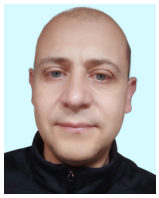
Cumplimiento legal

PID_00286167

Albert Portugal Brugada

Tiempo mínimo de dedicación recomendado: 3 horas

Universitat Oberta de Catalunya



Albert Portugal Brugada

El encargo y la creación de este recurso de aprendizaje UOC han sido coordinados por el profesor: Josep Jorba Esteve

Primera edición: febrero 2022

Av. Tibidabo, 39-43, 08035 Barcelona
Autoría: Albert Portugal Brugada
Producción: FUOC

Índice

Introducción

El concepto de *cloud computing* se refiere al uso remoto a través de internet de software, almacenamiento o procesamiento de datos. Si bien esto puede ayudar a empresas, administraciones públicas y ciudadanía para poder utilizar estos recursos en términos de eficiencia y eficacia, también entraña riesgos, especialmente en el ámbito jurídico (seguridad y privacidad de los datos).

Lectura recomendada

Para ampliar la información sobre *cloud computing*, podéis ver la guía siguiente:

INCIBE (2017). *Cloud computing. Una guía de aproximación para el empresario* [en línea]. <https://www.incibe.es/sites/default/files/ contenidos/guias/doc/guia-cloud-computing_0.pdf>

El *cloud computing* permite el uso de estos recursos que no están en la infraestructura tecnológica propia para un uso interno o para ofrecer servicios a terceros (de manera simple o agregada). Este hecho pone de manifiesto el incremento de actores que participan en la prestación de un servicio y la necesidad del cumplimiento del marco normativo por parte de todos ellos y para todos ellos.

Internet es una red global que es accesible a nivel mundial, lo que facilita que el uso del *cloud computing* se realice también desde esta perspectiva global y que por esta razón los actores que participan en la prestación y el consumo de sistemas *cloud* puedan tener localizaciones diferentes y, por lo tanto, sujeción a marcos normativos particulares (según desde dónde se presta el servicio, a dónde se dirige el servicio prestado o quién es el receptor del servicio).

El que recibe el servicio deberá tener en cuenta que el prestador pueda dar cumplimiento al marco normativo que le afecte en el uso de servicios *cloud*, mientras que el prestador deberá dar cumplimiento al marco normativo que aplique a él mismo y al receptor del servicio y a los acuerdos de servicio entre el prestador y el consumidor.

Objetivos

Los materiales didácticos de este módulo contienen las herramientas necesarias para que el estudiantado logre los objetivos siguientes:

1. Identificar el marco normativo y los estándares nacionales e internacionales aplicables a las políticas de seguridad de los sistemas *cloud*.

2. Conocer las figuras delictivas de los ciberdelitos que afectan a los sistemas *cloud*.

3. Conocer los principios para la obtención de evidencias electrónicas para su aportación en sede judicial en forma de prueba electrónica.

4. Conocer la figura del perito informático y el desarrollo de su actividad.

1. El marco normativo

Dentro del marco normativo hemos de diferenciar el ***hard law*** –que son aquellos instrumentos o prácticas generales con carácter obligatorio y vinculante– del ***soft law*** –que son reglas de conducta sin carácter vinculante–. Esta diferenciación es relevante desde el punto de vista de la exigencia en su cumplimiento.

El marco normativo de referencia en relación con el *cloud computing* más relevante es el relativo a la ciberseguridad, ya que la prestación de servicios se realiza a través de internet.

En el ámbito de la ciberseguridad no existe *hard law* internacional que lo regule, pero sí un conjunto de *soft law* de referencia a nivel internacional y supranacional (Unión Europea):

- **Carta de Naciones Unidas**: reconoce el principio de no hacer uso de la fuerza en las relaciones internacionales y en la legítima defensa.

- **Convenio de Budapest sobre ciberdelincuencia** (2004): tratado internacional para perseguir los delitos informáticos y de internet mediante la armonización de leyes.

- **Resolución de la Asamblea de Naciones Unidas** (2009): se determina la necesidad de revisión de la normativa de cada país para la investigación y el enjuiciamiento de la delincuencia cibernética.

- **Estrategia de ciberseguridad EU** (2013): promueve los principios de ciberseguridad según los valores de la UE.

Si nos centramos en la normativa aplicable a la Unión Europea, debemos diferenciar entre el **derecho originario** (de dimensión constitucional, procedente de la UE, el derecho internacional y los tratados constitutivos de la UE) y el **derecho derivado** de este (reglamentos, directivas, decisiones, recomendaciones).

Lectura recomendada

Para ampliar la información sobre *hard law* y *soft law*, podéis consultar:

Luis Francisco Sánchez Cáceres (2019). «El sistema de Hard-Law y Soft-Law en relación con la defensa de los derechos fundamentales, la igualdad y la no discriminación» [en línea]. *Cuadernos electrónicos de filosofía del derecho* (núm. 39). <https://ojs.uv.es/index.php/CEFD/article/ view/14293/ pdf>

Reglamentos, directivas y otros actos legislativos

Los reglamentos son prescripciones generales de aplicación a todos los Estados miembros.

Las directivas requieren su transposición a la legislación nacional del Estado miembro, pero establecen un marco común.

Las decisiones son obligatorias en todos sus elementos a sus destinatarios de la decisión.

Las recomendaciones/dictámenes no son vinculantes, pero orientan.

Enlace complementario

Podéis ampliar la información sobre reglamentos, directivas y otros actos legislativos en el enlace siguiente:
<https://europa.eu/european-union/law/legal-acts_es>

En España, el marco normativo se encuentra compilado en el **Código de Derecho de la Ciberseguridad**, que relaciona la Constitución Española con las leyes, los decretos y las órdenes en este ámbito.

1.1. Ley 36/2015 de Seguridad Nacional

La Ley de Seguridad Nacional contempla la **ciberseguridad** como un ámbito de especial interés (art. 10), y se refiere especialmente a aquellas situaciones que, por su gravedad, efectos, dimensión, urgencia y transversalidad de las medidas para su resolución, requieren la coordinación reforzada de las autoridades (art. 23).

La ley pone de manifiesto que los **mecanismos** para afrontar estas situaciones se realizarán por medio de los poderes y medios ordinarios, y no pueden implicar la suspensión de derechos fundamentales y libertades de los ciudadanos. Precisamente, este punto puede ser controvertido, ya que existe constancia del uso de software de espionaje por parte de Gobiernos mediante mecanismos no ordinarios y que afectan, por lo tanto, a derechos fundamentales y libertades de los ciudadanos.

1.2. Ley 9/1968 de Secretos Oficiales

La Ley de Secretos Oficiales contempla que las actividades y materias reservadas no podrán ser comunicadas, difundidas o publicadas. Es evidente que esta información, catalogada como reservada, no sería susceptible de ser almacenada en sistemas *cloud*, o en su caso requeriría de medidas adicionales de seguridad para garantizar el cumplimiento de la ley.

1.3. Ley 1/2019 de Secretos Empresariales

De igual modo que el sector público establece aquella información con mayor confidencialidad, el sector privado ha de tener en especial consideración el uso de sistemas *cloud* para la gestión de información que tenga carácter confidencial o estratégico.

La Ley de Secretos Empresariales establece (art. 3) el carácter ilícito del acceso, la apropiación, la copia de información sin el consentimiento de su titular, así como la utilización y la revelación de información sin el consentimiento de su titular, sin respetar el contrato o acuerdo de confidencialidad entre las partes.

Asimismo, también contempla, cuando se realiza el acceso, la utilización o revelación por parte de una persona que debería conocer que obtenía secreto empresarial.

Todo esto pone de manifiesto la necesidad de regular los acuerdos de privacidad y confidencialidad con los **proveedores** *cloud*, así como establecer los protocolos con el **personal** que puede tener acceso a dicha información para minimizar los riesgos del uso ilícito de la información.

1.4. Ley 8/2011 de Protección de Infraestructuras Críticas

La Ley de Protección de Infraestructuras Críticas contempla los **ataques cibernéticos** a estas infraestructuras y sus sistemas de información y comunicaciones. Establece la necesidad de poder garantizar la confidencialidad, integridad y disponibilidad de la información (art. 15). También indica la necesidad de garantizar la seguridad de los datos clasificados (art. 18).

