

DIRECTIVA 2013/40/UE DEL PARLAMENTO EUROPEO Y DEL CONSEJO**de 12 de agosto de 2013****relativa a los ataques contra los sistemas de información y por la que se sustituye la Decisión marco 2005/222/JAI del Consejo**

EL PARLAMENTO EUROPEO Y EL CONSEJO DE LA UNIÓN EUROPEA,

Visto el Tratado de Funcionamiento de la Unión Europea (TFUE) y, en particular, su artículo 83, apartado 1,

Vista la propuesta de la Comisión Europea,

Previa transmisión del proyecto de acto legislativo a los Parlamentos nacionales,

Visto el dictamen del Comité Económico y Social Europeo ⁽¹⁾,

De conformidad con el procedimiento legislativo ordinario ⁽²⁾,

Considerando lo siguiente:

- (1) Los objetivos de la presente Directiva son aproximar las normas de Derecho penal de los Estados miembros en materia de ataques contra los sistemas de información, mediante el establecimiento de normas mínimas relativas a la definición de las infracciones penales y las sanciones aplicables, y mejorar la cooperación entre las autoridades competentes, incluida la policía y los demás servicios especializados encargados de la aplicación de la ley en los Estados miembros, así como los organismos especializados de la Unión, como Eurojust, Europol y su Centro Europeo contra la Ciberdelincuencia y la Agencia Europea de Seguridad de las Redes y de la Información (ENISA).
- (2) Los sistemas de información son un elemento esencial para la interacción política, social y económica en la Unión. La dependencia de este tipo de sistemas por parte de la sociedad es muy grande y sigue aumentando. El buen funcionamiento y la seguridad de estos sistemas en la Unión es clave para el desarrollo del mercado interior y de una economía competitiva e innovadora. Garantizar un adecuado nivel de protección de los sistemas de información debe formar parte de un marco general efectivo de medidas de prevención que acompañen a las respuestas del Derecho penal a la ciberdelincuencia.
- (3) Los ataques contra los sistemas de información y, en particular, los ataques vinculados a la delincuencia organizada, son una amenaza creciente en la Unión y en el resto del mundo, y cada vez preocupa más la posibilidad de ataques terroristas o de naturaleza política contra los sistemas de información que forman parte de las infraestructuras críticas de los Estados miembros y de la Unión. Esta situación pone en peligro la realización de una sociedad de la información segura y de un espacio de libertad, seguridad y justicia y exige, por tanto, una respuesta por parte de la Unión, así como una cooperación y coordinación reforzadas a escala internacional.

(4) Existe en la Unión una serie de infraestructuras críticas cuya perturbación o destrucción tendría repercusiones transfronterizas importantes. De la necesidad de incrementar en la Unión la capacidad de protección de estas infraestructuras se desprende que las medidas contra los ataques informáticos deben complementarse con penas estrictas que reflejen la gravedad de tales ataques. Por «infraestructura crítica» se entiende un elemento, sistema o parte de este situado en los Estados miembros que es esencial para el mantenimiento de funciones vitales de la sociedad, la salud, la seguridad, la protección y el bienestar económico y social de la población, como las centrales eléctricas, las redes de transporte y las redes de los órganos de gobierno, y cuya perturbación o destrucción tendría un impacto significativo en un Estado miembro al no poder mantener esas funciones.

(5) Se comprueba una tendencia hacia ataques de gran escala cada vez más graves y recurrentes contra sistemas de información, que a menudo pueden ser críticos para los Estados miembros o para determinadas funciones del sector público o privado. Esta tendencia coincide con el desarrollo de métodos cada vez más sofisticados, como la creación y utilización de redes infectadas (*botnets*), que conllevan fases múltiples del acto delictivo, cada una de las cuales puede por sí sola constituir un grave peligro para el interés público. La presente Directiva tiene por objeto, entre otros, establecer sanciones para la fase en que se crea la red infectada, es decir, cuando se establece un control remoto sobre un número significativo de ordenadores infectándolos mediante programas nocivos a través de ataques informáticos dirigidos. Una vez establecida la red, los ordenadores infectados, que constituyen la red infectada, pueden activarse sin el conocimiento de los usuarios para realizar un ataque informático a gran escala, que en circunstancias normales puede causar daños graves, como menciona la presente Directiva. Los Estados miembros deben poder establecer qué constituyen daños graves de conformidad con su ordenamiento jurídico y práctica nacionales, tales como interrumpir los servicios del sistema de una importancia pública relevante, o causar importantes costes económicos o pérdidas de datos de carácter personal o de información sensible.

