Los delitos de descubrimiento y revelación de secretos en el ciberespacio. Especial mención a la prueba pericial digital

ÁNGELA CASALS FERNÁNDEZ

Profesora doctora adjunta de Derecho Penal y Derecho Penitenciario
Universidad CEU San Pablo
Doctorada Universidad de Alcalá

RESUMEN

Las nuevas tecnologías e Internet han cambiado la forma en la que las personas nos relacionamos y eso ha llegado también al ámbito jurídico. Las actividades delictivas que pueden cometerse a través de la red o utilizando medios informáticos y electrónicos tienen difícil limitación. En este estudio analizamos los delitos de descubrimiento y revelación de secretos recogidos en el capítulo I del Título X del Libro II del Código Penal, siendo el bien jurídico protegido la intimidad. Finaliza este trabajo con una especial mención a la prueba pericial digital, para poder dar a conocer por un experto perito la información digital empleada por las partes para acreditar la realidad de un hecho durante el proceso judicial.

Palabras clave: *Intimidad, ciberdelitos, ciberespacio, prueba pericial digital.*

ABSTRACT

New technologies and the Internet have changed the way in which people relate to each other, and this has also affected the legal sphere. The criminal activities that can be committed through the network or using computer and electronic means are difficult to limit. In this study, we analyse the crimes of discovery and disclosure of secrets included in Chapter I of Title X of Book II of the Criminal Code, the protected legal right being privacy. This work ends with a special mention of digital expert evidence, *in order to provide an expert witness with the digital information used by the parties to accredit the reality of a fact during the judicial process.*

Key words: *Privacy, cybercrime, cyberspace, digital forensic evidence.*

I. INTRODUCCIÓN

Las tecnologías de la información y la comunicación (TIC), en general, e Internet como red global, en particular, han supuesto la creación de un lugar de comunicación social transnacional, universal y en permanente evolución tecnológica, que ha sido denominado el ciberespacio(1). En la era de la llamada ciber-civilización(2) la sociedad muestra una constante preocupación por conocer el nivel de protección que el

(1) *Cfr.* Vila Lozano, J. (2022): «Protección de datos en el ciberespacio de la Unión Europea: control de contenidos y perfilaciones digitales», en *Revista Aranzadi de derecho y nuevas tecnologías,* núm. 58, p. 1.

(2) *Cfr.* Wiener, N (1958): *Cibernética y sociedad,* (traducción de José Novo Cerro), Editorial Sudamérica, Buenos Aires, p. 15.

Derecho confiere a las víctimas de delitos cometidos a través de medios tecnológicos. De este modo, el Derecho penal no queda extramuros de tipificar delitos cometidos en el mundo cibernético.

Es por ello por lo que cuando hablamos de cibercriminalidad lo realizamos desde un nuevo ámbito o espacio con características estructurales intrínsecas y extrínsecas tan distintas a las del espacio físico en el que se ejecuta la delincuencia tradicional, que nos obliga a una revisión criminológica de la explicación de la actuación delictiva, así como una adaptación de las normas jurídicas(3).

En las últimas décadas, el secreto de las comunicaciones y la protección de datos personales requieren una atención más específica y amplia, para poder responder a esta continua transformación digital. En tal sentido, si bien las TIC constituyen un adelanto ampliamente reconocido, novedoso y favorable en todos los sectores, también existen diversos problemas derivados de los avances tecnológicos.

La STC 70/2002, de 3 de abril, afirmó que «los avances tecnológicos que en los últimos tiempos se han producido en el ámbito de las telecomunicaciones, especialmente en conexión con el uso de la informática, hacen necesario un nuevo entendimiento del concepto de comunicación y del objeto de protección del derecho fundamental, que extienda la protección a esos nuevos ámbitos, como se deriva necesariamente del tenor literal del artículo 18.3 de la Constitución española».

El desarrollo de Internet ha transformado las comunicaciones en términos de velocidad, sencillez y accesibilidad. Desde un mismo dispositivo podemos realizar una llamada telefónica, pero también a través de un servicio de voz *IP;* enviar mensajes; hacer videollamadas; intercambiar correos electrónicos desde diversas cuentas instaladas en una única aplicación gestora; chatear, tanto a través de sistemas de mensajería instantánea como mediante las utilidades de este tipo disponibles en redes sociales o, incluso, intercambiar mensajes con nuestro asesor a través de la propia aplicación bancaria(4). Todo esto provoca amplias funcionalidades comunicativas de la red que ofrecen crecientes y más fáciles posibilidades de interceptar procesos comuni-

(3) *Vid.* Miró Linares, F. (2011): «La oportunidad criminal en el ciberespacio. Aplicación y desarrollo de la teoría de las actividades cotidianas para la prevención del cibercrimen», en *Revista Electrónica de Ciencias Penal y Criminológica,* RECPC 13-07, p. 3. Disponible en: http://criminet.ugr.es/recpc/13/recpc13-07.pdf.

(4) *Cfr.* Ocón García, J. (2022): «La incidencia del conocimiento tecnológico en la delimitación del secreto de las comunicaciones», en Arruego Rodríguez, G. y Pascual Medrano, A. (dir.): *La evidencia científica y tecnológica como recurso jurídico,* Comares, Granada, p. 338.

cativos, pero, también, una mayor exposición a acciones de vigilancia masiva o de recopilación generalizada de datos de tráfico.

Debemos tener en cuenta que el derecho a la intimidad es inherente a la persona, que necesita de espacios libres de intromisiones en su vida individual y familiar, para lograr el pleno desarrollo de su personalidad y su identidad. Todos los seres humanos cuentan con una vida privada, conformada por aquella parte de la vida que no está consagrada a una actividad pública y que no trasciende a la sociedad de manera directa.

Según datos del INE, el número de delitos de descubrimiento y revelación de secretos en el año 2019 fueron un total 484, en 2020 descendió levemente a 421 y en 2021 ascendió a 592(5). Por lo tanto, nos encontramos en un ascenso preocupante de estos delitos.

II. EL DERECHO A LA INTIMIDAD COMO BIEN JURÍDICO PROTEGIDO

El derecho a la intimidad se encuentra reconocido en las declaraciones internacionales de derechos surgidas tras las II Guerra Mundial. Figura en el artículo 12 de la Declaración Universidad de Derechos Humanos de 1948; en el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos de 1966; en el artículo V de la Declaración Americana de Derechos y Deberes del Hombre de 1948; en el artículo 11, incisos 2 y 3, de la Convención Americana de Derechos Humanos de 1969; en el artículo 8, inciso 1, del Convenio Europeo de Derechos Humanos de 1950; y en el artículo 7 de la Carta de los Derechos Fundamentales de la Unión Europea de 2000. El primer texto constitucional en Europa que recogió de forma expresa el derecho a la intimidad fue la Constitución Portuguesa de 1976 en el artículo 26.1 y, posteriormente, lo hizo la Constitución española de 1978.

El derecho a la intimidad, recogido en las Constituciones, tiene su origen en un trabajo doctrinal: *the right to privacy.* Su objetivo era establecer un límite jurídico que vedase las intromisiones de la prensa en la vida privada de las personas; con propósito de dar respuesta a un nuevo fenómeno social, el poder de la prensa. A finales del siglo XIX, los medios de comunicación ejercieron una gran influencia con una

(5) Datos extraídos del INE. Disponible en: https://www.ine.es/jaxiT3/Datos.htm?t=25997

capacidad de entrometerse y lesionar la vida privada desconocida hasta la difusión generalizada de los periódicos(6).

En España, el artículo 18 de la Constitución española garantiza el derecho a la intimidad personal en todas sus manifestaciones. En el apartado primero se recoge la personal, familiar y la propia imagen; en el apartado segundo la inviolabilidad del domicilio; en el apartado tercero el secreto de las comunicaciones; y en el apartado cuarto el uso de la informática.

Debemos tener en cuenta que la privacidad no es equivalente a la intimidad. El primero de los términos, privacidad, significa pertenencia a la esfera de lo privado, es decir, el ámbito de la vida privada que se tiene derecho a proteger de cualquier intromisión. Es lo particular y personal de cada individuo, que se realiza a vista de pocos. El término privado proviene del latín *privatus,* lo que significa privar y está relacionado con la propiedad, propiedad privada, zona privada, uso privado, acceso privado, mensaje privado, reunión privada, todo esto para señalar lo contrario a lo público(7). Por otro lado, la intimidad es un término mucho más restringido y contenido dentro de la esfera general de la vida privada, nos remite a un significado semántico análogo a lo reservado. Lo íntimo es un adjetivo que proviene del latín *intimus* y que alude a lo interior, a lo interno, a lo recóndito, que está en el fondo de algo. Hace referencia a aquello que queremos ocultar de los demás, que queremos preservar sin que se vea(8).

La intimidad es el conjunto de sentimientos, pensamientos e inclinaciones más guardadas en el interior (la ideología, la religión o las creencias), las tendencias personales que afectan a la vida sexual, determinados problemas de salud que se desea mantener en total secreto, u otras inclinaciones, como conductas o hábitos(9). En cuanto a la intimidad personal, la STC 257/1985, de 17 de abril, en su fundamento jurídico segundo, señala que el derecho a la intimidad que reconoce el artículo 18.1 de la Constitución española, por su propio contenido y naturaleza, se refiere a la vida privada de las personas individuales, en la que nadie puede inmiscuirse sin estar debidamente

(6) *Vid.* Dupuy de Repetto, D. S. (2019). *Revelación de imágenes y grabaciones íntimas obtenidas con consentimiento (art. 197.7 CP)*, Tesis doctoral dirigida por Miguel Polaino Navarrete, Universidad de Sevilla, p. 257.

(7) *Vid.* González Porras, A. (2015): *Privacidad en Internet: los derechos fundamentales de privacidad e intimida den Internet y su regulación jurídica. La vigilancia masiva,* Tesis doctoral de la Universidad de Castilla-La Mancha, Toledo, p. 56.

(8) *Ibidem*, p. 57.

(9) *Vid.* Nebrera González, M. (coord.) (2002): *Intimidad y seguridad: dos conceptos y un conflicto,* Associació Isegs per a la Promoció dels Estudis sobre la Governabilitat, Barcelona, p. 17.

autorizado. Por lo tanto, la privacidad está constituida por las facetas que forman la vida personal, frente a la dimensión pública o profesional y la intimidad es lo más interno del sujeto.

