VNiVERSiDAD D SALAMANCA

CAMPUS DE EXCELENCIA INTERNACIONAL

TRABAJO DE FIN DE MÁSTER

Título Propio de Máster en Derecho Procesal

Curso 2021/2022

LAS DILIGENCIAS DE INVESTIGACIÓN Y LA PRUEBA ELECTRÓNICA DEL CIBERCRIMEN

Nombre del/la estudiante: Arnau GUIX SANTANDREU

Director/a: Prof. Dr. Federico BUENO DE MATA

Mes: Julio

Año: 2022

TRABAJO DE FIN DE MÁSTER
TÍTULO PROPIO DE MÁSTER EN DERECHO PROCESAL

LAS DILIGENCIAS DE INVESTIGACIÓN Y LA PRUEBA ELECTRÓNICA DEL CIBERCRIMEN

THE INVESTIGATIVE ACTIONS AND THE ELECTRONIC EVIDENCE OF CYBERCRIME

Nombre del/la estudiante: **Arnau GUIX SANTANDREU**

Visto
Director/a: **Prof. Dr. Federico BUENO DE MATA**

[Castellano] RESUMEN

La hiperconectividad de las sociedades tecnológicamente avanzadas expone a numerosas personas y actividades a un elevado número de riesgos digitales. Así, los ciberdelitos hoy en día son frecuentes. A grandes rasgos, sus perpetradores aprovechan las vulnerabilidades técnicas y humanas para causar estragos en la operatividad de los sistemas informáticos y llegar a lucrarse con ello, afectar a la privacidad de los ciudadanos y finalmente dañar a los intereses generales y la estabilidad institucional. En este escenario, la prueba electrónica juega un papel decisivo para evitar la impunidad de sus autores, que ya de por sí aprovechan las ventajas derivadas del anonimato y las incertidumbres legales en relación a la competencia judicial, que persisten aunque se haya articulado un cuerpo de normativa internacional. Para superar las deficiencias anteriores, la Ley Orgánica 13/2015, de 5 de octubre, ha supuesto un hito en la regulación de las diligencias de investigación en España, concretamente de los registros de equipos de almacenamiento masivo de información y los registros remotos de equipos informáticos, entre otros aspectos, estableciendo una regulación más garantista con la preservación de los Derechos Fundamentales, pero con limitaciones que deben ser abordadas.

PALABRAS CLAVE: ciberdelitos, cibercrimen, prueba electrónica, diligencias de investigación, registro de equipos informáticos, registro remoto, pericial informática.

[English] ABSTRACT

The hyperconnectivity of technologically advanced societies exposes many people and activities to a high number of digital risks. Thus, cybercrime today is frequent. In a general sense, its perpetrators take advantage of technical and human vulnerabilities to cause damages on the operation of computer systems and obtain profits from it, affect the privacy of citizens and ultimately damage the general interests and the institutional stability. In this scenery, electronic evidence plays a decisive role at avoiding impunity for its perpetrators, who already take advantage from anonymity and legal uncertainties in relation to court jurisdictions, which persist even if a corpus of international regulations has been articulated. To overcome the previous deficiencies, the Organic Law 13/2015, of October 5, has been a milestone in the regulation of the investigative actions in Spain, more specifically in the registrations of mass storage devices and remote records of computer equipment, among other aspects, establishing a regulation which guarantees better the preservation of Fundamental Rights, but with limitations that must be addressed.

KEYWORDS: cybercrime, electronic evidence, investigative actions, registration of computer equipment, remote registration, computer forensics.

[Français] SOMMAIRE

L'hyperconnectivité des sociétés technologiquement avancées expose de nombreuses personnes et activités à un grand nombre de risques numériques. Ainsi, les cybercrimes sont aujourd'hui fréquents. D'une manière générale, ses auteurs profitent des vulnérabilités techniques et humaines pour faire des dégâts dans le fonctionnement des systèmes informatiques et en tirer profit, affecter la vie privée des citoyens et, en fin de compte, nuire aux intérêts généraux et à la stabilité institutionnelle. Dans cette scène, les preuves électroniques jouent un rôle décisif pour éviter l'impunité de leurs auteurs, qui profitent déjà des avantages provenant de l'anonymat et des incertitudes juridiques en matière de compétence judiciaire, qui persistent même si un ensemble de réglementations internationales a été articulé. Pour surmonter les lacunes précédentes, la Loi Organique 13/2015, du 5 octobre, a été un point culminant dans la réglementation des dispositions d'enquête en Espagne, plus concretement dans les registres des dispositifs de stockage de masse et des registres à distance des équipements informatiques, entre autres aspects, établissant une règlementation plus soucieuse avec la préservation des Droits Fondamentaux, mais avec des limitations qui doivent être abordées.

MOTS-CLÉS: cybercriminalité, preuve électronique, dispositions d'enquête, registre des équipements informatiques, registre à distance, rapport d'expert en informatique.

[Català] RESUM

La hiperconnectivitat de les societats tecnològicament avançades exposa a nombroses persones i activitats a un elevat nombre de riscos digitals. Així, els ciberdelictes avui en dia són freqüents. A grans trets, els seus perpetradors aprofiten les vulnerabilitats tècniques i humanes per a causar estralls en l'operativitat dels sistemes informàtics i arribar a lucrar-se, afectar la privacitat dels ciutadans i finalment malmetre els interessos generals i l'estabilitat institucional. En aquest escenari, la prova electrònica juga un paper decisiu per a evitar la impunitat dels seus autors, que ja de per si aprofiten els avantatges derivats de l'anonimat i les incerteses legals en relació a la competència judicial, que persisteixen encara que s'hagi articulat un corpus de normativa internacional. Per a superar les deficiències anteriors, la Llei Orgànica 13/2015, de 5 d'octubre, ha suposat una fita en la regulació de les diligiències d'investigació a Espanya, concretament dels registres d'equips d'emmagatzematge massiu d'informació i els registres remots d'equips informàtics, entre altres aspectes, establint una regulació més garantista amb la preservació dels Drets Fonamentals, però amb limitacions que han de ser abordades.

PARAULES CLAU: ciberdelictes, cibercrim, prova electrònica, diligències d'investigació, registre d'equips informàtics, registre remot, pericial informàtica.

ABREVIATURAS

Art.	Artículo
CE	Constitución Española
CEDH	Convenio Europeo de Derechos Humanos
FGE	Fiscalía General del Estado
FJ	Fundamento Jurídico
IA	Inteligencia Artificial
LAJ	Letrado/a de la Administración de Justicia
LEC	Ley de Enjuiciamiento Civil
LECRIM	Ley de Enjuiciamiento Criminal
LO	Ley Orgánica
OTAN	Organización del Tratado del Atlántico Norte
RD	Real Decreto
Rec.	Número de recurso
SAN	Sentencia de la Audiencia Nacional
STC	Sentencia del Tribunal Constitucional
STEDH	Sentencia del Tribunal Europeo de Derechos Humanos
STS	Sentencia del Tribunal Supremo
TICs	Tecnologías de la Información y la Comunicación

En el Anexo se encuentra un glosario de anglicismos técnicos donde también se incluyen abreviaturas utilizadas en el lenguaje informático habitual.

ÍNDICE

Introducción

Al momento presente, en los países occidentales la mayor parte de las interacciones humanas ya están teniendo lugar en el mundo virtual. Trabajamos con equipos informáticos, usamos las redes sociales y el correo electrónico para comunicarnos y mantener las relaciones, verificamos los saldos bancarios desde aplicaciones de *smartphone* y con tales fondos hacemos compras en línea, accedemos a contenidos de entretenimiento y descubrimos la actualidad más inmediata, etc. Existen grandes posibilidades y también grandes riesgos, exponiéndonos a numerosos abusos contra nuestros propios intereses[1]. Como es bien conocido, la tecnología evoluciona de una forma más veloz que el Derecho. Aquí se encuentra la necesidad de legislar de una forma lo suficientemente equilibrada, para que la normativa no resulte inmediatamente obsoleta una vez entre en vigor y a la vez las situaciones nuevas gocen de la pertinente cobertura jurídica[2].

Los datos se han convertido en una fuente de riqueza y de poder. Los entes que son capaces de poseerlos, administrarlos e interpretarlos disponen de unas herramientas muy superiores a las del Estado liberal clásico, con una capacidad de influencia planetaria solo reservada para auténticas potencias. Al *Big Data* se deben añadir los cambios radicales en los sistemas de producción, dentro de la denominada *Cuarta revolución industrial*, donde se prevé un impacto considerable de la Inteligencia Artificial (IA). Pero del mismo modo que se construye un nuevo orden, también existen hechos de cariz destructivo: el cibercrimen se ha implementado dentro de las sociedades hiperconectadas y aprovecha sus vulnerabilidades para causar estragos y permitir el lucro de *minorías digitalizadas*.

La cibercriminalidad ha tenido un impacto de 5,7 billones de euros en todo el mundo durante el año 2021, exponiendo a Europa a una quinta parte de los ataques[3]. Es un hecho ampliamente aceptado que la pandemia de COVID-19 ha amplificado la cibercriminalidad. El confinamiento provocó la creación de nuevos hábitos de uso de Internet, conductas que antes no existían o que se practicaban de forma limitada. Así, los agresores encontraron en el ciberespacio la oportunidad de acercarse a sus víctimas inexpertas[4].

Entre otras prácticas, se extendió el teletrabajo en las relaciones laborales que podían realizarse mediante conexiones remotas, exponiéndose a la intromisión de *hackers* y pérdidas de datos; aumentaron las compras en Internet y algunas Administraciones Públicas que buscaban desesperadamente material sanitario para suplir sus urgentes carencias fueron víctimas de estafas; las videoconferencias fueron en aumento y algunos usuarios terminaron instalando aplicaciones que imitaban a las legítimas y contenían *malware*; y ante la incertidumbre social proliferó la desinformación.

---

[1] GALÁN MUÑOZ, Alfonso (2019): *Los ciberdelitos en el ordenamiento español*. Barcelona, Editorial UOC, p. 13.

[2] BUENO DE MATA, Federico (2019): *La diligencias de investigación penal en la cuarta revolución industrial. Principios teóricos y problemas prácticos*. Cizur Menor (Navarra), Editorial Aranzadi – Thomson Reuters, pp. 18-19.

[3] FRANCE 24 (10.05.2022): *La cibercriminalidad costó más de 6 billones de dólares en 2021*. Accesible en: https://www.france24.com/es/minuto-a-minuto/20220510-la-cibercriminalidad-cost%C3%B3-m%C3%A1s-de-6-billones-de-d%C3%B3lares-en-2021 [Última consulta realizada en 23.06.2022].

[4] MIRÓ LLINARES, Fernando (2021): "Crimen, cibercrimen y COVID-19: desplazamiento (acelerado) de oportunidades y adaptación situacional de ciberdelitos". Barcelona, *Revista de Internet, Derecho y Política*, nº 32, p. 6.

Las universidades españolas no han estado exentas de los desastres causados por ciberataques. En los últimos años, en Castilla y León, las universidades de Valladolid[5] (2019), Burgos[6] (2020) y Salamanca[7] (2021, coincidiendo con la jornada de elecciones al cargo de Rector) han sido víctimas de estas prácticas delictivas. La UNIVERSITAT AUTÒNOMA DE BARCELONA (UAB) sufrió el pasado 11 de octubre de 2021 uno de los mayores asaltos informáticos jamás producidos en una universidad española, en que un virus del tipo *ransomware* infectó a 10.000 ordenadores después de haberse apoderado del sistema central y encriptó los archivos de los usuarios, impidiendo cualquier uso de ellos y repercutiendo en el día a día de 50.000 alumnos y personal de la corporación. La Administración catalana aportó 3,5 millones de euros a la UAB para recuperarse de los estragos y renovar los equipos, negando en todo momento que las cuantías fueran destinadas a asumir el *rescate* presuntamente requerido por los atacantes[8].

La finalidad de la presente investigación radica en determinar, desde la perspectiva del Derecho procesal penal, si el actual acervo legal español de las diligencias de investigación informática y la prueba electrónica relacionadas con la persecución de los ciberdelitos puede atender a las necesidades cambiantes de nuestra *sociedad de la información*[9]. De este modo, la estructura del trabajo se ajusta para realizar un acompañamiento hacia una comprensión progresiva de la temática de estudio, alcanzando a objetivos de investigación más específicos: en el Capítulo 1, se sitúan los conceptos de prueba electrónica y de diligencias de investigación, destacando el marco jurídico vigente; en el Capítulo 2, se clasifica a los ciberdelitos para presentar sus riesgos e impactos, a la vez que se descubren las dificultades procesales que los caracterizan; en el Capítulo 3, se desgranan las características de las principales diligencias de investigación asociadas a los ciberdelitos y se observan los instrumentos de prueba electrónica de uso más generalizado; y finalmente, el análisis se completa con las conclusiones y las referencias, junto a un glosario de anglicismos técnicos.

El trabajo utiliza una metodología basada en la revisión bibliográfica y el posterior análisis crítico, en que se han consultado a fuentes documentales primarias (es decir, leyes, normativa emanada de organizaciones internacionales y jurisprudencia de las más altas instancias del Estado) y fuentes secundarias (monografías y publicaciones científicas de revistas especializadas en Derecho). Teniendo en cuenta la necesidad de disponer de contenidos actualizados, se han priorizado las referencias publicadas durante los últimos diez años, con especial interés en los últimos cinco años. El estilo de citación utilizado es el denominado APA, con indicación de los nombres propios de los autores/as para visibilizar el género.

---

[5] EL ECONOMISTA (14.01.2019): *La Universidad de Valladolid sufre un ataque informático*. Accesible en: https://www.eleconomista.es/ecoaula/noticias/9632786/01/19/La-Universidad-de-Valladolid-sufre-un-ataque-informatico.html [Última consulta realizada en 23.06.2022].

[6] EL DIARIO.ES (16.01.2020): *La Universidad de Burgos, víctima de un ataque informático que afecta a datos personales de 6.800 usuarios*. Accesible en: https://www.eldiario.es/castilla-y-leon/sociedad/universidad-burgos-ciberataque-personales-usuarios_1_1076339.html [Última consulta realizada en 23.06.2022].

[7] LA GACETA DE SALAMANCA (30.11.2021): *La Universidad de Salamanca sufre un ataque informático el día de las elecciones a rector*. Accesible en: https://www.lagacetadesalamanca.es/salamanca/la-universidad-de-salamanca-sufre-un-ataque-informatico-el-dia-de-las-elecciones-a-rector-HF9733832 [Última consulta realizada en 23.06.2022].

[8] LA VANGUARDIA (23.11.2021): *El Govern destina 3,5 millones a la UAB para recuperarse del ciberataque*. Accesible en: https://www.lavanguardia.com/vida/20211123/7883348/govern-destina-3-5-millones-uab-recuperarse-ataque-informatico.html [Última consulta realizada en 23.06.2022].

[9] Me interesa estudiar la relación entre el Derecho y la Tecnología. La preocupación por el impacto actual de la ciberdelincuencia y mi disposición hacia el estudio del Derecho Procesal me han motivado a elaborar el análisis.

1. La investigación y prueba en el contexto de una sociedad tecnificada.

1.1. Situación de la prueba electrónica en los albores de la Justicia 2.0.

Antes de adentrarnos en la presente investigación, conviene realizar un escrutinio de índole conceptual que resultará de utilidad en el presente trabajo. Se trata de la diferenciación entre *diligencias de investigación* y *actos de prueba*. Aunque ambas nociones permiten *aportar hechos al proceso*, se distinguen en que las primeras tienen lugar en la fase de instrucción y permiten decidir la apertura o no del juicio oral, después de comprobar los hechos objeto de litigio y si existen indicios de criminalidad suficientes para articular la acusación contra una persona concreta[10]; en cambio, los actos de prueba proceden únicamente en el caso de la fase de juicio oral[11], cuando la acusación pretende desvirtuar a la presunción de inocencia y obtener la convicción del órgano judicial para que dicte una resolución condenatoria del acusado, una vez practicadas las pruebas bajo los principios de inmediación, contradicción, igualdad y licitud.

Ante la necesidad de acreditar la comisión de los ciberdelitos se estructura la llamada *prueba electrónica*. Algunos autores la han llegado a considerar como una tipología de prueba diferenciada, o incluso un nuevo medio de prueba comprendido en el contenido del artículo 299 LEC[12], que prevé que *[t]ambién se admitirán, conforme a lo dispuesto en esta Ley, los medios de reproducción de la palabra, el sonido y la imagen, así como los instrumentos que permiten archivar y conocer o reproducir palabras, datos, cifras y operaciones matemáticas llevada a cabo con fines contables o de otra clase, relevantes para el proceso* (ap. 2). Otros autores se han decantado por considerar la prueba electrónica como aquella en que el dato está presente en código binario, es decir, en ceros y unos[13].

Resulta preferible no atribuir a la *prueba electrónica* esta exclusividad definitoria, separada de la documental, la testifical y la pericial. Conviene matizar que la Ley no regula ningún medio de prueba de este tipo[14]; la prueba resulta siempre un acto de origen antrópico, de modo que es imposible *probar electrónicamente*, ya se trate un hecho electrónico o no. De este modo, se aportará al proceso la prueba documental, consistente en correos electrónicos, mensajes, grabaciones o documentos con firma digital, por ejemplo, todos ellos obtenidos mediante medios tecnológicos; también se tomará declaración de testigos o miembros de los Cuerpos y Fuerzas de Seguridad; y finalmente, se proporcionará un dictamen pericial informático, que interprete todo lo relativo a los hechos electrónicos. Este último medio es relevante también para reforzar la

[10] Igualmente, para valorar la procedencia de aplicar medidas cautelares.
[11] Con las excepciones de las llamadas pruebas anticipadas y las pruebas preconstituidas, que tienen lugar antes de la fase de juicio oral.
[12] RICHARD GONZÁLEZ, Manuel (2017): *Investigación y prueba mediante medidas de intervención de las comunicaciones, dispositivos electrónicos y grabación de imagen y sonido*. Las Rozas (Madrid), Wolters Kluwer, p. 52.
[13] Discrepando de esta visión exclusiva, *Vid*. BUJOSA VADELL, Lorenzo Mateo; BUSTAMANTE RÚA, Mónica María; TORO GARZÓN, Luis Orlando (2021): "La prueba digital producto de la vigilancia secreta: obtención, admisibilidad y valoración en el proceso penal en España y Colombia". Porto Alegre, *Revista Brasileira de Direito Processual Penal*, vol. 7, nº 2, p. 1353.
[14] El Convenio sobre la Ciberdelincuencia, adoptado en Budapest en 2001, menciona a *la obtención de pruebas electrónicas de un delito* en su artículo 14.2; sin embargo, no realiza una definición expresa de esta tipología.

autenticidad de la prueba documental. El/La titular del órgano judicial únicamente puede valorar la prueba mediante la vista y el oído[15].

Según BUJOSA VADELL, BUSTAMENTE RÚA y TORO GARZÓN, la prueba digital como tal está compuesta de los siguientes elementos: en primer lugar, la fuente de la prueba (la autenticidad); en segundo lugar, que la misma no haya sido alterada o manipulada (la integridad); en tercer lugar, la garantía de permanencia del mensaje en su forma original (la inalterabilidad); en cuarto lugar, el acceso a la fuente original de información (la rastreabilidad); en quinto lugar, la posibilidad de realizar una consulta posterior (la recuperabilidad); y, en sexto lugar, su conservación en el tiempo (la perdurabilidad)[16].

1.2. Derechos Fundamentales afectados por las diligencias de investigación y la prueba electrónica del cibercrimen.

Las diligencias de investigación y la prueba electrónica afectan de forma directa a los Derechos Fundamentales recogidos en el artículo 18 de la Constitución española, concretamente el derecho al honor, a la intimidad personal y familiar y a la propia imagen (ap. 1); eso no obstante, otros derechos pueden resultar significativamente dañados, como la inviolabilidad del domicilio (ap. 2), el secreto de las comunicaciones (ap. 3), la protección de datos (ap. 4), la tutela judicial efectiva (art. 24 CE), y según algunos autores, hasta la libertad de residencia y circulación (art. 19 CE)[17]. La doctrina científica y la jurisprudencia del TRIBUNAL SUPREMO[18] han llegado a definir el *derecho al propio entorno digital*, que se integraría en el artículo 18 CE y representaría una combinación de los Derechos Fundamentales del precepto, habida cuenta que en un mismo dispositivo pueden guardarse datos y comunicaciones, entre otros aspectos[19].

A parte de la Constitución, el Convenio Europeo de Derechos Humanos es otra esfera de protección a considerar, regulando en su artículo 8 el respeto a la vida privada y familiar y del domicilio. El TRIBUNAL EUROPEO DE DERECHOS HUMANOS se ha pronunciado en varias ocasiones sobre la necesidad que las medidas tecnológicas estén previstas por la ley[20], y que las circunstancias no excedan de las previsiones de la misma, para evitar situaciones abusivas o arbitrarias por parte de los agentes públicos[21]. En los supuestos excepcionales de terrorismo, el TEDH ha admitido que las medias de vigilancia son necesarias en una sociedad democrática para la preservación de la seguridad nacional, siempre con las garantías adecuadas[22].

---

[15] RICHARD GONZÁLEZ, Manuel (2017): *Investigación y prueba mediante medidas (...) (op. cit.),* p. 55.

[16] BUJOSA VADELL, Lorenzo Mateo; BUSTAMANTE RÚA, Mónica María; TORO GARZÓN, Luis Orlando (2021): "La prueba digital producto de la vigilancia secreta *(...)*" *(op. cit.*), p. 1378.

[17] Este caso es más dudoso, aunque el artículo 588 ter d), ap. 2, reconoce que la medida de intervención telefónica podrá aplicarse a determinar: *B) El conocimiento de su origen o destino, en el momento en el que la comunicación se realiza. C) La localización geográfica del origen o destino de la comunicación*.

[18] STS 489/2018, de 23 de octubre, rec. 1674/2017, FJ 5.

[19] PÉREZ ESTRADA, Miren Josune (2019): "La protección de los datos personales en el registro de dispositivos de almacenamiento masivo de información". Porto Alegre, *Revista Brasileira de Direito Processual Penal*, vol. 5, nº 3, p. 1314.

[20] SSTEDH *Malone c. Reino Unido*, de 2 de agosto de 1984; *Kruslin c. Francia* y *Huvig c. Francia*, de 24 de abril de 1990, *Valenzuela Contreras c. España*, de 30 de julio de 1998, y *Prado Bugallo c. España*, de 18 de febrero de 2003, entre otras.

[21] BARRIO ANDRÉS, Moisés (2018): *Delitos 2.0. Aspectos penales, procesales y de seguridad de los ciberdelitos*. Las Rozas (Madrid), Wolters Kluwer, p. 192.