(6) Los ciberataques a gran escala pueden causar graves perjuicios económicos, tanto por la paralización de los sistemas de información y de las comunicaciones como por la pérdida o alteración de información confidencial de importancia comercial o de otros datos. Debe prestarse especial atención a sensibilizar más a las pequeñas y medianas empresas innovadoras sobre las amenazas vinculadas con tales ataques y su vulnerabilidad ante los mismos, que les afectan debido a su mayor dependencia del correcto funcionamiento y de la disponibilidad de los sistemas de información y al hecho de que sus recursos para la seguridad de la información son, con frecuencia, limitados.

⁽¹⁾ DO C 218 de 23.7.2011, p. 130.

⁽²⁾ Posición del Parlamento Europeo de 4 de julio de 2013 (no publicada aún en el Diario Oficial) y Decisión del Consejo de 22 de julio de 2013.

- (7) Es importante en esta materia disponer de definiciones comunes a fin de garantizar la aplicación coherente de la presente Directiva en los Estados miembros.
- (8) Es necesario llegar a un enfoque común respecto de los elementos constitutivos de las infracciones penales introduciendo las infracciones comunes de acceso ilegal a un sistema de información, de intromisión ilegal en el sistema, de intromisión ilegal en los datos y de interceptación ilegal.
- (9) La interceptación abarca, sin limitarse necesariamente a ello, la escucha, el seguimiento y el análisis del contenido de comunicaciones, así como la obtención del contenido de los datos bien directamente, mediante el acceso y recurso a ese sistema de información, o indirectamente, mediante el recurso a sistemas de escucha y grabación electrónicos por medios técnicos.
- (10) Los Estados miembros deben establecer sanciones para los ataques contra los sistemas de información. Estas sanciones deben ser efectivas, proporcionadas y disuasorias y deben contemplar penas privativas de libertad o multas.
- (11) La presente Directiva establece penas al menos para los casos que no son de menor gravedad. Los Estados miembros deben poder determinar cuáles son los casos de menor gravedad de conformidad con su ordenamiento jurídico y práctica nacionales. Un caso puede considerarse de menor gravedad, por ejemplo, cuando el daño causado por la infracción o el riesgo que acarree para intereses públicos o privados, como la integridad de un sistema o datos informáticos, la integridad, derechos u otros intereses de una persona, resulte insignificante o sea de una índole tal que no resulte necesario imponer una pena dentro del umbral jurídico ni exigir responsabilidad penal.
- (12) La identificación y comunicación de las amenazas y los riesgos que plantean los ciberataques, así como las vulnerabilidades de los sistemas de información que les afectan, constituye un elemento pertinente para una prevención y respuesta eficaces frente a dichos ataques y para la mejora de la seguridad de los sistemas de información. Ofrecer incentivos a la comunicación de las insuficiencias en materia de seguridad podría contribuir a producir ese efecto. Los Estados miembros deben comprometerse a brindar oportunidades que permitan la detección y comunicación legales de las deficiencias en materia de seguridad.
- (13) Es conveniente establecer sanciones más severas cuando un ataque contra un sistema de información se comete en el contexto de una organización delictiva, tal como se define en la Decisión marco 2008/841/JAI del Consejo, de 24 de octubre de 2008, relativa a la lucha contra la delincuencia organizada⁽¹⁾, o cuando el ciberataque se realiza a gran escala y afecta a un número importante de sistemas de información, en particular cuando el ataque tiene por objeto crear una red infectada o si el ciberataque causa un daño grave, incluido cuando se lleva a cabo a través de una red infectada. Conviene también establecer sanciones más severas cuando el ataque se lleva a cabo contra una infraestructura crítica de los Estados miembros o de la Unión.