El contenido esencial de la intimidad puede identificarse con esa capacidad de decisión respecto a ciertos aspectos para los que se quiera impedir cualquier tipo de intromisión de terceros. Ese contenido, que podemos considerar clásico, de la intimidad ha cambiado como consecuencia de la evolución de las relaciones sociales y el avance de las nuevas tecnologías que han modificado los ámbitos sobre los que ejercer, desarrollar y garantizar el derecho a la intimidad.

La actual sociedad donde se busca desde conocer a otros, o que se nos conozca, o que seamos conocidos o, incluso, cómo seamos conocidos, provoca la necesidad inevitable de facilitar datos o informaciones en cualquiera de los soportes que puedan ser válidos para darlos a conocer, como las redes sociales. Por lo tanto, en este dinámico juego de información, presupuesto de nuestras relaciones sociales, el derecho a la intimidad cobra un nuevo significado. Abandona la dimensión impeditiva de injerencias de terceros, para adquirir una dimensión dinámica y de control de la información personal. Es decir, este derecho a la intimidad se transforma en la facultad de toda persona de controlar qué datos o informaciones pueden conocerse o utilizarse(10).

III. MODALIDADES DELICTIVAS

El Código Penal en el Título X del Libro II titulado «Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio», regula en su Capítulo I «Del descubrimiento y revelación de secretos» recogido en los artículos 197 a 201.

El bien jurídico protegido en estos delitos es la intimidad, como anteriormente hemos mencionado. Además de este bien jurídico genérico, también queda incluido dentro de estos tipos penales, el bien jurídico específico de protección de datos personales especialmente sensibles y que contiene información reservada del sujeto pasivo. La propia reforma operada por la Ley Orgánica 1/2015 ha sugerido esta matización, al entender que la intimidad personal no es el único objeto jurídico de tutela penal de este capítulo.

(10) *Vid.* Sainz-Cantero Caparrós, J. (2021): «Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio (I)», en Morillas Cueva, L. (dir.): *Sistema de Derecho penal. Parte Especial,* Dykinson, Madrid, p. 308.

El contenido de este Título tiene una dimensión pluridimensional, esto se debe a que los atentados a la intimidad afectan a la dignidad o integridad moral de la persona que puede convertirse en objeto de contemplación como una simple cosa si no tiene suficientemente garantizada su intimidad o un ámbito de privacidad en que desarrollarse. También se ve afectada su libertad, toda vez que la intimidad supone un ejercicio de voluntad por el que se fija un ámbito estrictamente propio, íntimo, del que quedan excluidas terceras personas. y ese ámbito propio o personal es el que garantiza la seguridad de toda persona frente a injerencias de terceros, abarcando no solo las injerencias inocuas, sino también las que pudieran ser nocivas o lesivas para la persona(11).

Por un lado, se sanciona el descubrimiento, que hay que entender como el acceso o toma de conocimiento de datos o informaciones voluntariamente excluidos por su titular del conocimiento ajeno o cuyo conocimiento se limita por la autorización de su titular que fija que puede conocerse, quien puede tener tal conocimiento y para qué puede utilizarse tal conocimiento. Y, por otro lado, la revelación, difusión o cesión a terceros de tales conocimientos en lo que supondría una vulneración de la voluntad del control de los datos e informaciones por parte de su titular.

Con la reforma llevada a cabo por la Ley Orgánica 1/2015, de 30 de marzo, se añadió una nueva modalidad delictiva de intrusismo en sistema de información, el llamado *hacking.*

Por lo tanto, el contenido del capítulo I se articula sobre una doble modalidad. Por un lado, los delitos de descubrimiento de secretos o datos reservados (artículos 197.1 y 197.2 del Código Penal). Los delitos de revelación de tales secretos o datos (artículo 197.3 del Código Penal). El artículo 197.4 del Código Penal contempla una modalidad agravada en función del sujeto pasivo. El artículo 197.5 del Código Penal se refiere al núcleo duro de la *privacy(12).* El artículo 197.6 del Código Penal contempla una modalidad agravada en función de la finalidad lucrativa. El artículo 197.7 del Código Penal contempla el *sexting,* ilícito que se añadió en la reforma de 2015 y que, actualmente, ha sufrido una modificación con la Ley Orgánica 10/2022, de 6 de septiembre. Las modalidades específicas se encuentran contempladas en el artículo 199 CP, regulan la revelación de secretos profesionales y

(11) *Ibid.* p. 307.

(12) *Cfr.* Alonso de Escamilla, A. (2022): «Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio» en Lamarca Pérez, C.; Alonso de Escamilla, A.; Mestre Delgado, E., y Rodríguez Núñez, A.: *Delitos. La parte especial del Derecho penal,* 7.ª edición, Dykinson, Madrid, p. 242.

del profesional. Y, por otro lado, los delitos de intrusión en sistema de información (artículos 197 bis y 197 ter).

Se incluye la criminalidad organizada (artículo 197 *quater* del Código Penal); la responsabilidad criminal a personas jurídicas (artículo 197 *quinquies* del Código Penal); el delito especial impropio, siendo el sujeto activo la autoridad o funcionario público (artículo 198 del Código Penal). Además, se recoge una cláusula extensiva referida a la tutela penal de la intimidad de las personas jurídicas (artículo 200 del Código Penal). Y, por último, unas disposiciones comunes respecto a la perseguibilidad de estos delitos (artículo 201 del Código Penal).

1. **Los delitos de descubrimiento y revelación de secretos**

1.1. El apoderamiento para descubrir y la interceptación de las comunicaciones (art. 197.1 CP)

El artículo 197.1 del Código Penal castiga con una pena de prisión de uno a cuatro años y multa de doce a veinticuatro meses al que «para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales, intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación».

El descubrimiento tiene por objeto material del delito, es decir, el ámbito físico sobre el que recae la conducta se divida, por un lado, en formato físico (papeles, cartas o cualesquiera otros documentos o efectos personales). El término documento debe ser interpretado en su acepción amplia, en este sentido, cualquier escrito que ilustra acerca de algún hecho. En cuanto a los efectos personales, debe entenderse todo tipo de bienes, cosas muebles o enseres(13). Por otro lado, en formato electrónico o digital (mensajes de correo electrónico(14) o cualesquiera otros documentos electrónicos). El delito se presenta con tres comportamientos: apoderarse, interceptar o utilizar artificios técnicos.

(13) *Vid.* Lloria García, P. (2013): «Delitos y redes sociales: los nuevos atentados a la intimidad, el honor y la integridad moral. Especial referencia al "*sexting*"». *La Ley Penal*, núm. 105, p. 5.

(14) La primera definición de documento electrónico en España se encuentra en el artículo 3.5 de la Ley 59/2003, de 19 de diciembre, de firma electrónica «se considera documento electrónico la información de cualquier naturaleza en forma electrónica, archivada en un soporte electrónico según un formato determinado y susceptible de identificación y tratamiento diferenciado».

La primera modalidad de conducta, «se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documento», debe realizarse para descubrir los secretos de otro o vulnerar la intimidad(15). Especial mención, a la incorporación, como objeto material, de los mensajes de correo electrónico, consecuencia lógica y necesaria por el avance de la tecnología, y permite incluir también todo tipo de archivos, ficheros o documentos electrónicos, agrupados en la expresión «cualesquiera otros documentos».

Obviamente, la conducta ha de realizarse en todo caso sin consentimiento del titular de las informaciones. Por lo tanto, el consentimiento se recoge como elemento negativo del hecho, por lo que su concurrencia determina la atipicidad de la conducta.

La acción de apoderamiento ha sido interpretada con diversidad de significados, normalmente como la aprehensión u obtención ilícita del objeto material. González Rus(16) señala que «se precisa de alguna actuación material del sujeto activo en relación con el soporte, en virtud de la cual, este entre, siquiera sea por unos instantes, en su esfera de disponibilidad, entendida esta como capacidad para acceder al conocimiento del secreto o información personal reservada que el mismo contiene».

Sin embargo, como se ha señalado en la STS 1391/2000, de 14 de septiembre, y en la más reciente STS 538/2021, de 17 de junio, «el apoderamiento de documentos exigido en el artículo 197 CP, no puede considerarse estrictamente como el apoderamiento físico de los mismos. Basta con su aprehensión virtual, de manera que el sujeto activo del delito se haga con su contenido de cualquier forma técnica que permita su reproducción posterior, como, por ejemplo, mediante su fotografiado». Atendiendo al momento consumativo, la Sala explica en los siguientes términos: «se consuma tan pronto el sujeto activo accede a los datos, esto es, tan pronto los conoce y tiene a su disposición, pues solo con eso se ha quebrantado la reserva que los cubre. Es ello lo que lleva a entender que la norma requiere la existencia de un perjuicio añadido para que la violación de la reserva integre el tipo, un perjuicio que puede afectar al titular de los datos o a un tercero» (SSTS 803/2017, de 11 de diciembre; 312/2019, de 17 de junio; 392/2020, de 15 de julio, y 260/2021, de 22 de marzo, entre otras).

---

(15) *Vid.* Alonso de Escamilla, A.: *op. cit.,* p. 238. En igual sentido, STS 5/2019, de 9 de enero.

(16) *Cfr.* González Rus, J. J. (2005): «Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio», en Cobo del Rosal, M. (coord.): *Derecho penal español. Parte Especial,* Dykinson, Madrid, p. 348.

La segunda modalidad es la interceptación de las telecomunicaciones, como modalidad específica de apoderamiento o de acceso a los datos o informaciones, generalmente interviniendo en canal comunicativo entre emisor y receptor del mensaje o comunicación. La conducta se consumará en el momento en que produzca el apoderamiento o el acceso a la información, cuando se tenga disponibilidad sobre los datos, aunque no se comprendan. Por ello, utilizar un dispositivo de escucha sin acceder al contenido de la conversación sería un supuesto de tentativa(17).

Y, la última modalidad castiga el uso de artificios técnicos que permitan ese acceso a la esfera privada o íntima, ya sea mediante la escucha no consentida de conversaciones, la grabación, transmisión o reproducción de las mismas, o de sonidos e imágenes o cualquier otra señal de comunicación. En relación a las escuchas telefónicas la jurisprudencia se ha pronunciado en numerosas sentencias, siendo relevante la SSTS 2005/1995 y 2954/1995 que establecen doctrina general respecto a la intervención de comunicaciones. Se señalan una serie de requisitos básicos para no vulnerar el derecho fundamental a la intimidad cuando se realizan escuchas bajo autorización judicial. En primer lugar, la proporcionalidad y motivación de la medida. Y, en segundo lugar, se exige especialidad, es decir, la intervención telefónica ha de hacerse para el descubrimiento de delitos concretos y no para propiciar el descubrimiento genérico de posibles infracciones penales(18).

