que el administrador de cualquier página web pudiera tener acerca de concretas comunicaciones que se hayan podido desarrollar a través de la misma (identificación de los comunicantes, fecha y hora de la comunicación o contenido de la comunicación, entre otros).

En mi opinión, la regulación de la limitación en el derecho a la protección de datos, desde la perspectiva del derecho al entorno digital, contenida en la Ley de Enjuiciamiento Criminal, con la modificación introducida por la Ley Orgánica 13/2015, resulta imprecisa e induce a cierta confusión, al haber integrado su regulación con el derecho al secreto de las comunicaciones, planteando interrogantes respecto al acceso a esos datos en el curso de las investigaciones judiciales y policiales, desde el punto de vista de la gravedad de los delitos que van a ser objeto de investigación. A mi juicio, hubiese sido deseable que el legislador hubiese regulado en un capítulo diferente la limitación en del derecho a la protección de datos, desde la perspectiva de este entorno virtual.

5. HACIA UN CONCEPTO DEL DERECHO AL ENTORNO DIGITAL

La Sala Segunda de nuestro Tribunal Supremo recogió por primera vez la expresión «entorno virtual» en la Sentencia 342/2013, de 17 de abril[54]. En dicha sentencia se alegaba por la representación de los acusados que el primer auto de entrada y registro al domicilio del interesado no especificaba la autorización de las Fuerzas y Cuerpos de Seguridad del Estado para intervenir los ordenadores, estableciendo la obligatoriedad del presupuesto habilitante de autorización judicial para acceder al contenido de cualquier ordenador, argumentando el Tribunal Supremo lo siguiente:

> «El acceso de los poderes públicos al contenido del ordenador de un imputado, no queda legitimado a través de un acto unilateral de las fuerzas y cuerpos de seguridad del Estado. El ordenador y, con carácter general, los dispositivos de almacenamiento masivo, son algo más que una pieza de convicción que, una vez aprehendida, queda expuesta en su integridad al control de los investigadores. El contenido de esta clase de dispositivos no puede degradarse a la simple condición de instrumento recipiendario de una serie de datos con mayor o menor relación con el derecho a la intimidad de su usuario. En el ordenador coexisten,

[54] Sentencia del Tribunal Supremo 342/2013, de 17 de abril (Sala de lo Penal, Sección 1.ª), Fundamento de Derecho Octavo.

es cierto, datos técnicos y datos personales susceptibles de protección constitucional en el ámbito del derecho a la intimidad y la protección de datos (art. 18.4 de la CE). Pero su contenido también puede albergar –de hecho, normalmente albergará– información esencialmente ligada al derecho a la inviolabilidad de las comunicaciones. El correo electrónico y los programas de gestión de mensajería instantánea no son sino instrumentos tecnológicos para hacer realidad, en formato telemático, el derecho a la libre comunicación entre dos o más personas […]».

[…] En consecuencia, el acceso a los contenidos de cualquier ordenador por los agentes de policía, ha de contar con el presupuesto habilitante de una autorización judicial. Esta resolución ha de dispensar una protección al imputado frente al acto de injerencia de los poderes públicos. Son muchos los espacios de exclusión que han de ser garantizados. No todos ellos gozan del mismo nivel de salvaguarda desde la perspectiva constitucional. De ahí la importancia de que la garantía de aquellos derechos se haga efectiva siempre y en todo caso, con carácter anticipado, actuando como verdadero presupuesto habilitante de naturaleza formal […]».

Y, a continuación, el Tribunal Supremo afirmaba que:

«[…] la ponderación judicial de las razones que justifican, en el marco de una investigación penal, el sacrificio de los derechos de los que es titular el usuario del ordenador, ha de hacerse sin perder de vista la multifuncionalidad de los datos que se almacenan en aquel dispositivo. Incluso su tratamiento jurídico puede llegar a ser más adecuado si los mensajes, las imágenes, los documentos y, en general, todos los datos reveladores del perfil personal, reservado o íntimo de cualquier encausado, se contemplan de forma unitaria. Y es que, más allá del tratamiento constitucional fragmentado de todos y cada uno de los derechos que convergen en el momento del sacrificio, existe un derecho al propio entorno virtual, definiendo, seguidamente, el entorno digital o virtual como «toda la información en formato electrónico que, a través del uso de las nuevas tecnologías, ya sea de forma consciente o inconsciente, con voluntariedad o sin ella, va generando el usuario, hasta el punto de dejar un rastro susceptible de seguimiento por los poderes públicos».