- (14) Otro elemento importante de un enfoque integrado contra la ciberdelincuencia es el establecimiento de medidas eficaces contra la usurpación de identidad y otras infracciones relacionadas con la identidad. Las necesidades inherentes a la actuación de la Unión relativa a este tipo de conducta delictiva podrían también ser tomadas en consideración en el contexto de la evaluación de la necesidad de un instrumento horizontal global de la Unión.
- (15) Las Conclusiones del Consejo de 27 y 28 de noviembre de 2008 indicaron que debía desarrollarse una nueva estrategia con los Estados miembros y la Comisión, teniendo en cuenta el contenido del Convenio del Consejo de Europa de 2001 sobre la ciberdelincuencia. Este Convenio es el marco jurídico de referencia para la lucha contra la ciberdelincuencia, incluidos los ataques contra los sistemas de información. La presente Directiva se basa en dicho Convenio. Debe considerarse como prioritario terminar cuanto antes el proceso de ratificación de dicho Convenio por todos los Estados miembros.
- (16) Dadas las diferentes formas en que pueden realizarse los ataques y la rápida evolución de los programas y equipos informáticos, la presente Directiva se refiere a los «instrumentos» que pueden utilizarse para cometer las infracciones enumeradas en la presente Directiva. Dichos instrumentos pueden ser programas informáticos maliciosos, incluidos los que permiten crear redes infectadas, que se utilizan para cometer ciberataques. Aun cuando uno de estos instrumentos sea adecuado o incluso especialmente adecuado para llevar a cabo las infracciones enumeradas en la presente Directiva, es posible que dicho instrumento fuera creado con fines legítimos. Teniendo en cuenta la necesidad de evitar la tipificación penal cuando estos instrumentos sean creados y comercializados con fines legítimos, como probar la fiabilidad de los productos de la tecnología de la información o la seguridad de los sistemas de información, además del requisito de intención general también debe cumplirse el requisito de que dichos instrumentos sean utilizados para cometer una o varias de las infracciones enumeradas en la presente Directiva.
- (17) La presente Directiva no establece responsabilidades penales cuando se cumplen los criterios objetivos de las infracciones enumeradas en la misma pero los actos se cometen sin propósito delictivo, por ejemplo cuando la persona de que se trate no sabía que el acceso no estaba autorizado o en caso de intervención autorizada o de protección de los sistemas de información, o cuando una empresa o un vendedor designen a una persona para probar la solidez de su sistema de seguridad. En el contexto de la presente Directiva, las obligaciones o los acuerdos contractuales tendentes a restringir el acceso a los sistemas de información en virtud de una política de usuarios o de las condiciones de prestación del servicio, así como los conflictos colectivos de trabajo en relación con el acceso a los sistemas de información de un empresario o con la utilización de los mismos con fines privados, no deben acarrear responsabilidad penal cuando se estime que el acceso en dichas circunstancias no está autorizado y, por tanto, constituye la única base para incoar una acción penal. La presente Directiva se entiende sin perjuicio del derecho de acceder a la información, establecido en el Derecho nacional y de la Unión, pero al mismo tiempo no sirve de justificación para un acceso ilícito o arbitrario a la información.