El uso de las nuevas tecnologías permite otras formas de comunicación, por ejemplo, correo electrónico, WhatsApp, Telegram, Skype o cualquier otra red social con mensajería, ha supuesto una revolución en todos los ámbitos creando un nuevo escenario delictual. Surgen dudas acerca de qué aspectos de estas comunicaciones deben ampararse por el secreto de las comunicaciones y cuáles por el derecho a la intimidad(19).

1.2. Los delitos cometidos a través de medios informáticos (art. 197.2 CP)

El artículo 197.2 del Código Penal castiga con una pena de prisión de uno a cuatro años y multa de doce a veinticuatro meses al que «sin estar autorizado, se apodere, utilice o modifique, en perjuicio de ter-

(17) *Vid.* González Rus, J. J. (1999): «Protección penal de sistemas, elementos, datos, informaciones, documentos y programas informáticos», en *Revista Electrónica de Derecho penal y Criminología,* 01-14, p. 1. Disponible en: http://criminet.ugr.es/recpc/recpc_01-14.html.

(18) *Vid.* Alonso de Escamilla, A.: *Op. cit.,* p. 239.

(19) *Vid.* Lloria García, P.: *Op. cit.*p. 6.

cero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado». Y, mismas penas «a quien, sin estar autorizado, acceda por cualquier medio a los mismos y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero».

Este apartado recoge el tipo base de los delitos contra la libertad informática o *habeas data*, derecho de nueva generación que otorga a cada ciudadano el control sobre la información que nos concierne personalmente, para preservar la propia identidad, la dignidad y la libertad, en desarrollo del precepto constitucional que protege la intimidad como derecho fundamental(20).

El bien jurídico protegido es la autodeterminación informática(21), referida en el artículo 18.4 de la Constitución española. Un sector doctrinal considera que en el artículo 197.2 del Código Penal se protegen dos bienes jurídicos. Por una parte, la intimidad del sujeto pasivo, en relación con las conductas de apoderarse, acceder y utilizar los datos. Por otra parte, la integridad de los datos, en relación con los comportamientos de modificar o alterar. Distinción, no obstante, relativa por el hecho de quien pretende modificar o alterar, primero debe acceder, con lo que se habría lesionado también la intimidad en estas modalidades de conducta.

Las acciones nucleares de este apartado son: apoderarse, es decir, la traslación de los datos a otro soporte para su posesión; utilizar, es decir, hacer uso de los datos, emplearlos o aprovecharse de los mismos; modificar, es decir, transformar o cambiar los datos; acceder, es decir, entrar o tener acceso a los datos, en este caso sin tener autorización; y alterar, es decir, dañar o estropear los datos. En todas las modalidades, se sanciona al que ejecuta esa conducta sin estar autorizado, lo que se entiende por algunos autores como un elemento normativo del tipo: realizar la conducta fuera de los casos permitidos por la ley. En sentido contrario, otros autores consideran que se trata de una especial causa de justificación, porque la protección de la intimidad no debe cesar, si no es a causa de un conflicto con otro interés de mayor entidad.

En cuanto al término en perjuicio, según STS 40/2016, de 3 de febrero, no supone que el delito incorpore una finalidad económica. El perjuicio se refiere al peligro de que los datos albergados en las bases de datos protegidas puedan llegar a ser conocidos por personas no autorizadas. El perjuicio se realiza cuando se apodera, utiliza, modi-

(20) *Cfr.* Alonso de Escamilla, A.: *Op. cit.,* p. 239.
(21) *Ibidem.*

fica o accede a un dato protegido con la intención de que su contenido salga del ámbito de privacidad en el que se incluyó en una base de datos. El perjuicio exigido va referido a la invasión de la intimidad y no a la producción de un quebranto económico patrimonial concreto.

Por último, ante la reiteración de conductas que enumera, al sancionar primero al que «se apodere, utilice o modifique en perjuicio de tercero» y, posteriormente, al que «sin estar autorizado, acceda por cualquier medio a los mismos y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero», explica y encuentra la doctrina(22), su diferenciación sistemática en la posición subjetiva del autor en relación con los datos: que esté o no autorizado para acceder a ellos, aunque de estarlo pueda rebasar el nivel de acceso para el que ha sido autorizado. Si bien, con relación a la persona externa al registro, una vez realizado el acceso ilícito son irrelevantes los siguientes comportamientos previstos en el párrafo segundo del artículo197.2 del Código Penal (alterar o utilizar), pues quedarán absorbidos por el primero (acceder), salvo que la prueba de estos últimos sea determinante para establecer el perjuicio al que alude el tipo. En la jurisprudencia de la Sala Segunda del Tribunal Supremo, son escasas las resoluciones que contemplan supuestos similares y solo en relación con mensajería instantánea (STS 544/2016, de 21 de junio; STS 237/2007, de 21 de marzo; STS 377/2018, de 23 de julio). Existen sin embargo, múltiples ejemplos de las Audiencias Provinciales, que contemplan el acceso o la apropiación del dispositivo electrónico personal (desde el que se posibilitaba el acceso a los ficheros; así entre otras: SAP Almería, Sección 2.ª núm. 394/2019, de 7 de octubre ; SAP Madrid, Sección 2.ª núm. 551/2019, de 24 de junio; SAP Tarragona, Sección 4.ª, núm. 222/2019, de 17 de junio; SAP Madrid, Sección 27.ª, 544/2016, de 27 de septiembre; SAP de Burgos, Sección 1.ª, 189/2016, de 13 de mayo; SAP Soria núm. 22/2019, de 21 de marzo).

Respecto de lo que entendemos por dato, la jurisprudencia, STS 374/2020, de 8 julio, relata con sumo detalle de actualización que el contenido y alcance del concepto se encuentra definido en el nuevo Reglamento Europeo sobre Protección de Datos, 2016/679 del Parlamento europeo y del Consejo de 27 de abril, al tener la Unión Europea la competencia para legislar en materia de protección de datos. Su artículo 4.1 delimita el concepto de dato personal en los siguientes términos: «toda información sobre una persona física identificada o identificable (el interesado), indicando a continuación que se considerará persona física identificable toda persona cuya identidad pueda

(22) *Vid.* Sainz-Cantero Caparrós, J.: *Op. cit.,* p. 315.

determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo, un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona». La Directiva de 2016 incluye la misma definición en el artículo 3.

La Sala Segunda en la STS 538/2021, de 17 de junio, ha explicado el concepto de dato de carácter personal de la siguiente manera: «El epigrama dato reservado de carácter personal es un concepto normativo que ha de interpretarse conforme a la legislación protectora de ese derecho de nueva generación consolidado al amparo del artículo 18.4 de la CE, esto es, el derecho a autodeterminación informativa, o lo que es lo mismo, el derecho a conocer y controlar lo que los demás conocen de uno mismo, derecho que adquiere especial pujanza cuando la información que nos afecta se incorpora –en la mayoría de las ocasiones, de forma irreversible– a una red social. De ahí que el concepto de datos personales no pueda ser identificado a efectos penales como dato secreto». Continúa la sentencia exponiendo que «es indudable que una información referida a lo que se ha llamado historia social de una persona, en la que se recogen datos, siendo ciertos, no tienen por qué ser objeto de acceso y conocimiento público en contra de la voluntad de la interesada, pudiendo tener plena cabida en el concepto normativo de dato reservado de carácter personal. No se olvide que los datos que se contienen en el historial de asistencia social de una persona pueden ser incluso datos susceptibles de precipitar una imagen que se proyecta sobre el círculo de la privacidad de cualquier ciudadano. Pueden afectar a la salud, a sus circunstancias familiares o, en fin, a su nivel de pobreza que justifica el ingreso en una casa de acogida. En definitiva, banalizar el impacto que en la privacidad de una persona puede producir la incorporación de esos datos a una red social, con el argumento de que no son secretos o que fueron conocidos hace ya varios años, supondría desproteger a la interesada del derecho que le confiere el artículo 18.4 de la CE».

1.3. La difusión, revelación o cesión de los datos reservados a terceros (art. 197.3 CP)

El artículo 197.3 del Código Penal castiga, en el primer párrafo, con pena de prisión de dos a cinco años «si se difunden, revelan o ceden a terceros los datos o hechos descubiertos o las imágenes captadas a que se refieren los números anteriores». Nos encontramos con un tipo agravado. Para que opere esta cláusula se tiene que haber cometido previamente cualesquiera de las modalidades delictivas a que se refieren los tipos bases del artículo 197.1 y 2 del Código Penal, por lo que esta cláusula agravatoria se comporta como un tipo penal compuesto. Estamos, por tanto, ante un delito especial impropio que solamente podrán realizar como sujetos activos aquellos que previamente hayan cometido alguna de las conductas de los artículos 197.1 y 2 del Código Penal y mixto alternativo (al ser varias las conductas por las que puede cometerse).

El tiempo transcurrido desde que se obtuvo la información que se pretende difundir, esto es, la actualidad o novedad de esta, no es relevante, pues como se afirma en la STS 538/2021, de 17 de junio, «el artículo 197.3 del CP no subordina su aplicación a que la información difundida en perjuicio de la víctima sea de reciente conocimiento». Tampoco varía la pena tanto si hay un solo destinatario como si llega a recibir la información una pluralidad de personas, lo que puede producirse por medio de Internet.

La difusión alude a la transmisión a través de un medio de comunicación, con lo que esta llegaría a un buen número de personas. La revelación va dirigida a un número más reducido de personas, por lo que se trata de una comunicación más controlada. La cesión parece ir referida a la transmisión para que el tercero haga uso de esa información, por lo que el delito suele ir asociado a una contraprestación de tipo económico, que hará aplicable la agravación del artículo 197.6 del Código Penal(23).

En el segundo párrafo del artículo 197.3 del Código Penal se castiga con «penas de prisión de uno a tres años y multa de doce a veinticuatro meses, el que, con conocimiento de su origen ilícito y sin haber tomado parte en su descubrimiento, realizare la conducta descrita en el párrafo anterior». Se tipifica de este modo lo que podríamos denominar un delito de receptación impropio o, es decir, un delito de receptación de datos informáticos(24), cuando el sujeto activo utilice datos provenientes de una fuente delictiva. Se trata de un supuesto común, mixto alternativo, de mera actividad y privilegiado con relación a la pena, teniendo en cuenta que aquí el sujeto activo no ha cometido previamente el delito de descubrir la intimidad.