Asimismo, establece como ilícito la producción, la oferta, la comercialización, la importación, la exportación o el almacenaje cuando la persona conozca que se trata de secretos empresariales.

Los aspectos de confidencialidad, integridad y disponibilidad también veremos que tienen su correspondencia en el Esquema Nacional de Seguridad.

1.5. Reales decretos 12/2018 y 43/2021, de seguridad en las redes y sistemas de información

Los reales decretos 12/2018 y 43/2021 transponen la Directiva (UE) 2016/1148, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión (NIS), donde se contempla la protección de la información clasificada, el mantenimiento del orden público y la detección, investigación y persecución de delitos (art. 5).

Los reales decretos se aplican a los servicios esenciales, dependientes de redes y sistemas de información, de sectores estratégicos y servicios digitales (mercados en línea, buscadores y servicios de computación en la nube).

Asimismo, se detallan los equipos de respuesta rápida de **incidentes** de seguridad informática (CSIRT), la obligación de comunicación de incidentes de seguridad y las infracciones por la no comunicación y la no observación de las medidas de seguridad.

Detalla la necesidad del establecimiento de políticas de seguridad que contemplen el análisis y la gestión de **riesgos** (incluidos terceros, como los proveedores *cloud*), el catálogo de medidas (de seguridad, organizativas, tecnológicas y físicas), la detección y la gestión de incidentes y los planes de recuperación.

El alcance de servicios afectados es importante, y por eso determinados servicios *cloud* se pueden ver afectados por la necesidad de cumplimiento.

1.6. Ley 9/2014 General de Telecomunicaciones y Ley 25/2007 de Conservación de Datos Relativos a las Comunicaciones Electrónicas y a las Redes Públicas de Comunicaciones

Los operadores de redes públicas de comunicaciones han de garantizar el secreto de las comunicaciones y colaborar con las autoridades en la investigación a los agentes facultados. Este secreto se puede garantizar por medio de **cifrado**, pero se podrá imponer la obligación de facilitar los algoritmos o procedimientos de cifrado al órgano competente.

La Ley 25/2007 establece la necesidad de conservar un año la información relativa a las comunicaciones, pero se puede ampliar hasta los dos años.

1.7. Ley 34/2002 de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSI)

La LSSI se aplica a los **prestadores** de servicios de la sociedad de la información a distancia, por vía telemática, a petición individual del interesado y normalmente de forma onerosa. También se aplica a los **servicios de intermediación** que facilitan la prestación del servicio, utilizan otros servicios o dan acceso a la información.

En relación con estos servicios, es relevante que las autoridades pueden llegar a interrumpir la prestación del servicio, así como solicitar medidas para identificar a la persona responsable de la vulneración y la retirada de contenidos o impedir su acceso.

Asimismo, los prestadores tienen la obligación de colaborar en dar información, acceso a las instalaciones y documentación a las autoridades, y cooperar también con los CSIRT en relación con la resolución de incidentes de ciberseguridad.

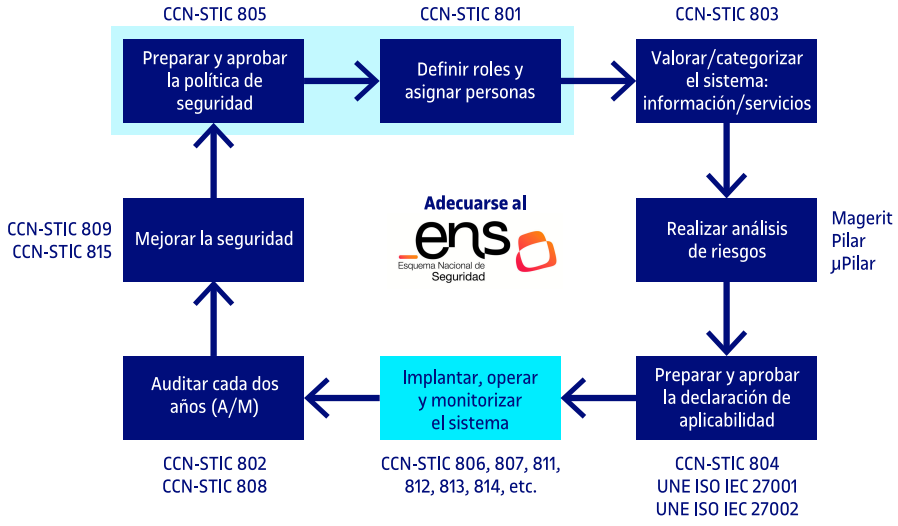
1.8. Real Decreto 3/2010. Esquema Nacional de Seguridad (ENS)

El Real Decreto 3/2010 establece un conjunto de criterios y recomendaciones en materia de seguridad por medio de **principios básicos y requisitos mínimos** para la protección de la información para las **administraciones públicas**, es decir, que ha de ser cumplido por estas y por las empresas que les prestan servicios en este ámbito (figura y tabla 1).

Asimismo, parte del **sector privado** también ha adoptado el ENS como mecanismo para garantizar la seguridad de los sistemas de información. Estos mecanismos inciden en la seguridad de los sistemas de información mediante el análisis de riesgos y la propuesta de medidas en los ámbitos organizativos, operacionales y de medidas de protección.

El ENS analiza los activos de información a partir de las dimensiones de disponibilidad, integridad, confidencialidad, autenticidad, trazabilidad y categorización del riesgo, y propone medidas para mitigar o eliminar dichos riesgos.

Figura 1. Adecuación al Esquema Nacional de Seguridad



Fuente: elaboración propia

En la valoración de los sistemas de información se establecen criterios comunes en la valoración de las dimensiones de seguridad[1] (disponibilidad, autenticidad, integridad, confidencialidad o trazabilidad) en función del impacto negativo sobre la seguridad y sus repercusiones desde la perspectiva de cum-

(1)Art. 43 Real Decreto 3/2010 (<https://www.boe.es/buscar/act.php?id=BOE-A-2010-1330>).

plimiento legal, perjuicios directos a personas físicas o jurídicas, pérdidas económicas, reputación del organismo, posibilidad de protestas o la comisión de delitos.

Estos criterios se catalogan en niveles de riesgo alto, medio, bajo o sin aplicación al activo de información analizado y cada uno de estos dispone de una etiqueta (del tipo COM.DIS.N) que permite el establecimiento posterior de medidas que minimicen los riesgos. En la tabla 1 se detallan algunos de ellos.

Enlace recomendado

Para consultar la lista completa de los criterios podéis consultar: **Centro Criptológico Nacional** (2020, mayo). *Guía de Seguridad de las TIC. CCN-STIC 803* [en línea]. Madrid: Ministerio de Defensa. <https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/682-ccn-stic-803-valoracion-de-sistemas-en-el-ens-1/file.html>

Tabla 1a. Criterios comunes aplicables a todas las dimensiones de tipos de información y servicios

		No aplicable (N/A)	Bajo	Medio	Alto
Disposición legal o administrativa		COM.DIS.N No existe ninguna disposición legal o administrativa que condicione su nivel.	COM.DIS.B Por disposición legal o administrativa: ley, decreto, orden, resolución, etc.	COM.DIS.M Por disposición legal o administrativa: ley, decreto, orden, resolución, etc.	COM.DIS.A Por disposición legal o administrativa: ley, decreto, orden, resolución, etc.
Perjuicio directo al ciudadano (de cualquier índole)		COM.PER.N No supone ningún perjuicio directo al ciudadano.	COM.PER.B Algún perjuicio.	COM.PER.M Daño importante, aunque subsanable.	COM.PER.A Grave daño, de difícil o imposible reparación.
Incumplimiento de una norma	**Legal o administrativa**	COM.LEG.N No implica incumplimiento de una norma jurídica.	COM.LEG.B Incumplimiento formal leve de una norma jurídica, de carácter subsanable.	COM.LEG.M Incumplimiento material de una norma jurídica, o incumplimientode formal no subsanable.	COM.LEG.A Incumplimiento formal y material grave de una norma jurídica.
	Regulatoria	COM.REG.N No implica incumplimiento de normativa de un regulador.	COM.REG.B Implica incumplimiento de normativa de un regulador.	COM.REG.M Implica sanción significativa de un regulador.	COM.REG.A Implica sanción grave de un regulador y/o pérdida de licencia de operar.
	Contractual	COM.CON.N No implica incumplimiento de normativa de una obligación contractual.	COM.CON.B Incumplimiento formal leve de una obligación contractual.	COM.CON.M Incumplimiento material o formal de una obligación contractual.	COM.CON.A Incumplimiento formal o material grave de una obligación contractual.
	Interna	COM.INT.N No implica incumplimiento de normativa interna.	COM.INT.B Incumplimiento formal leve de una norma interna.	COM.INT.M Incumplimiento material o formal de una norma interna.	COM.INT.A Incumplimiento formal o material grave de una norma interna.