Ya incluso, en el año 2011, el Tribunal Constitucional, en Sentencia 173/2011, de 7 de noviembre[55], sin recoger el concepto de entorno digital o virtual, recordaba la importancia de dispensar protección constitucional al cúmulo de información personal derivada del uso de los instrumentos tecnológicos de nueva generación, describiendo, en primer lugar, una serie de supuestos que suponían injerencia en el derecho a la intimidad tales como la información relativa a la salud física y psíquica de las personas, los datos relativos a la situación económica de una persona, la apertura de una agenda, su examen y la lectura de los papeles que se encuentran en su interior por las Fuerzas y Cuerpos de Seguridad del Estado, o la reseña fotográfica de un detenido respecto de la cual los miembros de las Fuerzas y Cuerpos de Seguridad del Estado están obligados, en principio, al deber de secreto profesional; y, en segundo lugar, haciendo referencia al conjunto de la información que genera el uso de las nuevas tecnologías, en el que estaría comprometido no solo el derecho a la intimidad sino también otros derechos fundamentales, recogiendo la siguiente doctrina:

> «[…] Si no hay duda de que los datos personales relativos a una persona individualmente considerados, a que se ha hecho referencia anteriormente, están dentro del ámbito de la intimidad constitucionalmente protegido, menos aún pueda haberla de que el cúmulo de la información que se almacena por su titular en un ordenador personal, entre otros datos sobre su vida privada y profesional (en forma de documentos, carpetas, fotografías, vídeos, etc.) –por lo que sus funciones podrían equipararse a los de una agenda electrónica–, no solo forma parte de este mismo ámbito, sino que además a través de su observación por los demás pueden descubrirse aspectos de la esfera más íntima del ser humano. Es evidente que cuando su titular navega por internet, participa en foros de conversación o redes sociales, descarga archivos o documentos, realiza operaciones de comercio electrónico, forma parte de grupos de noticias, entre otras posibilidades, está revelando datos acerca de su personalidad, que pueden afectar al núcleo más profundo de su intimidad por referirse a ideologías, creencias religiosas, aficiones personales, información sobre la salud, orientaciones sexuales, etc. Quizás, estos datos que se reflejan en un ordenador personal puedan tacharse de irrelevantes o livianos si se consideran aisladamente, pero si se analizan en su conjunto, una vez convenientemente entremezclados, no cabe duda que configuran todos ellos un perfil altamente descripti-

[55] Sentencia del Tribunal Constitucional 173/2011, de 7 de noviembre, Fundamento de Derecho Tercero.

> vo de la personalidad de su titular, que es preciso proteger frente a la intromisión de terceros o de los poderes públicos, por cuanto atañen, en definitiva, a la misma peculiaridad o individualidad de la persona. A esto debe añadirse que el ordenador es un instrumento útil para la emisión o recepción de correos electrónicos, pudiendo quedar afectado en tal caso, no solo el derecho al secreto de las comunicaciones del art. 18.3 CE (por cuanto es indudable que la utilización de este procedimiento supone un acto de comunicación), sino también el derecho a la intimidad personal (art. 18.1 CE), en la medida en que estos correos o *email*, escritos o ya leídos por su destinatario, quedan almacenados en la memoria del terminal informático utilizado. Por ello deviene necesario establecer una serie de garantías frente a los riesgos que existen para los derechos y libertades públicas, en particular la intimidad personal, a causa del uso indebido de la informática, así como de las nuevas tecnologías de la información […]».