(23) Sainz-Cantero Caparrós, J.: *Op. cit.,* p. 320.

(24) *Vid.* Quintero Olivares, G. (2016): *Compendio de la parte especial del Derecho penal,* Aranzadi, Cizur Menor, p. 366.

1.4 El apoderamiento para descubrir y la interceptación de las comunicaciones y los delitos cometidos a través de medios informáticos realizados por encargados o responsables o mediante la utilización no autorizada de datos personales de la víctima (art. 197.4 CP)

El artículo 197.4 castiga con una pena de prisión de tres a cinco años los hechos descritos en los apartados 1 y 2 del artículo 197 del Código Penal cuando « a) Se cometan por las personas encargadas o responsables de los ficheros, soportes informáticos, electrónicos o telemáticos, archivos o registros; o b) Se lleven a cabo mediante la utilización no autorizada de datos personales de la víctima».

En primer lugar, el apoderamiento para descubrir y la interceptación de las comunicaciones y los delitos cometidos a través de medios informáticos realizados por encargados o responsables, se trata de un tipo agravado en función del sujeto activo, un delito especial impropio. Se fundamenta la agravación debido a la esfera del dominio profesional del sujeto activo y el tipo conecta con las funciones de los encargados o responsables de los sistemas que prevé la Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales. Otros autores interpretan que estamos ante un supuesto de posición de garante por vía legal de los encargados o responsables de los datos(25). Finalmente, otros autores consideran que el fundamento de la agravación se encuentra en el mayor desvalor de la conducta y del resultado(26).

En segundo lugar, si se lleven a cabo mediante la utilización no autorizada de datos personales de la víctima. Algunos autores entienden que estamos ante un subtipo superfluo, ya que la conducta se superpone con el acceso ilícito y no parece que hubiera ninguna necesidad de incluir este segundo inciso en el precepto, por cuanto el relativo a las personas o responsables de los sistemas ya abarca los supuestos en los cuales se está trabajando con datos personales ajenos. Sin embargo, el verbo típico utilizar puede ser interpretado como usar los mismos sin apoderamiento, en el sentido de aprovechar tales datos(27).

La parte final del artículo 197.4 del Código Penal se refiere a la difusión, cesión o revelado a terceros, con una imposición de penas en su mitad superior. Se trata de un supuesto privilegiado con relación a

(25) *Ibid.*, p. 370.

(26) *Vid.* Carbonell Mateu, J. C. y González Cussac, J. L. (2022): *Derecho penal. Parte Especial,* 7.ª edición, Tirant Lo Blanch, Valencia, p. 523.

(27) *Ibid.*, p. 524.

la pena, tiendo en cuenta que aquí el sujeto activo no ha cometido previamente el delito de descubrir la intimidad. El tipo penal señala que el sujeto tengo conocimiento de su origen ilícito, pero sin haber tomado parte en su descubrimiento. En opinión de algún autor se trataría de una especie de receptación de secretos personales o de intimidad(28).

1.5. Datos sensibles o que afecten a personas especialmente vulnerables (art. 197.5 CP)

El artículo 197.5 del Código Penal se refiere al denominado núcleo duro de la privacidad, es decir, la esfera más sensible, los «datos de carácter personal que revelen la ideología, religión, creencias, salud, origen racial o vida sexual, o la víctima fuere un menor de edad o una persona con discapacidad necesitada de especial protección», imponiéndose las penas previstas en su mitad superior. Son los datos especialmente protegidos recogidos en el artículo 7 de la Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales.

La jurisprudencia ha realizado algunas matizaciones respecto a algunos de los contenidos del núcleo duro de la privacidad. Ejemplo de ello es la STS 302/2008, de 27 de mayo, donde se sostiene que la referencia del artículo 197.5 CP a los datos que revelen la ideología, religión, creencias, salud, origen racial o vida sexual no abarca la investigación ilícita de infidelidades o relaciones sexuales de cualquier índole, sino solamente aquellas que se refieran a la orientación sexual de la víctima, estableciéndose la agravante en función de la discriminación social, lo que es radicalmente distinto de la posible inquietud, ansiedad o desasosiego que pueda producir en una persona el hecho de que se conozcan sus relaciones sexuales.

La relación y distinción entre los preceptos de los apartados 197.2 y 197.5 del Código Penal ha sido señalada por el Tribunal Supremo al resaltar la exigencia de una especial lesividad en orden al dato descubierto para poder situarnos en la agravación del artículo 197.5 CP. Así, para un supuesto de acceso inconsentido a datos personales referidos a la salud, en la STS 171/2021, de 1 de marzo, se ha venido a señalar que «la diferenciación entre uno y otro apartado del artículo 197 CP, radica en la naturaleza de los datos a los que de manera inconsentida y no justificada se accede. Uno, los del artículo 197.2 CP, son datos reservados personales o familiares que se hallen registrados en ficheros o soportes informáticos, en tanto que los del apartado 5 del ar-

(28) *Vid.* Quintero Olivares, G.: *Op. cit.,* p. 371.

tículo 197 CP, trata de datos de carácter personal, obviamente reservados, que revelan la ideología, religión, creencias, salud, origen racial o vida sexual, o respecto de personas necesitadas de especial protección. Se trata de supuestos especialmente graves que cuando afectan a la salud, han de ser interpretados, como tipo agravado, cuando concurra una especial lesividad, dañosidad, en ordena al dato descubierto; o la afectación y concurrencia del daño junto a otros bienes jurídicos».

1.6. El ánimo de lucro (art. 197.6 CP)

El artículo 197.6 del Código Penal contiene una modalidad agravada en función de la finalidad lucrativa, la interposición de un precio por la comisión de algunos de los delitos de revelación o descubrimiento de secretos supone una motivación especialmente rechazable socialmente. La STS 10/2020, de 10 marzo, indica que el legislador ha querido agravar, mediante la aplicación del artículo 197.6 CP, aquellas conductas en las que la vulneración del derecho a la intimidad esté filtrada por un propósito lucrativo.

Como ha señalado Marcos Ayjón(29), «se trata de agravar la penalidad ante las conductas que pretenden sacar provecho del tráfico de datos personales, ya sean actividades más o menos profesionalizadas, con el consiguiente aumento del desvalor del injusto de la conducta y del posible daño al bien jurídico protegido».

Las penalidades en este apartado serán en la mitad superior según las penas previstas en los apartados 1 al 4 del artículo 197 del Código Penal. En el caso de que afecte a datos sensibles, los recogidos en el apartado 6, tendrán pena de prisión de cuatro a siete años.

1.7. El delito de *sexting* (art. 197.7 CP)

El delito de *sexting*(30) se regula en el artículo 197.7 del Código Penal que castiga, en el primer párrafo, con pena de prisión de tres meses a un año o multa de seis a doce meses «el que, sin autorización de la persona afectada, difunda, revele o ceda a terceros imágenes o grabaciones audiovisuales de aquella que hubiera obtenido con su

(29) *Vid.* Marcos Ayjón, M. (2020): *La protección de datos de carácter personal en la justicia penal,* Bosch, Barcelona, p. 450.

(30) Según SSAP de Granada 315/2014, de 5 de junio y 486/2014, de 18 de septiembre, el *sexting* supone el envío de imágenes estáticas (fotografías) o dinámicas (vídeos) de contenido sexual, con mayor o menor carga erótica, entre personas que voluntariamente consienten en ello, formando parte de su actividad sexual que se desarrolla de manera libre.

anuencia en un domicilio o en cualquier otro lugar fuera del alcance de la mirada de terceros, cuando la divulgación menoscabe gravemente la intimidad personal de esa persona».

Según las SSTS 70/2020 y 37/2021, el sujeto activo «es aquel a quien le es remitida voluntariamente la imagen o grabación audiovisual y posteriormente, sin el consentimiento del emisor, quebrantando la confianza en él depositada, la reenvía a terceros, habitualmente con fines sexistas, discriminatorios o de venganza. Este es, además, el criterio de la Circular de la Fiscalía General del Estado 3/2017».

La tipificación de esta conducta supone la introducción de un insólito deber de sigilo para toda la población, convirtiendo a los ciudadanos en confidentes necesarios de los demás respecto de personas que han decidido abandonar sus expectativas de intimidad en relación con grabaciones o imágenes propias que son cedidas voluntariamente a terceros(31).

El artículo alude a contenidos cuya divulgación menoscabe gravemente la intimidad personal. La esfera sexual es, desde luego, una de las manifestaciones de lo que se ha denominado el núcleo duro de la intimidad, pero no es la única. Según la STS 70/2020, de 24 febrero, los requisitos que se establecen son, en primer lugar, la acción debe ser consistente en divulgar imágenes obtenidas con el consentimiento de la víctima en un ambiente privado. En segundo lugar, la imagen o grabación de que se trate debe haber sido remitido voluntariamente por la víctima. En tercer lugar, no exige que se haya realizado en el domicilio, sino que basta con haberse fotografiado o grabado fuera del alcance de la mirada de terceros. En cuarto lugar, se requiere que haya una difusión, revelación o cesión a un tercero, es decir, cualquiera que no entre en el círculo de confianza en el cual se remite la imagen o grabación. En quinto lugar, comete el delito la persona que recibe voluntariamente la fotografía o grabación y que quebranta la confianza que depositó la víctima enviándola o exhibiéndola a terceros. Y, en último lugar, no se exige que sea una divulgación masiva, es suficiente con que se remita a una persona.

Lo que caracteriza a esta conducta es que las imágenes y/o grabaciones, debemos entender tanto los contenidos perceptibles únicamente por la vista, como los que se captan conjuntamente por el oído y la vista y también aquellos otros que, aun no mediando imágenes, pueden percibirse por el sentido auditivo, se obtienen con la anuencia de la persona afectada, sobre la base, generalmente, de una relación de confianza, disponiéndose después de ellas, en perjuicio de la víctima,

(31) *Vid.* Cámara Arroyo, S. (2019): «*Sexting* (art. 197.7 CP)», en Gil Gil, A. y Hernández Berlinches, R. (Coords.): *Cibercriminalidad*, Dykinson, Madrid.

muchas veces por motivos de venganza o despecho, así lo señala la Circular 3/2017.