Fuente: Centro Criptológico Nacional (2020, mayo). *Guía de Seguridad de las TIC. CCN-STIC 803* [en línea]. Madrid: Ministerio de Defensa. <https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/682-ccn-stic-803-valoracion-de-sistemas-en-el-ens-1/file.html>

Tabla 1b. Criterios comunes aplicables a todas las dimensiones de tipos de información y servicios

	No adscrito (N/A)	Bajo	Medio	Alto
Pérdidas económicas	COM.ECO.N No implica pérdidas económicas.	COM.ECO.B Pérdidas económicas (no superiores al 4 % del presupuesto anual de la organización).	COM.ECO.M Pérdidas económicas importantes (superiores al 4 % e inferiores añ 10 % del presupuesto anual de la organización).	COM.ECO.A Pérdidas económicas o alteraciones financieras significativas (superiores al 10 % del presupuesto anual de la organización).
Reputación	COM.REP.N No implica daño reputacional.	COM.REP.B Daño reputacional moderado con los ciudadanos o con otras organizaciones.	COM.REP.M Daño reputacional significativo con los ciudadanos o con otras organizaciones.	COM.REP.A Daño reputacional grave con los ciudadanos o con otras organizaciones.
Protestas	COM.PRO.N No se prevé que pueda desembocar en protestas.	COM.PRO.B Múltiples protestas individuales.	COM.PRO.M Protestas públicas (alteración del orden público).	COM.PRO.A Protestas masivas (alteración seria del orden público).
Delitos	COM.DEL.N No facilitaría la comisión de delitos ni dificultaría su investigación.	COM.DEL.B Favorecería la comisión de delitos.	COM.DEL.M Favorecería significativamente la comisión de delitos o dificultaría su investigación.	COM.DEL.A Podría incitar a la comisión de delitos, constituiría en sí un delito, o dificultaría enormemente su investigación.

Fuente: Centro Criptológico Nacional (2020, mayo). *Guía de Seguridad de las TIC. CCN-STIC 803* [en línea]. Madrid: Ministerio de Defensa. <https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/682-ccn-stic-803-valoracion-de-sistemas-en-el-ens-1/file.html>

El Centro Criptológico Nacional Computer Emergency Response Team (CCN-CERT) pone a disposición del sector público la herramienta Pilar, que permite el establecimiento del mapa de calor de riesgos y la propuesta de medidas para la disminución del riesgo hasta un límite aceptable (figura 2).

Figura 2. Herramienta Pilar

Fuente: elaboración propia

1.9. Reglamento (UE) 2016/679 (RGPD), relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, y Ley Orgánica 3/2018 de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD)

El Reglamento (UE) 2016/679 (RGPD), 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, se aplica a toda la Unión Europea sin necesidad de transponerlo en leyes nacionales. El Reglamento europeo obliga a la implantación de políticas de privacidad –por diseño y por defecto–, a la aplicación de los principios de limitación de finalidad, minimización de datos y conservación, y a la existencia de una base legal para su tratamiento. Estos elementos también están recogidos en la Ley Orgánica 3/2018, de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD).

El RGPD y la LOPDGDD contemplan los derechos de los interesados y su ejercicio, así como las obligaciones de los responsables y encargados del tratamiento de los datos personales.

En cuanto a las **medidas de seguridad**, establece la necesidad de una revisión periódica, así como la obligación de notificación de los incidentes de seguridad a las autoridades de control en un plazo de 72 horas y la colaboración en su investigación.

Dentro de los **datos de carácter personal**, contempla como categorías especiales los datos relativos a origen étnico o racial, opiniones políticas, convicciones religiosas o filosóficas, afiliación sindical, datos genéticos, biométricos, de salud, vida u orientación sexual.

Es relevante que este reglamento contempla que es de aplicación, no solo cuando el encargado o responsable de tratamiento esté en la Unión Europea, sino también cuando el tratamiento se refiera a ciudadanos de esta o cuando la oferta de bienes o servicios se dirija a sus ciudadanos. Este punto es relevante, ya que obliga a proveedores de servicios *cloud* al cumplimiento de la normativa europea de protección de datos, **aunque no se encuentren en la UE**.

A escala mundial, los niveles de protección en relación con el tratamiento de datos de carácter personal difieren de modo significativo, y la normativa de la UE es una de las más garantistas de los derechos de los ciudadanos. Aun así, también a escala mundial podemos encontrar múltiples normativas en este ámbito, que añaden complejidad a la prestación de servicios *cloud* y a su cumplimiento global.

El RGPD y la LOPDGDD establecen las **sanciones** por el incumplimiento de la normativa de protección de datos, que pueden llegar al 4 % de la facturación de la empresa o hasta 20.000.000 euros.

1.10. Estándares internacionales para la seguridad de sistemas *cloud*

Los estándares internacionales (ISO) formarían parte del *soft law*. Sin ser de obligado cumplimiento, establecen los **principios de calidad** en la prestación de servicios *cloud* por parte de las empresas que los cumplen.

Las ISO más relevantes en la prestación de servicios *cloud* serían las siguientes:

- **ISO 27001**: para los sistemas de gestión de la seguridad de la información. Se centra en la evaluación de riesgos y la aplicación de controles imprescindibles para su mitigación y eliminación.

- **ISO 27002**: guía de buenas prácticas, que describe los objetivos de control y controles recomendables en relación con la seguridad de la información.

- **ISO/IEC 27017**: controles de seguridad para servicios *cloud*. Se centra en aspectos de responsabilidad, eliminación y devolución de activos en la finalización del contrato, operaciones y procedimientos administrativos, etc.

- **ISO/IEC 27018**: para el control de la protección de datos en los servicios *cloud*.

También es importante destacar el **National Institute of Standards and Technology Framework (NIST)**, una herramienta voluntaria destinada a ayudar a las organizaciones a identificar y gestionar el riesgo de la privacidad para construir productos y servicios innovadores, y que protejan la privacidad de las personas.

2. Los delitos informáticos

Los delitos informáticos se materializan, habitualmente por medio de equipos informáticos e internet, en distintos mecanismos técnicos y reciben diversas denominaciones, principalmente vinculadas al mecanismo utilizado en la realización del delito o a la finalidad de este.

Estos delitos se caracterizan por la **anonimidad** que confiere la red al sujeto delictivo, lo que a su vez otorga una percepción de seguridad en su comisión. Por otra parte, la utilización de los **mecanismos técnicos** que permiten la consecución del delito puede ser desde extremadamente sencilla, mediante herramientas, hasta mecanismos complejos que requieren un conocimiento técnico elevado para su desarrollo. Esto identifica un conjunto de perfiles delictivos muy amplio.

Los delitos informáticos han tenido un fuerte incremento en los últimos años debido a la generalización en el uso de las nuevas tecnologías por parte de la ciudadanía, las empresas y los organismos públicos (figura 3).

Figura 3. Quejas recibidas por el IC3 del FBI relacionadas con delitos informáticos

Fuente: elaboración propia

El avance de la técnica posibilita el desarrollo constante de nuevos mecanismos, y por ello requiere que los ordenamientos jurídicos contemplen mecanismos que permitan la lucha eficaz y se adapten a la realidad de cada momento en este ámbito.

En la mayoría de los ordenamientos jurídicos, entre estos el español (tabla 2), se realiza una clasificación de los delitos informáticos en relación con los efectos que estos producen:

- delitos económico-patrimoniales,
- delitos contra la intimidad/privacidad y
- delitos contra intereses generales de las personas o los países.