Con posterioridad a estas dos sentencias, podemos destacar diversos pronunciamientos del Tribunal Supremo, que han culminado en la elaboración de este nuevo derecho al entorno digital. La Sentencia 587/2014, de 18 de julio[56], señalaba que «…el contenido del ordenador está íntimamente ligado al derecho fundamental al entorno digital, que a su vez se descompone en los derechos a la inviolabilidad de las comunicaciones, a la intimidad y a la protección de datos». La Sentencia del Tribunal Supremo 786/2015, de 4 de diciembre[57], tras definir el entorno digital como «toda la información en formato electrónico que, a través del uso de las nuevas tecnologías, ya sea de forma consciente o inconsciente, con voluntariedad o sin ella, va generando el usuario, hasta el punto de dejar un rastro susceptible de seguimiento por los poderes públicos», afirmaba la necesidad de que exista una resolución jurisdiccional habilitante para la invasión del derecho al entorno digital de todo investigado; la Sentencia del Tribunal Supremo 489/2018, de 23 de octubre[58], apuntaba la proclamación de un derecho al entorno digital como derecho de nueva generación que justifi-

[56] Sentencia del Tribunal Supremo 587/2014, de 18 de julio (Sala de lo Penal, Sección 1.ª), Fundamento de Derecho Cuarto.

[57] Sentencia del Tribunal Supremo 786/2015, de 4 de diciembre (Sala de lo Penal, Sección 1.ª, Fundamento de Derecho Primero. En el mismo sentido, la Sentencia del Tribunal Supremo 864/2015 de 10 diciembre (Sala de lo Penal, Sección 1.ª), Fundamento de Derecho Séptimo.

[58] Sentencia del Tribunal Supremo, 489/2018, de 23 de octubre, (Sala de lo Penal, Sección 1.ª), Fundamento de Derecho Quinto. En el mismo sentido la Sentencia 462/2019, de 14 de octubre (Sala de lo Penal, Sección 1.ª), Fundamento de Derecho Primero.

ca distintos niveles de protección jurisdiccional, partiendo todo ello de la plurifuncionalidad de los datos que se almacenan en cualquier ordenador y otros dispositivos asimilables por su capacidad de acumular información vinculada a una persona (*smartphone*).

Igualmente, se debe destacar la Sentencia del Tribunal Supremo 723/2018, de 23 de enero[59], que se pronunciaba sobre el alcance de los registros de dispositivos de almacenamiento masivo de información, y, por tanto, con la nueva regulación contenida en los artículos 588 *sexies* a) y b)[60] de la Ley de Enjuiciamiento Criminal llevada a cabo por la Ley Orgánica 13/2015, que también recoge, con cita en la Sentencia 204/2016, el derecho al entorno digital:

> «[…] la razón de ser de la necesidad de esta autorización con carácter generalizado es la consideración de estos instrumentos como lugar de almacenamiento de una serie compleja de datos que afectan de modo muy variado a la intimidad del investigado (comunicaciones a través de sistemas de mensajería, por ejemplo, tuteladas por el art 18 3.º CE, contactos o fotografías, por ejemplo, tuteladas por el art 18 1.º CE que garantiza el derecho a la intimidad, datos personales y de geolocalización, que pueden estar tutelados por el derecho a la protección de datos, art 18 4.º CE). La consideración de cada uno de estos datos de forma separada y con un régimen de protección diferenciado es insuficiente para garantizar una protección eficaz, pues resulta muy difícil asegurar que una vez permitido, por ejemplo, el acceso directo de los agentes policiales a estos instrumentos para investigar da-

[59] Sentencia del Tribunal Supremo 723/2018, de 23 de enero (Sala de lo Penal, Sección 1.ª), Fundamento de Derecho Tercero.

[60] Artículo 588 *sexies* a) de la Ley de Enjuiciamiento Criminal: «1. Cuando con ocasión de la práctica de un registro domiciliario sea previsible la aprehensión de ordenadores, instrumentos de comunicación telefónica o telemática o dispositivos de almacenamiento masivo de información digital o el acceso a repositorios telemáticos de datos, la resolución del juez de instrucción habrá de extender su razonamiento a la justificación, en su caso, de las razones que legitiman el acceso de los agentes facultados a la información contenida en tales dispositivos. 2. La simple incautación de cualquiera de los dispositivos a los que se refiere el apartado anterior, practicada durante el transcurso de la diligencia de registro domiciliario, no legitima el acceso a su contenido, sin perjuicio de que dicho acceso pueda ser autorizado ulteriormente por el juez competente».