Tras la reforma introducida por la Ley Orgánica 10/2022, de 6 de septiembre, de garantía integral de la libertad sexual, se amplía el precepto, a través del párrafo segundo, y se considera delictiva la conducta de revelar, difundir o ceder a terceros dichas imágenes por persona distinta del destinatario principal. Es decir, en la primera conducta, el que comete el delito es la persona a la que la víctima envía dichas imágenes o grabaciones, mientras que en la segunda conducta es un tercero que, tras recibirlo del primero, lo difunde o revela a otros, si bien en este caso la pena es considerablemente inferior al ser una pena de multa de uno a tres meses.

En el último párrafo del artículo 197.7 del Código Penal, el legislador ha previsto la imposición de la pena en su mitad superior en tres supuesto. En primer lugar, cuando el responsable fuera el cónyuge o la persona que esté, o haya estado unida a la víctima, por análoga relación de afectividad, aun sin convivencia. Se trata de una inserción que se enmarca dentro del concepto de violencia de género, aunque en este caso particular no se diferencia entre hombres y mujeres como sujetos activos del delito. Por tanto, estamos más bien ante la introducción de un elemento accidental típico por razón de un vínculo específico de parentesco no sanguíneo con base en el vínculo de confianza existente entre aquellos que han mantenido, esto provoca que se elimine la posibilidad de aplicar la agravante de parentesco del artículo 23 del Código Penal. No se exige, sin embargo, convivencia, lo que aleja la justificación de la agravación del concepto de violencia doméstica o intrafamiliar. En segundo lugar, cuando la víctima fuera un menor, en cuyo caso se cometerá también un delito de pornografía infantil, o una persona con discapacidad necesitada de especial protección. Se trata de agravaciones por razón del sujeto pasivo, basadas en un incremento del desvalor de la conducta y del resultado. Por menor de edad debe entenderse a quienes aún no hayan cumplido los dieciocho años y por persona con discapacidad necesitada de especial protección a aquellos que reúnen las características expuestas en el artículo 25 del Código Penal. Y, en tercer lugar, cuando los hechos se hubieran cometido con finalidad lucrativa. Se añade, por tanto, un elemento subjetivo específico que se fundamenta en el mayor desvalor social de la conducta(32).

---

(32) *Vid.* Fernández Nieto, J. (2016): «Reforma del Código Penal: hacia una nueva dimensión de la protección de la víctima en los delitos de *sexting* y *grooming*», en *La Ley*, núm. 863, p. 4.

1.8. El acceso ilícito a los sistemas informáticos y la interceptación de transmisiones no públicas de datos: el vandalismo electrónico (art. 197 bis CP)

Por primera vez el Código Penal regula el acceso a datos y programas contenidos en sistemas informáticos(33) y el mantenimiento dentro de ellos, lo que una parte de la doctrina ha considerado un adelantamiento en la barrera de protección de la intimidad(34). Su justificación se encuentra en la necesidad de limitar y controlar el uso de la informática y los medios que facilita su uso y las posibilidades de uso que abre, para de esta forma dar protección a la intimidad personal, sin olvidarnos del interés por tutelar la seguridad de los sistemas informáticos o la intimidad del domicilio informático. Con coherencia con el carácter de *ultima ratio* del Derecho penal se pretende imponer limitaciones al acceso informático a sistemas de información, o a los medios por los que tales medios normalmente se utilizan de forma que se pueda evitar la realización efectiva de intromisiones ilegítimas en la intimidad ajena. Esta inclusión, en un primer momento, responde al mandato armonizador contenido en la Convención del Consejo de Europa sobre criminalidad informática, de 23 de noviembre de 2001 y a la Decisión Marco 2005/222/JAI, del Consejo, de 24 de febrero de 2005 relativa a los ataques contra los sistemas de información. Con la reforma operada por la Ley Orgánica 1/2015, de 30 de marzo, se realiza una nueva redacción más completa y acorde a las exigencias supranacionales, como consecuencia de las exigencias contenidas en la Directiva 2013/40/UE, de 12 de agosto.

El artículo 197 bis del Código Penal es un tipo penal alternativo que regula el acceso a un sistema informático y también el mantenimiento dentro del mismo, sin consentimiento. El punto primero es conocido como *hacking* (vandalismo informático), allanamiento virtual o intrusismo informático. Estamos ante un delito común y de mera actividad. Nos señala que «el que por cualquier medio o procedimiento, vulnerando las medidas de seguridad establecidas para

(33) La Directiva 2013/40/UE, de 12 de agosto, define sistema de información como todo aparato o grupo de aparatos interconectados o relacionados entre sí, uno o varios de los cuales realizan, mediante un programa, el tratamiento automático de datos informáticos, así como los datos informáticos almacenados, tratados, recuperados o transmitidos por dicho aparato o grupo de aparatos para su funcionamiento, utilización, protección y mantenimiento.

(34) *Vid.* Alonso de Escamilla, A.: *Op. cit.,* p. 244. De igual manera, en Miro Llinares, F. (2010): «Delitos informáticos. *Hacking*. Daños en reforma penal 2010», en Ortiz Ubrina Gimeno, I.: *Memento Experto. Reforma penal,* Ediciones Francis Lefebvre, Madrid.

impedirlo, y sin estar debidamente autorizado, acceda o facilite a otro el acceso al conjunto o una parte de un sistema de información o se mantenga en él en contra de la voluntad de quien tenga el legítimo derecho a excluirlo», consiste, por lo tanto, en el acceso por cualquier medio o procedimiento de forma directa o remota. Se trataría de llevar a cabo un delito de intrusismo informático(35). La conducta no persigue una finalidad concreta, ya que no contempla apoderamiento ni interceptación. El acceso, es decir, penetrar en el sistema o en una parte de este, debe llevarse a cabo sin autorización y vulnerando las medidas de seguridad establecidas. Es difícil contemplar la tentativa, pero no imposible, puesto que el intento de acceso que se ve interceptado por agentes de policía virtuales daría lugar a un delito intentado.

La Circular 3/2017, de 21 de septiembre, de la Fiscalía General del Estado indica que lo que el legislador castiga es el acceso no autorizado que se lleva a efecto desplegando una especial energía criminal, la aplicación del tipo requiere el quebrantamiento de medidas o códigos de seguridad, resultando atípica la intrusión no autorizada en la que no concurra dicha circunstancia. Esta misma Circular indica que tendrá la consideración de medida de seguridad toda aquella que se haya establecido con la finalidad de impedir el acceso al sistema con independencia de que la misma sea más o menos sólida, compleja o robusta y también de que haya sido establecida por el administrador, el usuario, o por el instalador del sistema, siempre que se mantenga operativa como tal medida de seguridad por quien está legitimado para evitar el acceso.

No podemos olvidarnos de que estas conductas pueden llevarse a cabo por los propios encargados o responsables de los sistemas informáticos cuando acceden, intencionadamente, superando barreras de seguridad, a una parte del sistema a la que no se extiende su autorización personal. En estos supuestos podría ser aplicable la circunstancia de agravación de abuso de confianza del artículo 22.6 del Código Penal, si la vulneración de las medidas se ve facilitada por la posición privilegiada que ocupa el agente como usuario del sistema atacado.

Por un lado, se podría dar un concurso medial con el artículo 197.1 y 2 del Código Penal, como igualmente si se produjera el caso de que el acceso ilegal tuviera por objeto el descubrimiento de secretos de empresa (artículo 278 del Código Penal) o se buscara el descubrimiento de secretos oficiales (artículos 598 y siguiente del Código Penal). Por otro lado, cuando para sortear las medidas de seguridad

(35) *Vid.* Tamarit Sumalla, J. (2010): «Delincuencia informática: intrusismo, sabotaje informático y uso ilícito de tarjetas (art. 197.3 y 8, 264 y 248», en *La reforma penal de 2010: análisis y comentarios,* Aranzadi, p. 183.

fuera preciso utilizar datos de carácter personal de la víctima, la aplicación del artículo 197 bis.1 del Código Penal junto con el artículo 197.4.b) del Código Penal supondría una infracción del principio *non bis in idem*, debiendo aplicarse en estos casos este último precepto, por el principio de especialidad establecido en el artículo 8.1 del Código Penal.

La pena de prisión recogida para el punto primero del artículo 197 bis es de seis meses a dos años.

El segundo punto del artículo 197 bis del Código Penal, «el que mediante la utilización de artificios o instrumentos técnicos, y sin estar debidamente autorizado, intercepte transmisiones no públicas de datos informáticos que se produzcan desde, hacia o dentro de un sistema de información, incluidas las emisiones electromagnéticas de los mismos», se refiere a la interceptación ilegal de datos informáticos. Estamos, también, ante un delito común y de mera actividad con los medios tasados: mediante utilización de artificios o instrumentos técnicos. Son objeto de protección las comunicaciones entre dos o más sistemas informáticos, las que tienen lugar entre distintos ordenadores dentro de un mismo sistema o incluso las que median entre una persona y un ordenador. Se incluye la interceptación de transmisiones automáticas entre equipos, no personales(36).

Según la Circular 3/2017 el objeto de protección en este tipo penal es doble. Por un lado, los datos informáticos que se transmiten entre los distintos dispositivos de un sistema, o entre dos o más sistemas, en forma no pública, es decir aquellos datos que queda excluidos del conocimiento por parte de terceros. Por otro lado, se protegen los datos informáticos susceptibles de obtenerse a partir de las emisiones electromagnéticas de un sistema de información.

Cuando se habla del término «no públicas» matiza la naturaleza del proceso de transmisión y no la naturaleza de los datos transmitidos(37). Los datos comunicados pueden ser información que esté accesible al público, pero que las partes quieren comunicar de forma

(36) *Vid.* Marcos Ayjón, M.: *Op. cit.,* p. 453.

(37) En el Anexo II de la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones, una red pública de comunicaciones electrónicas es aquella que «se utiliza, en su totalidad o principalmente, para la prestación de servicios de comunicaciones electrónicas disponibles para el público y que soporta la transferencia de señales entre puntos de terminación de la red» y según el glosario de la Organización Mundial del Comercio «una red no pública es aquella que se utiliza para establecer comunicaciones dentro de una organización o para suministrar esas comunicaciones a organizaciones basándose en una configuración de instalaciones propias o arrendadas» (el término comprende las redes utilizadas por las compañías privadas, las empresas estatales o entidades gubernamentales.

confidencial. Por lo tanto, debemos incluir tanto las redes de área local (*Local Area Network,* LAN), así como las redes locales extensas (*Wide Area Nerwork,* WAN), pero también debemos considerar las redes privadas de carácter virtual (VPN), que son redes establecidas con garantías de privacidad pero que utilizan la infraestructura de la red pública de comunicaciones.