Tabla 2. Evolución de delitos informáticos en España por categoría delictiva

Hechos conocidos	2016	2017	2018	2019	2020
Acceso e interceptación ilícita	3.243	3.150	3.384	4.004	4.653
Amenazas y coacciones	12.036	11.812	12.800	12.782	14.066
Contra el honor	1.546	1.561	1.448	1.422	1.550
Contra la propiedad industrial/intelectual	129	121	232	197	125
Delitos sexuales*	1.231	1.392	1.581	1.774	1.783
Falsificación informática	3.017	3.280	3.436	4.275	6.289
Fraude informático	70.178	94.792	136.656	192.375	257.907
Interferencia datos y en sistema	1.336	1.291	1.192	1.473	1.590
Total hechos conocidos	**92.716**	**117.399**	**160.729**	**218.302**	**287.963**

Fuente: Javier López Gutiérrez y otros (2020). *Estudio sobre la cibercriminalidad en España* (pág. 41) [en línea]. Madrid: Ministerio del Interior. <http://www.interior.gob.es/documents/10180/11389243/Estudio+sobre+la+Cibercriminalidad+en+España%C3%B1a+2020.pdf/ed85b525-e67d-4058-9957-ea99ca9813c3>

*Excluidos las agresiones sexuales con/sin penetración y los abusos sexuales con penetración

2.1. Los delitos informáticos y la obsolescencia de las normas legales

Si bien los marcos normativos se han ido adaptando a las nuevas tipologías de delitos informáticos, es evidente que la capacidad de evolución de la tecnología es muy superior a la de la normativa legal.

Aunque existe una evolución constante de los tipos de ciberdelitos, estos se centran en delitos económico-patrimoniales, delitos contra la intimidad/privacidad y delitos contra intereses generales de las personas o los países. Precisamente, este hecho permite que muchos ciberdelitos puedan ser perseguidos desde la perspectiva de delitos preexistentes en los marcos normativos.

Las normas se han ido modificando para contemplar estos ciberdelitos, desde una perspectiva general, para evitar la obsolescencia de las normas. Asimismo, la jurisprudencia ha ido interpretando las normas existentes para contemplar las nuevas tipologías de delitos informáticos.

2.2. Los delitos informáticos en el Código Penal español

El Código Penal español se ha ido actualizando para permitir la persecución de los delitos informáticos en sus diferentes modalidades.

Los principales delitos informáticos contemplados en el Código Penal son los siguientes:

1) Descubrimiento de secretos o vulneración de la intimidad (197.1 y 197.2 CP): cuando sin su consentimiento se apodere, utilice, modifique o revele datos de carácter personal, intercepte las comunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción de sonido o imagen o de cualquiera otra comunicación, o conociendo el origen ilícito participe de su difusión (castigo de 1 a 5 años y multa de 12 a 24 meses).

2) Intrusión informática (197.1 bis CP): quien, por cualquier medio o procedimiento, vulnerando las medidas de seguridad establecidas para impedirlo, sin estar debidamente autorizado, acceda o facilite a otro el acceso al conjunto o una parte del sistema de información o se mantenga en él en contra de la voluntad y tenga el legítimo derecho a excluirlo (castigo de 6 meses a 2 años).

3) Interceptación de las transmisiones de datos (197.2 bis CP): quien, mediante la utilización de artificios o instrumentos técnicos, y sin estar debidamente autorizado, intercepte transmisiones no públicas de datos informáticos que se producen desde, hasta o dentro de un sistema de información, incluidas las emisiones electromagnéticas de estos (castigo de 3 meses a 2 años o multa de 3 a 12 meses).

4) Cooperación en la comisión del delito (197 ter CP): quien, sin estar debidamente autorizado, produzca, adquiera para su uso, importe o, de cualquier forma, facilite a terceros (programa informático, contraseñas, códigos de acceso o datos similares) con la intención de facilitar la comisión de alguno de los delitos anteriores (castigado de 6 meses a 2 años o multa de 3 a 18 meses).

5) Delitos informáticos relacionados con la propiedad intelectual e industrial (270 y sigs. CP): obtención de beneficio económico, en perjuicio de tercero, reproduciendo, plagiando, distribuyendo, comunicando públicamente, facilitando de forma activa acceso o de cualquier otro modo de explotación económica de una obra o prestación literaria, artística o científica sin autorización de los titulares de los derechos de propiedad intelectual o de sus cesionarios (castigo de 6 meses a 4 años o multa de 12 a 24 meses).

6) Fraudes informáticos (248 y sigs. CP): manipulación informática o artificio similar que consigan una transferencia no consentida de cualquier activo patrimonial en perjuicio de otro, fabricación, introducción, posesión o facilitar programas informáticos destinados a la realización de estafas y uso fraudulento de tarjetas, cheques o datos contenidos en ellos (castigado de 6 meses a 3 años).

7) Sabotaje informático (263 y sigs. CP): borrar, dañar, alterar o hacer inaccesibles datos informáticos, programas, sistemas informáticos o documentos electrónicos (castigo de 6 meses a 5 años).

8) Otros delitos contemplados en el Código Penal aplicables a delitos informáticos:

- Amenazas (169 y sigs. CP).
- Calumnias e injurias (205 y sigs. CP).
- Inducción a la prostitución de menores (187 CP).
- Producción, venta, distribución, exhibición o posesión de material pornográfico donde intervengan o sean utilizados menores de edad o incapaces (189 CP).

2.3. La persecución de los delitos informáticos

El delito informático (a diferencia de la mayoría de los delitos) se caracteriza por que, en la mayoría de los casos, existe una diferenciación entre el lugar en el que se inicia o dirige el delito del lugar donde este despliega su resultado.

La **ubicuidad** del delito implica normalmente diferentes países, y esto obliga a tener en cuenta el derecho internacional, especialmente en relación con la **competencia para el enjuiciamiento** de estos delitos, evitando el *bis in idem*, y favorecer que este sea juzgado en el país que tenga el mejor foro (donde se encuentren los autores o las víctimas o las pruebas, por ejemplo). Esto no impide que cada uno de los países donde ha tenido efectos el delito informático pueda iniciar los procedimientos de investigación del hecho y que se puedan acumular en el tribunal competente para su enjuiciamiento.

El factor internacional implica la existencia de diferentes jurisdicciones y la necesidad de una cooperación judicial, además de la posibilidad de requerimientos de información a empresas fuera del ámbito territorial de la jurisdicción que la requiere.

Por otro lado, las diferentes jurisdicciones donde el delito ha tenido presencia pueden tipificar y castigar de manera diferenciada los actos delictivos llevados a cabo.

La complejidad en el desarrollo de las investigaciones y el enjuiciamiento de los delitos informáticos contrastan con la necesidad de agilidad en la obtención de **evidencias** del delito antes de que estas puedan desaparecer. Los delitos informáticos se caracterizan por que el autor suele intentar eliminar el rastro de evidencias incriminatorias, y el tiempo durante el que las empresas y los sistemas de información almacenan información relevante (para la investigación) es limitado.

Asimismo, los delitos informáticos suelen tener implícitos la acumulación de delitos que permiten su enjuiciamiento en una sola causa, así como la aplicación de **agravaciones** del delito, atendiendo a la cantidad de personas afecta-

das, al importe y al propio hecho delictivo. Esto redunda en la ampliación de los periodos de prescripción de los delitos, así como de la competencia para su enjuiciamiento.

Finalmente, cabe señalar que el desarrollo de las operaciones de investigación de esta tipología de delitos requiere el uso de perfiles cualificados en equipos policiales especializados, peritos forenses del ámbito tecnológico y el uso de herramientas tecnológicas especializadas.

2.4. La responsabilidad penal y la responsabilidad civil

Los delitos informáticos implican una responsabilidad penal para los autores de los hechos delictivos, pero también la obligación de reparar los daños y perjuicios ocasionados o la restitución de la cosa (art. 109 del Código Penal y art. 100 de la Ley de Enjuiciamiento Criminal).

> En el caso de los delitos informáticos, por su naturaleza y en muchos casos por su alcance, resulta complejo que se pueda llevar a cabo la reparación del perjuicio.

La **restitución** de los delitos no económicos implica la devolución de la información robada o su destrucción. En este punto puede ser extremadamente complejo garantizar, en el mundo electrónico, que se ha producido la destrucción total o que se ha producido la devolución fidedigna de la información robada.