[22] GONZÁLEZ MONJE, Alicia (2017): "Amenazas a la seguridad y privacidad: la dificultad del equilibrio perfecto". Madrid y Elche, *Revista Europea de Derechos Fundamentales*, nº 29, p. 285.

Actualmente, existe un elenco de principios rectores que limitan la práctica de las diligencias de investigación tecnológicas. Éstos han sido plasmados en el artículo 588 bis a) LECRIM, que actúa de marco general y refuerza la aplicación garantista del Derecho Procesal como un instrumento que atiende a una finalidad legítima de limitación del ejercicio de los Derechos Fundamentales para que el Estado de Derecho pueda ejercer sus funciones básicas y se pueda garantizar la paz social. Tales principios son los siguientes: especialidad, idoneidad, excepcionalidad, necesidad y proporcionalidad[23] y serán brevemente tratados a continuación.

El principio de especialidad se basa en que una medida esté relacionada con la investigación de un delito concreto. No se podrán ordenar diligencias tecnológicas preventivas o de despejar meras sospechas, so pena de crear un Estado Policial con una vigilancia generalizada de la población[24]. El principio de idoneidad pretende definir el ámbito objetivo y subjetivo y la duración de la medida en virtud de su utilidad. Los principios de excepcionalidad y necesidad presentan un carácter complementario, en que únicamente se podrá acordar la medida *cuando no estén a disposición de la investigación, en atención a sus características, otras medidas menos gravosas para los derechos fundamentales del investigado o encausado e igualmente útiles para el esclarecimiento del hecho*. En la mayoría de los casos, la solicitud de tales medidas tendrá lugar en el comienzo de la investigación judicial, en la fase de las diligencias previas del procedimiento abreviado; así, será necesario acreditar una investigación policial previa y suficiente, que demuestre que es necesario avanzar en las técnicas[25]. Finalmente, el principio de proporcionalidad valora la injerencia causada al derecho del investigado y el beneficio extraído con su aplicación, analizando la gravedad del hecho, la trascendencia social, el ámbito tecnológico de producción, la intensidad de los indicios existentes y la relevancia del resultado[26] con la restricción producida en el derecho (*balancing test*)[27].

En referencia al derecho a la intimidad, el TRIBUNAL CONSTITUCIONAL ha indicado que éste consiste en *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 la vida humana*[28]. Es claro que el derecho a la intimidad resultará afectado durante medidas como intervenciones telefónicas, telemáticas o durante el registro de dispositivos informáticos, donde se pueden encontrar contenidos que pertenecen a la esfera de privacidad de la persona investigada.

El TRIBUNAL CONSTITUCIONAL ha precisado los requisitos necesarios para articular una injerencia objetiva y razonable al derecho a la intimidad: en primer lugar, la existencia de un fin constitucionalmente legítimo; en segundo lugar, que la medida limitativa del derecho esté prevista en la Ley (principio de legalidad); en tercer lugar, que como regla general se acuerde mediante una resolución judicial motivada; y, finalmente, que se produzca la estricta observancia del principio de proporcionalidad, desarrollando el que ha sido calificado de *triple test* por sus

[23] *Vid.* STS 173/2016, de 2 de marzo, rec. 1864/2015, FJ 1.
[24] BUENO DE MATA, Federico (2019): *La diligencias de investigación (…) (op. cit.)*, p. 31.
[25] BARRIO ANDRÉS, Moisés (2018): *Delitos 2.0. Aspectos penales, procesales (…) (op.* cit.), p. 194.
[26] BUENO DE MATA, Federico (2019): *La diligencias de investigación (…) (op. cit.)*, pp. 37-38.
[27] BARRIO ANDRÉS, Moisés (2018): *Delitos 2.0. Aspectos penales, procesales (…) (op.* cit.), pp. 193-194.
[28] Más recientemente, SSTC 66/2020, de 2 de junio, rec. 6313/2019, FJ 4; 172/2020, de 19 de noviembre, rec. 2896/2015, FJ 4; y 115/2013, de 9 de mayo, rec. 1246/2011, FJ 3, entre otras.

tres comprobaciones: idoneidad de la medida, necesidad de la misma y proporcionalidad en sentido estricto[29].

Sobre el derecho al secreto de las comunicaciones, el TRIBUNAL SUPREMO ha declarado que su protección constitucional *abarca todos los medios de comunicación conocidos en el momento de aprobarse la norma fundamental, y también los que han ido apareciendo o puedan aparecer en el futuro, no teniendo limitaciones derivadas de los diferentes sistemas técnicos que puedan emplearse*[30]. Cualquier intromisión que se produzca en las comunicaciones personales deberá estar justificada, por lo que resultará imprescindible la autorización del Juez de Instrucción. En este sentido, las compañías operadoras tienen la obligación de custodiar los datos, que únicamente podrán ser cedidos para la investigación de delitos graves y bajo mandato judicial[31].

Resulta relevante diferenciar los momentos concretos en los que se producirían las injerencias a los derechos a la intimidad y al secreto de las comunicaciones. Así, por ejemplo, para los mensajes de correo electrónico o redes sociales elaborados pero aún no enviados, se afectaría únicamente al derecho a la intimidad. En cambio, el acceso a un mensaje que está en tránsito hacia el destinatario, o que todavía no ha sido leído por éste pero que ya ha sido guardado por la operadora, sí que se vulnera el derecho al secreto de las comunicaciones[32]. No vulneraría los Derechos Fundamentales el acceso a los contenidos publicados en las redes sociales y que pueden ser accedidos libremente por sus usuarios o que corresponden a un perfil público, excepto que se trate de un grupo restringido de interlocutores, caso en el que sí operan las garantías del artículo 18.3 CE[33].

Las diligencias de investigación serán declaradas nulas en caso que no se cumplan los requisitos legales necesarios para articular su validez y licitud como pruebas[34]. La jurisprudencia del TRIBUNAL CONSTITUCIONAL ha reconocido la teoría de *los frutos del árbol envenenado* desde la STC 114/1984, de 29 de noviembre, que posteriormente se plasmó en el artículo 11.1 de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial, que establece que *En todo tipo de procedimiento se respetarán las reglas de la buena fe. No surtirán efecto las pruebas obtenidas, directa o indirectamente, violentando los derechos o libertades fundamentales*. El TC se ha pronunciado sobre la vulneración del derecho al secreto de las comunicaciones y la resultante invalidez de la prueba obtenida[35], entre otros Derechos Fundamentales.

La figura del Ministerio Fiscal es clave ante una situación de menoscabo de Derechos Humanos. Si bien es cierto que su dependencia orgánica del Poder Ejecutivo no lo convierten en un elemento destinado a ser exclusivo de la fase de investigación en el proceso penal, que debe recaer necesariamente sobre un órgano judicial de instrucción, la Fiscalía cuenta con un nivel de especialización elevado en el terreno de los ciberdelitos.

[29] STC 207/1996, de 16 de diciembre, rec. 1789/1996, FJ 4. *Vid.* STS 311/2015, de 27 de mayo, rec. 10813/2014.
[30] STS 714/2016, de 26 de septiembre, rec. 1951/2015, FJ 6.
[31] RICHARD GONZÁLEZ, Manuel (2017): *Investigación y prueba mediante medidas (...) (op. cit.),* p. 33.
[32] ARMENTA DEU, Teresa (2018): "Regulación legal y valoración probatoria de fuentes de prueba digital (correos electrónicos, WhatsApp, redes sociales): entre la insuficiencia y al incertidumbre". Barcelona, *Revista de Internet, Derecho y Política,* nº 27, p. 71.
[33] ARMENTA DEU, Teresa (2018): "Regulación legal y valoración probatoria *(...)*" *(op. cit.)*, p. 74.
[34] RICHARD GONZÁLEZ, Manuel (2017): *Investigación y prueba mediante medidas (...) (op. cit.),* p. 380.
[35] SSTC 26/2006, de 30 de enero, rec. 623/2004; 253/2006, de 11 de septiembre, rec. 44/2003, entre otras.

Como orientación de futuro, BUENO DE MATA propone como reforma futura la creación de Juzgados de Instrucción especializados en delincuencia informática[36], una posibilidad que no debería descartarse ante la creciente complejidad de los supuestos de infracción y el valor de disponer de conocimientos precisos. Asimismo, existe un amplio consenso en la doctrina en que la digitalización en la Administración de Justicia conllevará la introducción de algoritmos de inteligencia artificial que simplificaran las tareas de todos los operadores jurídicos: abogados, jueces, magistrados, fiscales y otros funcionarios[37].

1.3. Marco jurídico de las diligencias de investigación y la prueba electrónica del cibercrimen.

Las diligencias de investigación tecnológicas y la prueba electrónica del cibercrimen se encuadran dentro de un entorno relativamente complejo de disposiciones aplicables. La fuerte tendencia a la digitalización de nuestras sociedades ha obligado a redefinir las normas procesales existentes y a promulgar nuevas leyes para combatir a una creciente inseguridad jurídica y a una praxis ineficiente de los tribunales, buscando una óptica *global* para un problema *global*. En primer lugar, se tratará la legislación internacional, y posteriormente, la española y la considerada bajo la denominación de *Soft Law*, teniendo al cibercrimen como eje normativo central.

1.3.1. Legislación internacional.

Dejando a un lado las contribuciones de cariz menor realizadas por la organización de las NACIONES UNIDAS[38], a nivel del CONSEJO DE EUROPA, destaca el Convenio sobre Ciberdelincuencia de 23 de noviembre de 2001, adoptado en Budapest y vigente desde julio de 2004[39]. Es el resultado de cuatro años de negociaciones entre 45 Estados miembros del Consejo de Europa, Estados Unidos, Canadá y Japón. Dicha normativa ha tenido un impacto significativo en las modificaciones de la Ley Orgánica 13/2015, de 5 de octubre, que modificó las diligencias de investigación en la LECRIM[40]. Asimismo, un indicador de la calidad legislativa del Convenio es que determinados países latinoamericanos, como Perú en 2014, han solicitado la adhesión al Convenio, entrando en vigor la normativa en el país andino al comienzo del año 2019[41], universalizando así su ámbito de aplicación. En 2015 España ratificó el primer protocolo adicional al convenio, sobre la penalización de actos de índole racista y xenófoba cometidos por medio de sistemas informáticos, adoptado en Estrasburgo en enero de 2003. En 2017 se iniciaron los trabajos para la aprobación de un segundo protocolo adicional a la Convención, relativo a la cooperación reforzada y la revelación de pruebas electrónicas[42].

[36] BUENO DE MATA, Federico (2019): *La diligencias de investigación (…) (op. cit.)*, p. 40.
[37] MUÑOZ RODRÍGUEZ, Ana Belén (2020): "El impacto de la inteligencia artificial en el proceso penal". Badajoz, *Anuario de la Facultad de Derecho. Universidad de Extremadura*, nº 36, pp. 695-728.
[38] La Asamblea General de las NACIONES UNIDAS elaboró las Resoluciones 55/63 y 56/121, sobre la lucha contra la utilización de la tecnología de la información con fines delictivos. La Convención de las Naciones Unidas sobre la utilización de las comunicaciones electrónicas en los contratos internacionales, promulgada el Nueva York en 2005 y entrada en vigor en 2013, también es una pieza a citar dentro del acervo probatorio multilateral.
[39] En España entró en vigor el 1 de octubre de 2010, después de ser ratificado el mismo año.
[40] RODRÍGUEZ RUBIO, Carmen (2020): "Nuevas diligencias de investigación y de prueba: el registro de dispositivos de almacenamiento masivo de información". *Foro, Nueva Época*, vol. 23, nº 1, p. 275.
[41] VILCHEZ LIMAY, Roberto Carlos (2020): "La ciberdelincuencia en el contexto de la pandemia del coronavirus. Una aproximación desde el marco convencional". Salamanca, *Ars Iuris Salmanticensis*, vol. 8, p. 22.
[42] Los trabajos de este segundo Protocolo fueron parados debido a la pandemia. Desde mayo de 2022 se encuentra a la espera de ser ratificado por los Estados partes. Entrará en vigor después de alcanzar las cinco ratificaciones.

Dentro del ámbito de la UNIÓN EUROPEA, existen diversas normativas a citar. En primer lugar, la Directiva 2013/40/UE, del Parlamento europeo y el Consejo, de 12 de agosto de 2013, relativa a los ataques contra los sistemas de información (DAI), es la pieza básica del acervo comunitario y establece obligaciones de tipificación penal a los Estados miembros para incluir en su ordenamiento jurídico a los delitos informáticos. En segundo lugar, es de interés la Directiva 2016/680/UE, del Parlamento europeo y el 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.

No se puede olvidar de mencionar al Reglamento 2016/679, del Parlamento europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. Su artículo 22 trata de las decisiones automatizadas. Actualmente, muchas de estas operaciones se concentran en la elaboración de perfiles, pero en un futuro cercano numerosas decisiones serán íntegramente autónomas, fruto de una cadena de procedimientos[43]. Es en el rastro de tales movimientos que recaerá la prueba electrónica, que se obtendrá sin que medie intervención humana. El Reglamento 2021/784, del Parlamento europeo y del Consejo, de 29 de abril de 2021, sobre la lucha contra la difusión de contenidos terroristas en línea, establece obligaciones de conservación de este tipo de datos y su retirada en el marco transfronterizo.

1.3.2. Legislación española.

A nivel de la legislación procesal española, en el orden penal destaca el Real Decreto de 14 de septiembre de 1882, de la Ley de Enjuiciamiento Criminal (en adelante, LECRIM), que a nivel de regulación de las diligencias de investigación tecnológicas experimentó una reforma importante a través de la Ley Orgánica 13/2015, de 5 de octubre, que añadió 39 preceptos nuevos en el articulado del Título VIII del Libro II, dedicado a *las medidas de investigación limitativas de los derechos reconocidos en el artículo 18 de la Constitución* del procedimiento del sumario, con una clara proyección en el resto de procesos. Con anterioridad, únicamente había un artículo de la LECRIM, el 579, destinado a tales supuestos, que había sido introducido por la Ley Orgánica 4/1988, de 25 de mayo[44]. El precepto no proporcionaba una solución efectiva a la investigación de los delitos cometidos mediante el uso de las TICs[45].

La reforma llevada a cabo por la Ley Orgánica 13/2015 se estructura mediante cuatro bloques diferenciados: en primer lugar, la interceptación de las comunicaciones telefónicas y telemáticas; en segundo lugar, la captación y grabación de comunicaciones orales e imágenes mediante la utilización de dispositivos electrónicos; en tercer lugar, la utilización de dispositivos técnicos de seguimiento, localización y captación de imágenes; y en cuarto lugar, el registro de dispositivos de almacenamiento masivo de información.

[43] ROIG BATALLA, Antoni (2020): *Las garantías frente a las decisiones automatizadas. Del Reglamento General de Protección de Datos a la gobernanza algorítmica*. Barcelona, J. M. Bosch, p. 35.
[44] RICHARD GONZÁLEZ, Manuel (2017): *Investigación y prueba mediante medidas (…) (op. cit.),* p. 53.
[45] BUENO DE MATA, Federico (2019): *La diligencias de investigación (…) (op. cit.)*, p. 17.

Según BUENO DE MATA, el diseño en bloques es un acierto y deja espacio para la futura adaptación a los nuevos medios tecnológicos. La citada Ley Orgánica surgió ante la necesidad de reformar el ámbito de investigación de los delitos digitales y la imposibilidad de introducir el proyecto de Código Procesal Penal de 2012, que sustituyera íntegramente el texto de la vetusta LECRIM[46]. Es una reforma arriesgada, pero ventajosa y necesaria[47], que presenta nuevas diligencias, entre las que destacan la interceptación integral de las comunicaciones, la figura del agente encubierto informático, las balizas GPS, la utilización de vehículos aéreos no tripulados (*drones*) y de virus espía para conseguir un control a distancia de los dispositivos informáticos[48]. El 6 marzo de 2019, la FISCALÍA GENERAL DEL ESTADO publicó cinco Circulares relevantes, proporcionando una interpretación dirigida a operadores jurídicos de diversa índole, no solo a los integrantes del Ministerio Fiscal. Así, afectan a la Policía Judicial, jueces y magistrados, abogados, investigados y víctimas. Sus contenidos se interpretan como un todo unitario, según la recomendación emitida por la propia Fiscalía[49]. En la presente investigación se hará una mención especial a la Circular 5/2019, sobre registro de dispositivos y equipos informáticos.

Siguiendo a la función supletoria que corresponde al orden civil, la Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil (en adelante, LEC), regula las disposiciones generales de la prueba en el Capítulo V del Título I del Libro II[50]. Otras normas de aplicación significativa en el contexto de la prueba electrónica son la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información; la Ley 6/2020, de 11 de noviembre, fundamental para regular la firma electrónica como medio inequívoco de identificación del firmante; la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones; y la Ley 18/2011, de 5 de julio, de uso de tecnologías de la información y la comunicación en la Administración de Justicia.

1.3.3. Instrumentos de *Soft Law*.

La primera referencia se encuentra en el Manual de las NACIONES UNIDAS para la Prevención y Control de Delitos Informáticos de 1977. Existen diversas instituciones con ánimo de promover la adopción de medidas preventivas y técnicas para mejorar los estándares de seguridad informática en instituciones y empresas, como el Centro de Excelencia de la OTAN para la Ciberdefensa Cooperativa en Tallin y el EUROPEAN CYBERCRIME CENTRE (EC3). En España, el INSTITUTO NACIONAL DE CIBERSEGURIDAD[51] publica recomendaciones y cuenta con una unidad de apoyo preventivo y reactivo en seguridad de las TICs, el denominado CERTSI. De la misma forma, la AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS y las instituciones autonómicas correlativas incentivan el despliegue de políticas de preservación de datos de carácter personal. Asimismo, el CENTRO CRIPTOLÓGICO NACIONAL efectúa recomendaciones dirigidas a las Administraciones Públicas.

[46] BUENO DE MATA, Federico (2019): *La diligencias de investigación (…) (op. cit.)*, pp. 20-21.
[47] BUENO DE MATA, Federico (2015): "Comentarios y reflexiones sobre la Ley Orgánica 13/2015 de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica". *Diario La Ley*, nº 8627.
[48] BUENO DE MATA, Federico (2015): "Fortalecimiento de garantías procesales y medidas de investigación tecnológica". Salamanca, *Ars Iuris Salmanticensis*, vol. 4, p. 326.
[49] BUENO DE MATA, Federico (2019): *La diligencias de investigación (…) (op. cit.)*, pp. 23-24.
[50] Asimismo, la Sección VIII del Capítulo VI del citado Título cubre los medios de reproducción de la palabra, el sonido y la imagen y de los instrumentos que permiten archivar y conocer datos relevantes para el proceso, usando una terminología amplia para evitar la obsolescencia de los preceptos.
[51] INCIBE, por sus iniciales; hasta 2014 era llamado INTECO. Su sede central está ubicada en León.

2. El cibercrimen: clasificación penal y obstáculos procesales

2.1. La cibercriminalidad opera de forma múltiple en el orden penal.

La doctrina ha realizado diversas aproximaciones para sistematizar la cibercriminalidad de forma reciente. En efecto, el Derecho penal y procesal penal clásico, junto a los principios de garantía de los Derechos Fundamentales, se han construido sobre un modelo de criminalidad física, de tipo marginal y en que el infractor es uno o pocos individuos. Sin lugar a dudas, la revolución digital de la segunda mitad del siglo XX hasta ahora ha supuesto un cambio de paradigma[52]. En este sentido, la doctrina se refirió primero a los *delitos informáticos* y posteriormente, como una evolución o segunda generación de los mismos, a los *ciberdelitos* o *delitos 2.0*, como comportamientos desviados, realizados a través de los sistemas informáticos y que tienen una repercusión social nociva; están completamente determinados por el uso de la red y la existencia de las TIC[53].

El concepto de *Derecho penal informático* podría llegar inducir a una perspectiva errónea, de pensar incluso que estamos frente a un sector de tal rama del ordenamiento jurídico que agrupa a ciertos tipos penales que tienen elementos técnicos configuradores comunes que obligan a hacer una distinción respecto otras figuras del Código Penal. Según GALÁN MUÑOZ, no existe un bien jurídico común, por ejemplo, como la seguridad de los sistemas informáticos, que obligue a realizar tal separación[54], hecho que es refutado por BARRIO ANDRÉS, que califica la seguridad en la Sociedad de la Información de *bien jurídico de primer orden*, pero no se posiciona a favor de seccionar al Derecho Penal[55]. No se puede prescindir del peso real de los ciberdelitos, ya que con ellos se pueden consumar un elenco de tipos penales significativo, desde delitos contra los consumidores, homicidios[56] y hasta supuestos de terrorismo.

Es fundamental comprender el papel que las TIC tienen para la consecución del delito. Así, la postura era inicialmente considerar la distinción en que los sistemas informáticos eran o bien un instrumento para perpetrar el delito (*computer assisted crimes*) o bien el objetivo del ciberataque (*computer focused crimes*). Actualmente esta clasificación ha sido superada: en numerosas ocasiones las tecnologías ya son simultáneamente la herramienta (*tool*) y el objetivo (*target*) del ilícito penal y deberíamos ceñirnos únicamente a estos supuestos múltiples para llegar a definir al cibercrimen satisfactoriamente[57]. A efectos de análisis, BARRIO ANDRÉS ha representado a los ciberdelitos a partir de la siguiente propuesta, siguiendo la ubicación de los preceptos en el Código Penal[58]:

[52] BARRIO ANDRÉS, Moisés (2018): *Delitos 2.0. Aspectos penales, procesales y de seguridad de los ciberdelitos*. Las Rozas (Madrid), Wolters Kluwer, p. 29.
[53] BARRIO ANDRÉS, Moisés (2018): *Delitos 2.0. Aspectos penales, procesales (...) (op.* cit.), pp. 35-36.
[54] GALÁN MUÑOZ, Alfonso (2019): *Los ciberdelitos en el ordenamiento español*. Barcelona, Editorial UOC, p. 16.
[55] BARRIO ANDRÉS, Moisés (2018): *Delitos 2.0. Aspectos penales, procesales (...) (op.* cit.), p. 92.
[56] Pensamos para este supuesto, por ejemplo, el *hackeo* de un vehículo con sistemas de conducción autónomos.
[57] MIRÓ LLINARES, Fernando (2012): *El cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio*. Madrid, Marcial Pons, pp. 47-49.
[58] Tabla adaptada de BARRIO ANDRÉS, Moisés (2018): *Delitos 2.0. (...) (op.* cit.), pp. 71-72.