Las emisiones electromagnéticas no pueden ser consideras en sí mismas datos informáticos, pero es posible que los datos puedan ser reconstruidos a partir de dichas emisiones. Es por ello que la interceptación de los datos provenientes de las emisiones electromagnéticas de un sistema informático está incluida como delito.

En definitiva, para que la conducta sea delictiva han de concurrir dos requisitos. En primer lugar, que quien efectúe la interceptación no esté autorizado para ello. Y, en segundo lugar, que la misma se realice utilizando como medios artificios o instrumentos técnicos.

En el supuesto de que la concurrencia se produzca entre la interceptación ilegal del artículo 197 bis.2 del Código Penal y los delitos del artículo 197.1 del Código Penal, el criterio a aplicar será el del concurso de normas, según el principio de absorción. En el supuesto de que la interceptación ilegal concurra con alguna de las conductas ilícitas contempladas en el artículo 197.2 del Código Penal se apreciará un concurso medial.

La penalidad recogida para el punto segundo del artículo 197 bis es de prisión de tres meses a dos años o multa de tres a doce meses.

1.9. La facilitación delictiva (art. 197 ter CP)

La reforma producida con la Ley Orgánica 1/2015 introdujo este delito que tipifica la facilitación, adquisición, importación o la producción de programas informáticos o equipos específicamente diseñados o adaptados para la comisión de estos delitos. Estamos ante un delito común, de peligro abstracto y de intención, toda vez que no requiere ninguna lesión, pero sí un elemento finalista específico, facilitar la comisión de alguno de los delitos a que se refieren los apartados 1 y 2 del artículo 197 o el artículo 197 bis del Código Penal. Podemos considerarlo un cibercrimen en sentido estricto(38).

La Circular 3/2017 indica que los comportamientos objeto de sanción se encuentran definidos de una forma abierta que incluye tanto la elaboración para uso propio, o para distribución a terceros, como la importación, la adquisición, bien sea para uso propio o para la distri-

(38) *Vid.* Gil Gil, A. y Hernández Berlinches, R. (Coords.) (2019): *Cibercriminalidad,* Dykinson, Madrid, p. 167.

bución o entrega a otros u otros y, en general, cualquier forma de puesta a disposición de terceros de estos instrumentos o herramientas. Estamos ante unos actos preparatorios elevados a delitos autónomos y punibles, con un evidente adelantamiento de la intervención penal(39).

En cuanto a los medios concretos a través de los que se cometen las conductas típicas distinguimos entre programas informáticos(40), contraseñas de ordenador, códigos de acceso o datos similares que permitan acceder a la totalidad o a una parte del sistema.

La penalidad para la facilitación delictiva es de prisión de seis meses a dos años o multa de tres a dieciocho meses.

1.10. La criminalidad organizada (art. 197 *quater* CP)

El artículo 197 *quater* CP constituye una modalidad agravada de comisión cuando los hechos se cometan en el seno de organizaciones o grupos criminales, aplicándose las penas superiores respectivamente. Esta previsión supone el cumplimiento al mandato armonizador contenido en la Decisión-Marco 2005/222/JAI del Consejo de Europa de 25 de febrero de 2005, relativa a los ataques contra los sistemas de información, que ha sido sustituida por la Directiva 2013/40/UE del Parlamento Europeo y del Consejo, de 12 de agosto de 2013, relativa a los ataques contra los sistemas de información.

1.11. La responsabilidad de las personas jurídicas (art. 197 *quinquies* CP)

El artículo 197 *quinquies* CP regula la responsabilidad de las personas jurídicas por la comisión de delitos recogidos en los artículos 197, 197 bis y ter del Código Penal, estableciendo una pena de multa de seis meses a dos años, haciendo una remisión expresa al artículo 66 bis del Código Penal, relativo a las penas que corresponden a las personas jurídicas. Concluye el precepto disponiendo la potestad de jueces y tribunales para aplicar las penas de disolución de la persona jurídica, la suspensión de sus actividades, la clausura de sus locales y establecimientos, la prohibición de realizar determinadas actividades, la inhabilitación para obtener determinadas subvenciones o ayudas o

(39) *Vid.* Alonso de Escamilla, A.: *Op. cit.*p 246.

(40) Según la Directiva 2013/40/UE, los programas informáticos sirven para que el sistema de información realice una función. En este caso, debe tratarse de un sistema informático malicioso (*malware, spyware)*, diseñado para infiltrarse, para obtener información o para dañar un dispositivo o sistema de información sin el consentimiento de su propietario.

para disfrutar de determinados beneficios fiscales o sociales o intervención judicial.

1.12. El delito especial impropio (art. 198 CP)

Nos dice el artículo 198 del Código Penal que «la autoridad o funcionario público que, fuera de los casos permitidos por la Ley, sin mediar causa legal por delito, y prevaliéndose de su cargo, realizare cualquiera de las conductas descritas en el artículo anterior, será castigado con las penas respectivamente previstas en el mismo, en su mitad superior y, además, con la de inhabilitación absoluta por tiempo de seis a doce años». Nos encontramos ante un delito especial impropio donde el sujeto activo es la autoridad o funcionario público, que actúa como un particular, fuera del ámbito de sus competencias, prevaliéndose de su cargo. Además, se trata de un supuesto agravatorio al permitir imponer las penas correspondientes en su mitad superior, así como la de inhabilitación absoluta.

No podemos considerarlo una conducta pluriofensiva, toda vez que lo que protege de forma exclusiva es la intimidad y no el correcto funcionamiento de la función pública(41).

1.13. El secreto profesional (art. 199 CP)

El artículo 199 se divide en dos apartados. El primero castiga con pena de prisión de uno a tres años y multa de seis a doce meses «el que revelare secretos ajenos, de los que tenga conocimiento por razón de su oficio o sus relaciones laborales». Y, el segundo, castiga con pena de prisión de uno a cuatro años, multa de doce a veinticuatro meses e inhabilitación especial para dicha profesión por tiempo de dos a seis años al «profesional que, con incumplimiento de su obligación de sigilo o reserva, divulgue los secretos de otra persona».

Nos encontramos ante delitos especiales que solo pueden cometerse por un núcleo determinado de personas, siendo necesario que el secreto se conozca como consecuencia de una determinada relación entre la persona que revela el secreto y el titular de este.

Los dos párrafos presentan similitudes, pero también diferencias. El primero se refiere el Código Penal a la relación laboral y oficio, en

(41) *Vid.* Alonso de Escamilla, A.: *Op. cit.,* p 247. Así como Barreiro, A. J. y Guérez Tricario, P. (2019): «Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio», en *Memento Práctico,* Ediciones Francis Lefebvre, Madrid, p. 1112. También Sanz Delgado, E. y Fernández Bermejo, D. (Coords.), (2021): *Tratado de delincuencia cibernética*, Thomson Reuters Aranzadi, Pamplona, p. 342.

los que el sujeto activo vulnera la obligación de sigilo, por razón de su relación laboral. En el segundo, hace referencia al profesional, respecto del que impone, no una mera obligación de sigilo, sino una obligación de guardar secreto profesional. Este último es una de las bases fundamentales en las que se sustenta el ejercicio de determinadas profesiones(42).

La STC 115/2000, de 5 de mayo, define el secreto profesional, en cuando deber que se impone a determinadas personas. Esta obligación resulta exigible no solo a quien se halla vinculado por una relación estrictamente profesional, sino también a aquellos que, por su relación laboral conviven en el hogar de una persona. En tales casos, es indudable que la observancia del deber de secreto es una garantía de que no serán divulgados datos pertenecientes a la esfera personal y familiar del titular del hogar, con vulneración de la relación de confianza que permitió el acceso a los mismos.

Dentro del secreto profesional, debemos referirnos al quebrantamiento de tal obligación por los denominados confidentes necesarios(43), es decir, los profesionales con especial deber de sigilo. A esta categoría pertenecen los abogados, los procuradores, los médicos, los detectives, los profesionales del sector bancario, los profesionales de la informática, los eclesiásticos y ministros de cultos y los periodistas. Por lo tanto, nos debemos ir a la normativa extrapenal para ver la regulación de cada actividad profesional: al artículo 22 del Estatuto de la Abogacía (Real Decreto 135/2021); el artículo 263 de la Ley de Enjuiciamiento Criminal o el artículo 542.3 de la Ley Orgánica del Poder Judicial, los procuradores, de conformidad con el artículo 38 f del Estatuto General de los Procuradores (Real Decreto 1281/2002); los detectives, según el artículo 8.4 de la Ley de Seguridad privada (Ley 5/2014, de 4 de abril); los sanitarios de cualquier ámbito, en virtud del, entre otros, artículo 16.6 de la Ley 41/2002, 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica; los profesionales del sector bancario según el artículo 82 y 83 de la Ley 10/2014, de 26 de junio, de ordenación, supervisión y solvencia de entidades de crédito; para los profesionales de la informática se encuentra en el artículo 10 de la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carác-

(42) *Cfr.* García Sanz, J. (2005): «El secreto profesional», en *Anales de la Facultad de Derecho,* 22 de diciembre, p. 187.

(43) *Vid.* Mestre Delgado, E. (2001): *La eximente de ejercicio legítimo de un derecho y las causas supralegales de justificación penal,* Edisofer, Madrid, p. 102.

ter persona; para los profesionales de la información se consagra en el artículo 20.1.d) de la Constitución española.

1.14. Cláusula extensiva referida a la tutela penal de la intimidad en las personas jurídicas (art. 200 CP)

El artículo 200 del Código Penal recoge una cláusula extensiva referida a la tutela penal de la intimidad de las personas jurídicas. Nos debemos plantear si las personas jurídicas pueden ser titulares de derechos fundamentales. Al respecto, el Tribunal Constitucional se ha pronunciado, STC 231/1988, de 2 de diciembre, estableciendo que los derechos fundamentales son de carácter personalísimo y están ligados a la existencia del individuo. Por lo tanto, las personas jurídicas no podrían ser titulares del derecho fundamental a la intimidad, es por ello por lo que debemos entender esta cláusula extensiva con relación a la intimidad de terceros o de los miembros integrantes de la persona jurídica(44).