La reparación supone una serie de obligaciones de dar y hacer (o no hacer) por parte del autor o responsable de la culpa derivada. En muchos casos, la **reparación del daño** puede ser altamente compleja debido a su magnitud o por la imposibilidad material de reparación. Asimismo, las tecnologías procedentes de la inteligencia artificial se han incorporado para su uso en los delitos informáticos (y para la prevención). La inteligencia artificial dificulta la predictibilidad de su comportamiento y por eso incide en la dificultad de la determinación del daño ocasionado y su magnitud.

En relación con los delitos informáticos y la **responsabilidad civil** para la reparación del daño, es relevante observar que la **omisión** de acciones en materia de seguridad o **negligencia** en su aplicación por parte de los prestadores *cloud* puede tener implicaciones en materia de responsabilidad civil de estos últimos. Es decir, aunque sean los ciberdelincuentes los responsables penales del hecho, los prestadores de servicios *cloud*, si no hubieran implantado las medidas mínimas de seguridad o no hubieran actuado de manera diligente en la detección del delito y la minimización del daño, podrían incurrir en

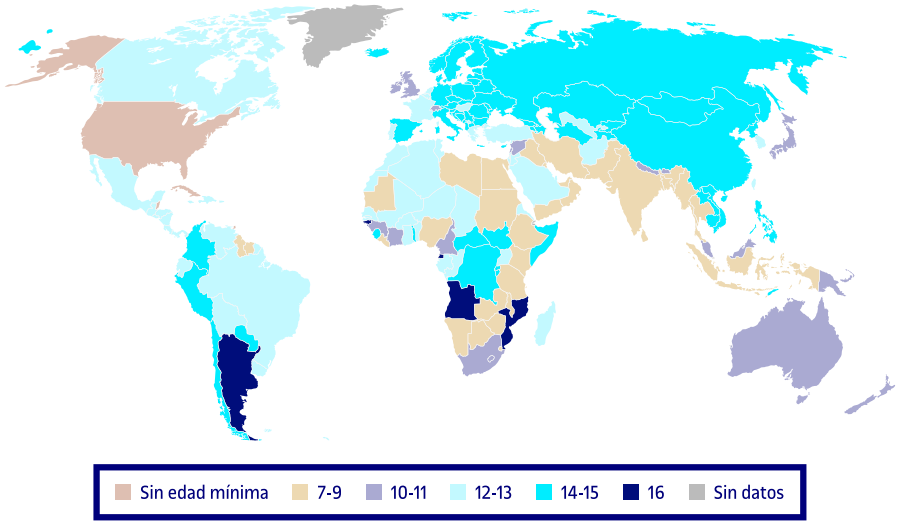
responsabilidad contractual, extracontractual, administrativa e incluso penal. Esto podría implicar la reparación del daño y los perjuicios ocasionados o sanciones administrativas en materia de protección de datos.

2.5. Los menores de edad y los ciberdelitos

Los delitos informáticos son llevados a cabo principalmente a través de internet de manera telemática y remota. La comisión del delito utiliza desde técnicas sencillas a técnicas extremadamente complejas. Estos elementos facilitan que el desarrollo de las actividades delictivas sea llevado a cabo por parte de menores de edad.

Este hecho es especialmente relevante, dado que mundialmente existen diferencias relevantes tanto en la tipificación de los hechos delictivos y su castigo, como en la edad en la que una persona puede ser legalmente responsable de un acto desde la perspectiva penal (figura 4). Esto pone de manifiesto que, según la jurisdicción competente en el enjuiciamiento del hecho, puede implicar la responsabilidad penal o no del menor por la comisión del acto delictivo.

Figura 4. Edad mínima de responsabilidad criminal en el mundo



Fuente: elaboración propia a partir de <https://www.economist.com/graphic-detail/2019/11/05/if-a-13-year-old-murders-a-ten-year-old-is-it-a-crime>

En el caso del Código Penal español, los menores no son responsables, y es la Ley Orgánica 5/2000 la que regula la responsabilidad penal de los menores entre 14 y 18 años.

El juez de menores determina la conversión de las penas del Código Penal en **medidas de reeducación**: tratamiento, libertad vigilada, prohibición de hacer, prestaciones en beneficio de la comunidad y tareas socioeducativas, entre otras, valorando siempre la edad, las circunstancias familiares y sociales, la personalidad y el interés del menor. Los menores de 14 años serían irresponsables penalmente.

2.6. La cibercriminología

La aparición de los ciberdelitos ha implicado el estudio específico desde el punto de vista de la criminología de los sujetos que llevan a cabo estas acciones delictivas. En este sentido, se denomina ***hackers*** a aquellos individuos expertos en la seguridad de los sistemas de información, y reciben diferente clasificación en función de las acciones que llevan a cabo:

Enlace complementario

Podéis ampliar la información sobre los *hackers* en el enlace siguiente:

<https://es.wikipedia.org/wiki/Hacker_(seguridad_inform%C3%A1tica)>

- ***White hat hackers*** son aquellos individuos que realizan acciones con el objetivo de estudiar y reforzar la seguridad de los sistemas de información.

- ***Gray hat hackers*** son aquellos individuos con la misma motivación que los *white hat hackers*, pero que ofrecen sus servicios para resolver los fallos de seguridad a cambio de dinero.

- ***Black hat hackers*** serían aquellos que encajarían en la figura de los ciberdelincuentes por intereses personales o económicos. Dentro de esta clasificación encontramos a los *crackers*, *viruckters*, traficantes de armas (herramientas informáticas), *banquers*, contratistas, agentes especiales, ninjas, cibersoldados, *spammers*, *domainers*, espías informáticos, *sniffers*, terroristas informáticos, *phishers*, *hoaxers*, hacktivista-anarquistas.

Desde el punto de vista criminológico, el estudio de los **perfiles delictivos** se centra en las motivaciones y la psicología de los sujetos que cometen estas acciones (tabla 3).

Tabla 3. Clasificación de los ciberdelincuentes

	Motivación	Tipología	Perfil
Psico-ciberdelincuente	Reconocimiento, seguridad, pertenencia a un grupo.	**Ciber-psicópata**	Exitoso: nuevas sensaciones, narcisista, beneficio económico, manipulador. Ejecutor: antisocial, egocéntrico, violento, disfruta humillando.
		Ciber-neurótico	Introvertido, manipulable, inseguro, con poco control sobre sus acciones.
		Ciber-psicótico	Alienado: pérdida de contacto con la realidad, escoge víctimas porque se siente humillado, amenazado por ellas. Salvador: busca seguidores, tiene sentimiento de superioridad, quiere salvar al mundo de peligros indeterminados.
		Ciber-sociópata	Inadaptado: necesidad de pertenencia a un grupo, autoestima y realización; reconoce la autoría y justifica el acto para mejorar la seguridad.

Fuente: elaboración propia a partir de Sergio Cámara Arroyo (2020). «Estudios criminológicos contemporáneos (IX): La Cibercriminología y el perfil del ciberdelincuente» [en línea]. *Derecho y Cambio Social* (núm. 60, págs. 470-512). <https://dialnet.unirioja.es/servlet/articulo?codigo=7524987>

	Motivación	Tipología	Perfil
Normo-ciberdelincuente	Económica.	**Ciber-oportunista**	Ventajista.
		Ciber-común	Canalla, rebelde.
		Ciber-habitual	Profesional, mercenario.

Fuente: elaboración propia a partir de Sergio Cámara Arroyo (2020). «Estudios criminológicos contemporáneos (IX): La Cibercriminología y el perfil del ciberdelincuente» [en línea]. *Derecho y Cambio Social* (núm. 60, págs. 470-512). <https://dialnet.unirioja.es/servlet/articulo?codigo=7524987>

2.7. Nuevas respuestas a los ciberdelitos

Si bien la interconexión de los sistemas de información e internet ha facilitado el crecimiento exponencial de los ciberdelitos, también ha permitido dar nuevas respuestas a estos para impedir su efectividad.