Ciberdelito	***Artículo del CP***
Descubrimiento y revelación de secretos	197
Intrusismo informático e interceptación de las comunicaciones (*hacking*)	197 bis
Utilización no autorizada de imágenes previamente obtenidas con consentimiento (*revenge pornography*)	197.7
Daños informáticos y sabotajes (*cracking*)	264 y ss.
Obstaculización o interrupción de un sistema informático	264 bis
Estafas	248
Abuso de sistemas informáticos (*phreaking*)	256
Calumnias	205
Injurias	208
Ciberacoso (*cyberstalking*)	172 ter
Pornografía infantil	187 y ss.
Acercamiento y embaucamiento a menores (*online grooming*)	183 ter
Delitos contra la propiedad intelectual	270 y ss.
Ciberterrorismo	571 y ss.

En cambio, MIRÓ LLINARES ha optado por ilustrar la siguiente clasificación práctica de los ciberdelitos, de forma entrecruzada, que es la que estudiaremos con mayor detenimiento[59]:

	Ciberataques puros	***Ciberataques réplica***	***Ciberataques de contenido***
Cibercrímenes económicos	• *Hacking* • *Malware* intrusivo • *Malware* destructivo • Ataques de *insiders* • Ataques DoS • *Spam* • Ciberocupación red • *Antisocial networks*	• Ciberfraudes (*phishing*, *pharming*, *scam*, *auction fraud*, etc.) • *Cyberspyware* • *Identity theft* • *Spoofing* de ARP, DNS, IP y web • Ciberblanqueo de capitales • Ciberextorsión • Ciberocupación	• Distribución de pornografía infantil en Internet • Ciberpiratería intelectual
Cibercrímenes sociales	-	• *Spoofing* • *Cyberstalking* • *Cyberbullying* • *Online harassment* • *Sexting* • *Online grooming*	-
Cibercrímenes políticos	• Ataques DoS (*cyberwar*) • Ataques DoS (*cyberhacktivism*) • *Malware* intrusivo	• Ciberespionaje terrorista • Ciberguerra	• *Online hate speech* • Ciberterrorismo (difusión de mensajes radicales con fines terroristas)

En algunos supuestos, el ciberespacio es el único escenario viable para perpetrar la infracción, produciéndose crímenes que nunca antes hubieran podido realizarse: son los llamados *ciberataques puros*. En otros casos, no se han generado ilícitos nuevos, sino que se han reproducido las características básicas de tipos penales ya existentes en nuestras sociedades en el entorno de la red: se trata de los *ciberataques réplica*.

[59] Tabla adaptada de MIRÓ LLINARES, Fernando (2012): *El cibercrimen. (…) (op. cit.)*, p. 50.

Para concluir, el ciberespacio se ha convertido en un ámbito privilegiado para la difusión de masa de contenidos, amplificando significativamente el daño de tales ilícitos hacia una esfera global: son los llamados *ciberataques de contenido*. El primer tipo de ciberataques plantea problemas para incriminar a los presuntos criminales y concluir un proceso penal con éxito. La segunda categoría también presenta características de rápida evolución y no está exenta de dificultades para aplicar los preceptos penales vigentes. Y la tercera categoría presenta obstáculos en la prevención, con riesgos de afectar a Derechos Fundamentales ejercidos libremente, y naturalmente en la atribución de las responsabilidades penales a los autores.

Asimismo, como se puede apreciar en la tabla anterior el cibercrimen puede ser analizado desde otra perspectiva cruzada, diferenciando entre los ciberataques *económicos*, *sociales* y *políticos*, según su particular ámbito de incidencia. Se trata de una clasificación más pragmática, procedente de los tres grandes ámbitos funcionales de utilización de las tecnologías de la información y la comunicación. Especialmente, los dos primeros entornos resultan más claros: el ciberespacio se visualiza en un área de desenvolvimiento económico y también de desarrollo de relaciones sociales y el contacto interpersonal entre individuos[60]. Seguidamente analizaremos separadamente dichas tres categorías de ciberataques:

2.1.1. Delitos económicos y patrimoniales vinculados a las tecnologías.

Los *ciberataques económicos* tienen su razón de ser en la voluntad del autor de obtener beneficios patrimoniales, ya sean directos o indirectos a partir de sus conductas delictivas en la red. Es indudable que esta es la principal categoría de ciberataques por su impacto a diario en los países desarrollados y sus implicaciones contra las prácticas mercantiles. La digitalización ha supuesto que dinero, datos de valor elevado y nuevos servicios se ofrecen mediante las redes. Este hecho expone a empresas y particulares, éstos últimos entendidos más bien como clientes o consumidores, al cibercrimen de índole económica y patrimonial, en que los atacantes pretenden lucrarse de las actividades legítimas de otros sujetos. En la mayoría de supuestos los cibercriminales encadenarán distintos ataques para conseguir su propósito último.

Los *cibercrímenes económicos puros* encuentran en el *hacking* y el uso de *malware* sus principales supuestos. El *hacking* es una conducta por la cual un atacante accede a un sistema informático sin autorización de su titular. Con esta posición privilegiada, está en condiciones de utilizarlo o aprovechar los datos que se encuentran allí contenidos. Se puede diferenciar entre el *white hat hacking*, es decir, el *hacking blanco*, que no tiene un propósito de sabotear o utilizar la información más tarde, únicamente entrar al sistema informático, o el *black hat hacking*, en otras palabras, el *cracking*, en que el *cracker* busca de dañar el sistema, causar un perjuicio al titular, o apropiarse, modificar o eliminar los datos allí contenidos[61].

Es importante tener presente que en ciertas ocasiones los *hackers* informan de las vulnerabilidades que han detectado a los propios titulares de los equipos informáticos, de modo que se consigue avanzar en la mejora de los estándares de seguridad; sin embargo, la conducta sancionada como ilícito penal en el artículo 197 bis CP[62] y con el calificativo de ciberataque se

[60] MIRÓ LLINARES, Fernando (2012): *El cibercrimen. Fenomenología (...) (op. cit.)*, pp. 116-118.
[61] MIRÓ LLINARES, Fernando (2012): *El cibercrimen. Fenomenología (...) (op. cit.)*, pp. 53-54.
[62] *Vid.* STS 494/2020, de 8 de octubre, rec. 10018/2020, FJ 6, en que se aplica el citado precepto al supuesto de un acceso no autorizado a una base de datos de antecedentes policiales.

basa en el mero acceso[63], aquí no prevalece la distinción entre *hackers* y *crackers*[64]. El precepto es fruto de la reforma del 2015 y contempla en el artículo 197 ter la sanción para actos preparatorios destinados a la comisión de los delitos del artículo 197 bis[65].

Otro de los instrumentos del *cibercrimen económico puro* es el llamado *malware*, es decir, un programa malicioso que tiene como objetivo dañar, controlar o modificar un sistema informático[66]. Existen dentro de esta amplia categoría de *software* un amplio abanico de técnicas, desde los clásicos virus, que pretenden destruir el sistema o la información almacenada en él, a los *worms* (gusanos; saturan los ordenadores y redes mediante su replicación constante y consumen la capacidad de procesamiento), los *trojans* (troyanos, infectan los sistemas bajo una apariencia benévola y proporcionan un acceso remoto a los atacantes), los *rootkits* (se introducen al núcleo del sistema informático para evitar ser detectados y permiten al agresor tomar el control de la máquina), los *keyloggers* (capturan las pulsaciones realizadas en el teclado y envían los datos al atacante) y el *spyware* (programa espía; transfiere datos de la operativa del sistema capturado[67]).

Con las capacidades del *malware* es posible que el autor exija a la víctima un *rescate* para volver a restablecer el sistema informático a su estado original, o que se contente en destruir los datos o perturbar el funcionamiento de los equipos, provocando pérdidas cuantiosas en el caso de las empresas y administraciones afectadas. El *malware* es normalmente la antesala del *hacking*, donde los expertos cibercriminales dispondrán de elementos de control de los terminales infectados para expandir su ataque y multiplicar su poder devastador. En otros casos, existen los llamados *insiders*, es decir, trabajadores o personas vinculadas que sabotean los sistemas de sus propias organizaciones aprovechando su posición ventajosa en el interior[68].

Dentro de los *cibercrímenes económicos puros* es importante mencionar a los ataques *DoS* (del inglés *denial of service*, denegación de servicio), que provocan una saturación del servidor del sistema de la víctima e impiden que pueda atender a otras peticiones que no sean las del propio agresor. Este hecho puede llegar a incapacitar a sitios web comerciales con una alta concurrencia, perjudicando a las actividades de las empresas e instituciones a las que representan y dañando a su reputación. Es más, existe una evolución aún más invasiva de los ataques *DoS*, los *DDoS* (*distributed denial of service*, denegación de servicio distribuida)[69]. Ante semejantes daños, se ha llegado a articular un verdadero mercado del ciberdelito[70], en el que se alquilan *botnets* a

[63] Así, el artículo 197 bis del Código Penal condena al que *por cualquier medio o procedimiento, vulnerando las medidas de seguridad establecidas para 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*.
[64] MIRÓ LLINARES, Fernando (2012): *El cibercrimen. Fenomenología (...) (op. cit.)*, pp. 55-56.
[65] BARRIO ANDRÉS, Moisés (2018): *Delitos 2.0. Aspectos penales, procesales (...) (op.* cit.), pp. 90-91.
[66] MIRÓ LLINARES, Fernando (2012): *El cibercrimen. Fenomenología (...) (op. cit.)*, p. 59.
[67] Sobre el *software* espía, también se podría designar dentro de la categoría de *cibercrímenes económicos réplica*, ya que el espionaje naturalmente también es una práctica anterior a la existencia del propio ciberespacio.
[68] Es el caso de Hervé Falciani, cuya *lista* fue finalmente validada como prueba por parte del Tribunal Supremo.
[69] Los ataques *DDos* realizan una saturación del servidor mediante peticiones procedentes de múltiples atacantes a la vez o redes de *bots* que actúan de forma coordinada, incluso trabajando desde varios terminales infectados. En estos casos es más difícil distinguir a los *visitantes* ilícitos de los lícitos.
[70] En otros términos, el *ciberdelito como servicio* (CaaS – *cybercrime as a service*, en inglés).

ciberdelincuentes por un precio reducido de 60 dólares al día, que pueden causar estragos a una sola empresa por la cuantiosa cifra de 580.000 euros[71].

El Código Penal español ha tipificado en el artículo 264 CP un tipo básico para punir los daños derivados de la interferencia ilegal en datos informáticos[72], una conducta asimilable a la introducción de *malware* o la realización de ataques *DoS*. El articulado pretende de responder a las especificaciones del artículo 5 de la Directiva 2013/40/UE, del Parlamento europeo y el Consejo, de 12 de agosto de 2013, relativa a los ataques contra los sistemas de información (DAI), aunque en ésta no se especifica la necesidad de cubrir supuestos *graves* en la definición del delito, de forma que el legislador hispánico ha optado por crear un concepto jurídico indeterminado que deberá ser actualizado a través de la praxis de los órganos jurisdiccionales[73]. Sin embargo, existen pocas resoluciones condenatorias en los repertorios de jurisprudencia que permitan delimitar la gravedad de los ataques con carácter general[74].

Los *cibercrímenes económicos réplica* tienen en los ciberfraudes su mayor representatividad. Éstos se caracterizan para que los autores del delito logren un lucro a partir de un perjuicio patrimonial de la víctima. Centraron la atención del legislador incluso antes que éste comprendiera la necesidad de punir los daños informáticos y los accesos ilegítimos a los sistemas, dado a la tendencia expansiva de tratamiento automatizado de datos bancarios en Administraciones Públicas y grandes corporaciones en los años setenta y ochenta en los países tecnológicamente más avanzados[75]. Aproximadamente dos tercios de los ciberdelitos están cuantificados bajo la categoría de los fraudes informáticos, una cifra elevada que se ha mantenido relativamente estable a lo largo de la última década[76].

Para llegar a cometerlos se han diseñado infinidad de técnicas que se han perfeccionado a lo largo del tiempo a la par de las mejoras en seguridad y divulgación de las prácticas de estafa: fraudes de cheques y tarjetas de crédito, estafas de inversión con productos financieros falsos, *ponzi frauds* o estafas piramidales, engaños con falsos premios o presuntas loterías, *auction frauds* en las subastas en línea en las que no se entrega el producto o se engaña sobre sus propiedades, los *scam* o ciberfraudes burdos como las llamadas *cartas nigerianas*, etc.[77]. Actualmente, el artículo 248.2 a) del Código Penal comprende el tipo penal básico de la llamada *estafa informática*.

El caso paradigmático después de la irrupción de la banca electrónica y las aplicaciones financieras es el llamado *phishing*[78], una técnica de suplantación de identidad de una entidad bancaria o una empresa para posteriormente extraer los datos personales de los clientes y lucrarse

[71] BARRIO ANDRÉS, Moisés (2018): *Delitos 2.0. Aspectos penales, procesales (...) (op.* cit.), p. 37.
[72] Dicho precepto reza que *El que por cualquier medio, sin autorización y de manera grave borrase, dañase, deteriorase, alterase, suprimiese o hiciese inaccesibles datos informáticos, programas informáticos o documentos electrónicos ajenos, cuando el resultado producido fuera grave, será castigado con la pena de prisión de seis meses a tres años.*
[73] GALÁN MUÑOZ, Alfonso (2019): *Los ciberdelitos en el ordenamiento español (...) (op. cit.)*, p. 172.
[74] BARRIO ANDRÉS, Moisés (2018): *Delitos 2.0. Aspectos penales, procesales (...) (op.* cit.), p. 113.
[75] GALÁN MUÑOZ, Alfonso (2019): *Los ciberdelitos en el ordenamiento español (...) (op. cit.)*, p. 139.
[76] PONS GAMÓN, Vicente (2017): "Internet, la nueva era del delito: ciberdelito, ciberterrorismo, legislación y ciberseguridad". Quito, *URVIO - Revista Latinoamericana de Estudios de Seguridad*, nº 20, p. 84.
[77] MIRÓ LLINARES, Fernando (2012): *El cibercrimen. Fenomenología (...) (op. cit.)*, pp. 69-71.
[78] Término procedente de la transformación del inglés *fishing*, pesca, para referirse metafóricamente a las víctimas como los peces que *muerden al anzuelo*. En la jerga informática es habitual encontrar términos que comienzan mediante la raíz *ph*.

con operaciones fraudulentas, fundamentalmente a través de mensajes de correo electrónico engañosos que redireccionan a los usuarios a sitios web falsos. Se utiliza la ingeniería social para aparentar la identidad de una organización ajena (*spoofing*), a la vez que se puede llegar a monitorear el comportamiento de la víctima a través del sitio web verdadero (*pharming*)[79]. Además, si la incursión hacia los sistemas se realiza por mensaje de SMS en lugar de e-mail, por ejemplo, recibiendo un enlace que al abrirlo infecta el dispositivo, recibe el nombre de *smishing*[80].

El dinero robado se transferirá a las cuentas de *muleros*[81], que retendrán un porcentaje y reenviarán los fondos a otras cuentas bancarias, muchas de ellas situadas en el extranjero para dificultar la trazabilidad de las operaciones[82]. En otras ocasiones, el objetivo de los atacantes no son los perfiles del consumidor típico sino los directivos de grandes corporaciones o Administraciones Públicas, para llegar a obtener sus credenciales (*whaling*, caza de *ballenas*)[83]. Aunque los atacantes de *phishing* llevan años tratando de encontrar métodos óptimos para aprovecharse de las distracciones de sus víctimas sin poder ser perseguidos, existen algunos indicios generalizados que permiten detectarlos[84] [85]. Incluso se llegan a aprovechar de emociones humanas como el afán de lucro (regalos, ofertas y premios) o la compasión hacia las personas vulnerables (peticiones de fondos ante guerras, crisis o calamidades naturales).

En la misma categoría de *cibercrímenes económicos réplica* también encontraríamos a la ciberextorsión. Algunas organizaciones criminales amenazan a sus víctimas de realizar ataques informáticos y exigen el pago de sumas importantes de dinero para no llegar a ejecutarlos. Algunas casas de apuestas y juegos de azar *online* han sucumbido a estas presiones para que sus sistemas no fueran paralizados y perdieran su potencial recaudatorio, especialmente durante fechas señaladas[86].

Finalmente, existen *cibercrímenes económicos de contenido*, en los que podemos identificar a la distribución de pornografía infantil en Internet y los ciberdelitos relativos a la propiedad intelectual. En lo que atañe a la primera, en primer lugar resulta difícil realizar una definición socialmente aceptada de este fenómeno[87]. La pornografía infantil se recoge en el ordenamiento español en el artículo 189 CP.

---

[79] MIRÓ LLINARES, Fernando (2012): *El cibercrimen. Fenomenología (…) (op. cit.)*, p. 72.
[80] BARRIO ANDRÉS, Moisés (2018): *Delitos 2.0. Aspectos penales, procesales (…) (op.* cit.), p. 128.
[81] Los llamados *muleros* también participan del ciberblanqueo de capitales. Normalmente son captados a través de las secciones de empleo de portales de anuncios clasificados, para *trabajar* o bien *ganar dinero desde casa*.
[82] LA GACETA DE SALAMANCA (24.05.2022): *Alerta por nuevos casos de estafas bancarias a través del correo electrónico*. Accesible en: https://www.lagacetadesalamanca.es/virales/alerta-por-nuevos-casos-de-estafas-bancarias-a-traves-del-correo-electronico-EE11262262 [Última consulta realizada en 23.06.2022].
[83] MIRÓ LLINARES, Fernando (2012): *El cibercrimen. Fenomenología (…) (op. cit.)*, pp. 76-77.
[84] Entre estos indicios se encuentran: utilizar direcciones de e-mail no oficiales, realizar un saludo no personalizado, solicitar datos del usuario que el remitente verdadero no pediría porque ya le constan, requerir realizar gestiones con urgencia, proferir amenazas de desactivación de cuentas, contener faltas de ortografía y hasta adjuntar ficheros con *malware* para que los sistemas informáticos se infecten en ejecutarlos.
[85] EL PERIÓDICO (23.05.2022): *Phishing: ¿Qué es y cómo evitarlo?* Accesible en: https://www.elperiodico.com/es/tecnologia/20220523/phishing-que-es-dv-13695404 [Última consulta realizada en 23.06.2022].
[86] MIRÓ LLINARES, Fernando (2012): *El cibercrimen. Fenomenología (…) (op. cit.)*, pp. 83-84.
[87] Según la Decisión Marco 2004/68/JAI, de 22 de diciembre de 2003, del Consejo (ahora derogada), se entiende por pornografía infantil cualquier material pornográfico que describa o represente de manera visual: *un niño real practicando o participando en una conducta sexualmente explícita, incluida la exhibición lasciva de los genitales o de la zona púbica de un niño, (…) a una persona real que parezca ser un niño practicando o participando en la*

La pornografía infantil no tiene un origen puramente cibernético, aunque su uso se ha multiplicado exponencialmente a partir de la irrupción de las nuevas tecnologías. Inicialmente, la divulgación de estos contenidos se hacía en sitios web accesibles por el público e indexados en motores de búsqueda, hecho que provocó su rápida detección por las autoridades y el bloqueo en su uso. Más tarde, se trasladó a foros de menor exposición pública, en que los pedófilos chateaban para intercambiarse los archivos, y en plataformas de descarga, en que el traspaso de datos es inmediato[88]. El hecho que hubiera agentes encubiertos realizando un seguimiento de estas actividades ilícitas motivó la traslación hacia cuentas de correo electrónico compartidas, la deslocalización de diferentes fases de la producción de contenidos en distintos países[89] y el uso de la llamada *dark web*, donde no es posible rastrear a los cibercriminales. La Comisión Europea inició en 2020 un plan para combatir a estos delitos.

Ya en otro ámbito, la ciberpiratería intelectual ha afectado sin lugar a dudas a los creadores de contenidos, ya sea dentro de la industria musical o la editorial. El valor estimado del lucro cesante es considerable y desde las Administraciones Públicas de los países occidentales se ha procurado limitar las actividades de portales de descargas[90] y de visualización de videos en *streaming*, y a la vez incentivar a los ciudadanos para que adquirieran los productos únicamente en negocios legítimos.

En España, el artículo 270.1 del Código Penal comprende el tipo básico de delito contra la propiedad intelectual, en que es un requisito fundamental del injusto que éste se cometa *con ánimo de obtener un beneficio económico directo o indirecto y en perjuicio de tercero*, a la vez que el precepto otorga protección hacia las obras o prestaciones literarias, artísticas o científicas, o su transformación, interpretación o ejecución artística. De este modo, como requisitos de las obras, conviene matizar que en primer lugar, las creaciones deben ser innovaciones o manifestación del ingenio o creatividad humana; en segundo lugar, las creaciones tienen que ser originales, es decir, que se puedan diferenciar de otras creaciones o producciones anteriores; y en tercer lugar, tal creación o producto se debe poder calificar de artístico, literario o científico[91].

2.1.2. Afectaciones por medios informáticos a la intimidad y la privacidad.

Los *cibercrímenes sociales* parten de la traslación a Internet de las relaciones sociales existentes en la vida real. En concreto, se reflejan en los crímenes ya tipificados que surgen de las relaciones y los conflictos entre las personas. La pandemia de coronavirus, que afectó con fuerza a los países occidentales a partir de marzo de 2020, supuso un antes y un después en el uso de las TICs para evitar los encuentros presenciales, ya fuera desde una perspectiva laboral (teletrabajo), como de una óptica de amistad y afectiva, incrementando la incidencia de los *cibercrímenes sociales*. Los *millennials* o nativos digitales, que usan los dispositivos electrónicos para gran parte de sus

conducta mencionada (...) o (...) imágenes realistas de un niño inexistente practicando o participando en la conducta mencionada (...) (art. 1).

[88] MIRÓ LLINARES, Fernando (2012): *El cibercrimen. Fenomenología (...) (op. cit.)*, pp. 109-110.

[89] Por ejemplo, filmaciones de menores realizadas en Filipinas, posteriormente enviadas a Internet en Tailandia y alojadas en un servidor de un país del África occidental, accesibles globalmente.

[90] Como el caso del portal *Megaupload*, que fue cerrado por el FBI en el año 2012.

[91] Hasta la fecha actual, la tendencia ha sido que los creadores de contenidos se han dirigido hacia una selecta lista de plataformas consideradas válidas para difundir sus contenidos y obtener así una remuneración en base al número de visitas o reproducciones, como el caso de los servicios de YOUTUBE o de SPOTIFY. El uso de tales gigantes como intermediarios termina derivando una uniformización global de las preferencias culturales.

actividades diarias, son la generación con una exposición más elevada para sufrir las repercusiones de esta categoría de ciberdelitos.