El AAP de Madrid de 28 de abril de 1999 declara que «si bien pudiera plantearse alguna duda en relación con el artículo 200 del Código Penal al referirse esta a datos reservados de las personas jurídicas decir que aunque en este precepto el Código Penal extienda la tutela brindada al derecho a la intimidad de las personas físicas a las jurídicas –frente a conducta de descubrimiento, revelación o cesión de datos reservados pertenecientes a estas últimas– se entiende que solo es posible aplicar dicha cláusula extensiva cuando la conducta consistente en descubrir, divulgar o ceder los secretos o datos reservados pueda afectar a la intimidad personal de terceros o a los propios individuos que forman parte de la correspondiente asociación o fundación. Todo lo anterior se fundamenta en el entendimiento del derecho a la intimidad personal como un bien de naturaleza personal cuya titularidad corresponde exclusivamente a las personas físicas (SSTC 231/1988 y 139/1995). En definitiva, no se trata en el artículo 200 del Código Penal de proteger aquellos secretos de empresa cuyo descubrimiento lesionaría otros bienes jurídicos distintos a la intimidad personal».

Es posible, no obstante, defender que las personas jurídicas tienen derecho a mantener una esfera de reserva y confidencialidad y a preservar datos que les conciernan, y no constituyan estrictamente secreto

(44) *Vid.* Barreiro, A. J. y Guérez Tricario, P.: *Op. cit.,* p. 590; así como Alonso de Escamilla, A.: *Op. cit.,* p. 251.

de empresa(45). El objeto de protección del artículo 200 del Código Penal está constituido por informaciones que no atañen directamente a las personas físicas que componen la persona jurídica (que es un ente autónomo y distinto de estas) ni puede considerarse, propiamente, secreto empresarial(46).

1.15. Condiciones de perseguibilidad (art. 210 CP)

Los delitos comprendidos en este Capítulo que hemos ido desarrollando, y según el artículo 210.1 del Código Penal, «será necesaria denuncia de la persona agraviada o de su representante legal». Por lo tanto, se configuran procesalmente como semipúblicos.

En el segundo punto, y después de la redacción introducida por la modificación de la disposición final sexta punto veintiséis de la Ley Orgánica 8/2021, de 4 junio, de protección integral a la infancia y la adolescencia frente a la violencia, se establece que «no será precisa la denuncia exigida en el apartado anterior para proceder por los hechos descritos en el artículo 198 de este Código, ni cuando la comisión del delito afecte a los intereses generales, a una pluralidad de personas o si la víctima es una persona menor de edad o una persona con discapacidad necesitada de especial protección». Por lo tanto, en todos estos supuestos, el delito se convierte en público.

Y, por último, en el punto tercero hace la referencia al perdón del ofendido y a sus consecuencias con relación a estos delitos, considerando que se «extingue la acción penal sin perjuicio de lo dispuesto en el artículo 130.1.5.º, párrafo segundo». Por lo tanto, tal perdón es causa de extinción de la responsabilidad criminal, aun cuando respecto de menores e incapaces, los Jueces o Tribunales, oído el Ministerio Fiscal, podrán rechazar la eficacia del perdón otorgado por sus representantes.

IV. LA PRUEBA PERICIAL DIGITAL

Después de haber hecho un estudio pormenorizado de los delitos de descubrimiento y revelación de secretos consideramos adecuado hacer una especial mención a la prueba pericial digital, ya que puede

(45) *Cfr.* Gómez Navajas, J. (2008): «La protección de los datos personales en el Código Penal español», en *Revista Jurídica de Castilla y León,* núm. 16, p. 360.

(46) *Vid.* Gómez Navajas, J. (2005): *La protección de los datos personales. Un análisis desde la perspectiva del Derecho penal,* Civitas, Madrid, p. 342.

ser fuente probatoria para estos tipos de delitos cuando se realicen en el ciberespacio.

Utilizo el término digital, toda vez que, lo considerado digital agrupa, en primer lugar, un conjunto de tecnologías del acrónimo SMACIT(47) (redes sociales, movilidad, analítica de datos, computación en la nube y la internet de las cosas); y, en segundo lugar, su utilización intensiva para transformar la relación con los clientes para automatizar completamente las operaciones dentro de la empresa y en su relación con otras o para crear nuevos productos, servicios y modelos de negocio basados en información. Lo digital se refiere así tanto a la tecnología como a los sistemas de información, serían dos caras de la misma moneda(48).

La prueba digital o evidencia electrónica(49) no ha sido descrita por ninguna norma jurídica en España. Debemos irnos a la Decisión 2002/630/JAI del Consejo de Europa, de 22 de julio de 2002, relativa a la creación del programa marco para la cooperación policial y judicial en materia penal, para comprobar que define la prueba electrónica como «la información obtenida a partir de una dispositivo electrónico o medio digital, el cual sirve para adquirir convencimiento de la certeza de un hecho». También define los medios de prueba electrónicos como «los soportes técnicos que recogen la prueba electrónica». Martínez Galindo define la prueba digital como «aquella cuya fuente de obtención radica en los datos producidos en los procesos de comunicación, en la información contenida, almacenada, tratada o transmitida por medios electrónicos o que obra en los soportes técnicos o informáticos, y que dado el carácter efímero y manipulable que tiene, mayor que el de las otras pruebas, debe ser incorporada al proceso mediante un análisis pericial que garantice su integridad y originalidad, que contribuirá a producir un conocimiento probable respecto de las circunstancias de lugar, hecho y autoría(50)».

La prueba digital o evidencia digital implica su necesaria contextualización en el ámbito de las tecnologías de la comunicación e infor-

---

(47) SMACIT significa Social, Mobile, Analytics, Cloud e Internet de las cosas.

(48) *Vid.* Rodríguez, J. R. (2017): «Informática, IT, IS y digital: ¿cuál es la diferencia?» en *Blog de Estudios de Informática, Multimedia y Telecomunicaciones,* p.1. Disponible en: https://blogs.uoc.edu/informatica/informatica-it-is-y-digital-cual-es-la-diferencia/.

(49) *Cfr.* Martínez Galindo, G. (2022): «Problemática jurídica de la prueba digital y sus implicaciones en los principios penales», en *Revista Electrónica de Ciencia Penal y Criminología,* 24-23, p. 6.

(50) *Ibidem.*

mación, este tipo de pericia se realiza por ingenieros informáticos(51). La información que generan las operaciones de informática de carácter delictivo resulta producida, almacenada o transmitida mediante dispositivos o instrumentos digitales(52). Por lo tanto, con carácter general se entiende por prueba informática o evidencia electrónica la referida a la que contiene cualquier tipo de información almacenada o transmitida a través de dispositivos informáticos que tiene la virtualidad de poder acreditar los hechos sobre los que versa el proceso(53).

La ISO/IEC 27042/2015 establece una serie de presupuestos para el análisis e interpretación de las evidencias digitales y proporciona directrices sobre cómo un perito informático puede abordar la evidencia digital en un incidente o en una intervención pericial, desde su identificación (evidencia digital potencial), pasando por su análisis (evidencia digital), hasta que es aceptada como prueba en un juicio (prueba digital).

La Ley de Enjuiciamiento Criminal no regula expresamente el régimen jurídico de la incorporación al proceso de la prueba digital, esto no impide que dicha incorporación al proceso esté exonerada de la observación más elemental de la denominada disciplina de prueba y, muy especialmente, de la posibilidad de contradecir por parte del inculpado las supuestas evidencias digitales que pudieran obrar en su contra. Por lo tanto, el peritaje informático de parte se constituye en el garante de uno de los derechos fundamentales más importantes en el orden penal como es el de la presunción de inocencia consagrado en el artículo 24 de la Constitución española.

En los supuestos de análisis de evidencias digitales, el acceso a la información contenida en estos instrumentos queda sometido a la extensión previa y vinculante de una autorización judicial específica. Debemos recordar que en STC 173/2011, de 7 de noviembre, se expresa la importancia de dispensar protección al cúmulo de la información deriva del uso de los instrumentos tecnológicos, «si no hay duda de que los datos personales relativos a una persona individualmente considerados, 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 funcio-

(51) *Vid.* De Aguilar Gualda, S. (2019): La prueba digital en el proceso judicial: ámbito civil y penal, Bosch, Barcelona, p. 125.

(52) *Cfr.* González Reyes, J. M. (2021): «La prueba pericial digital y la cadena de custodia», en *Anales de la Facultad de Derecho,* núm. 38, p. 44.

(53) *Ibid.*, p. 45.

nes 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 artículo 18.3 de la Constitución española (por cuanto es indudable que la utilización de este procedimiento supone un acto de comunicación), sino también el derecho a la intimidad personal (artículo 18.1 de la Constitución española), 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».

Por otro lado, debemos tener en cuenta el artículo 588.c) de la Ley de Enjuiciamiento Criminal que establece que el juez fijará las condiciones para asegurar la integridad de los datos y las garantías de su preservación, pero no se especifica en qué modo se debe proceder al acceso de la información para preservar los datos contenidos en los dispositivos intervenidos. Además, se deben asegurar las garantías que permiten preservar la cadena de custodia para que no se tenga duda acerca de la identidad e integridad de los dispositivos intervenidos y de las copias que se efectúen. Se debe acreditar que se realicen las periciales oportunas que acrediten que no ha habido ninguna manipulación no autorizada judicialmente.

Aunque en principio la prueba pericial informática pueda parecer una prueba pericial más, dado que no tiene un tratamiento procesal diferenciado con respecto a las otras, lo cierto es que ostenta un carácter especial. Esta singularidad deriva de las características particulares de las fuentes de prueba digitales, especialmente su volatilidad y su facilidad de replicación y alteración, que las distingue del resto de fuentes de prueba utilizadas en otro tipo de pericias y, en particular, de las fuentes de prueba documentales(54). La prueba pericial alcanza relevancia por sus aspectos técnicos y especialmente complejos como es el ámbito informático.