La Revolución Industrial 4.0 ha supuesto que en muchos casos el coste marginal de producción es cero, lo que supone que la sustracción de estos productos o la utilización de manera fraudulenta de productos o servicios digitales no supone en sí misma pérdidas al productor o prestador de servicios, sino que afecta al rendimiento económico (**lucro cesante**).

Coste marginal de producción

El coste marginal de producción es cero cuando el coste de producir una unidad adicional o prestar servicio a un nuevo cliente el coste es cero. Esto es habitual en la nueva economía digital, en la que el coste se soporta en la producción del primer producto o servicio y fabricar más productos o prestar servicio a más clientes no supone un incremento de costes de producción.

Referencia bibliográfica

Jeremy Rifkin (2014). *La sociedad de coste marginal cero*. Barcelona: Paidós. <https://www.thezeromarginalcostsociety.com>

Las **licencias de uso de software** son un ejemplo de la economía de producción cero. En este sentido, existe software que altera los softwares originales para permitir su uso sin licencia; en otros casos se produce la venta ilegal de licencia obtenida de manera fraudulenta; en otros se adquieren mediante tarjetas de crédito robadas, etc. Estos mecanismos de uso ilegal de licencias se combaten por parte de los productores de software mediante diferentes estrategias, especialmente aprovechando la interconexión de sistemas en internet:

- Identificación de patrones de fraude y desactivación de licencias.
- Rastreo de licencias publicadas para su utilización ilegal.
- Limitación de características del producto.
- Ofertas especiales a los usuarios de licencias fraudulentas para su regularización.
- Auditorías de red para la detección de uso fraudulento de software.

La Revolución Industrial 4.0 ha supuesto la aparición de las **criptomonedas** como, por ejemplo, Bitcoin. Las criptomonedas son activos inmateriales representados por cadenas de caracteres y que se transmiten a través de transacciones entre monederos digitales, también representados por cadenas de caracteres. Este modelo permite trazar completamente las transacciones realizadas, pero también permite garantizar la anonimidad de los actores que participan de las transacciones. Este hecho ha fomentado el uso de criptomonedas para el pago de rescates de delitos informáticos, así como la apropiación indebida de criptomonedas de los monederos digitales.

Apropiación de criptomonedas

En 2021, la empresa Poly Network sufrió un ataque informático que supuso la apropiación indebida por parte de los ciberdelincuentes de 611 millones de dólares en criptomonedas Binance Smart Chain (BSC), Ethereum (ETH) y Polygon (MATIC). La empresa afectada comunicó las direcciones de los monederos electrónicos donde se habían remitido las criptomonedas para que fueran incluidas en las listas negras los *tokens* de estas direcciones. Finalmente, los ciberdelincuentes devolvieron las criptomonedas sustraídas.

La Revolución Industrial 4.0 supone la **interconectividad de los bienes en internet** para poder obtener todas las funcionalidades del bien y una experiencia de usuario adecuada. Actualmente, no solo los equipos informáticos y de telefonía requieren la conexión a internet, sino que muchos otros también lo requieren y otros se prevé que lo hagan en el futuro. Hoy en día, los **televisores** requieren conectividad a internet para la utilización completa de sus características. Precisamente, este hecho permite a los fabricantes del producto interactuar/actualizar el dispositivo. Y esta conectividad de los televisores puede tener efectos negativos en relación con ciberataques (especialmente en la privacidad de las personas), así como constituir un mecanismo de protección de los ciberdelitos.

Internet como mecanismo de defensa

En el año 2021, un almacén logístico de Sudáfrica sufrió el robo masivo de equipos de televisión de la marca Samsung. En julio de ese mismo año, Samsung anunciaba la funcionalidad TV Block, que permitía al fabricante bloquear aquellas televisiones que se hubieran obtenido de manera fraudulenta a partir del bloqueo del código de serie asociado a cada unidad de televisión. Si bien no se trata de un ciberdelito, las empresas sí que utilizan internet como mecanismo de defensa ante los delitos convencionales y, de paso, de desincentivación para que no se produzcan.

2.8. La ética

Considerando la evolución constante de la tecnología, las prácticas que pueden llegar a ser consideradas delictivas y la dificultad en otros casos de delimitar si una actividad puede ser considerada delictiva (podéis ver el caso de los *gray hat hackers*), nos encontramos con la necesidad de tener en cuenta la ética como una medida para analizar las actividades que se llevan a cabo en el mundo tecnológico.

El derecho es el conjunto de normas imperativas aplicables a la sociedad con el objetivo de imponer un orden o un bien común. Por el contrario, la ética es la puesta en práctica de valores que tienen como objetivo el bien común

sobre el bien individual. Por esta razón, el derecho se centra en lo que está permitido (o prohibido), mientras que la ética, en lo que podríamos esperar **más allá del derecho**.

El periodista Steven Levy publicó en 1984 *Hackers: Heroes of the Computer Revolution*, donde se describen los **principios morales** que tenían que regir a los *hackers*, que surgieron en los años cincuenta en el Instituto Tecnológico de Massachusetts (MIT). Algunos de sus principios son los siguientes:

- Se requiere un acceso ilimitado y total a los ordenadores para poder enseñar cómo funciona el mundo.
- La información debe ser libre.
- Los sistemas han de ser abiertos, descentralizados, sin autoridades y burocracia.
- Los ordenadores pueden cambiar la vida de las personas a mejor.

Asimismo, contemplaba diferentes elementos éticos en forma de **valores** como la pasión, libertad, conciencia social, verdad, honestidad, anticorrupción, igualdad social, libre acceso a la información, valor social, accesibilidad, preocupación responsable, etc.

La ética no solo es relevante dentro de la cultura *hacker*, sino que también es relevante en la prestación de servicios tecnológicos para impedir que se lleven a cabo conductas que, siendo lícitas, pueden tener afectación sobre el bien común.

En la prestación de servicios *cloud*, es habitual que exista cierta controversia en el uso de los datos personales por parte de estos prestadores y las políticas de privacidad que imponen a los consumidores de estos servicios. Es manifiesto que no existe un marco normativo común global y tampoco la percepción de si determinados usos con los datos personales son éticos. Al mismo tiempo, la percepción de la ética también puede variar en función de cada grupo de personas o sociedad.

Para suplir los límites del derecho y reforzar la dimensión ética del uso de las tecnologías, empresas, sectores industriales y administraciones públicas llevan a cabo códigos de conducta. Estos **códigos de conducta** se establecen como mecanismos de autorregulación de colectivos con la finalidad de demostrar un correcto cumplimiento de la normativa o del comportamiento ético. En este sentido, la propia normativa legal[2] hace referencia a la posibilidad de establecer estos códigos éticos.

(2)Art. 18 LSSI y art. 40 RGPD.

3. La prueba electrónica en juicio

La **prueba judicial** es «el conjunto de reglas que regulan la admisión, producción, asunción y valoración de los diversos medios que pueden emplearse para llevar al juez la convicción sobre los hechos que interesan al proceso». Estas pruebas han de permitir demostrar y fundamentar la certeza de un hecho.

La prueba contempla la manifestación formal (medios de prueba), sustancial (los hechos que se prueban) y el resultado subjetivo (valoración de la certeza por parte del juez).

La **prueba digital** se refiere a aquellos métodos de prueba que se realizan por medio de mecanismos electrónicos que por su naturaleza presentan unas características particulares.

> La prueba digital se basa en la prueba presentada informáticamente y que puede estar compuesta por un elemento material (ordenador o dispositivo electrónico) y un intangible (programa, datos o documentos electrónicos).

El **soporte electrónico** tiene un carácter más efímero y manipulable que los soportes físicos, y se entiende que en los primeros resulta más difícil determinar la no manipulación (pueden ser iguales en apariencia) y es más sencilla su destrucción.

La Ley de Enjuiciamiento Civil contempla como medios de prueba los documentos públicos y privados, dictámenes de peritos y otros que puedan obtener certeza de hechos relevantes (art. 299). Estos medios de prueba pueden tener su correspondencia en documentos digitales.

Asimismo, el Reglamento (UE) 910/2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior (art. 41), establece que los **sellos cualificados de tiempo electrónicos** disfrutarán de una presunción de exactitud de la fecha y hora que indican y de la integridad de los datos a los que la fecha y hora estén vinculadas. Asimismo, contempla que un sello cualificado de tiempo electrónico emitido en un Estado miembro será reconocido como sello cualificado de tiempo electrónico en todos los Estados miembros.