Como es bien sabido, las personas se pueden acosar a través de medios digitales. El ciberespacio ofrece la posibilidad de realizar, a miles de kilómetros de distancia, injurias, calumnias, amenazas, coacciones y otras agresiones a un coste mínimo, propulsadas fácilmente a través de las redes sociales. En estos casos, concurren dos elementos básicos: que el autor del delito atente contra la dignidad o la libertad de la víctima y que estas acciones tengan lugar a través de las TICs[92]. El ciberacoso se puede diferenciar entre el *cyberstalking* (hostigamiento, persecución o amenazas digitales, es decir, una sucesión de actos de *online harassment*), el ciberacoso sexual (como atentado a la libertad sexual de otra persona) y el *cyberbullying* (es decir, el ciberacoso escolar o entre menores, en el que por definición no intervienen adultos).

El artículo 172 ter del Código Penal ha previsto al tipo básico de *stalking* o acoso la inclusión de una previsión en que el agresor *establezca o intente establecer contacto con ella a través de cualquier medio de comunicación, o por medio de terceras personas*[93]. En cambio, el acoso laboral o *mobbing* está cubierto de forma generalista en el artículo 173.1 CP, sin una especificación para los ciberdelitos. Más silenciado, el *bullying* no dispone de una tipificación particular y la jurisprudencia se ha tenido que remitir al citado precepto[94], entre otros. Eso no obstante, la creación de un tipo penal específico no necesariamente mejoraría la respuesta penal a tales agresiones, ya que existen bienes jurídicos distintos a proteger; por ejemplo, el honor, la libertad, la intimidad y la integridad moral[95].

Uno de los comportamientos que más se ha expandido en el contexto pandémico es el llamado *sexting*, una práctica que consiste en la captación propia y envío de imágenes de contenido erótico o sexual a otras personas, junto a textos sugerentes[96]. Algunos análisis distinguen entre *sexting activo* (la realización de fotos o vídeos propios) y el *sexting pasivo* (la recepción de fotos o vídeos de otra persona)[97]. Evidentemente, existe un riesgo elevado que las imágenes o vídeos sean difundidas a terceros hasta el punto que la reputación personal sea dañada de forma incontrolable e irreversible. Es por esta razón que el Código Penal ha contemplado un tipo cualificado en el artículo 197.7 CP, después de la explosión de un caso mediático relacionado con la filtración pública de un vídeo íntimo de una concejala de un municipio situado en la provincia de Toledo[98] y la necesidad de incorporar el contenido de la Directiva 2013/40/UE (DAI) en la reforma de 2015[99]. El legislador también ha querido hacer frente al fenómeno de la *revenge pornography* o pornografía vengativa, en que el cónyuge o personas relacionadas por análoga relación de afectividad menoscaban a la intimidad de la otra persona, agravando la pena en la mitad superior para estos supuestos[100].

---

[92] MIRÓ LLINARES, Fernando (2012): *El cibercrimen. Fenomenología (…) (op. cit.)*, pp. 84-85.

[93] También si el agresor *adquiera productos o mercancías, o contrate servicios, o haga que terceras personas se pongan en contacto con ella* a través del uso indebido de sus datos personales, una posibilidad amplificada por el uso de las TICs. Así, el *cyberstalking* parte de dos rasgos propios.

[94] BARRIO ANDRÉS, Moisés (2018): *Delitos 2.0. Aspectos penales, procesales (…) (op.* cit.), p. 143.

[95] MIRÓ LLINARES, Fernando (2013): "Derecho penal, «cyberbullying» y otras formas de acoso (no sexual) en el ciberespacio". Barcelona, *Revista de Internet, Derecho y Política*, nº 16, p. 65.

[96] De aquí el origen del término, ya que es un anglicismo procedente de la fusión de los vocablos *sex* y *texting*.

[97] MIRÓ LLINARES, Fernando (2012): *El cibercrimen. Fenomenología (…) (op. cit.)*, p. 93.

[98] GALÁN MUÑOZ, Alfonso (2019): *Los ciberdelitos en el ordenamiento español (…) (op. cit.)*, p. 101.

[99] BARRIO ANDRÉS, Moisés (2018): *Delitos 2.0. Aspectos penales, procesales (…) (op.* cit.), p. 98.

[100] BARRIO ANDRÉS, Moisés (2018): *Delitos 2.0. Aspectos penales, procesales (…) (op.* cit.), pp. 100-101.

Según un estudio realizado por un conocido portal de contactos íntimos en España, el 59% de los usuarios encuestados han declarado que un año después del confinamiento total se sentían más inclinados a realizar *sexting*, mayoritariamente hacia personas desconocidas[101] [102]. Evidentemente, no son fenómenos exclusivos del contexto ibérico. Sobre el uso no autorizado de imágenes íntimas de otras personas, la LAW COMMISSION del Reino Unido ha publicado en julio de 2022 un informe en el cual propone la penalización del llamado *downblousing*[103], que consiste en la captura y difusión de imágenes de los senos de las mujeres, normalmente desde un ángulo vertical, siguiendo la política criminal anteriormente realizada contra el *upskirting*[104].

Para finalizar la visión de los *cibercrímenes sociales* conviene referirnos al llamado *online grooming*, *childgrooming* o *cybergrooming*, es decir, la captación de menores de edad a través de Internet para la consumación de un abuso o agresión sexual (art. 183 CP), o la realización de pornografía y delitos de corrupción de menores (art. 189 CP)[105]. El bien jurídico protegido es la indemnidad sexual del menor, pero también se preserva la formación y desarrollo de la personalidad y sexualidad del mismo[106]. El abusador detecta a los perfiles más débiles, que se proyectan en las redes como jóvenes incomprendidos familiar y socialmente, y se aproximan a ellos simulando que son un interlocutor confiable y cercano[107]. El *groomer* estudia detalladamente su perfil, sus contactos, fotografías y opiniones, para después enviar preguntas de apariencia inocente y empezar el trato nefasto con la víctima[108].

El Código Penal recoge el *cybergrooming* en el artículo 183 ter CP, fijando el contacto hacia un menor de 16 años, a través de cualquier TIC, proponiéndole de concertar un encuentro con el mismo para las finalidades expuestas. Se trata de un *delito de peligro* que no requiere que haya contacto físico entre la persona agresora y la agredida[109]. El bien jurídico protegido es doble: por un lado, el individual, en relación al menor afectado; por el otro lado, supraindividual, sobre la protección de la infancia en general contra la actuación de pederastas[110]. Con este objetivo, la ONG en defensa de los derechos de los niños/as TERRE DES HOMMES y la EUROPOL crearon un perfil de una niña mediante la inteligencia artificial (*Sweetie*), que atrajo la atención de más de

[101] NOTICIAS SALAMANCA (04.05.2021): *El "sexting" crece con la pandemia: el 59% asegura que ahora se siente más motivado a practicarlo*. Accesible en: https://noticiassalamanca.com/sociedad/el-sexting-crece-con-la-pandemia/ [Última consulta realizada en 23.06.2022].

[102] Los adolescentes no valoran suficientemente los riesgos asociados a la práctica del *sexting*, realizándola para impresionar a otros, divertirse o autoafirmarse en una etapa clave y convulsa de la formación de su personalidad.

[103] GREEN, Justice; HOPKINS, Nick; PAINES, Nicholas; GREEN, Sarah; LEWIS, Penney (2022): *Intimate image abuse: a final report*. Londres, The Law Commission of the United Kingdom, nº 407, p. 56.

[104] El *upskirting* consiste en la realización no consentida de fotografías de las nalgas y genitales femeninos por debajo de la falda.

[105] Las personas menores de entre 12 y 14 años son especialmente vulnerables por encontrarse en una fase temprana de la adolescencia, disponer de un amplio acceso y realizar uso intensivo de las TICs y no comprender el cariz sexual de muchas de las conversaciones.

[106] DE LA MATA BARRANCO, Norberto (2017): "El contacto tecnológico con menores del art. 183 ter 1 CP como delito de lesión contra su correcto proceso de formación y desarrollo personal sexual". Granada, *Revista Electrónica de Ciencia Penal y Criminología*, nº 19-10, p. 5.

[107] MIRÓ LLINARES, Fernando (2012): *El cibercrimen. Fenomenología (...) (op. cit.)*, p. 97.

[108] GRANJA, Pedro Javier (2020): "«Grooming»: el minotauro en Internet. El derecho penal del enemigo frente al pederasta de la era digital". Bogotá, *Revista de Derecho Penal y Criminología*, vol. 41, nº 111, p. 81.

[109] BARRIO ANDRÉS, Moisés (2018): *Delitos 2.0. Aspectos penales, procesales (...) (op. cit.)*, p. 154.

[110] GRANJA, Pedro Javier (2020): "«Grooming»: el minotauro en Internet *(...)*" *(op. cit.)*, p. 82.

20.000 pedófilos en todo el mundo entre 2013 y 2014 a través de una estrategia coordinada por el EUROPEAN CYBERCRIME CENTRE (EC3)[111].

2.1.3. Ataques contra intereses generales: ciberespionaje y ciberterrorismo.

El reciente conflicto en Ucrania ha puesto de relieve, todavía más, el uso de las redes para causar estragos en infraestructuras y servicios estratégicos de otros Estados. Según la empresa MICROSOFT, Rusia habría realizado ciberataques e intentos de ciberespionaje a instituciones de 42 países que habrían apoyado a Ucrania desde el inicio de la intervención de marzo de 2022, situadas principalmente en Estados Unidos, Polonia, las Repúblicas Bálticas y los países miembros del Consejo Nórdico. En un 29% de los casos los atacantes habrían conseguido su propósito e incluso se habrían apoderado de informaciones privadas[112].

Es en estos escenarios donde se producen los llamados *cibercrímenes políticos*. En su naturaleza cibernética pura, se tratará de ataques de denegación de servicio en el marco de las llamadas *cyberwar* y el *cyberhacktivism*, junto al uso de *malware* intrusivo para afectar al funcionamiento de los sistemas clave. No se tiene que olvidar que el *ius ad bellum* desarrollado en el contexto de la Carta de las Naciones Unidas considera que los ciberataques son una expresión del uso de la fuerza, de modo que en legítima defensa los Estados podrían responder con armamento convencional[113]. Los *cibercrímenes políticos* también representan en su vertiente general una manifestación de una modalidad delictual tan antigua como la existencia de grupos cohesionados de seres humanos: la guerra y el espionaje han existido desde siempre.

En el contexto pre-bélico de marzo del 2022 y advertida, como otras instituciones públicas, de posibles injerencias informáticas procedentes de la Federación Rusa, la UNIVERSIDAD DEL PAÍS VASCO ordenó el cambio de contraseña urgente a 7.800 trabajadores de los cuerpos docentes y de administración para evitar las graves consecuencias que un ciberataque de gran envergadura podría llegar a comportar en la institución[114] [115]. Este mismo año 2022 la UNIVERSITAT OBERTA DE CATALUNYA ya había padecido una agresión de tipo *ransomware* que había bloqueado el campus virtual durante 20 horas, coincidiendo con el periodo de exámenes telemáticos[116].

---

[111] BUENO DE MATA, Federico (2022): "Novas tendências na investigação de crimes complexos em um contexto europeu globalizado". Rio de Janeiro, *Revista Eletrônica de Direito Processual*, vol. 23, nº 1, pp. 440-441.

[112] 20 MINUTOS (22.06.2022): *Microsoft asegura que Rusia ha lanzado ciberataques contra 42 países aliados de Ucrania desde que empezó la guerra*. Accesible en: https://www.20minutos.es/noticia/5020016/0/microsoft-asegura-que-rusia-ha-lanzado-ciberataques-contra-42-paises-aliados-de-ucrania-desde-que-empezo-la-guerra/ [Última consulta realizada en 23.06.2022].

[113] PONS GAMÓN, Vicente (2017): "Internet, la nueva era del delito *(…)*" *(op. cit.)*, p. 87.

[114] EL MUNDO (03.03.2022): *La Universidad vasca ordena a toda su plantilla proteger sus cuentas electrónicas ante un "ciberataque inminente".* Accesible en: https://www.elmundo.es/pais-vasco/2022/03/03/622115d3fc6c83ed028b457f.html [Última consulta realizada en 23.06.2022].

[115] La Universidad era consciente que se habría producido una venta de credenciales de usuarios propios a terceros después de un presunto ciberataque inicial y adoptó una decisión prudente.

[116] 20 MINUTOS (03.01.2021): La Universitat Oberta de Catalunya vuelve a la normalidad tras el ataque de ransomware que había dañado los servidores centrales de su Campus Virtual. Accesible en: https://www.20minutos.es/tecnologia/ciberseguridad/la-universitat-oberta-de-catalunya-vuelve-a-la-normalidad-tras-el-ataque-de-ransomware-que-habia-danado-los-servidores-centrales-de-su-campus-virtual-4935636/ [Última consulta realizada en 23.06.2022].

A pesar de la relativa reciente conflagración en Ucrania, el uso de las TICs en el marco de la *ciberguerra* no es nuevo en el siglo XXI. En 2007, Estonia sufrió una oleada de ciberataques considerable[117] [118]. Posteriormente, la OTAN instauró el CENTRO DE EXCELENCIA DE CIBERDEFENSA COOPERATIVA en Tallin para asistir a los Estados miembros en situaciones asimilables y a empresas e instituciones[119]. Un año después, presuntos *hackers* rusos produjeron un ataque de denegación de servicio múltiple a sitios web oficiales de la Administración de Georgia después del inicio del conflicto de Osetia del Sur.

Otro ejemplo remarcable es el virus tipo *worm* llamado *Stuxnet*[120], que ha sido considerado la primera arma digital de la historia[121]. En este campo especialmente, la informatización entraña graves riesgos para la gestión de las amenazas nucleares y el uso de la capacidad disuasoria de las grandes potencias, ya que podría provocar el estallido de una escalada involuntaria de *destrucción mutua asegurada*, ya sea solo entre Estados o con la intromisión de agentes no nacionales. Así, en materia de armamento nuclear es fundamental conservar los sistemas de control analógicos y la desconexión total de Internet[122].

Los *cibercrímenes políticos* también adoptan la forma de conductas de *ciberterrorismo*. *Ab initio*, se puede tratar de *ciberataques directos*, como las infecciones con *malware* intrusivo y destructivo, o los ya mencionados ataques DoS. Este es el supuesto que ha sido contemplado en el artículo 573.2 del Código Penal, que establece por remisión que tendrán la consideración de delitos terroristas, los supuestos de daños informáticos contemplados en los artículos 264 a 264 quater CP cuando concurran finalidades terroristas. En el caso de desestabilización grave en el funcionamiento de las estructuras económicas o sociales de un país (artículo 573.1.1 CP), el artículo 573.2 CP no se podría aplicar conjuntamente con el precepto anterior por identidad de fundamento y se debería realizar un concurso de leyes, a ser resuelto por alternatividad[123].

El tipo básico del delito de terrorismo se recoge en el artículo 573.1 del Código Penal y se trata de un *tipo mixto alternativo*[124]. Así, será considerada terrorista la conducta de quien busque de subvertir el orden constitucional, obligar a los poderes públicos a realizar un acto o abstenerse de hacerlo, alterar la paz pública, desestabilizar a una organización internacional o provocar terror en una parte de la población.

Asimismo, la noción de *infraestructuras críticas* es esencial. Éstas comprenden el conjunto de bienes jurídicos, de carácter tangible o intangible, que resultan necesarios para desarrollar las

[117] Después que las autoridades estonianas retiraran una estatua dedicada al *soldado soviético* en el puerto de Tallin, se produjeron una secuencia de ciberataques al país que saturó el ciberespacio y tardó un mes a recuperarse, impactando en el parlamento, ministerios, entidades financieras y medios de comunicación.
[118] BARRIO ANDRÉS, Moisés (2018): *Delitos 2.0. Aspectos penales, procesales (...) (op.* cit.), p. 107.
[119] PONS GAMÓN, Vicente (2017): "Internet, la nueva era del delito: *(...)*" *(op. cit.)*, p. 90.
[120] Después de infiltrarse en el portátil de un especialista en 2010, posiblemente a través de una memoria USB, el virus alteró la programación de las centrifugadoras de enriquecimiento del programa nuclear iraní en la planta de Natanz. El *gusano* modificó su velocidad normal de rotación de los sistemas y el país tuvo dificultades para continuar con la producción un arsenal atómico propio.
[121] WIRED (11.03.2014): *An Unprecedented Look at Stuxnet, the World's First Digital Weapon*. Accesible en: https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/ [Última consulta realizada en 23.06.2022].
[122] FUTTER, Andrew (2022): "La ciberseguridad de los sistemas de armas nucleares. Amenazas, vulnerabilidades y consecuencias". Barcelona, *Vanguardia Dossier*, nº 84, pp. 86-90.
[123] GALÁN MUÑOZ, Alfonso (2019): *Los ciberdelitos en el ordenamiento español (...) (op. cit.)*, p. 197.
[124] BARRIO ANDRÉS, Moisés (2018): *Delitos 2.0. Aspectos penales, procesales (...) (op.* cit.), p. 182.

actividades básicas de gobiernos, organizaciones de complexión diversa y ciudadanos, pertenecientes a una determinada zona geográfica y tiempo. Las *infraestructuras críticas en línea* deberían recibir un tratamiento y tutela jurídicos diferenciados, acorde con su impacto real en la vida de las personas o las actividades de instituciones[125]. No se puede obviar que las TICs pueden usarse para difundir propaganda e incitar a la realización de actos terroristas[126], a la vez que permitirían recabar datos clave, obtener financiación, reclutar participantes para realizar las acciones y adiestrarlos en la fabricación de artefactos, por ejemplo[127]. La red es un medio de gran utilidad para crear un sentimiento de pertenencia entre individuos muy distantes geográficamente y coordinar a células aisladas[128].

Es en este escenario virtual que proliferan los discursos de odio u *online hate speech*, que también son ciberdelitos de cariz político. Inicialmente se han formado entorno a la persecución de grupos étnicos concretos, difundiendo mensajes de odio y violencia contra ellos que se amplifican por el alcance transnacional de las redes y la facilidad con la que se encubren los agresores, con muchos más recursos para aprovecharse del anonimato[129].

En la última década los autores del discurso de odio se han decantado también en contra de otros colectivos significativos, como las personas LGTBIQ+, las que tienen algún tipo de discapacidad o las que manifiestan tener unas preferencias políticas distintas. Para camuflarse bajo una apariencia legítima se han creado las *cloaked websites*, que son sitios web con aspecto de periódicos, ONG u asociaciones para la defensa los derechos civiles que difunden mensajes discriminatorios encubiertos. El diseño de algunas redes sociales como TWITTER, que son plataformas de *microblogging* o difusión de mensajes cortos, dificulta la expresión de sentidos de comunicación distintos y favorece la identificación de un sentido único. Los mensajes de estas redes son pobres en matices y acrecientan la comunicación violenta[130].

2.2. Dificultades procesales propias de los delitos cibernéticos.

2.2.1. Competencia judicial difusa.

El lugar de comisión de los ciberdelitos es una noción fundamental pero a la vez difusa, con impacto en la esfera internacional. Por ejemplo, podría resultar que un ciberatacante introduce un

[125] COAQUIRA FLORES, Ángel Jeancarlo (2020): *Aproximación a la naturaleza jurídica de las infraestructuras críticas: delineando las bases para la ciberseguridad peruana*. En BUENO DE MATA, Federico (Dir.); GONZÁLEZ PULIDO, Irene (Coord.) (2020): *Fodertics 8.0. Estudios sobre tecnologías disruptivas y justicia*. Granada, Editorial Comares, p. 339.

[126] En efecto, el Código Penal contempla condenas para los tipos de enaltecimiento del terrorismo en el artículo 578 CP, con unas penas superiores si los contenidos son difundidos a través de medios de comunicación, Internet, o por medio de servicios de comunicaciones electrónicas o mediante el uso de las TICs. Se justifica esta previsión para punir la rapidez de la difusión que aportan estos medios.

[127] MIRÓ LLINARES, Fernando (2012): *El cibercrimen. Fenomenología (…) (op. cit.)*, p. 129.

[128] Como en el caso del autoproclamado ISIS, que ha realizado un uso extraordinario de los medios audiovisuales y las redes sociales en Internet para captar a jóvenes de países occidentales que se sentían frustrados y discriminados por sus propios orígenes familiares. *Vid.* SAN 3/2017, de 17 de febrero, rec. 6/2016. En este aspecto, resultó de gran interés la ponencia presentada por un miembro investigador del Cuerpo Nacional de Polícia en el *Fórum de Expertos y Jóvenes Investigadores en Derecho y Nuevas Tecnologías – Fodertics 11.0*, que se desarrolló en la UNIVERSIDAD DE SALAMANCA el pasado 5 y 6 de mayo de 2022.

[129] MIRÓ LLINARES, Fernando (2012): *El cibercrimen. Fenomenología (…) (op. cit.)*, p. 114.

[130] MIRÓ LLINARES, Fernando (2016): "Taxonomía de la comunicación violenta y el discurso del odio en Internet". Barcelona, *Revista de Internet, Derecho y Política*, nº 22, p. 97.

peligroso *malware* en un país, este virus circula por servidores ubicados en otros Estados y finalmente causa estragos en terceras naciones, como terminó siendo el caso del mencionado virus *Stuxnet*, que a pesar de estar orientado hacia los sistemas iraníes afectó a infraestructuras de Indonesia y otros países asiáticos. Aquí surge la dificultad de determinar el Derecho aplicable y qué órganos judiciales estarán en condiciones de perseguir el delito[131].

La *teoría de la actividad* defiende que será competente el Estado en el que la acción fue ejecutada, es decir, donde se llevó a cabo la conducta delictiva (*forum loci delicti comissi*). Existen argumentos razonables: el Tribunal dispone de mayores facilidades para obtener pruebas y probablemente para detener y condenar a los presuntos autores. Sin embargo, pueden tratarse de Estados fallidos o *ciberparaísos*, sin ningún interés en perseguir a los criminales, o lugares que el autor ha visitado temporalmente y abandona al cabo de poco tiempo[132]. En cambio, la *teoría del resultado* postula que será competente el Estado donde se produce el resultado típico que termina consumando la infracción. En el caso de los llamados *delitos de resultado*, éste es sencillo de determinar. También se debe atender que es un lugar más próximo a la víctima, donde se lesiona el bien jurídico[133], pero por el contrario es significativamente más difícil llegar a condenar al autor.

Para superar las anteriores dificultades, se creó la *teoría de la ubicuidad*, con ánimo de obtener lo mejor de los dos mundos. Así, basta con que haya acaecido la conducta o el resultado en el Estado respectivo y puedan ser competentes dos o más Estados, a título de ejemplo. Este mecanismo garantiza que las lagunas de punición pueden superarse, en el caso que si el Estado del lugar de comisión considerara la teoría del resultado, y el Estado del lugar del resultado optara por la teoría del lugar de la comisión.