Artículo 588 *sexies* b) de la Ley de Enjuiciamiento Criminal: «La exigencia prevista en el apartado 1 del artículo anterior será también aplicable a aquellos casos en los que los ordenadores, instrumentos de comunicación o dispositivos de almacenamiento masivo de datos, o el acceso a repositorios telemáticos de datos, sean aprehendidos con independencia de un registro domiciliario. En tales casos, los agentes pondrán en conocimiento del juez la incautación de tales efectos. Si este considera indispensable el acceso a la información albergada en su contenido, otorgará la correspondiente autorización».

> tos únicamente protegidos por el derecho a la intimidad (por ejemplo, los contactos incluidos en la agenda), no se pueda acceder o consultar también otros datos tutelados por el derecho a la inviolabilidad de las comunicaciones albergados en el mismo dispositivo. Es por ello por lo que el Legislador otorga un tratamiento unitario a los datos contenidos en los ordenadores y teléfonos móviles, reveladores del perfil personal del investigado, configurando un derecho constitucional de nueva generación que es el derecho a la protección del propio entorno virtual.»

Y, más recientemente, la Sentencia del Tribunal Supremo 311/2020, de 15 de junio[61], señalaba lo siguiente:

> «La ponderación judicial de las razones que justifican, en el marco de una investigación penal, el sacrificio de los derechos de los que es titular el usuario del ordenador, ha de hacerse sin perder de vista la multifuncionalidad de los datos que se almacenan en aquel dispositivo. Incluso su tratamiento jurídico puede llegar a ser más adecuado si los mensajes, las imágenes, los documentos y, en general, todos los datos reveladores del perfil personal, reservado o íntimo de cualquier encausado, se contemplan de forma unitaria. Y es que, más allá del tratamiento constitucional fragmentado de todos y cada uno de los derechos que convergen en el momento del sacrificio, existe un derecho al propio entorno virtual. En él se integraría, sin perder su genuina sustantividad como manifestación de derechos constitucionales de *nomen iuris propio*, toda la información en formato electrónico que, a través del uso de las nuevas tecnologías, ya sea de forma consciente o inconsciente, con voluntariedad o sin ella, va generando el usuario, hasta el punto de dejar un rastro susceptible de seguimiento por los poderes públicos. Surge entonces la necesidad de dispensar una protección jurisdiccional frente a la necesidad del Estado de invadir, en las tareas de investigación y castigo de los delitos, ese entorno digital. Sea como fuere, lo cierto es que tanto desde la perspectiva del derecho de exclusión del propio entorno virtual, como de las garantías constitucionales exigidas para el sacrificio de los derechos a la inviolabilidad de las comunicaciones y a la intimidad, la intervención de un ordenador para acceder a su contenido exige un acto jurisdiccional habilitante [...]».

[61] Sentencia del Tribunal Supremo 311/2020, de 15 de junio (Sala de lo Penal (Sección 1.ª), Fundamento de Derecho Tercero. La Sentencia cita al respecto la Sentencia del Tribunal Constitucional 173/2011, de 7 de noviembre y las Sentencias del Tribunal Supremo 864/2015, de 10 de diciembre y 342/2013, de 17 de abril.

Desde el punto de vista doctrinal, Sanchís Crespo[62] considera que el derecho al propio entorno virtual tendría dos firmes anclajes: uno se sustentaría en la necesaria interpretación del artículo 18.4 de la Constitución de acuerdo a un criterio sociológico acorde al tiempo al que vivimos, lo que supone tener en cuenta que el uso de la informática puede ser especialmente lesivo para el derecho a la intimidad de los propios datos conservados privadamente y, por ello, la ley ha de limitar el uso de la informática en estos supuestos y no restringirse tan solo a la protección de los datos personales que se ceden a terceros; y, otro, se encontraría en el desarrollo legislativo acometido por la Ley Orgánica 13/2015, al exigir autorización judicial cuando se trata de acceder al contenido de los dispositivos electrónicos del investigado, afirmando que se trata de la plasmación concreta de esa ley limitadora del uso de la informática.