La prueba electrónica, al igual que el resto de las pruebas, requiere asegurar la cadena de custodia para garantizar la autenticidad e integridad de la prueba durante todo el ciclo de vida hasta su contradicción en juicio.

Las pruebas que están indisolublemente ligadas a una prueba primariamente viciada (ilícita) no pueden ser valoradas en juicio. Esto representa la **teoría del árbol envenenado** y que el fin no justifica los medios. No obstante, no estaríamos en este caso si la prueba se obtiene mediante una vía de investigación diferente que permita obtener la misma prueba (**teoría de la fuente independiente**). Tampoco en el caso de que las circunstancias conlleven al mismo resultado, sin existir vinculación de causalidad entre la obtención de la primera prueba y la segunda (**teoría del descubrimiento inevitable**). Asimismo, y especialmente relevante en la obtención de la prueba digital, la **teoría de la conexión de antijuricidad** representa que no se pueden valorar aquellas pruebas que han sido obtenidas violentando derechos o libertades fundamentales.

Lectura recomendada

Para ampliar información sobre la teoría del árbol envenenado, podéis consultar:

José Antonio Martínez Rodríguez; María Angélica Moreno Cabello (2015, 31 de marzo). «La doctrina del fruto del árbol envenenado» [en línea]. *Noticias Jurídicas*. <https://noticias.juridicas.com/ conocimiento/articulos-doctrinales/8944-la-doctrina-del-fruto-del-arbol-envenenado>

Otro elemento relevante en la prueba digital es la **carga de la prueba**. Es decir, la necesidad de las partes de probar unos hechos aplicables a un caso concreto. La carga de la prueba puede verse modificada en el caso de normas específicas que establezcan otra cosa.

Carga de prueba modificada

El Reglamento (UE) 910/2014 presupone la exactitud de la fecha y hora de los sellos de tiempo cualificados electrónicos.

La **fuerza de la prueba** es el valor probatorio que tiene. Este valor probatorio se determinará en función de la robustez del contenido inmaterial (autenticidad e integridad) y el procedimiento elegido para su aportación en juicio. En este sentido, los documentos firmados electrónicamente (dependiendo del nivel de firma) tienen consideración de prueba documental.

En el mundo digital, uno de los principales problemas para la obtención de la prueba es la volatilidad del contenido electrónico que puede constituir la prueba y su necesidad de preservación. En este sentido, puede ser de ayuda el uso de fedatarios públicos, así como el desarrollo de informes periciales informáticos.

Los **informes periciales informáticos** se llevan a cabo mediante procedimientos encaminados a preservar las evidencias electrónicas del contenido electrónico que se quiera aportar en juicio. Esta **preservación** se obtiene a partir de la obtención de copias forenses exactas del contenido digital que se quiere preservar.

4. El peritaje informático

El peritaje informático es el trabajo realizado por un experto en la materia que tiene como objetivo la **obtención de una prueba electrónica** para su aportación y valoración en juicio, o bien para determinar un hecho o para poder resolver discrepancias cuando la informática es un elemento relevante para el desarrollo del hecho. El hecho investigado podría ser constitutivo de un delito.

Para el desarrollo del peritaje informático, se requiere llevar a cabo un conjunto de actividades con el fin de que el resultado pueda llegar a ser constitutivo de la prueba:

1) Identificación del incidente o proceso que se quiere analizar.

2) Acotación del entorno que se va a investigar.

3) Recopilación de evidencias (recuperación de datos y aplicación de técnicas de investigación).

4) Preservación de las evidencias (almacenaje, etiquetado, cadena de custodia).

5) Análisis de las evidencias (reconstrucción, respuestas).

6) Documentación y resultados.

7) Ratificación en juzgado y defensa del informe.

El acceso a dispositivos electrónicos permitiría a su vez el acceso a un conjunto amplio de información almacenado en estos dispositivos, que podría determinar la comisión de otros delitos, diferentes al investigado y sin conexión, o acceder a información íntima de personas. Por ello, del mismo modo que en el proceso de investigación, se requiere delimitar el **alcance del peritaje** que se va a realizar.

En este **proceso de investigación** se utilizan herramientas software y hardware que permiten analizar los dispositivos y obtener un conjunto amplio de información relativa al incidente o proceso que se debe investigar. Normalmente, estas operaciones con herramientas se realizan sobre copias de los sistemas de almacenamiento de estos dispositivos, para asegurar que el dispositivo original no recibe ninguna manipulación durante el proceso. Asimismo, se permite que el proceso se pueda reproducir las veces que sea requerido y poder garantizar la obtención de evidencias como si del dispositivo original se tratara.

Al igual que cualquier evidencia de un proceso de investigación, se requiere la **trazabilidad y custodia** de esta, y de ahí la aplicación de técnicas que aseguren que no se han manipulado durante el proceso de custodia de dichas evidencias.

Las evidencias electrónicas presentan una serie de **ventajas** en relación con las evidencias convencionales, en el sentido de que:

- Permiten su **reproducción** las veces que sea necesario conservando el original y las copias.

- Permiten la **manipulación** de las copias de las evidencias obtenidas tantas veces como sea necesario.

- Existen en el mercado herramientas informáticas que permiten la **copia (clonado)** exacta del original sin producir alteración en el original.

- Es posible obtener **huellas digitales** de las evidencias (*hash*) que se pueden preservar para garantizar que la evidencia no ha sido manipulada.

Por el contrario, las evidencias electrónicas también presentan ciertas **dificultades** para garantizar su efectividad como prueba:

- La obtención de las evidencias requiere la utilización de métodos que no alteren el contenido del dispositivo original. Cualquier acción puede alterar el contenido de un dispositivo y presentar dudas sobre la obtención de las evidencias.

- Los dispositivos electrónicos pueden ser manipulados y continuar teniendo apariencia de integridad. La duda afecta a la fuerza de la probatoria de las evidencias.

- Las evidencias pueden estar localizadas en países en los que la legislación nacional no tiene acceso.

- Para garantizar la integridad, se puede requerir la participación de un tercero de confianza que garantice su autenticidad e integridad.

Bibliografía

Aguilar Cárceles, Marta María (2012). «Los delitos informáticos: cuantificación y análisis legislativo en el Reino Unido». *Cuadernos de Política Criminal* (núm. 110, págs. 221-260).

Agustina, José Ramón (2012). «Analyzing sexting from a criminological perspective. Beyond child pornography issues: Sexting as a threshold for victimization». En: Pauline C. Reich (ed.). *Cybercrime & Security* (págs. 64-96). Eagan, Minnesota: West.

Agustina, José Ramón (2014). «Victimología y Victimodogmática en el uso de las TIC». En: Noemí Pereda; Josep M. Tamarit (coords.). *La respuesta de la victimología ante las nuevas formas de victimización* (págs. 109-158). Madrid: Edisofer.

Almazán Salazar, Elena (2021). *La personalidad electrónica de los robots*. Zaragoza: Juristas con Futuro («Desafíos Legales»).

Álvarez Rodríguez, Ignacio (2020, marzo). «El Derecho del ciberespacio. Una aproximación». *IDP. Revista de Internet, Derecho y Política* (núm. 30).

Barrio Andrés, Moisés (2011). «Los delitos cometidos en internet. Marco comparado, internacional y derecho español tras la reforma penal de 2010». *La ley penal: revista de derecho penal, procesal y penitenciario* (núm. 86). <https://dialnet.unirioja.es/servlet/articulo?codigo=3738334>

Cámara Arroyo, Sergio (2020). «Estudios criminológicos contemporáneos (IX): La Cibercriminología y el perfil del ciberdelincuente» [en línea]. *Derecho y Cambio Social* (núm. 60, págs. 470-512). <https://dialnet.unirioja.es/servlet/articulo?codigo=7524987>

Centro Criptológico Nacional (2020, mayo). *Guía de Seguridad de las TIC. CCN-STIC 803* [en línea]. Madrid: Ministerio de Defensa. <https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/682-ccn-stic-803-valoracion-de-sistemas-en-el-ens-1/file.html>

De la Mata Barranco, Norberto Javier; Pérez Machío, Ana Isabel (2012). «La normativa internacional para la lucha contra la cibercriminalidad como referente de la regulación penal española». En: José Luis De la Cuesta Arzamendi (dir.). *Delincuencia informática: tiempos de cautela y amparo* (págs. 253-272). Cizur Menor: Aranzadi.