Con el concepto de la *ubicuidad* se produce una mayor seguridad jurídica[134]. El Derecho internacional ha aceptado esta postura en el Convenio de Budapest de 2001, pero con la problemática de considerar que los órganos judiciales deben ceñirse a investigar únicamente a los dispositivos situados en el propio país, excluyendo la búsqueda transfronteriza en el artículo 19.2, hecho que limita las capacidades incriminatorias[135]. El Pleno del TRIBUNAL SUPREMO ha aceptado la *teoría de la ubicuidad* en un acuerdo no jurisdiccional de 3 de febrero de 2005, indicando que el delito se comete en todas las jurisdicciones en las que se haya realizado algún elemento del tipo y que el órgano judicial que primero haya iniciado actuaciones procesales será el competente para instruir la causa[136].

[131] CÁRDENAS ARAVENA, Claudia (2008): "El lugar de comisión de los denominados ciberdelitos". Talca, *Política Criminal. Revista Electrónica Semestral de Políticas Públicas en Materias Penales*, nº 6, p. 2.
[132] CÁRDENAS ARAVENA, Claudia (2008): "El lugar de comisión *(...) (op. cit.)*, pp. 6-7.
[133] CÁRDENAS ARAVENA, Claudia (2008): "El lugar de comisión *(...) (op. cit.)*, pp. 8.
[134] CÁRDENAS ARAVENA, Claudia (2008): "El lugar de comisión *(...) (op. cit.)*, pp. 10-11.
[135] BLANCO, Hernán (2021): "El hackeo con orden judicial en la legislación procesal española a partir de la Ley Orgánica 13/2015 del 5 de octubre". Barcelona, *InDret*, nº 1/2021, p. 489.
[136] MARTÍN CANO, Ángel (2020): *Investigación penal de delitos tecnológicos*. En BUENO DE MATA, Federico (Dir.); GONZÁLEZ PULIDO, Irene (Coord.) (2020): *Fodertics 8.0. (...) (op. cit.)*, p. 287.

2.2.2. Pluralidad indeterminada de personas perjudicadas.

Los delitos cibernéticos pueden afectar a un gran número de ciudadanos, en algunos casos de muy difícil determinación[137] y por razones obvias de posterior personación en un proceso. A modo ilustrativo, se estima que los estragos causados por un virus *ransomware* activo desde abril de 2022 contra una treintena de instituciones públicas en Costa Rica han supuesto unas pérdidas para el país equivalentes a 30 millones de dólares diarios. El MINISTERIO DE HACIENDA y la CAJA COSTARRICENSE DEL SEGURO SOCIAL son algunos de los organismos más afectados, con un impacto en toda la población[138]. En otros casos, las personas perjudicadas pretenderán evitar personarse por miedo o vergüenza a revelar su identidad. A título de ejemplo, en el año 2019 el portal de citas canadiense *Ashley Madison*, que cuenta con una elevada implantación en países occidentales y se caracteriza por promover encuentros sexuales entre personas casadas, sufrió un ciberataque a gran escala y se filtraron los datos personales y financieros correspondientes a más de 37 millones de usuarios[139].

2.2.3. Autoría delictiva y anonimato.

La autoría de los ciberdelitos es en la mayoría de casos un aspecto difícil de ser determinado. El uso de determinadas *personalidades virtuales* encubre la identificación de los delincuentes y permite su impunidad, causando un escenario de *macrovictimización*. Así, sistemas como la red TOR (*The Onion Router*) impiden la trazabilidad de los autores en la *Internet profunda*, creando capas superpuestas asimilables a una cebolla que interrumpen cualquier posibilidad de seguimiento. Es más, el hecho de ser titular de una dirección IP no determina la autoría del delito[140]. A la vez, en el entorno digital las pruebas pueden resultar fácilmente alterables, o sencillamente destruibles e inutilizables para imposibilitar la identificación de los autores[141].

En relación a la autoría delictiva, resulta fundamental la exégesis del TRIBUNAL SUPREMO, concretamente de una reconocida resolución de mayo de 2015, calificada generalmente de la *sentencia de los pantallazos*, para acreditar el contenido de mensajes instantáneos en redes sociales y aplicaciones de mensajería[142]. El Alto Tribunal expresa que *la impugnación de la autenticidad de cualquiera de esas conversaciones, cuando son aportadas a la causa mediante archivos de impresión, desplaza la carga de la prueba hacia quien pretende aprovechar su idoneidad probatoria. Será indispensable en tal caso la práctica de una prueba pericial que identifique el verdadero origen de esa comunicación, la identidad de los interlocutores y, en fin, la integridad de su contenido*[143]. Sin embargo, como acertadamente señala BUENO DE MATA, la resolución podía haber proporcionado recomendaciones más extensas para la aportación de

[137] BARRIO ANDRÉS, Moisés (2018): *Delitos 2.0. Aspectos penales, procesales (…) (op.* cit.), p. 53.
[138] LA VANGUARDIA (17.06.2022): *Costa Rica sigue enfrentando las consecuencias de dos meses de ciberataques*. Accesible en: https://www.lavanguardia.com/vida/20220618/8349187/costa-rica-sigue-enfrentando-consecuencias-dos-meses-ciberataques.html [Última consulta realizada en 23.06.2022].
[139] LA GACETA DE SALAMANCA (11.01.2019): *Millones de adúlteros al descubierto gracias al hackeo de una web*. Accesible en: https://www.lagacetadesalamanca.es/hemeroteca/millones-adulteros-descubierto-gracias-hackeo-web-IRGS149634 [Última consulta realizada en 23.06.2022].
[140] BARRIO ANDRÉS, Moisés (2018): *Delitos 2.0. Aspectos penales, procesales (…) (op.* cit.), pp. 44-45.
[141] BARRIO ANDRÉS, Moisés (2011): "La ciberdelincuencia en el derecho español". Madrid, *Revista de las Cortes Generales*, nº 83, pp. 278-279.
[142] La resolución se pronuncia en relación a la red TUENTI, aunque los argumentos sientan una doctrina extrapolable a plataformas como WHATSAPP o el propio correo electrónico.
[143] STS 300/2015, de 19 de mayo, rec. 2387/2014, FJ 4.

pruebas electrónicas, como el sellado de tiempo (*time stamping*), la cooperación con las plataformas digitales o la obligatoriedad de las pruebas periciales en el enjuiciamiento por instancias superiores[144].

Algunos aspectos podrán ser fácilmente acreditados ante el Tribunal mediante una navegación con la presencia del Letrado de la Administración de Justicia, que podrá proporcionar fe pública de la forma en que se han extraído los documentos basados en impresiones de pantalla. Ahora bien, este hecho no excluye que se produzcan falsificaciones o fraudes, y aquí resultará de interés acreditar la veracidad del contenido mediante la declaración de testigos y el desarrollo de una prueba pericial informática. Hay elementos que solo se pueden percibir a través de una comprobación de expertos, por ejemplo, la real existencia del sitio web, quien es su titular, un análisis de metadatos informativos sobre los accesos realizados, etc.[145].

3. La obtención y custodia de la prueba electrónica en los delitos cibernéticos

Como señala GONZÁLEZ MONJE, resulta especialmente dificultoso encontrar un equilibrio entre seguridad y privacidad. Tienen que existir garantías y controles para que la *vigilancia* de los ciudadanos esté sujeta al imperio de la ley, y no al libre arbitrio de empresas y gobiernos, que nos aboquen a un *Estado preventivo de pleno derecho*[146]. En la presente sección se estudiarán las reglas relativas a las principales diligencias de investigación que afectan a los delitos cibernéticos: en primer lugar, el registro de dispositivos de almacenamiento masivo de información; y en segundo lugar, el registro remoto de equipos informáticos, en ambos casos con observancia de la Circular 5/2019, sobre registro de dispositivos y equipos informáticos, elaborada por la FISCALÍA GENERAL DEL ESTADO. El capítulo contará con un análisis de la figura del agente encubierto informático, clave en la investigación de los delitos tecnológicos vinculados a organizaciones criminales. Finalmente, ya en el terreno de la prueba, se observarán instrumentos de prueba de los ciberdelitos de uso generalizado en sede judicial.

3.1. El registro de dispositivos de almacenamiento masivo de información.

3.1.1. Necesidad de motivación concreta.

El registro de dispositivos y equipos informáticos es un acto con una elevada injerencia en los Derechos Fundamentales de la persona investigada, ya que permite descubrir adscripciones ideológicas y religiosas, aficiones, datos de salud y orientación sexual, etc.[147]. En este sentido, según la argumentación del TRIBUNAL CONSTITUCIONAL, *quizás, estos datos que se reflejan en un ordenador personal pueden tacharse de irrelevantes o livianos si se consideran aisladamente,*

[144] BUENO DE MATA, Federico (2015): "Acerca de la validez de los pantallazos como prueba electrónica en juicio". Salamanca, *Ars Iuris Salmanticensis*, vol. 3, p. 324.
[145] RICHARD GONZÁLEZ, Manuel (2017): *Investigación y prueba mediante medidas (...) (op. cit.),* p. 50.
[146] GONZÁLEZ MONJE, Alicia (2017): "Amenazas a la seguridad y privacidad: la dificultad del equilibrio perfecto". Madrid y Elche, *Revista Europea de Derechos Fundamentales*, nº 29, p. 293.
[147] BUENO DE MATA, Federico (2019): *La diligencias de investigación penal en la cuarta revolución industrial. Principios teóricos y problemas prácticos*. Cizur Menor (Navarra), Editorial Aranzadi – Thomson Reuters, p. 161.

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[148].

El artículo 588 sexies a) LECRIM refuerza, desde la reforma del año 2015, la necesidad de una motivación individualizada del registro de dispositivos de almacenamiento masivo de información, expresando que con motivo 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* (ap. 1).

La FISCALÍA GENERAL DEL ESTADO se ha referido en estos casos al *derecho al propio entorno virtual*[149], considerándolo un Derecho Fundamental de última generación después de invocar a la jurisprudencia del TRIBUNAL SUPREMO, que quedaría integrado dentro del artículo 18 CE[150]. El Alto Tribunal ya había matizado el tratamiento jurídico de tal derecho en una jurisprudencia precedente a la reforma de 2015, reiterando que *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 (…) siempre y en todo caso, con carácter anticipado, actuando como verdadero presupuesto habilitante de naturaleza formal*[151].

Es importante tener en cuenta que el precepto no autoriza el acceso al contenido de los dispositivos por el mero hecho de efectuar un registro domiciliario. La mera incautación de un sistema informático es equivalente a recoger y custodiar un arma o cualquier objeto vinculado con la perpetración del crimen, es decir, el cuerpo del delito[152], pero el acceso a los datos presenta una calificación distinta; no se trata de un simple instrumento recipiendario de datos con una mayor o menor vinculación con el derecho a la intimidad del usuario afectado[153], sino que se debe atender a que contiene datos de carácter personal y comunicaciones o conversaciones con otras personas[154], con informaciones reveladoras de su salud, aficiones, tendencias sexuales, ideologías, creencias religiosas, etc.[155].

[148] STC 173/2011, de 7 de noviembre, rec. 5928/2009, FJ 3.
[149] FISCALÍA GENERAL DEL ESTADO (2019): *Circular 5/2019, sobre registro de dispositivos y equipos informáticos*. Madrid, p. 5.
[150] STS 489/2018, de 23 de octubre, rec. 1674/2017, FJ 5.
[151] STS 342/2013, de 17 de abril, rec. 1461/2012, FJ 8.
[152] RICHARD GONZÁLEZ, Manuel (2017): *Investigación y prueba mediante medidas de intervención de las comunicaciones, dispositivos electrónicos y grabación de imagen y sonido*. Las Rozas (Madrid), Wolters Kluwer, p. 172.
[153] STS 785/2008, de 25 de noviembre, rec. 227/2008, FJ 4.
[154] PÉREZ ESTRADA, Miren Josune (2019): "La protección de los datos personales en el registro de dispositivos de almacenamiento masivo de información". Porto Alegre, *Revista Brasileira de Direito Processual Penal*, vol. 5, nº 3, p. 1310.
[155] FERNÁNDEZ-GALLARDO, Javier Ángel (2016): "Registro de dispositivos de almacenamiento masivo de información". Santiago de Compostela, *Dereito*, vol. 25, nº 2, p. 35.

Según la FISCALÍA GENERAL DEL ESTADO, esta situación es más garantista al momento presente que antes de la reforma de la LECRIM[156], opinión diferida en la doctrina autorizada[157]. Así, actualmente *la simple incautación de cualquiera de los dispositivos (...) 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* (ap. 2). Las mismas reglas se aplican para el caso de dispositivos electrónicos incautados fuera del domicilio de la persona investigada, en que prevalecerá la decisión del juez sobre la indispensabilidad del acceso a la información albergada en ellos para poder autorizar su análisis (art. 588 sexies b) LECRIM).

3.1.2. Características de la autorización judicial.

El artículo 588 sexies c) LECRIM es un extenso precepto que contiene las principales características que rigen la autorización judicial. En primer lugar, la norma no menciona el tipo de resolución del órgano de instrucción, pero se puede entender que se trata de un auto por la necesaria motivación que lo caracteriza. Con esta resolución establecerá *los términos y el alcance del registro y podrá autorizar la realización de copias de los datos informáticos. Fijará también las condiciones necesarias para asegurar la integridad de los datos y las garantías de su preservación para hacer posible, en su caso, la práctica de un dictamen pericial* (ap. 1). Así, el precepto resalta la importancia de la cadena de custodia de la prueba y la previsión que intervenga un perito informático.

Para evitar causar perjuicios a los titulares o propietarios de los equipos informáticos, la LECRIM ha enfatizado la posibilidad de obtener una copia de los datos o archivos *en condiciones que garanticen la autenticidad e integridad de los datos* (ap. 2). Esta opción no se contempla si los dispositivos han sido el objeto o instrumento del delito, o existen otras razones que justifiquen la incautación. Asimismo, el registro se puede ampliar a otros sistemas informáticos si existan razones fundadas para ello, mediando autorización judicial, salvo que la aquiescencia inicial ya lo previera. Las particularidades del registro de dispositivos hacen que en este caso no se apliquen las reglas de concurrencia de sujetos en el acto que impone el artículo 596 LECRIM para el registro domiciliario, donde se llegan a prever supuestos de desobediencia grave a la autoridad si familiares o testigos se resisten a presenciar el acto[158].

Ante situaciones de urgencia, *la Policía Judicial o el fiscal podrán llevarlo a cabo, informando al juez inmediatamente, y en todo caso dentro del plazo máximo de veinticuatro horas, de la actuación realizada, la forma en que se ha efectuado y su resultado* (ap. 3). Posteriormente, el juez competente revocará o confirmará la actuación en un máximo de 72 horas desde que fue ordenada la interceptación, también de forma motivada. El *modus operandi* de las situaciones de urgencia de la ampliación del registro se proyecta en casos urgentes *en que se aprecie un interés constitucional legítimo* (ap. 4). En caso que la orden de autorización judicial no se haya ampliado para cubrir tales diligencias de investigación, se podría aplicar la teoría del fruto del árbol

[156] *Con anterioridad a la reforma de la LECrim, el modo habitual de proceder era el de considerar amparado su registro por la resolución judicial que autorizaba la entrada en el domicilio del investigado y el registro de los libros, papeles y demás documentos del mismo que pudieran tener relación con el delito*. Extracto de FISCALÍA GENERAL DEL ESTADO (2019): *Circular 5/2019 (...) (op. cit.)*, p. 18.
[157] BUENO DE MATA, Federico (2019): *La diligencias de investigación (...) (op. cit.)*, p. 167.
[158] RODRÍGUEZ RUBIO, Carmen (2020): "Nuevas diligencias de investigación *(...)*" *(op. cit.)*, p. 289.

envenenado y la teoría de la conexión de antijuridicidad, que es aceptada por la jurisprudencia desde la década de 1980[159]. La prueba ilícita provocará su rechazo o exclusión, dependiendo del momento procesal en que se verifique este estado desfavorable[160]. Es interesante la argumentación desarrollada por el Tribunal Supremo en una reciente resolución controvertida[161].

Es interesante que el indicado precepto permita compeler *a cualquier persona que conozca el funcionamiento del sistema informático o las medidas aplicadas para proteger los datos informáticos (...) que facilite la información que resulte necesaria, siempre que de ello no derive una carga desproporcionada para el afectado, bajo apercibimiento de incurrir en delito de desobediencia* (ap. 5). De forma natural, se excepciona al propio investigado o encausado, las personas dispensadas de la obligación de declarar por razón de parentesco y las que no pueden declarar por secreto profesional (art. 416.2 LECRIM). Además, si la colaboración produce gastos, se pretende resarcirlos[162].

Según BUENO DE MATA, el hecho que el precepto se refiera a *cualquier persona* es perjudicial para la imagen de capacidad técnica de los cuerpos de la Policía Judicial; asimismo, se abriría la puerta a la contratación encubierta por la Administración de *hackers* y expertos informáticos que operen con fines criminales o sin una ética mínima[163]. En cambio, para RICHARD GONZÁLEZ, el artículo 588 sexies c) LECRIM es una previsión para contratar a especialistas informáticos desde la Administración de Justicia, que decidirán libremente su colaboración[164]. Esta previsión de colaboración proviene del mandato hacia los Estados parte establecido en el artículo 19.4 del Convenio de Budapest, que literalmente ya menciona a *cualquier persona*[165].

Aunque el precepto ha previsto la autorización judicial como formalidad previa para el acceso, la Circular 5/2019 de la FISCALÍA GENERAL DEL ESTADO ha ido más allá y ha colmado una laguna legal significativa, que es el consentimiento del investigado para permitir el registro del dispositivo de almacenamiento masivo de información, sin necesidad de disponer de autorización judicial[166]. Tal consentimiento se manifestará de forma expresa, recogiéndose por escrito y mediando una fase previa de información, explicando las consecuencias procesales asociadas. El otorgante tiene que disponer de capacidad para otorgar el consentimiento, esto es, tener capacidad de obrar suficiente y no encontrarse en un estado emocional que imposibilite comprender sus consecuencias.

---

[159] BUENO DE MATA, Federico (2015): "Comentarios y reflexiones sobre la Ley Orgánica 13/2015 de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica". *Diario La Ley*, nº 8627.

[160] BUJOSA VADELL, Lorenzo Mateo; BUSTAMANTE RÚA, Mónica María; TORO GARZÓN, Luis Orlando (2021): "La prueba digital producto de la vigilancia secreta: obtención, admisibilidad y valoración en el proceso penal en España y Colombia". Porto Alegre, *Revista Brasileira de Direito Processual Penal*, vol. 7, nº 2, p. 1368.

[161] *Vid.* STS 597/2022, de 15 de junio, rec. 10705/2021, FJ 1. El punto de partida es una víctima de abusos sexuales que aprovecha el desprecio que tiene su agresor contra ella para retener y entregar su teléfono móvil a la Policía. En el dispositivo se encuentran pruebas relevantes y su análisis se produce, *ab initio*, sin autorización judicial.

[162] MARTÍN CANO, Ángel (2020): *Investigación penal de delitos tecnológicos*. En BUENO DE MATA, Federico (Dir.); GONZÁLEZ PULIDO, Irene (Coord.) (2020): *Fodertics 8.0. Estudios sobre tecnologías disruptivas y justicia.* Granada, Editorial Comares, p. 295.

[163] BUENO DE MATA, Federico (2015): "Comentarios y reflexiones sobre la Ley Orgánica *(...) (op. cit.)*.

[164] RICHARD GONZÁLEZ, Manuel (2017): *Investigación y prueba mediante (...) (op. cit.),* p. 181.

[165] RODRÍGUEZ RUBIO, Carmen (2020): "Nuevas diligencias de investigación y de prueba: el registro de dispositivos de almacenamiento masivo de información". *Foro, Nueva Época*, vol. 23, nº 1, p. 277.

[166] BUENO DE MATA, Federico (2019): *La diligencias de investigación (...) (op. cit.)*, p. 170.

Por analogía se podría aplicar el artículo 551 LECRIM sobre la entrada en el domicilio[167] y la jurisprudencia sentada en la STC 173/2011, de 7 de noviembre, sobre el consentimiento tácito del titular del dispositivo para el acceso a datos personales sin extralimitaciones[168], que trató el caso de un pedófilo que fue denunciado por el técnico informático al que acudió para realizar una reparación ordinaria del equipo, y de la que la doctrina no ha aceptado de forma unánime el fallo desestimatorio del amparo del TC por vulneración de derechos[169]. La jurisprudencia ha descartado las llamadas *investigaciones prospectivas* o *inquisitio generalis* en dispositivos de almacenamiento masivo para encontrar indicios penales a determinadas personas[170]. Para evitar una intromisión excesiva en el derecho a la intimidad de la persona investigada, según RICHARD GONZÁLEZ la policía deberá realizar una búsqueda en el dispositivo a través de palabras clave[171], una previsión garantista que puede terminar generando mayores incentivos a los cibercriminales para realizar un camuflaje de ficheros bajo denominaciones inocuas. No se puede permitir un registro *ilimitado*, pero delimitar el grado de injerencia *ex ante*, sin que el órgano judicial conozca la dificultad de la intervención, resulta ser una tarea compleja[172].

Otro aspecto digno de mención es la realización de registros de almacenamiento masivo de forma urgente y sin autorización judicial por parte de la Policía Judicial. Dicha posibilidad excepcional está avalada por la jurisprudencia Constitucional previa, fundamentada en proteger el interés general del Estado en materia de política criminal por encima de la protección de datos personales[173]: *(…) Esa regla general se excepciona en los supuestos en que existan razones de necesidad de intervención policial inmediata, para la prevención y averiguación del delito, el descubrimiento de los delincuentes y la obtención de pruebas incriminatorias. En esos casos estará justificada la intervención policial sin autorización judicial, siempre que la misma se realice también desde el respeto al principio de proporcionalidad*[174].