Para que la prueba o evidencia digital pueda alcanzar relevancia en sede judicial, se requiere cumplir las siguientes características: verificable (se debe poder comprobar la veracidad de las conclusiones extraídas a partir de la realización del análisis); reproducible (se deben poder reproducir en todo momento las pruebas realizadas durante el proceso); documentada (de manera comprensible y detallada); independiente (las conclusiones obtenidas deben ser las mismas, independientemente de la persona que realice el proceso y de la metodología utilizada); auténtica (debe ser verídica y no haber sufrido manipulación alguna, garantizando y asegurando para ello su total integridad); completa (debe representar la prueba desde un punto de vista objetivo y técnico, sin valoraciones personales, ni prejuicios); creíble (debe ser comprensible por los órganos judiciales profanos en la materia); y, finalmente, confiable (las técnicas utilizadas para su obtención no deben generar ninguna duda sobre su veracidad y autenticidad)(55).

En lo que respecta al objeto de la pericia informática se centra en el análisis de los equipos intervenidos o dispositivos de almacenamiento. Unas veces se realiza para concretar el tipo penal que se persigue, así lo expone la STS 1102/2007, de 21 de diciembre. Otras veces se pretende conocer la autoría del delito. Así, las fases y elementos básicos que componen todo análisis forense digital son la identificación del hecho tratado y su entorno; la recopilación de evidencias; la preservación de evidencias; el análisis de la evidencia; la contextualización de la evidencia; y la documentación y presentación de los resultados. Con todo ello el perito informático forense elaborará el informe pericial que presentará ante el tribunal(56).

Y, por último, en cuanto a la valoración de la prueba digital rige la previsión del artículo 741 de la Ley de Enjuiciamiento Criminal refe-

---

(54) *Vid.* Dolz Lago, M. J. (dir.); Figueroa Navarro, C; (coord.) (2012): *La prueba pericial científica*, Edisofer, Madrid, p. 201.

(55) *Cfr.* González Reyes, J. M. (2021): *Op. cit.,* p. 65.

(56) *Vid.* Ocón García, J.: *Op. cit.,* p. 340.

rente a la «íntima convicción o apreciación en conciencia» del juzgador a la relevancia de la evidencia digital. y en relación con ello, el artículo 726 del mismo texto legal concreta que «el Tribunal examinará por sí mismo los libros, documentos, papeles y demás piezas de convicción que puedan contribuir al esclarecimiento de los hechos o a la más segura investigación de la verdad», términos extensivos a cualquier clase de soporte o evidencia digital.

V. CONCLUSIONES

El Tribunal Constitucional (STC 143/1999, de 9 de mayo) ha declarado que el derecho a la intimidad implica la existencia de un ámbito propio y reservado frente a la acción y el conocimiento de los demás, necesario, según las pautas de nuestra cultura, para mantener una calidad mínima de vida humana. Las innovaciones tecnológicas han remodelado el sistema de comunicaciones afectando, entre otros, a uno de los derechos fundamentales, la intimidad. Ejemplo de ello son las redes sociales que sirven, ante todo, como canal de exposición o comunicación de la propia intimidad, a través de fotos, vídeos, información sobre gustos, actividades, aunque obviamente también operan como vehículo de difusión de lo que puede afectar a la intimidad de terceros no usuarios que no hayan prestado su consentimiento a dicha exposición. Es por ello por lo que se ha realizado un análisis detallado de las modalidades delictivas recogidas en los delitos de descubrimiento y revelación de secretos, donde se entrelazan delitos de esta naturaleza cometidos en el ciberespacio, recogidos en los artículos 197, 197 bis, 197 ter, 197 *quater*, 197 *quinquies*, 198, 199, 200 del Código Penal, finalizando con el artículo 200, la cláusula extensiva referida a la tutela penal de la intimidad de las personas jurídicas.

La preocupación por la cibercriminalidad, realizada desde un nuevo espacio con características estructurales intrínsecas y extrínsecas tan distintas a las del espacio físico en el que se ejecuta la delincuencia tradicional, nos obliga a hacer una especial mención a la prueba pericial digital, ya que se considera una prueba frágil, al poder modificarse o desaparecer con relativa facilidad, además de ser fácilmente manipulable. Se comprueba una falta de cobertura legal específica que determine en el proceso penal la incorporación de la evidencia digital como medio de prueba, por su dificultad en la obtención, conservación e incorporación al proceso penal, lo que puede incidir en la aplicación de la norma penal y la determinación de la culpabilidad.

La sociedad digital o ciber-civilización demanda, cada vez más, soluciones a las ilicitudes y problemas judiciales en los escenarios digitales, es por ello por lo que debemos seguir perfilando tanto la normativa penal como los mecanismos para poder acreditar los nuevos escenarios delictivos cibernéticos que cada año se incrementan.

VI. BIBLIOGRAFÍA

Alonso de Escamilla, A. (2022): «Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio» en Lamarca Pérez, C.; Alonso de Escamilla, A.; Mestre Delgado, E., y Rodríguez Núñez, A.: *Delitos. La parte especial del Derecho penal,* 7.ª edición, Dykinson, Madrid.

Barreiro, A. J. y Guérez Tricario, P. (2019): «Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio», en *Memento Práctico,* Ediciones Francis Lefebvre, Madrid.

Cámara Arroyo, S. (2019): «*Sexting* (art. 197.7 CP)», en Gil Gil, A. y Hernández Berlinches, R. (Coords.): *Cibercriminalidad*, Dykinson, Madrid.

Carbonell Mateu, J. C.; González Cussac, J. L. (2022): *Derecho penal. Parte Especial,* 7.ª edición, Tirant Lo Blanch, Valencia.

De Aguilar Gualda, S. (2019): *La prueba digital en el proceso judicial: ámbito civil y penal*, Bosch, Barcelona.

Dupuy de Repetto, D. S. (2019). *Revelación de imágenes y grabaciones íntimas obtenidas con consentimiento (art. 197.7 CP)*, Tesis doctoral dirigida por Miguel Polaino Navarrete, Universidad de Sevilla.

Fernández Nieto, J. (2016): «Reforma del Código Penal: hacia una nueva dimensión de la protección de la víctima en los delitos de *sexting* y *grooming*», en *La Ley*, núm. 863.

Dolz Lago, M. J. (dir.); Figueroa Navarro, C; (coord.) (2012): *La prueba pericial científica*, Edisofer, Madrid.

García Sanz, J. (2005): «El secreto profesional», en *Anales de la Facultad de Derecho,* 22 de diciembre.

Gil Gil, A. y Hernández Berlinches, R. (Coords.) (2019): *Cibercriminalidad,* Dykinson, Madrid.

Gómez Navajas, J. (2008): «La protección de los datos personales en el Código Penal español», en *Revista Jurídica de Castilla y León,* núm. 16.

— (2005): La protección de los datos personales. Un análisis desde la perspectiva del Derecho penal, Civitas, Madrid.

González Porras, A. (2015): *Privacidad en Internet: los derechos fundamentales de privacidad e intimida den Internet y su regulación jurídica. La vigilancia masiva,* Tesis doctoral de la Universidad de Castilla-La Mancha, Toledo.

González Reyes, J. M. (2021): «La prueba pericial digital y la cadena de custodia», en *Anales de la Facultad de Derecho,* núm. 38.

González Rus, J. J. (2005): «Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio», en Cobo del Rosal, M. (coord.): *Derecho penal español. Parte Especial,* Dykinson, Madrid.

— (1999): «Protección penal de sistemas, elementos, datos, informaciones, documentos y programas informáticos», en *Revista Electrónica de Derecho penal y Criminología,* 01-14, p. 1. Disponible en: http://criminet.ugr.es/recpc/recpc_01-14.html.

Lloria García, P. (2013): «Delitos y redes sociales: los nuevos atentados a la intimidad, el honor y la integridad moral. Especial referencia al "*sexting*"». *La Ley Penal*, núm. 105.

Marcos Ayjón, M. (2020): La protección de datos de carácter personal en la justicia penal, Bosch, Barcelona.

Martínez Galindo, G. (2022): «Problemática jurídica de la prueba digital y sus implicaciones en los principios penales», en *Revista Electrónica de Ciencia Penal y Criminología,* 24-23.

Mestre Delgado, E. (2001): *La eximente de ejercicio legítimo de un derecho y las causas supralegales de justificación penal,* Edisofer, Madrid.

Miró Linares, F. (2011): «La oportunidad criminal en el ciberespacio. Aplicación y desarrollo de la teoría de las actividades cotidianas para la prevención del cibercrimen», en *Revista Electrónica de Ciencias Penal y Criminológica,* RECPC 13-07, p. 3. Disponible en: http://criminet.ugr.es/recpc/13/recpc13-07.pdf.

— (2010): «Delitos informáticos. Hacking. Daños en reforma penal 2010», en Ortiz Ubrina Gimeno, I.: *Memento Experto. Reforma penal,* Ediciones Francis Lefebvre, Madrid.

Nebrera González, M (coord.) (2002): *Intimidad y seguridad: dos conceptos y un conflicto*, Associació Isegs per a la Promoció dels Estudis sobre la Governabilitat, Barcelona.

Ocón García, J. (2022): «La incidencia del conocimiento tecnológico en la delimitación del secreto de las comunicaciones», en Arruego Rodríguez, G. y Pascual Medrano, A. (dir.): *La evidencia científica y tecnológica como recurso jurídico,* Comares, Granada.

Quintero Olivares, G. (2016): *Compendio de la parte especial del Derecho penal,* Aranzadi, Cizur Menor.

Rodríguez, J. R. (2017): «Informática, IT, IS y digital: ¿cuál es la diferencia?» en *Blog de Estudios de Informática, Multimedia y Telecomunicaciones*. Disponible en: https://blogs.uoc.edu/informatica/informatica-it-is-y-digital-cual-es-la-diferencia/.

Sainz-Cantero Caparrós, J. (2021): «Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio (I)», en Morillas Cueva, L. (dir.): *Sistema de Derecho penal. Parte Especial,* Dykinson, Madrid.

Sanz Delgado, E. y Fernández Bermejo, D. (Coords.) (2021): *Tratado de delincuencia cibernética*, Thomson Reuters Aranzadi, Pamplona.

Tamarit Sumalla, J. (2010): «Delincuencia informática: intrusismo, sabotaje informático y uso ilícito de tarjetas (art. 197.3 y 8, 264 y 248», en *La reforma penal de 2010: análisis y comentarios,* Aranzadi.

Vila Lozano, J. (2022): «Protección de datos en el ciberespacio de la Unión Europea: control de contenidos y perfilaciones digitales», en *Revista Aranzadi de derecho y nuevas tecnologías,* 58.

Wiener, N (1958): *Cibernética y sociedad,* (traducción de José Novo Cerro), Editorial Sudamérica, Buenos Aires.