De este modo, define el derecho al entorno digital que el derecho fundamental que tiene el ciudadano a preservar de intromisiones externas el cúmulo de datos relativos a su propia intimidad que él mismo genera en formato digital, consciente e inconscientemente, mediante su interacción con dispositivos electrónicos.

Arrabal Platero[63], por su parte, señala que, en definitiva, el conjunto del contenido de un dispositivo tecnológico es tan variado y comprende tantos derechos fundamentales tutelables que la jurisprudencia ha creado una nueva garantía constitucional que ampara conjuntamente esta información frente a cualquier acceso ilegítimo de terceros o de poderes públicos a través de la exigencia de previa autorización judicial.

Martín Ríos[64] ha dicho que el derecho al propio entorno virtual o digital es un derecho fundamental de nueva generación, que supera la concepción clásica del derecho a la intimidad y que en él se integraría, sin perder la genuina sustantividad como manifestación de derechos constitucionales de *nomen iuris propio,* toda la información en formato electrónico que, a través del uso de las nuevas tecnologías, ya sea de forma consciente o inconsciente, con voluntariedad o sin ella, va generando el usuario, hasta el punto de dejar un rastro susceptible de seguimiento por los poderes públicos.

Ahora bien, debe señalarse que, si bien el derecho al entorno digital es un derecho de creación jurisprudencial, parece que sí ha tenido acogida ya

---

[62] Velasco Núñez, E. y Sanchís Crespo, C. (2019). *Delincuencia informática. Tipos delictivos e investigación… Op. cit*., p. 268.

[63] Arrabal Platero, P. (2020). *El derecho fundamental al propio entorno virtual y su incidencia en el proceso. Era Digital, Sociedad y Derecho*. Editorial Tirant lo Blanch, p. 436.

[64] Martín Ríos, P. (2020). *El alcance del derecho al propio entorno virtual… Op. cit.,* p. 1262.

por 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. Como dice la Circular 5/2019, de 6 de marzo, de la Fiscalía General del Estado[65], sobre registro de dispositivos y equipos informáticos:

> «[…] Este es el fundamento de la nueva regulación que incorpora la LO 13/2015. El registro de dispositivos de almacenamiento masivo de información o de equipos o sistemas informáticos se regirá ahora por las previsiones que la LECrim contiene para esta clase de diligencias. Resultará innecesario, por lo tanto, plantearse si resulta comprometido el derecho a la intimidad o el secreto de las comunicaciones. La nueva regulación legal encomienda ahora al Juez valorar normalmente con carácter previo, aunque, en algunos supuestos con posterioridad al registro, como se verá, la procedencia de la medida en el caso concreto, teniendo en cuenta que, con ella, como se ha señalado, los poderes públicos accederán a ese entorno virtual constitucionalmente protegido del que es titular el investigado».

Como expresa la STS n.º 786/2015, de 4 de diciembre, «la ponderación judicial de las razones que justifican, en el marco de una investigación penal, el sacrificio de los derechos de los que es titular el usuario del ordenador, ha de hacerse sin perder de vista la multifuncionalidad de los datos que se almacenan en aquel dispositivo». Solo a la hora de motivar específicamente la medida deberá descenderse al análisis particular de los derechos controvertidos, cuyo mayor o menor protagonismo y afectación, determinarán la mayor o menor exigencia de los principios rectores que habrán de presidir la medida.