3.1.3. Duración del registro y modo de preservación de los datos.

El capítulo de la LECRIM dedicado al registro de dispositivos de almacenamiento masivo de información no contiene una previsión de duración específica; así, se deberá atender a la regla general del artículo 588 bis e) LECRIM, que indica que las medidas *tendrán la duración que se especifique para cada una de ellas y no podrán exceder del tiempo imprescindible para el esclarecimiento de los hechos.* Asimismo, *la medida podrá ser prorrogada, mediante auto motivado, por el juez competente, de oficio o previa petición razonada del solicitante, siempre que subsistan las causas que la motivaron*. El registro de dispositivos y equipos informáticos tiene una naturaleza diferente al registro domiciliario, de modo que se podría llegar a prolongar durante días e incluso semanas, mientras que el otro requeriría de unas pocas horas[175]. En otros términos, el acceso al terminal se podría producir en un día y hora determinados, pero una vez

[167] FISCALÍA GENERAL DEL ESTADO (2019): *Circular 5/2019 (…) (op. cit.)*, p. 15.
[168] PÉREZ ESTRADA, Miren Josune (2019): "La protección de los datos personales *(…)*" *(op. cit.)*, p. 1319.
[169] FERNÁNDEZ-GALLARDO, Javier Ángel (2016): "Registro de dispositivos *(…)*" *(op. cit.)*, p. 52.
[170] *Vid.* SAN 343/2021, de 14 de junio, rec. 337/2021 y SAN 23/2019, de 20 de noviembre, rec. 5/2016, FJs 6 y 7, sobre registros practicados en dispositivos de almacenamiento masivo propiedad de la sociedad Abengoa, en aquel entonces una empresa de gran envergadura con cotización bursátil.
[171] RICHARD GONZÁLEZ, Manuel (2017): *Investigación y prueba mediante (…) (op. cit.),* p. 186.
[172] ARRABAL PLATERO, Paloma (2020): "Las diligencias de investigación tecnológica en el proceso penal español". Valparaíso, *Revista de Ciencias Sociales*, nº 76, p. 95.
[173] PÉREZ ESTRADA, Miren Josune (2019): "La protección de los datos personales *(…)*" *(op. cit.)*, p. 1318.
[174] STC 70/2002, de 3 de abril, rec. 3787/2001, FJ 9.
[175] FISCALÍA GENERAL DEL ESTADO (2019): *Circular 5/2019 (…) (op. cit.)*, p. 20.

extraída la información, la intimidad se vería menoscabada durante el tiempo de análisis posterior[176].

La *prueba electrónica*, entendida como proyección de la realidad fáctica adquirida por las diligencias de investigación, se caracteriza por tres elementos: en primer lugar, los datos; pero estos no existen solos, se requiere de un soporte y de un dispositivo. Por lo tanto, la realización de copias implica que el Letrado de la Administración de Justicia acredite, a través de la fe pública judicial, que se mantiene la integridad del contenido y se pone éste en conocimiento y en contacto directo del órgano judicial, para asegurar el principio de inmediación[177]. La Circular 5/2019 ha recalcado que para garantizar la integridad de los dispositivos *resultará necesario su adecuado precinto y puesta a disposición judicial en el momento de su incautación. Cualquier posterior apertura del precinto, como sería la necesaria para llevar a cabo el clonado del dispositivo, deberá hacerse bajo la fe del Letrado de la Administración de Justicia; una vez realizado el clonado, el dispositivo deberá ser nuevamente precintado*[178]. Sin embargo, la jurisprudencia de la Audiencia Nacional se ha mostrado flexible con este requisito de fe pública del LAJ, llegando a omitir su intervención en el momento del clonado[179].

Como ha quedado apuntado *ut supra*, el TRIBUNAL SUPREMO ha perfilado la doctrina general sobre el registro de dispositivos de almacenamiento masivo de información durante la década de 2010, delimitando el *derecho al propio entorno virtual*[180], que ha sido definido 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*[181]. Se muestra un tratamiento jurídico unitario de los derechos del artículo 18 CE, que permite articular un grado de protección superior que no sobre cada derecho individualizado[182], una decisión ciertamente lógica en una época en que cualquier dispositivo almacena una cantidad ingente de datos plurifuncionales de cada usuario[183].

3.2. El registro remoto de equipos informáticos.

3.2.1. Presupuestos procesales.

A diferencia de los registros de dispositivos de almacenamiento masivo de información, un registro remoto es susceptible de causar una afectación mayor a los Derechos Fundamentales de

[176] BUENO DE MATA, Federico (2019): *La diligencias de investigación (...) (op. cit.)*, p. 46.
[177] BUENO DE MATA, Federico (2019): *La diligencias de investigación (...) (op. cit.)*, p. 175.
[178] FISCALÍA GENERAL DEL ESTADO (2019): *Circular 5/2019 (...) (op. cit.)*, p. 30.
[179] *Vid.* SAN 23/2019, de 20 de noviembre, rec. 5/2016, FJ 10, ap. 4: *El clonado de los contenidos de archivos informáticos garantiza la integridad de la información y el mantenimiento de la cadena de custodia, lo que afecta a la valoración de la prueba documental, no siendo precisa para su validez la intervención del Juez ni siquiera del Secretario Judicial, lo que es jurisprudencia reiterada (...). Tampoco es necesaria la presencia del interesado o su Letrado (...).* En este mismo sentido se pronuncia la STS 580/2020, de 5 de noviembre, rec. 186/2019, FJ 12: *(...) el volcado de la información contenida en un dispositivo de almacenamiento masivo es meramente funcional, y no se lleva a cabo una selección, sino que se realiza una copia íntegra a fin de realizar una pericia sobre ese contenido (...). Por ello, ni siquiera es necesaria la presencia de la Letrada de la Administración de Justicia.*
[180] STS 786/2015, de 4 de diciembre, rec. 10447/2015, FJ 1, y STS 597/2022, de 15 de junio, rec. 10705/2021, FJ 1.
[181] STS 342/2013, de 17 de abril, rec. 1461/2012, FJ 8.
[182] PÉREZ ESTRADA, Miren Josune (2019): "La protección de los datos personales *(...)*" *(op. cit.)*, p. 1313.
[183] STS 489/2018, de 23 de octubre, rec. 1674/2017, FJ 5.

la persona investigada o encausada, teniendo en cuenta que ésta no estará informada que un *software* espía se encuentra infiltrado en sus equipos informáticos para facilitar datos de su actividad diaria de forma telemática y constante. Todos los derechos del artículo 18 CE son susceptibles de ser afectados[184]. Así, la doctrina lo ha llegado a calificar de *hacking judicial*[185].

Por esta razón, el legislador ha limitado a *casos extremos* los supuestos tasados en que se puede aplicar la medida en el artículo 588 septies a) LECRIM, concretamente a: los delitos cometidos en el seno de organizaciones criminales; los delitos de terrorismo; los delitos cometidos contra menores o personas con la capacidad modificada judicialmente; los delitos contra la Constitución, de traición y relativos a la defensa nacional; y los delitos cometidos a través de instrumentos informáticos o de cualquier otra de las TICs[186]. En cambio, en el acceso directo a equipos informáticos, el legislador podía llegar a contar con el consentimiento del investigado, naturalmente una circunstancia muy diferente a investigar un uso diario de un terminal[187].

Así, la resolución judicial que autorice el registro remoto deberá concretar los ordenadores, dispositivos electrónicos y sistemas informáticos sobre los que se pretende llevar a cabo la medida. Asimismo, constará su alcance, la forma de acceso y recolección de datos o archivos relevantes para la causa y el programa encargado de capturar las informaciones, junto a los agentes autorizados para ejecutar la medida, la realización y conservación de copias de los datos, y las medidas para preservar la integridad de los datos almacenados, *así como para la inaccesibilidad o supresión de dichos datos del sistema informático al que se ha tenido acceso* (ap. 2). Si los agentes consideran que los datos objeto de búsqueda se encuentran en otro sistema informático podrán solicitar al órgano judicial una ampliación del registro (ap. 3).

Es interesante que la Circular de la FGE se haya pronunciado sobre el acceso de datos situados en el extranjero. Según la Fiscalía, *el criterio deberá ser siempre el de exigir un vínculo territorial con España; el Juez podrá autorizar el registro remoto de un sistema informático que se encuentre en España, aunque a través de él se acceda a datos ubicados en el extranjero, pero no autorizar el registro de un sistema localizado en el extranjero, sin acudir para ello a la cooperación judicial internacional*[188]. Este hecho obliga a hacer uso a los instrumentos de cooperación procesal para el caso de ordenadores situados fuera de España. En consecuencia, resulta deseable una adición en el marco del Convenio de Budapest que permita incluir el registro remoto transfronterizo desde un Estado parte, con capacidades de seguimiento y acceso íntegro[189], en este contexto de Derecho internacional exitoso[190] y más extenso que el previsto en los instrumentos jurídicos para los Estados miembros de la Unión Europea.

[184] BUENO DE MATA, Federico (2019): *La diligencias de investigación (...) (op. cit.)*, p. 84.
[185] ARRABAL PLATERO, Paloma (2020): "Las diligencias de investigación tecnológica (…)" *(op. cit.)*, p. 99.
[186] Se detecta una falta de concreción significativa, que podría suponer el despliege de medidas de índole muy invasiva para ciberdelitos de una envergadura menor en proporción a los parámetros tipológicos del Código Penal.
[187] BUENO DE MATA, Federico (2019): *La diligencias de investigación (...) (op. cit.)*, p. 166.
[188] FISCALÍA GENERAL DEL ESTADO (2019): *Circular 5/2019 (...) (op. cit.)*, p. 18.
[189] GONZÁLEZ PULIDO, Irene (2022): *Diligencias de investigación tecnológicas para la lucha contra la ciberdelincuencia grave. Especial referencia a la utilización del registro remoto para la investigación de ciberataques contra infraestructuras críticas y estratégicas*. Tesis Doctoral, Universidad de Salamanca, Programa de Doctorado en Administración, Hacienda y Justicia en el Estado Social, p. 697.
[190] La red 24/7, regulada en el art. 35 del Convenio de Budapest de 2001, es un ejemplo de buena práctica de coordinación entre los sistemas de los distintos Estados parte durante las 24 horas del día, 7 días de la semana.

Eso no obstante, el redactado no es lo suficientemente clarificador y los parámetros de la intervención no son del todo terminantes para servidores ubicados fuera del Estado, en que por razones prácticas se acabaría aplicando normativa y jurisdicción española[191]. Así, difícilmente se puede obtener cooperación de países que ofrecen el llamado *bulletproof hosting*, es decir, *paraísos cibernéticos*, sin ningún control de contenido de los sitios web que albergan y que se niegan a cooperar ante solicitudes extranjeras de baja de la web, obtención de los datos almacenados o informaciones relativas a los clientes[192], porque no han tipificado los delitos[193].

3.2.2. Deber de colaboración de los prestadores de servicios.

El artículo 588 septies b) LECRIM define el *deber de colaboración* hacia los agentes investigadores de los prestadores de servicios y los titulares o responsables del sistema informático o base de datos objeto del registro. Tales sujetos prestarán *la colaboración precisa para la práctica de la medida y el acceso al sistema. Asimismo, están obligados a facilitar la asistencia necesaria para que los datos e información recogidos puedan ser objeto de examen y visualización* (ap. 1).

Los sujetos requeridos *tendrán la obligación de guardar secreto* sobre las actividades mencionadas, con responsabilidad, en caso de incumplimiento, de incurrir en un delito de desobediencia (art. 588 ter e) LECRIM). Como en el caso de los registros de dispositivos de almacenamiento masivo de información, los agentes y autoridades pueden compeler a los particulares que conozcan el funcionamiento del sistema informático o las medidas aplicadas a facilitar la colaboración que consideren pertinente (ap. 2). Acertadamente, la Circular de la FISCALÍA GENERAL DEL ESTADO ha valorado que los registros remotos sobre equipos informáticos *se encuentran a medio camino entre el registro de dispositivos de almacenamiento masivo de información y la interceptación de comunicaciones telemáticas*[194], una naturaleza que implica un mayor deber de colaboración de las corporaciones.

3.2.3. Duración del registro y modo de preservación de los datos.

El artículo 588 septies c) LECRIM ha establecido una duración máxima de la medida de un mes, *prorrogable por iguales períodos hasta un máximo de tres meses*. La norma guarda silencio sobre el momento de inicio del cómputo del plazo, siendo asimilable al instante de la autorización de la medida. Sin embargo, la Fiscalía ha razonado de forma práctica y considera plausible que se produzcan retrasos causados por los prestadores de servicios, de modo que resultaría necesario que el *dies a quo* empezara en el momento del efectivo funcionamiento de la medida de registro y no cuando se emita la autorización por parte del órgano judicial[195]. Esta posición es sustentada también por la doctrina[196].

---

[191] BUENO DE MATA, Federico (2019): *La diligencias de investigación (...) (op. cit.)*, p. 185.
[192] BLANCO, Hernán (2021): "El hackeo con orden judicial en la legislación procesal española a partir de la Ley Orgánica 13/2015 del 5 de octubre". Barcelona, *InDret*, nº 1/2021, p. 488.
[193] PONS GAMÓN, Vicente (2017): "Internet, la nueva era del delito: ciberdelito, ciberterrorismo, legislación y ciberseguridad". Quito, *URVIO - Revista Latinoamericana de Estudios de Seguridad*, nº 20, p. 82.
[194] FISCALÍA GENERAL DEL ESTADO (2019): *Circular 5/2019 (...) (op. cit.)*, p. 53.
[195] FISCALÍA GENERAL DEL ESTADO (2019): *Circular 5/2019 (...) (op. cit.)*, p. 69.
[196] BUENO DE MATA, Federico (2019): *La diligencias de investigación (...) (op. cit.)*, pp. 198-199.

Las técnicas propias del registro remoto se caracterizan por usar sistemas de *spyware*, o *software* espía, como los llamados *trojans* o los *keyloggers*, que infectan el terminal intervenido y permiten una monitorización continuada desde sistemas externos[197]. Si las contraseñas han sido guardadas en el dispositivo el registro será más veloz. De la misma forma, si el equipo se conecta a sistemas de red de área local (LAN) infectados el seguimiento resultará más cómodo. El futuro del llamado *IoT* (*Internet de las cosas*, por sus siglas en inglés) depara amplias expectativas para controlar de forma constante sistemas electrónicos de tipología diversa[198], desde ordenadores y teléfonos inteligentes a televisores y neveras, pudiendo llegar a trazar un retrato muy completo de la vida diaria de las personas investigadas.

Los datos obtenidos se preservarán en sistemas externos gestionados por la Policía Judicial. En algunos casos, es posible *la inaccesibilidad o supresión de dichos datos del sistema informático al que se ha tenido acceso*, como indica el mencionado precepto, para evitar que el sujeto investigado pueda eliminar fuentes de prueba. Para reforzar la inmutabilidad de las pruebas entre su adquisición y su invocación en el proceso penal BUENO DE MATA sugiere la preservación y conservación del dispositivo de almacenamiento, hecho que la Circular de la Fiscalía no ha llegado a concretar[199].

3.3. La intervención del agente encubierto.

La figura del agente encubierto o infiltrado tiene cabida perfectamente en el contexto informático. Regulado en el artículo 282 bis LECRIM, está previsto para combatir desde el interior de las propias organizaciones criminales sus actividades delictivas, que causan un daño social de gran envergadura en los tiempos presentes. A título de ejemplo, inciden en el tráfico de órganos humanos, el secuestro de personas, la trata de seres humanos, los delitos contra la salud pública, las acciones terroristas[200], etc. La actuación del agente encubierto permite una exploración óptima de los hechos a investigar, con un trazado preciso del aparato delincuencial mediante su infiltración[201]. Las organizaciones criminales aprovechan la división del trabajo para disolver la responsabilidad de sus integrantes en el conjunto de la entidad, junto a la combinación de actividades lícitas e ilícitas; así, los ojos infiltrados son muy relevantes[202]. Dicho investigador tiene que ser necesariamente un miembro voluntario de la Policía Judicial, de modo que quedan excluidos del contenido de la LECRIM los *agentes secretos*, es decir, los integrantes del Cuerpo Nacional de Inteligencia, regulado por la Ley 11/2002, de 6 de mayo[203].

Para el debido encubrimiento del agente se le proporciona una identidad supuesta, con expedición de documentos de identidad simulados; está autorizado para adquirir y transportar los objetos,

[197] Estados Unidos está en la primera línea de *software* espía con fines policiales. Algunos de los programas más utilizados són el *Carnivore*, la *Magic Lantern* o el *CIPAV* (*Computer and Internet Protocol Address Verifier*). A este conjunto se debe añadir el *Pegasus* israelí, que únicamente tiene permitida su compra por parte de Estados y es usado mayormente en labores de inteligencia, con graves repercusiones mediáticas este año 2022.
[198] BUENO DE MATA, Federico (2019): *La diligencias de investigación (...) (op. cit.)*, pp. 188-191.
[199] BUENO DE MATA, Federico (2019): *La diligencias de investigación (...) (op. cit.)*, p. 196.
[200] *Vid.* SAN 3/2017, de 17 de febrero, rec. 6/2016, en que el agente encubierto informático tuvo un papel significativo para la investigación de un delito de captación y adoctrinamiento terrorista.
[201] BARRIO ANDRÉS, Moisés (2018): *Delitos 2.0. Aspectos penales, procesales (...) (op.* cit.), p. 317.
[202] DEL POZO PÉREZ, Marta (2006): "El agente encubierto como medio de investigación de la delincuencia organizada en la Ley de Enjuiciamiento Criminal española". Santiago de Cali, *Criterio Jurídico*, vol. 6, p. 280.
[203] EXPÓSITO LÓPEZ, Lourdes (2015): "El agente encubierto". Madrid, *Revista de Derecho UNED*, nº 17, pp. 261-262.

efectos e instrumentos del delito, así como diferir su incautación. De la misma forma, está exento de responsabilidad criminal por aquellas conductas que sean consecuencia necesaria del desarrollo de la investigación; sin embargo, éstas deberán guardar la debida proporcionalidad con la finalidad de la misma y no constituirán una provocación a delinquir. El agente gozaría de cualidades como la empatía, la confidencialidad, la discreción o la autonomía personal en la toma de decisiones, además de disponer de altos conocimientos informáticos[204].

La reforma de la LECRIM llevada a cabo por la Ley Orgánica 13/2015 añadió dos nuevos apartados en el artículo 282 bis (aps. 6 y 7), instituyendo el *agente encubierto informático*. Sin embargo, en la autorizada opinión de BUENO DE MATA, la reforma continua manteniendo una regulación incompleta y escueta[205]. Se habilita a funcionarios de la Policía Judicial[206], bajo la aquiescencia del órgano de instrucción, para actuar a través de una identidad supuesta en comunicaciones mantenidas en canales *cerrados* de comunicación y así esclarecer los tipos penales propios del crimen organizado. La distinción entre canales *cerrados* y *abiertos* es significativa. Según BARRIO ANDRÉS, en los segundos se producirá una situación de *ciberpatrullaje* en la prevención de los delitos en Internet que no necesitará de habilitación judicial[207]. Pero esta previsión legal termina limitando el radio de acción del agente encubierto, que no gozaría de una identidad ficticia ante interacciones con contenido de acceso público en fórums, blogs, chats o algunas redes sociales[208].

Disponiendo de la autorización precisa del Juez de Instrucción (excluyéndose del articulado al Ministerio Fiscal), el agente encubierto informático *podrá intercambiar o enviar por sí mismo archivos ilícitos por razón de su contenido y analizar los resultados de los algoritmos aplicados para la identificación de dichos archivos ilícitos* (ap. 6). Naturalmente, el juez competente *podrá autorizar la obtención de imágenes y la grabación de las conversaciones que puedan mantenerse en los encuentros* (ap. 7).

Por consiguiente, el agente estará amparado para difundir material pornográfico, enviar *malware* como *troyanos* o programas espía, etc., obedeciendo a las reglas generales de debida proporcionalidad y sin constituir una provocación al delito[209]. Se trata de una novedad clara, ya que por primera vez existe cobertura legal para intercambiar material ilícito para descubrir al presunto infractor. Es una cuestión moralmente difícil por tratarse de un *engaño* seguido de una

[204] BUENO DE MATA, Federico (2012): "El agente encubierto en Internet: mentiras virtuales para alcanzar la justicia". En PÉREZ-CRUZ MARTÍN, Agustín; FERREIRO BAAMONDE, Xulio (Dirs.): *Los retos del Poder Judicial ante la sociedad globalizada. Actas del IV Congreso Gallego de Derecho Procesal, celebrado en A Coruña el 2 y 3 de junio de 2011*. Universidade da Coruña, pp. 300-301.
[205] BUENO DE MATA, Federico (2019): *La diligencias de investigación (...) (op. cit.)*, p. 110.
[206] Si bien podrían existir potenciales agentes infiltrados de calidad fuera de los Cuerpos y Fuerzas de Seguridad, la Ley ha mantenido la denominación del siglo XIX de *Policía Judicial*, como ámbito delimitador de los profesionales intervinientes. *Vid.* CARRIZO GONZÁLEZ-CASTELL, Adán (2012): "La lucha contra la criminalidad organizada como reto de la justicia penal ante una sociedad globalizada: análisis comparado de la infiltración policial en las regulaciones española y portuguesa". En PÉREZ-CRUZ MARTÍN, Agustín; FERREIRO BAAMONDE, Xulio (Dirs.): *Los retos del Poder Judicial ante la sociedad globalizada. Actas del IV Congreso Gallego de Derecho Procesal, celebrado en A Coruña el 2 y 3 de junio de 2011*. Universidade da Coruña, pp. 340-341.
[207] BARRIO ANDRÉS, Moisés (2018): *Delitos 2.0. Aspectos penales, procesales (...) (op.* cit.), p. 319-320.
[208] BUENO DE MATA, Federico (2022): "Novas tendências na investigação *(...) (op. cit.)*", pp. 451-452.
[209] Obviamente, es difícil definir la línea entre un agente encubierto y un agente provocador, que se extralimita de sus funciones e induce a realizar un acto ilícito a quien no tenía intención de cometerlo.

traición a los criminales investigados, en que deberá prevalecer el valor de la *eficacia* y la búsqueda de una situación más favorable para la sociedad[210].

No se trata de un *agente autorizado para delinquir*, sino de un operador policial que simula actividades delictivas de carácter cooperativo para engañar a los integrantes de la organización, con la finalidad de obtener pruebas[211]. Ante este objetivo de política criminal, resultaría preferible que no se intercambiara material delictivo real obtenido en redadas precedentes, ya que se estaría menoscabando a los derechos de las víctimas (por ejemplo, si se distribuyen imágenes de pornografía infantil) y se podrían difundir en un sinfín de ocasiones. En estos casos, sería preferible usar informaciones referentes a personas ficticias o contenidos creados con personas mayores de edad, buscando la generación de confianza en la persona investigada[212]. En el caso de la pornografía infantil, es importante tener en cuenta que sin aportar previamente material delictivo las páginas pedófilas no permiten acceder a ellas[213] y este hecho supondría una frustración de las actividades investigadoras.

3.4. Los instrumentos de prueba electrónica al alcance de tod@s.

Los instrumentos de prueba electrónica actuales están alcance de las Administraciones Públicas y también de la ciudadanía en general. Como se observará a continuación, ambos se pueden beneficiar de los sistemas de sellado de tiempo y los algoritmos *hash*, la fe pública judicial y notarial y el desarrollo de periciales informáticas.