Devis Echandía, Hernando Devis (1993). *Teoría General de la Prueba Judicial* (tomo I). Buenos Aires: Víctor P. de Zavalía.

Díaz Gómez, Andrés (2010). «El delito informático, su problemática y la cooperación internacional como paradigma de su solución: El Convenio de Budapest». *Revista Electrónica de Derecho de la Universidad de La Rioja (REDUR)* (núm. 8, pág. 173).

European Data Protection Board (2021, 4 de mayo). *EDPB contribution to the 6th round of consultations on the draft Second Additional Protocol to the Council of Europe Budapest Convention on Cybercrime* [en línea]. <https://edpb.europa.eu/system/files/2021-05/edpb_contribution052021_6throundconsultations_budapestconvention_en.pdf>

Fanjul Fernández, María Luisa (2017). *Conceptualización, evolución y clasificación del Ciberdelito Empresarial*. Madrid: Amec Ediciones.

Fernández García, Emilio Manuel (2001). «Ciberdelincuencia patrimonial e Internet». *Estudios Jurídicos Ministerio Fiscal* (vol. III).

Ibáñez Rodríguez, Juan Rafael (2012). «Investigación básica en los delitos informáticos». En: José Ibáñez Peinado (coord.). *Técnicas de Investigación Criminal* (2.ª ed.). Madrid: Dykinson.

INCIBE (2017). *Cloud computing. Una guía de aproximación para el empresario* [en línea]. <https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia-cloud-computing_0.pdf>

«ISO/IEC 27000-series» [en línea]. *Wikipedia*. <https://es.wikipedia.org/wiki/ISO/IEC_27000-series>

Levy, Steven (1984). *Hackers: Heroes of the Computer Revolution*. Nueva York: Dell.

López Gutiérrez, Javier; Sánchez Jiménez, Francisco; Herrera Sánchez, David y otros (2020). *Estudio sobre la cibercriminalidad en España* [en línea]. Madrid: Ministerio del

Interior. <http://www.interior.gob.es/documents/10180/11389243/Estudio+sobre+la+Cibercriminalidad+en+Espa%C3%B1a+2020.pdf/ed85b525-e67d-4058-9957-ea99ca9813c3>

Martínez de Carvajal Hedrich, Ernesto (2012). *Informática Forense. 44 casos reales*. Barcelona: autopublicación.

Martínez Rodríguez, José Antonio; Moreno Cabello, María Angélica (2015, 31 de marzo). «La doctrina del fruto del árbol envenenado» [en línea]. *Noticias Jurídicas*. <https://noticias.juridicas.com/conocimiento/articulos-doctrinales/8944-la-doctrina-del-fruto-del-arbol-envenenado>

Miró Llinares, Fernando (2021, marzo). «Crimen, cibercrimen y COVID-19: desplazamiento (acelerado) de oportunidades y adaptación situacional de ciberdelitos». *IDP. Revista de Internet, Derecho y Política* (núm. 32).

Montero Juanes, Francisco Javier (2002). «Internet. Responsabilidad civil y penal. Legislación». *Informática y derecho: Revista iberoamericana de derecho informático* (núm. 34, págs. 147-168).

Morillas Fernández, David Lorenzo; Patró Hernández, Rosa María; Aguilar Cárceles, Marta María (2014). *Victimología* (2.ª ed.). Madrid: Dykinson.

Oliva León, Ricardo; Valero Barceló, Sonsoles (2016). *La prueba electrónica. Validez y eficacia procesal*. Zaragoza: Juristas con Futuro («Desafíos Legales»).

Rifkin, Jeremy (2014). *La sociedad de coste marginal cero*. Barcelona: Paidós.

Sánchez Cáceres, Luis Francisco (2019). «El sistema de Hard-Law y Soft-Law en relación con la defensa de los derechos fundamentales, la igualdad y la no discriminación» [en línea]. *Cuadernos electrónicos de filosofía del derecho* (núm. 39). <https://ojs.uv.es/index.php/CEFD/article/view/14293/pdf>

Velasco Núñez, Eloy (2010, 30 de julio). «Los delitos informáticos: la reparación y las indemnizaciones. Especial referencia al fraude» [en línea]. *elderecho.com*. <https://elderecho.com/los-delitos-informaticos-la-reparacion-y-las-indemnizaciones-especial-referencia-al-fraude-2>

Legislación

Código de Derecho de la Ciberseguridad [en línea]. *Boletín Oficial del Estado*, 25 de octubre de 2021. <https://www.boe.es/biblioteca_juridica/codigos/codigo.php?id=173_Codigo_de_Derecho_de_la_Ciberseguridad&modo=1>

Ley 9/1968, de 5 de abril, sobre secretos oficiales [en línea]. *Boletín Oficial del Estado*, 26 de abril de 1968, núm. 84. <https://www.boe.es/buscar/act.php?id=BOE-A-1968-444>

Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil [en línea]. *Boletín Oficial del Estado*, 8 de enero de 2001, núm. 7. <https://www.boe.es/buscar/act.php?id=BOE-A-2000-323>

Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico [en línea]. *Boletín Oficial del Estado*, 12 de octubre de 2002, núm. 166. <https://www.boe.es/buscar/act.php?id=BOE-A-2002-13758>

Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones [en línea]. *Boletín Oficial del Estado*, 19 de octubre de 2007, núm. 251. <https://www.boe.es/buscar/act.php?id=BOE-A-2007-18243>

Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas [en línea]. *Boletín Oficial del Estado*, 30 de abril de 2011, núm. 102. <https://www.boe.es/buscar/act.php?id=BOE-A-2011-7630>

Ley 9/2014, de 9 de mayo, General de Telecomunicaciones [en línea]. *Boletín Oficial del Estado*, 11 de mayo de 2014, núm. 114. <https://www.boe.es/buscar/act.php?id=BOE-A-2014-4950>

Ley 36/2015, de 28 de septiembre, de Seguridad Nacional [en línea]. *Boletín Oficial del Estado*, 29 de septiembre de 2015, núm. 233, págs. 87106-87117. <https://www.boe.es/buscar/doc.php?id=BOE-A-2015-10389>

Ley 1/2019, de 20 de febrero, de Secretos Empresariales [en línea]. *Boletín Oficial del Estado*, 21 de febrero de 2019, núm. 45, págs. 16713-16727. <https://www.boe.es/buscar/doc.php?id=BOE-A-2019-2364>

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales [en línea]. *Boletín Oficial del Estado*, 6 de diciembre de 2018, núm. 294, págs. 119788-119857. <https://www.boe.es/buscar/doc.php?id=BOE-A-2018-16673>

Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica [en línea]. *Boletín Oficial del Estado*, 30 de enero de 2010, núm. 25. <https://www.boe.es/buscar/act.php?id=BOE-A-2010-1330>

Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información [en línea]. *Boletín Oficial del Estado*, 28 de enero de 2021, núm. 24, págs. 8187-8214. <https://www.boe.es/diario_boe/txt.php?id=BOE-A-2021-1192>

Real Decreto de 14 de septiembre de 1882 por el que se aprueba la Ley de Enjuiciamiento Criminal [en línea]. *Boletín Oficial del Estado*, 17 de septiembre de 1882, núm. 260. <https://www.boe.es/buscar/act.php?id=BOE-A-1882-6036>

Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información [en línea]. *Boletín Oficial del Estado*, 8 de septiembre de 2018, núm. 218, págs. 87675-87696. <https://www.boe.es/diario_boe/txt.php?id=BOE-A-2018-12257>

Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior [en línea]. *Diario Oficial de la Unión Europea*, 28 de agosto de 2014. <https://www.boe.es/doue/2014/257/L00073-00114.pdf>

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos [en línea]. *Diario Oficial de la Unión Europea*, 4 de mayo de 2016. <https://www.boe.es/doue/2016/119/L00001-00088.pdf>

Reglamentos, directivas y otros actos legislativos (UE) [en línea]. <https://europa.eu/european-union/law/legal-acts_es>