De acuerdo con la doctrina del Tribunal Constitucional y con los distintos pronunciamientos del Tribunal Supremo, y teniendo en cuenta el concepto dado por la doctrina científica, se puede aventurar, en consecuencia, una definición del derecho al entorno digital o virtual como un derecho constitucional de nueva generación surgido como consecuencia de la irrupción de las nuevas tecnologías en la vida de los ciudadanos, integrado por el derecho a la intimidad, el derecho al secreto de las comunicaciones y el derecho a la protección de datos y, por ello, con distintos niveles de

[65] Circular 5/2019, de 6 de marzo, de la Fiscalía General del Estado, sobre registro de dispositivos y equipos informáticos, publicada en el *Boletín Oficial del Estado* n.º 70, de 22 de marzo de 2019, p. 30162.

protección jurisdiccional y que tiene por objeto preservar de intromisiones externas toda la información que el ciudadano genera en formato digital, de manera consciente e inconsciente, mediante su interacción con dispositivos electrónicos.

6. CONCLUSIÓN

La reforma de la Ley de Enjuiciamiento Criminal llevada a cabo por la Ley Orgánica 13/2015, y la nueva regulación de las medidas de investigación tecnológica limitativas de los derechos reconocidos en el artículo 18 de la Constitución ha supuesto la consagración y limitación en el ámbito del proceso penal del derecho al entorno digital.

La regulación de la intromisión que supone el conocimiento del contenido de los datos de las personas que se contienen en formato electrónico y que está presente en los nuevos dispositivos o en el ciberespacio ha de realizarse de manera unitaria si se quiere llevar a cabo una protección efectiva de esos derechos más elementales del individuo y, por tanto, evitar vulneraciones de los derechos a la intimidad, secreto de las comunicaciones, y protección de datos, lo que justifica el nacimiento de este nuevo derecho como es el derecho al entorno digital.

El derecho al entorno digital es un derecho constitucional de nueva generación surgido como consecuencia de la irrupción de las nuevas tecnologías en la vida de los ciudadanos, integrado por el derecho a la intimidad, el derecho al secreto de las comunicaciones y el derecho a la protección de datos. En la medida que este derecho del individuo al entorno virtual está integrado, por distintos niveles de protección, en cada caso concreto, habrá que estar al derecho fundamental afectado al objeto de determinar el tratamiento y aplicación de las medidas de investigación restrictivas de los mismos introducidas por la Ley Orgánica 13/2015 que, en su caso, van a limitar los mismos.

BIBLIOGRAFÍA

Durán Silva, C. M. (2020). *Los medios de prueba tecnológicos como garantía de la correcta incorporación de las nuevas fuentes de prueba al juicio oral. Derecho probatorio y otros estudios procesales*. Madrid, Ediciones Jurídicas Castillo de Luna.

Bueno de Mata, F. (2020). *El Derecho probatorio ante la cuarta revolución industrial. Derecho probatorio y otros estudios procesales*. Madrid, Ediciones Jurídicas Castillo de Luna.

Fuentes Soriano, O. (2020). *La prueba prohibida aportada por particulares, a la luz de las nuevas tecnologías. Derecho probatorio y otros estudios procesales*. Madrid, Ediciones Jurídicas Castillo de Luna.

Velasco Núñez, E. y Sanchís Crespo, C. (2019). *Delincuencia informática. Tipos delictivos e investigación. Con jurisprudencia tras la reforma procesal y penal de 2015*. Valencia, Editorial Tirant lo Blanch.

Gimeno Sendra, V. *et al*. (2018), *Los Derechos fundamentales y su protección jurisdiccional*. Madrid, Edisofer, S.L.

Díez-Picazo, L. M. (2021). *Los derechos de la vida privada. Sistema de derechos fundamentales*. Valencia, Editorial Tirant lo Blanch.

Corral Maraver, N. (2020). *Intimidad personal, nuevas tecnologías y derecho penal: viejos conceptos y nuevos problemas*. *Era digital, sociedad y derecho*. Editorial Tirant lo Blanch.

Calaza López, S. (2020). *Tres verdades (material, formal y virtual) y una sola realidad: la prueba electrónica. Derecho probatorio y otros estudios procesales*. Madrid, Ediciones Jurídicas Castillo de Luna.

Arrabal Platero, P. (2020). *El derecho fundamental al propio entorno virtual y su incidencia en el proceso. Era Digital, Sociedad y Derecho*. Editorial Tirant lo Blanch.