3.4.1. El sellado de tiempo y los algoritmos *hash*.

Los sistemas de sellado de tiempo o *time stamping* permiten acreditar el momento exacto en que tiene lugar una determinada operación, normalmente la creación o modificación de un documento. Su funcionamiento se basa en la intervención de funciones *hash*, que son algoritmos criptográficos de un único sentido: su composición es singularizada para acreditar un determinado contenido, pero no pueden ser revertidas para reconstruir la fuente. Cada documento produce un *hash* único, de modo que si un solo bit del documento resultara modificado, el *hash* posterior variará respecto del precedente y se descubrirá la alteración[214]. Mediante la intervención de una *autoridad* o de un sistema descentralizado de *blockchain*, es posible acreditar de forma segura que el contenido no ha sido alterado y que el emisor es fiable[215]. Se vislumbra que el uso de estas técnicas pueda llegar a sustituir los servicios prestados por las notarías, habiendo una proyección sobre una parte importante del día a día del sector privado. De hecho, las Administraciones Públicas ya se sirven de los algoritmos *hash* en numerosos trámites telemáticos con ciudadanos y empresas. Eso no obstante, ya se está desarrollando formas para llegar a burlar

[210] BUENO DE MATA, Federico (2019): *La diligencias de investigación (...) (op. cit.)*, pp. 112-114.
[211] EXPÓSITO LÓPEZ, Lourdes (2015): "El agente encubierto" *(...) (op. cit.)*, p. 284.
[212] BUENO DE MATA, Federico (2015): "Comentarios y reflexiones sobre la Ley Orgánica 13/2015 de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica". *Diario La Ley*, nº 8627.
[213] BUENO DE MATA, Federico (2012): "El agente encubierto en Internet *(...)*" *(op. cit.)*, p. 304.
[214] MARTÍN CANO, Ángel (2020): *Investigación penal de delitos tecnológicos*. En BUENO DE MATA, Federico (Dir.); GONZÁLEZ PULIDO, Irene (Coord.) (2020): *Fodertics 8.0. (...) (op. cit.)*, p. 293.
[215] La introducción del *blockchain* requerirá nuevos desarrollos legales. *Vid.* CERDÁ MESEGUER, Juan Ignacio (2020): *Blockchain y Administración de Justicia: ¿un reto posible de alcanzar?*. En BUENO DE MATA, Federico (Dir.); GONZÁLEZ PULIDO, Irene (Coord.) (2020): *Fodertics 8.0. (...) (op. cit.)*, p. 146.

medidas de este elevado grado de complejidad[216], de modo que la seguridad de las cadenas de bloques no resultará definitiva.

3.4.2. La fe pública judicial y notarial.

El Letrado de la Administración de Justicia (LAJ) es un fedatario público calificado para intervenir en los casos de obtención de la prueba electrónica. Por ejemplo, cuando se acuerde la copia de un dispositivo, se deberá garantizar su autenticidad e integridad de los datos, de modo que el LAJ dará fe que el contenido de un terminal informático, correctamente referenciado, contiene la copia de otro dispositivo concreto[217]. Los profesionales de la notaría también pueden acreditar el contenido de los dispositivos, aunque como los anteriores no se presume que dispongan de conocimientos informáticos avanzados como para llegar a discernir posibles fraudes o falsedades. Por esta razón, el trabajo de los fedatarios públicos también es compatible con el uso de los citados algoritmos *hash*, que serán calculados en el momento en que se realice la copia del disco duro del sistema afectado o la copia del servidor relacionado con el caso[218].

Sin embargo, conviene recordar que la jurisprudencia del TRIBUNAL SUPREMO se ha mostrado cauta con las funciones del LAJ en el volcado de datos[219], revelando que *lo que no se puede pretender es que el fedatario público esté presente durante todo el proceso, extremadamente complejo e incomprensible para un profano que supone el análisis y desentrañamiento de los datos incorporados a un sistema informático. Ninguna garantía podría añadirse con la presencia del funcionario judicial al que no se le puede exigir que permanezca inmovilizado durante la extracción y ordenación de los datos, identificando su origen y procedencia*[220].

3.4.3. El dictamen pericial informático.

La prueba pericial informática es la prueba principal y preferente en sede judicial para el caso de los delitos cibernéticos, por su grado de especialización y fiabilidad. Este hecho no obsta para que en el proceso se puedan aportar otras pruebas, como imágenes, audios y otros documentos, acreditables a través de su visionado, escucha y lectura (art. 299.2 LEC). A título de ejemplo, existe un elevado riesgo de manipulación o suplantación de la identidad del emisor en la mensajería instantánea, motivo por el cual ha habido varios pronunciamientos de altas instancias judiciales que han reforzado la importancia de la prueba pericial[221]. Revestirá una utilidad significativa la intervención de peritos o testigos del gabinete técnico de la Policía en la vista, para explicar los aspectos particulares de la actuación, ya sean autores del informe o participantes en las propias actividades indagatorias, reforzando así la percepción de licitud del acceso y respeto de los parámetros fijados por el órgano judicial de instrucción[222].

---

[216] DIEHL, Eric (2016): *Ten Laws for Security*. Cham, Springer International Publishing, pp. 10-11.
[217] RICHARD GONZÁLEZ, Manuel (2017): *Investigación y prueba mediante (...) (op. cit.),* p. 174.
[218] ARMENTA DEU, Teresa (2018): "Regulación legal y valoración probatoria de fuentes de prueba digital (correos electrónicos, WhatsApp, redes sociales): entre la insuficiencia y al incertidumbre". Barcelona, *Revista de Internet, Derecho y Política*, nº 27, p. 72.
[219] FERNÁNDEZ-GALLARDO, Javier Ángel (2016): "Registro de dispositivos *(...)*" *(op. cit.)*, p. 42.
[220] STS 1599/1999, de 15 de noviembre, rec. 3831/1998, FJ 2.
[221] ARMENTA DEU, Teresa (2018): "Regulación legal y valoración probatoria (…)" *(op. cit.*), p. 73.
[222] RICHARD GONZÁLEZ, Manuel (2017): *Investigación y prueba mediante (...) (op. cit.),* pp. 328-329.

Es remarcable que según el TRIBUNAL SUPREMO, *los dictámenes y pericias emitidas por Organismos o Entidades oficiales, dada la imparcialidad, objetividad y competencia técnica de los miembros integrantes, ofrecen toda clase de garantías técnicas y de imparcialidad para atribuirles, "prima facie", validez plena*[223], hecho extensible a la pericial informática. Su valoración será llevada a cabo por el órgano judicial de acuerdo con las reglas de la sana crítica, a través de un contraste de todos los medios probatorios, siempre que sean lícitos, admitidos y practicados respetando las garantías procesales[224]. La pericial informática recaerá primero sobre la *fuente de la prueba*, para dictaminar su autenticidad e integridad, y después hacia el *contenido de la prueba* (por ejemplo, para descubrir si se han suprimido archivos).

No se puede olvidar que los análisis llevados a cabo por algoritmos presentarán una importancia creciente, ya sea en el ámbito de los ciberdelitos como fuera del entorno digital, y los particulares podrán invocar sus conclusiones como si se tratara de un dictamen pericial. Aquí resulta importante que los algoritmos estén configurados sin sesgos, so pena de afectar a la imparcialidad del juzgador y el derecho a un proceso con todas las garantías del artículo 24.2 de la Constitución. No deben existir privilegios o desigualdades que beneficien a una parte[225].

La prueba pericial en la fase de juicio oral se encuentra regulada en los artículos 723 a 725 LECRIM, que se remiten a los preceptos generales de los incidentes de recusación, y los artículos 456 a 485 LECRIM, que desarrollan el informe pericial como una diligencia del sumario. Huelga decir que la vinculación de los peritos con organismos oficiales no representará una causa de recusación, sin perjuicio que la parte pueda alegar otro motivo o pedir una prueba pericial contradictoria[226]. En general, el informe pericial será prestado por dos peritos, excepto que *no hubiese más de uno en el lugar y no fuere posible esperar la llegada de otro sin graves inconvenientes* (art. 459 LECRIM), o se trate de un procedimiento abreviado y un único dictamen sea suficiente, a criterio del órgano judicial (art. 778.1 LECRIM).

[223] STS 285/2012, de 18 de abril, rec. 1776/2011, FJ 3.
[224] ARMENTA DEU, Teresa (2018): "Regulación legal y valoración probatoria *(...)*" *(op. cit.*), p. 73.
[225] DE MIGUEL BERIAIN, Iñigo; PÉREZ ESTRADA, Miren Josune (2019): "La inteligencia artificial en el proceso penal español: un análisis de su admisibilidad sobre la base de los derechos fundamentales implicados". Madrid, *Revista de Derecho UNED*, nº 25, p. 551.
[226] RICHARD GONZÁLEZ, Manuel (2017): *Investigación y prueba mediante (...) (op. cit.),* p. 330.

Conclusiones

PRIMERA. **El cibercrimen es un fenómeno de difícil persecución. Se corre el riesgo que el sistema procesal penal únicamente actúe contra tipos penales de poca entidad, ya que serán los únicos en los que realmente existirá una trazabilidad asequible de la autoría delictiva**.

El cibercrimen tiene un impacto significativo en las sociedades tecnológicamente avanzadas. Causa daños económicos y patrimoniales remarcables, afecta a la intimidad y privacidad de los ciudadanos/as y llega a desestabilizar a la paz social de los Estados. En este contexto, las diligencias de investigación tecnológicas y la llamada *prueba electrónica* son decisivas para demostrar en sede judicial la perpetración de los ciberdelitos, aunque éstos por naturaleza ya tienen una condición de difícil perseguibilidad. En primer lugar, su autoría puede quedar difusa mediante subterfugios tecnológicos que robustecen el anonimato; en segundo lugar, pueden impactar sobre una pluralidad indeterminada de sujetos pasivos; y en tercer lugar, pueden cometerse en cualquier parte del mundo, aprovechando la ubicación en países con una nula voluntad de cooperación judicial, los llamados *ciberparaísos*.

SEGUNDA. El Convenio de Budapest de 2001 ha tenido un impacto en la Ley de Enjuiciamiento Criminal actual. **Sin embargo, la *teoría de la ubicuidad* no se ha desarrollado lo suficientemente para que los órganos judiciales de un país puedan investigar a dispositivos situados fuera de su propio territorio y se mejore en agilidad.**

El Convenio sobre Ciberdelincuencia de 23 de noviembre de 2001, adoptado en Budapest bajo los auspicios del Consejo de Europa, es un tratado fundamental que se ha proyectado más allá de las fronteras del *viejo continente*, llegando a América Latina y Asia por su calidad legislativa y guiando al desarrollo del ordenamiento español. Así, nuestro país ha adoptado el valiente paso de reformar la vetusta Ley de Enjuiciamiento Criminal para introducir 39 nuevos preceptos en el articulado del Título VIII del Libro II, que versa sobre *las medidas de investigación limitativas de los derechos reconocidos en el artículo 18 de la Constitución* del procedimiento sumario. De este modo, con la Ley Orgánica 13/2015, de 5 de octubre, se ha obtenido una regulación sólida para tratar la investigación de los delitos cometidos mediante el uso de las TICs. Era un paso necesario para la garantía de los Derechos Fundamentales. Ahora bien, con este nuevo escenario internacional se ha mantenido la competencia procesal de los órganos judiciales dentro del Estado donde se encuentran radicados, sin que puedan realizar una búsqueda transfronteriza en dispositivos situados en el extranjero. Es posible que nuevos protocolos al Convenio de Budapest permitan superar esta dificultad.

TERCERA. La Ley Orgánica 13/2015 presenta limitaciones a abordar: las metodologías policiales, como en el caso del agente encubierto informático, no pueden ser debidamente fiscalizadas con una regulación excesivamente exigua; la colaboración de *hackers* con las autoridades puede ir más allá de unos estándares éticos y de política criminal, constriñéndolos a actuar bajo una amenaza de condena penal; y la existencia de piezas separadas para cada una de las diligencias de investigación tecnológica no ayuda a simplificar los trabajos del órgano judicial de instrucción.

La presunta consistencia de la reformada LECRIM no está exenta de ciertas fisuras. La FISCALÍA GENERAL DEL ESTADO ha buscado superarlas mediante la publicación de diversas Circulares, entre las que ha destacado en el presente análisis la número 5/2019, sobre registro de dispositivos y equipos informáticos. Su contenido es interpretado por los diversos operadores jurídicos implicados en el proceso penal, aunque no llega a cubrir todo el espectro de la práctica habitual de los miembros de la Policía Judicial: por razones de seguridad y confidencialidad de la metodología, no se difunden qué programas y técnicas son usadas para practicar un registro remoto de dispositivos informáticos, o cómo se consigue desarrollar la labor del agente encubierto informático, que ahora presenta una regulación realmente exigua en la LECRIM.

Asimismo, la legislación ahora vigente no aclara si el deber de colaboración de *cualquier persona* con las actividades de las autoridades y agentes encargados de la investigación supondría que *hackers* profesionales y criminales informáticos prestaran servicios a la Administración sin unos estándares mínimos de ética, bajo el apercibimiento de incurrir en un delito de desobediencia si no proceden con los cometidos asignados. Otra de las limitaciones claras es que las diligencias de investigación tecnológicas están reguladas para desarrollarse en piezas separadas, individuales; así, ante un mismo procedimiento, podría resultar de interés que la legislación previera agruparlas para simplificar los trabajos judiciales.

CUARTA. La prueba pericial informática está destinada a perdurar como el máximo exponente probatorio disponible en sede judicial, por su elevada precisión y fiabilidad.

En este contexto de elevada digitalización, los particulares también disponen de herramientas para acreditar la comisión de los ciberdelitos, que igualmente se proyectan hacia la Administración de Justicia. Uno de los que tiene más vocación a llegar sustituir a la fe pública notarial es el representado por los algoritmos *hash*, que son sistemas criptográficos de un solo sentido: no pueden ser revertidos para reconstruir a la fuente original. Los sistemas de sellado de tiempo también aprovechan estas innovaciones técnicas que, sin embargo, no son absolutamente infalibles. Ante el cambio tecnológico constante y la incertidumbre, la prueba reina del cibercrimen es la pericial informática. Su precisión la hace idónea para formar la convicción del órgano judicial, que continuará decidiendo según las reglas de la sana crítica.

Referencias

Bibliografía

1. ARMENTA DEU, Teresa (2018): "Regulación legal y valoración probatoria de fuentes de prueba digital (correos electrónicos, WhatsApp, redes sociales): entre la insuficiencia y al incertidumbre". Barcelona, *Revista de Internet, Derecho y Política*, nº 27, pp. 67-78.

2. ARRABAL PLATERO, Paloma (2020): "Las diligencias de investigación tecnológica en el proceso penal español". Valparaíso, *Revista de Ciencias Sociales*, nº 76, pp. 67-108.

3. BARRIO ANDRÉS, Moisés (2018): *Delitos 2.0. Aspectos penales, procesales y de seguridad de los ciberdelitos*. Las Rozas (Madrid), Wolters Kluwer.

4. BARRIO ANDRÉS, Moisés (2011): "La ciberdelincuencia en el derecho español". Madrid, *Revista de las Cortes Generales*, nº 83, pp. 273-305.

5. BLANCO, Hernán (2021): "El hackeo con orden judicial en la legislación procesal española a partir de la Ley Orgánica 13/2015 del 5 de octubre". Barcelona, *InDret*, nº 1/2021, pp. 431-501.

6. BUENO DE MATA, Federico (2012): "El agente encubierto en Internet: mentiras virtuales para alcanzar la justicia". En PÉREZ-CRUZ MARTÍN, Agustín; FERREIRO BAAMONDE, Xulio (Dirs.): *Los retos del Poder Judicial ante la sociedad globalizada. Actas del IV Congreso Gallego de Derecho Procesal, celebrado en A Coruña el 2 y 3 de junio de 2011*. Universidade da Coruña, pp. 295-306.

7. BUENO DE MATA, Federico (2015): "Acerca de la validez de los pantallazos como prueba electrónica en juicio". Salamanca, *Ars Iuris Salmanticensis*, vol. 3, pp. 322-324.

8. BUENO DE MATA, Federico (2015): "Fortalecimiento de garantías procesales y medidas de investigación tecnológica". Salamanca, *Ars Iuris Salmanticensis*, vol. 4, pp. 326-328.

9. BUENO DE MATA, Federico (2015): "Comentarios y reflexiones sobre la Ley Orgánica 13/2015 de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica". *Diario La Ley*, nº 8627.

10. BUENO DE MATA, Federico (2019): *La diligencias de investigación penal en la cuarta revolución industrial. Principios teóricos y problemas prácticos*. Cizur Menor (Navarra), Editorial Aranzadi – Thomson Reuters.

11. BUENO DE MATA, Federico (2022): "Novas tendências na investigação de crimes complexos em um contexto europeu globalizado". Rio de Janeiro, *Revista Eletrônica de Direito Processual*, vol. 23, nº 1, pp. 434-457.

12. BUJOSA VADELL, Lorenzo Mateo; BUSTAMANTE RÚA, Mónica María; TORO GARZÓN, Luis Orlando (2021): "La prueba digital producto de la vigilancia secreta: obtención, admisibilidad y valoración en el proceso penal en España y Colombia". Porto Alegre, *Revista Brasileira de Direito Processual Penal*, vol. 7, nº 2, pp. 1347-1384.

13. CÁRDENAS ARAVENA, Claudia (2008): "El lugar de comisión de los denominados ciberdelitos". Talca, *Política Criminal. Revista Electrónica Semestral de Políticas Públicas en Materias Penales*, nº 6, pp. 1-14.

14. CARRIZO GONZÁLEZ-CASTELL, Adán (2012): "La lucha contra la criminalidad organizada como reto de la justicia penal ante una sociedad globalizada: análisis comparado de la infiltración policial en las regulaciones española y portuguesa". En PÉREZ-CRUZ MARTÍN, Agustín; FERREIRO BAAMONDE, Xulio (Dirs.): *Los retos del Poder Judicial ante la sociedad globalizada. Actas del IV Congreso Gallego de Derecho Procesal, celebrado en A Coruña el 2 y 3 de junio de 2011*. Universidade da Coruña, pp. 337-354.

15. CERDÁ MESEGUER, Juan Ignacio (2020): *Blockchain y Administración de Justicia: ¿un reto posible de alcanzar?*. En BUENO DE MATA, Federico (Dir.); GONZÁLEZ PULIDO, Irene (Coord.) (2020): *Fodertics 8.0. Estudios sobre tecnologías disruptivas y justicia*. Granada, Editorial Comares, pp. 137-146.

16. COAQUIRA FLORES, Ángel Jeancarlo (2020): *Aproximación a la naturaleza jurídica de las infraestructuras críticas: delineando las bases para la ciberseguridad peruana*. En BUENO DE MATA, Federico (Dir.); GONZÁLEZ PULIDO, Irene (Coord.) (2020): *Fodertics 8.0. Estudios sobre tecnologías disruptivas y justicia*. Granada, Editorial Comares, pp. 333-343.

17. DE MIGUEL BERIAIN, Iñigo; PÉREZ ESTRADA, Miren Josune (2019): "La inteligencia artificial en el proceso penal español: un análisis de su admisibilidad sobre la base de los derechos fundamentales implicados". Madrid, *Revista de Derecho UNED*, nº 25, pp. 531-561.

18. DE LA MATA BARRANCO, Norberto (2017): "El contacto tecnológico con menores del art. 183 ter 1 CP como delito de lesión contra su correcto proceso de formación y desarrollo personal sexual". Granada, *Revista Electrónica de Ciencia Penal y Criminología*, nº 19-10, pp. 1-28.

19. DEL POZO PÉREZ, Marta (2006): "El agente encubierto como medio de investigación de la delincuencia organizada en la Ley de Enjuiciamiento Criminal española". Santiago de Cali, *Criterio Jurídico*, vol. 6, pp. 267-310.

20. DIEHL, Eric (2016): *Ten Laws for Security*. Cham, Springer International Publishing.

21. EXPÓSITO LÓPEZ, Lourdes (2015): "El agente encubierto". Madrid, *Revista de Derecho UNED*, nº 17, pp. 251-286.

22. FERNÁNDEZ-GALLARDO, Javier Ángel (2016): "Registro de dispositivos de almacenamiento masivo de información". Santiago de Compostela, *Dereito*, vol. 25, nº 2, pp. 25-58.

23. FISCALÍA GENERAL DEL ESTADO (2019): *Circular 5/2019, sobre registro de dispositivos y equipos informáticos*. Madrid.

24. FUTTER, Andrew (2022): "La ciberseguridad de los sistemas de armas nucleares. Amenazas, vulnerabilidades y consecuencias". Barcelona, *Vanguardia Dossier*, nº 84, pp. 86-90.

25. GALÁN MUÑOZ, Alfonso (2019): *Los ciberdelitos en el ordenamiento español*. Barcelona, Editorial UOC.

26. GONZÁLEZ MONJE, Alicia (2017): "Amenazas a la seguridad y privacidad: la dificultad del equilibrio perfecto". Madrid y Elche, *Revista Europea de Derechos Fundamentales*, nº 29, pp. 267-294.

27. GONZÁLEZ PULIDO, Irene (2022): *Diligencias de investigación tecnológicas para la lucha contra la ciberdelincuencia grave. Especial referencia a la utilización del registro remoto para la investigación de ciberataques contra infraestructuras críticas y estratégicas*. Tesis Doctoral, Universidad de Salamanca, Programa de Doctorado en Administración, Hacienda y Justicia en el Estado Social.

28. GRANJA, Pedro Javier (2020): "«Grooming»: el minotauro en Internet. El derecho penal del enemigo frente al pederasta de la era digital". Bogotá, *Revista de Derecho Penal y Criminología*, vol. 41, nº 111, pp. 61-108.

29. GREEN, Justice; HOPKINS, Nick; PAINES, Nicholas; GREEN, Sarah; LEWIS, Penney (2022): *Intimate image* abuse: a final report. Londres, The Law Commission of the United Kingdom, nº 407.

30. MARTÍN CANO, Ángel (2020): *Investigación penal de delitos tecnológicos*. En BUENO DE MATA, Federico (Dir.); GONZÁLEZ PULIDO, Irene (Coord.) (2020): *Fodertics 8.0. Estudios sobre tecnologías disruptivas y justicia*. Granada, Editorial Comares, pp. 285-297.

31. MIRÓ LLINARES, Fernando (2012): *El cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio*. Madrid, Marcial Pons.

32. MIRÓ LLINARES, Fernando (2013): "Derecho penal, «cyberbullying» y otras formas de acoso (no sexual) en el ciberespacio". Barcelona, *Revista de Internet, Derecho y Política*, nº 16, pp. 61-75.

33. MIRÓ LLINARES, Fernando (2016): "Taxonomía de la comunicación violenta y el discurso del odio en Internet". Barcelona, *Revista de Internet, Derecho y Política*, nº 22, pp. 93-118.

34. MIRÓ LLINARES, Fernando (2021): "Crimen, cibercrimen y COVID-19: desplazamiento (acelerado) de oportunidades y adaptación situacional de ciberdelitos". Barcelona, *Revista de Internet, Derecho y Política*, nº 32, pp. 1-17.

35. MUÑOZ RODRÍGUEZ, Ana Belén (2020): "El impacto de la inteligencia artificial en el proceso penal". Badajoz, *Anuario de la Facultad de Derecho. Universidad de Extremadura*, nº 36, pp. 695-728.

36. PÉREZ ESTRADA, Miren Josune (2019): "La protección de los datos personales en el registro de dispositivos de almacenamiento masivo de información". Porto Alegre, *Revista Brasileira de Direito Processual Penal*, vol. 5, nº 3, pp. 1297-1330.

37. PONS GAMÓN, Vicente (2017): "Internet, la nueva era del delito: ciberdelito, ciberterrorismo, legislación y ciberseguridad". Quito, *URVIO - Revista Latinoamericana de Estudios de Seguridad*, nº 20, pp. 80-93.

38. RICHARD GONZÁLEZ, Manuel (2017): *Investigación y prueba mediante medidas de intervención de las comunicaciones, dispositivos electrónicos y grabación de imagen y sonido*. Las Rozas (Madrid), Wolters Kluwer.

39. RODRÍGUEZ RUBIO, Carmen (2020): "Nuevas diligencias de investigación y de prueba: el registro de dispositivos de almacenamiento masivo de información". *Foro, Nueva Época*, vol. 23, nº 1, pp. 267-304.

40. ROIG BATALLA, Antoni (2020): *Las garantías frente a las decisiones automatizadas. Del Reglamento General de Protección de Datos a la gobernanza algorítmica*. Barcelona, J. M. Bosch.

41. VILCHEZ LIMAY, Roberto Carlos (2020): "La ciberdelincuencia en el contexto de la pandemia del coronavirus. Una aproximación desde el marco convencional". Salamanca, *Ars Iuris Salmanticensis*, vol. 8, pp. 21-25.

Jurisprudencia

Tribunal Supremo

STS 1599/1999, de 15 de noviembre, rec. 3831/1998.
STS 785/2008, de 25 de noviembre, rec. 227/2008.
STS 285/2012, de 18 de abril, rec. 1776/2011.
STS 300/2015, de 19 de mayo, rec. 2387/2014.
STS 311/2015, de 27 de mayo, rec. 10813/2014.
STS 786/2015, de 4 de diciembre, rec. 10447/2015.
STS 173/2016, de 2 de marzo, rec. 1864/2015.
STS 714/2016, de 26 de septiembre, rec. 1951/2015.
STS 489/2018, de 23 de octubre, rec. 1674/2017.
STS 494/2020, de 8 de octubre, rec. 10018/2020.
STS 580/2020, de 5 de noviembre, rec. 186/2019.
STS 597/2022, de 15 de junio, rec. 10705/2021.

Tribunal Constitucional

STC 207/1996, de 16 de diciembre, rec. 1789/1996.
STC 70/2002, de 3 de abril, rec. 3787/2001.
STC 26/2006, de 30 de enero, rec. 623/2004.
STC 253/2006, de 11 de septiembre, rec. 44/2003.
STC 173/2011, de 7 de noviembre, rec. 5928/2009.
STC 115/2013, de 9 de mayo, rec. 1246/2011.
STC 66/2020, de 2 de junio, rec. 6313/2019.
STC 172/2020, de 19 de noviembre, rec. 2896/2015.

Audiencia Nacional

SAN 3/2017, de 17 de febrero, rec. 6/2016.
SAN 23/2019, de 20 de noviembre, rec. 5/2016.
SAN 322/2021, de 7 de junio, rec. 299/2021.
SAN 343/2021, de 14 de junio, rec. 337/2021.

Noticias de prensa

1. WIRED (11.03.2014): *An Unprecedented Look at Stuxnet, the World's First Digital Weapon*. Accesible en: https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/ [Última consulta realizada en 23.06.2022].

2. LA GACETA DE SALAMANCA (11.01.2019): *Millones de adúlteros al descubierto gracias al hackeo de una web*. Accesible en: https://www.lagacetadesalamanca.es/hemeroteca/millones-adulteros-descubierto-gracias-hackeo-web-IRGS149634 [Última consulta realizada en 23.06.2022].

3. EL ECONOMISTA (14.01.2019): *La Universidad de Valladolid sufre un ataque informático*. Accesible en: https://www.eleconomista.es/ecoaula/noticias/9632786/01/19/La-Universidad-de-Valladolid-sufre-un-ataque-informatico.html [Última consulta realizada en 23.06.2022].

4. EL DIARIO.ES (16.01.2020): *La Universidad de Burgos, víctima de un ataque informático que afecta a datos personales de 6.800 usuarios*. Accesible en: https://www.eldiario.es/castilla-y-leon/sociedad/universidad-burgos-ciberataque-personales-usuarios_1_1076339.html [Última consulta realizada en 23.06.2022].

5. LA VANGUARDIA (23.11.2021): *El Govern destina 3,5 millones a la UAB para recuperarse del ciberataque*. Accesible en: https://www.lavanguardia.com/vida/20211123/7883348/govern-destina-3-5-millones-uab-recuperarse-ataque-informatico.html [Última consulta realizada en 23.06.2022].

6. LA GACETA DE SALAMANCA (30.11.2021): *La Universidad de Salamanca sufre un ataque informático el día de las elecciones a rector*. Accesible en: https://www.lagacetadesalamanca.es/salamanca/la-universidad-de-salamanca-sufre-un-ataque-informatico-el-dia-de-las-elecciones-a-rector-HF9733832 [Última consulta realizada en 23.06.2022].

7. 20 MINUTOS (03.01.2021): La Universitat Oberta de Catalunya vuelve a la normalidad tras el ataque de ransomware que había dañado los servidores centrales de su Campus Virtual. Accesible en: https://www.20minutos.es/tecnologia/ciberseguridad/la-universitat-oberta-de-catalunya-vuelve-a-la-normalidad-tras-el-ataque-de-ransomware-que-habia-danado-los-servidores-centrales-de-su-campus-virtual-4935636/ [Última consulta realizada en 23.06.2022].

8. NOTICIAS SALAMANCA (04.05.2021): *El "sexting" crece con la pandemia: el 59% asegura que ahora se siente más motivado a practicarlo*. Accesible en: https://noticiassalamanca.com/sociedad/el-sexting-crece-con-la-pandemia/ [Última consulta realizada en 23.06.2022].

9. EL MUNDO (03.03.2022): *La Universidad vasca ordena a toda su plantilla proteger sus cuentas electrónicas ante un "ciberataque inminente"*. Accesible en: https://www.elmundo.es/pais-vasco/2022/03/03/622115d3fc6c83ed028b457f.html [Última consulta realizada en 23.06.2022].

10. FRANCE 24 (10.05.2022): *La cibercriminalidad costó más de 6 billones de dólares en 2021*. Accesible en: https://www.france24.com/es/minuto-a-minuto/20220510-la-cibercriminalidad-cost%C3%B3-m%C3%A1s-de-6-billones-de-d%C3%B3lares-en-2021 [Última consulta realizada en 23.06.2022].

11. EL PERIÓDICO (23.05.2022): *Phishing: ¿Qué es y cómo evitarlo?* Accesible en: https://www.elperiodico.com/es/tecnologia/20220523/phishing-que-es-dv-13695404 [Última consulta realizada en 23.06.2022].

12. LA GACETA DE SALAMANCA (24.05.2022): *Alerta por nuevos casos de estafas bancarias a través del correo electrónico*. Accesible en: https://www.lagacetadesalamanca.es/virales/alerta-por-nuevos-casos-de-estafas-bancarias-a-traves-del-correo-electronico-EE11262262 [Última consulta realizada en 23.06.2022].

13. LA VANGUARDIA (17.06.2022): *Costa Rica sigue enfrentando las consecuencias de dos meses de ciberataques*. Accesible en: https://www.lavanguardia.com/vida/20220618/8349187/costa-rica-sigue-enfrentando-consecuencias-dos-meses-ciberataques.html [Última consulta realizada en 23.06.2022].

14. 20 MINUTOS (22.06.2022): *Microsoft asegura que Rusia ha lanzado ciberataques contra 42 países aliados de Ucrania desde que empezó la guerra*. Accesible en: https://www.20minutos.es/noticia/5020016/0/microsoft-asegura-que-rusia-ha-lanzado-ciberataques-contra-42-paises-aliados-de-ucrania-desde-que-empezo-la-guerra/ [Última consulta realizada en 23.06.2022].

Anexo. Glosario de anglicismos

Antispyware: aplicación informática que identifica y elimina programas espía.

Auction fraud: fraude producido en las subastas en línea, basado en el engaño sobre las características de la adquisición realizada o su no entrega.

Backdoor: programa que penetra en el sistema informático y genera una puerta trasera, que permite controlar el ordenador sin que los usuarios lleguen a tener conocimiento.

Blog: abreviatura del término *weblog*. Originalmente se trataba de una publicación digital de un diario personal, con las entradas ordenadas de forma cronológica.

Bot: abreviatura del término *robot*. Programa informático que realiza tareas repetitivas a través de Internet. En su acepción negativa, se trata de un virus que realiza un acceso remoto al ordenador.

Bring Your Own Device (BYOD): literalmente, *trae tu propio dispositivo*. Política de gestión de los dispositivos informáticos en un contexto empresarial, que permite que los empleados hagan uso de sus propios equipos de forma flexible, efectuando a la vez funciones relacionadas con sus cometidos laborales y sus usos personales.

Carnivore: sistema producido por el FBI en Estados Unidos, que permite la recolección de datos de aplicaciones de comunicaciones electrónicas, como el correo electrónico, a partir de una orden judicial y la colaboración de proveedores de servicios de Internet.

Chat: conversación a tiempo real, en línea y en formato escrito.

Child grooming (o *cybergrooming*): contacto con personas menores de edad a través de redes sociales u otros sistemas virtuales de comunicación, para aproximarse a ellos, embaucarles e intentar realizar abusos sexuales. El agresor normalmente aparenta ser un menor de edad con un perfil falso, genera un ambiente de confianza y posteriormente utiliza la información obtenida para coaccionar a la víctima. Es un tipo penal de peligro.

Cloaked websites: sitios web que, bajo una apariencia neutra o de transformación social (hipotéticas organizaciones no gubernamentales, fundaciones, etc.), transmiten una ideología de discriminación étnica o de persecución hacia determinados colectivos.

Cloud computing: computación en la nube, es decir, la utilización de servidores remotos conectados en la red para almacenar, gestionar y procesar datos. *Software* y *hardware* se encuentran integrados en un centro de datos.

Cookies: galletas; en otros términos, archivos que guardan datos sobre los usuarios dentro de su propio sistema informático y posibilitan su identificación cuando visitan sitios web.

Computer Emergency Response Team (CERT): equipo de respuesta ante emergencias informáticas; conjunto de profesionales destinados a desarrollar medidas reactivas y preventivas ante incidencias de seguridad en los sistemas de información.

Cracker: tipología de *hacker* que aprovecha los accesos a sistemas informáticos ajenos para causar estragos en ellos, obtener información o cometer fraudes.

Creative Commons (CC): iniciativa de gestión de los derechos de propiedad intelectual con carácter global auspiciada por la organización sin ánimo de lucro homónima, basada en diferentes grados de protección que los autores pueden elegir en función de sus propios intereses económicos, voluntad de difusión y autorización de obras derivadas.

Cyberbullying: ciberacoso escolar o entre menores, basado en la realización de amenazas, hostigamientos, humillaciones o conductas de índole desagradable a través de las TICs.

Cybercrime: ciberdelito; en otros términos, delito cometido en el ciberespacio, con las especificidades de este entorno.

Cyberhate speech: discurso del odio a través de las TICs, con fines de discriminación étnica o de estigmatizar públicamente a determinados colectivos sociales.

Cyberspace: ciberespacio; en otros términos, área de intercomunicación social, global y en cambio permanente.

Cyberstalking: ciberacoso continuo a una persona, basado en el intento de contacto constante y no aceptado por la víctima, uso no autorizado de su imagen, realización de amenazas u otros tipos de hostigamiento.

Cyberwarfare: guerra u operaciones militares cibernéticas entre Estados, con el objetivo de realizar estragos a los sistemas informáticos del contrario y afectar a sus infraestructuras y capacidades estratégicas.

Dark web: literalmente, la *red oscura*; es la parte no indexada de Internet en los motores de búsqueda y que requiere de configuraciones específicas para su acceso, como por ejemplo mediante el uso del sistema *TOR*.

Data breach: filtrado, fuga o escape de datos protegidos, sensibles o confidenciales, a través de la conducta deliberada de uno o más atacantes, que infringen los sistemas de seguridad sin estar autorizados por ello.

Data mining: minería de datos; en su definición asociada a los ciberdelitos, obtención de información sobre una persona determinada, para crear un perfil muy acurado que permita la comisión de un fraude contra la misma.

Denial of Service (DoS): denegación de servicio; es decir, ciberataque que provoca una saturación del servidor del sistema informático de la víctima, impidiendo que pueda atender a otras peticiones que no sean las del propio agresor.

Distributed Denial of Service (DDoS): denegación de servicio distribuida; evolución del mencionado ataque DoS, basado en una saturación del servidor del sistema informático de la víctima a través de peticiones procedentes de múltiples atacantes a la vez o redes coordinadas de bots.

Domain Name Server (DNS): sistema de nombres de dominio. Se encarga de transformar las direcciones de nombres de dominio desde un formato comprensible para los humanos a código binario o numérico, permitiendo una interacción global de terminales informáticos.

Downblousing: captura de imágenes de los senos femeninos desde un ángulo vertical, con ánimo de obtener una imagen con contenido sexual explícito sin el consentimiento de la mujer afectada. En Reino Unido se pondera su inclusión como tipo penal propio.

Electronic Data Interchange (EDI): intercambio electrónico de datos.

Encryption: encriptación o cifrado de datos, para impedir que nadie con la excepción del destinatario pueda descubrir su contenido. Uno de los algoritmos criptográficos más utilizados es el sistema RSA, que combina una clave pública y una clave privada.

File Transfer Protocol (FTP): protocolo de transferencia de ficheros.

Firewall: cortafuegos; en otros términos, sistema que impide los accesos no autorizados en redes privadas.

Hacker: inicialmente, pirata informático; en los últimos años se ha generalizado la definición de experto en la detección y mejora de las vulnerabilidades de los sistemas informáticos. *Vid. Hacking* y *Cracker*.

Hacking: conducta basada en el acceso no autorizado por el titular en un sistema o equipo informático ajeno, con capacidad de hacer uso del mismo o acceder a los datos guardados. El *hacking* blanco (*white hat hacking*) no tiene intención de causar estragos o realizar un uso posterior de los datos obtenidos; en cambio, el *hacking* negro (*black hat hacking*) pretende acometer un propósito destructivo o ilegal (*cracking*).

Hacktivism: activismo bajo la llamada ética *hacker*, que consiste en llevar a cabo ataques informáticos o accesos no autorizados con una finalidad ideológica, de protesta y de protección de la libertad en el uso de la red.

Hardware: elementos que conforman la parte física o tangible de un ordenador, por ejemplo, las cajas y los componentes electrónicos situados en su interior, los equipos periféricos y los cables.

Hypertext Transfer Protocol (HTTP): literalmente, *protocolo de transferencia de hipertexto*; es el protocolo de comunicación en la red que habilita a las transferencias de datos. El formato HTTPS es una evolución del mismo y permite acreditar las informaciones procedentes de un servidor considerado seguro, mediante un certificado de seguridad con protocolo SSL.

Identity theft: fraude o robo de la identidad en línea; se efectúa una suplantación de la personalidad, ya sea de individuos o personas jurídicas, para cometer un fraude.

Insider: cibercriminal que actúa contra la empresa o institución en la que está vinculado.

Internet: red informática global, de arquitectura descentralizada, basada en la interconexión directa entre terminales computacionales siguiendo un protocolo único.

Internet of Things (IoT): literalmente, *Internet de las cosas (IdC)*; dispositivos electrónicos o electrodomésticos proveídos de sensores, procesadores, *software* y tecnologías asociadas, que permiten una circulación de información continua a través de Internet u otras redes.

IP spoofing: sustitución de la dirección IP original por otra con fines invasivos.

Keylogger: programa que captura los datos referentes a las pulsaciones realizadas en el teclado de un dispositivo, conservando la información y enviándola al atacante. Con tales conocimientos éste podrá descubrir, por ejemplo, determinadas claves de acceso o conversaciones de carácter encriptado y confidencial.

Local Area Network (LAN): red de ordenadores interconectados a nivel local, normalmente en un mismo edificio o a poca distancia, para una comunicación de datos más eficiente y segura con uno o más servidores propios.

Mail spoofing: sustitución de la dirección de correo electrónico para desviar fraudulentamente el envío de mensajes legítimos.

Malware: programa o código maligno, que causa daños de forma deliberada a un sistema informático y sin que el usuario lo llegue a conocer.

Netiquette: etiqueta en la red; es decir, reglas para llevar a cabo una comunicación social acorde con buenos usos.

Netizen: ciudadano/a de la red o *ciberdano/a*.

Nickname: o simplemente *nick*, es un pseudónimo o apodo de un usuario para identificarse a sí mismo en la red y comunicarse con otras personas, generalmente desconocidas.

Non-fungible Token (NFT): activo digital encriptado que es considerado un valor único, indivisible, no replicable y transferible. Su escasez es verificable mediante sistemas de cadena de bloques. Actualmente forman parte de un mercado no regulado, asociado mayormente a creaciones artísticas.

Open source: literalmente, *de fuente abierta*; referido al programa de código abierto y distribución libre, cuya estructura puede ser verificada y mejorada.

Password guessing: descifrado de contraseñas o claves de acceso.

Peer-to-peer Protocol (P2P): protocolo de intercambio de información entre sujetos equivalentes.

Phishing: acción cibercriminal que usa interacciones sociales y/o sistemas informáticos sofisticados para manipular las vulnerabilidades de los consumidores y usuarios y extraer datos relativos a su identidad y claves de banca electrónica, para posteriormente lucrarse. El llamado *phishing* tradicional utiliza la imagen corporativa de una entidad financiera para simular un mensaje de correo electrónico y un sitio web de servicios bancarios legítimos.

Phreaking: abuso de sistemas informáticos, por ejemplo, pirateo de contraseñas de acceso a redes o servicios de pago, como contenidos audiovisuales bajo suscripción, bases de datos jurídicas o redes *wi-fi* ajenas, causando un perjuicio patrimonial a su legítimo titular.

Proxy: controlador de acceso; servidor que actúa como un actor intermedio entre un cliente y un servidor.

Ransomware: ataque informático basado en el *secuestro* o encriptación de archivos que se encuentran en el sistema informático de la víctima, de modo que la única forma posible de acceder a ellos es la asunción del pago de un rescate (*ransom*, en inglés) para obtener la clave de desbloqueo. Para evitar el rastreo de la identidad de los atacantes se exigirá el pago a través de criptodivisas.

Remote access tools (RAT): herramientas de acceso o control remoto, es decir, programas *troyanos* que infectan el ordenador y permiten a los atacantes apoderarse del equipo.

Rootkit: virus que se introduce en el núcleo del sistema informático para evitar ser detectado por los administradores y permite al atacante llegar a controlar el mismo.

Scriptkiddies: literalmente, «niñatos del código»; se trata de jóvenes con conocimientos limitados de prácticas de *hacking* que realizan ataques informáticos con programas y códigos sencillos, que a veces pueden resultar más dañosos de lo esperado por su falta de habilidad.

Secure Sockets Layer (SSL): protocolo que realiza una identificación exclusiva de personas físicas y sitios web, fundamental para generar una transmisión de datos segura y confidencial.

Sexting: realización de imágenes propias de tipo erótico o sexual y posterior envío a otras personas, acompañadas de textos de contenido poco decoroso, para posibilitar un acercamiento sexual o con mero carácter seductor. La difusión no deseada de tales contenidos hacia terceras personas puede resultar incontrolable y repercutir fuertemente contra la imagen personal.

Short Message Service (SMS): servicio de mensajes de texto cortos.

Smishing: modalidad de *phishing* que se desarrolla a partir del envío de mensajes de SMS.

Sniffing: captura de los paquetes de datos o intercepción del tráfico de la red para descubrir su contenido o corromper la infraestructura.

Snooping: literalmente, *fisgoneo*; acceso no autorizado a datos ajenos.

Software: elementos que conforman la parte abstracta o intangible de un ordenador, como los programas y las reglas de código, que determinan la ejecución de las tareas lógicas.

Spam: correo electrónico no deseado y enviado de forma masiva a numerosos usuarios, normalmente originado en un sistema informático infectado por un *hacker* que ha capturado las direcciones de e-mail de los contactos allí guardados.

Spyware: programa espía; es decir, tipología de virus que obtienen datos de los sistemas informáticos donde han penetrado y que posteriormente transfieren al atacante.

Streaming: reproducción de contenidos multimedia mediante la red, simultánea al proceso de descarga en el equipo del propio usuario, pudiendo ser una retransmisión en directo o en diferido.

Time stamping: literalmente, sellado de tiempo. Acreditación del momento exacto en que tiene lugar una operación, normalmente la creación o modificación de un documento, sin poder sufrir alteraciones.

Trojan: troyano; es decir, un programa malicioso que infecta a los sistemas informáticos bajo una apariencia benévola frente el usuario. En ser ejecutado, se proporciona al atacante un acceso remoto al sistema infectado. La denominación más adecuada sería la de *Trojan horse* (*caballo de Troya*), pero a lo largo del tiempo se ha extendido su uso de forma acortada y realizando una alteración del sentido mitológico clásico.

Troubleshooting: eliminación de problemas; localización de problemas.

Uniform Resource Locator (URL): dirección singularizada que permite identificar a una página web.

Upskirting: toma de imágenes de los genitales y nalgas de las mujeres mediante una cámara situada por debajo de su falda o prenda de vestir, sin el consentimiento de la mujer afectada. En Reino Unido se considera un tipo penal propio.

Voice Over Internet Protocol (VoIP): llamada de voz sobre protocolo de Internet (IP).

Whaling: tipología de ataques de *phishing* orientados hacia altos cargos y ejecutivos de administraciones públicas y empresas.

World Wide Web (WWW): la red informática mundial, sistema que opera mediante Internet, que permite la transmisión de datos a través del protocolo HTTP.

Worm: gusano; es decir, un programa infeccioso o *malware* que satura los ordenadores y redes en los que ha penetrado a partir de su replicación constante e impide la utilización normal del sistema, consumiendo la capacidad de procesamiento.