(¹) DO L 300 de 11.11.2008, p. 42.

- (18) Los ciberataques podrían verse facilitados por varias circunstancias, por ejemplo cuando el autor de los mismos tengan acceso, en el marco de su empleo, a los sistemas de seguridad inherentes a los sistemas de información afectados. En el contexto del Derecho nacional, estas circunstancias deben tenerse en cuenta, en su caso, en el transcurso del proceso penal.
- (19) Los Estados miembros deben prever en su derecho nacional las circunstancias agravantes, de conformidad con las normas aplicables establecidas por sus ordenamientos jurídicos en relación con dichas circunstancias. Deben velar por que esas circunstancias agravantes puedan ser conocidas por los jueces para que estos las tomen en consideración a la hora de dictar sentencia con respecto a los infractores. Se deja a la apreciación del juez evaluar dichas circunstancias junto con otros hechos del caso de que se trate.
- (20) La presente Directiva no se aplica a las condiciones para ejercer la competencia jurisdiccional sobre alguna de las infracciones contempladas en la misma, como una declaración de la víctima en el lugar donde se cometió la infracción, o la denuncia del Estado en el que se cometió, o el no procesamiento del delincuente en el lugar donde se cometió la infracción.
- (21) En el contexto de la presente Directiva, los Estados y sus organismos públicos están plenamente obligados a garantizar el respeto de los derechos y las libertades fundamentales, de conformidad con las obligaciones de la Unión e internacionales existentes.
- (22) La presente Directiva subraya la importancia de redes, tales como la red de puntos de contacto del G8 o la del Consejo de Europa, disponibles veinticuatro horas al día, siete días a la semana. Dichos puntos de contacto han de poder prestar asistencia efectiva, facilitando así, por ejemplo, el intercambio de la información relevante disponible o prestando asesoramiento técnico o información jurídica en el marco de investigaciones o procedimientos relativos a infracciones penales relacionadas con sistemas de información y de datos asociados que impliquen al Estado miembro solicitante. Para garantizar el buen funcionamiento de las redes, cada punto de contacto debe ser capaz de comunicarse de forma rápida con el punto de contacto de otro Estado miembro con el apoyo, entre otras cosas, de personal formado y equipado. Dada la velocidad a la que pueden realizarse los ciberataques a gran escala, todos los Estados miembros deben responder con prontitud a las solicitudes urgentes procedentes de dicha red de puntos de contacto. En tales casos, puede resultar conveniente que la solicitud de información vaya acompañada de contacto telefónico, a fin de garantizar que el Estado miembro que recibe la solicitud pueda tramitarla rápidamente y que se facilite una respuesta al respecto en el plazo de ocho horas.
- (23) La cooperación entre las autoridades públicas por un lado y el sector privado y la sociedad civil por otro es de gran importancia para evitar y combatir los ataques contra los sistemas de información. Es necesario fomentar y mejorar la cooperación entre los proveedores de servicios, los productores, los servicios encargados de la aplicación de la ley y las autoridades judiciales, dentro del pleno respeto del Estado de Derecho. Dicha cooperación podría incluir el apoyo prestado por los proveedores de servicios al contribuir a mantener posibles pruebas, a proporcionar elementos que ayuden a identificar a los infractores y, en última instancia, a cerrar, total o parcialmente, de conformidad con el Derecho y las prácticas nacionales, los sistemas de información o la supresión de las funciones que hayan creado una situación de peligro o se hayan utilizado con fines ilegales. Asimismo, los Estados miembros deben tomar en consideración el establecimiento de redes de cooperación y asociación con los proveedores de servicios y los productores para intercambiar información relativa a las infracciones en el marco de aplicación de la presente Directiva.
- (24) Es necesario recopilar datos comparables sobre las infracciones a las que se refiere la presente Directiva. Los datos relevantes deben ponerse a disposición de los organismos especializados competentes de la Unión, como Europol y la ENISA, teniendo en cuenta sus cometidos y necesidades en materia de información, a fin de obtener una visión más completa del problema de la ciberdelincuencia y de la seguridad de la red y de la información a escala de la Unión, y contribuir así a la formulación de unas respuestas más eficaces. Los Estados miembros deben facilitar a Europol y a su Centro Europeo de Ciberdelincuencia información relativa al modo de actuación de los infractores a fin de llevar a cabo evaluaciones de las amenazas y análisis estratégicos de la ciberdelincuencia, de conformidad con la Decisión 2009/371/JAI del Consejo, de 6 de abril de 2009, por la que se crea la Oficina Europea de Policía (Europol) ⁽¹⁾. Facilitar información puede ayudar a comprender mejor las amenazas presentes y futuras, y contribuir así a tomar decisiones de forma más adecuada y específica para combatir y prevenir los ataques contra los sistemas de información.
- (25) La Comisión debe presentar un informe sobre la aplicación de la presente Directiva y formular las propuestas legislativas necesarias que puedan llevar a ampliar su ámbito de aplicación, teniendo en cuenta la evolución que se produzca en el campo de la ciberdelincuencia. En dicha evolución podrían figurar las innovaciones tecnológicas que permitan, por ejemplo, una represión más eficaz en el ámbito de los ataques contra los sistemas de información, o que faciliten la prevención o reduzcan al máximo la incidencia de dichos ataques. A tal fin, la Comisión debe tener en cuenta los análisis y los informes disponibles realizados por las instancias pertinentes y, en particular, por Europol y ENISA.
- (26) Para combatir eficazmente la ciberdelincuencia, debe aumentarse la capacidad de adaptación de los sistemas de información mediante la adopción de las medidas adecuadas para protegerlos de manera más eficaz contra los ataques que les afecten. Los Estados miembros tomarán las medidas necesarias para proteger los sistemas de información que constituyen las infraestructuras críticas de los ciberataques, entre las cuales deben tomar en consideración las medidas tendentes a proteger sus sistemas de información y los datos asociados. Garantizar un nivel adecuado de protección y seguridad de los sistemas de información por personas jurídicas, por ejemplo en conexión con la facilitación de servicios de comunicación disponibles de forma electrónica de conformidad con la legislación de la Unión sobre la privacidad, la comunicación electrónica y la protección de datos, constituye una

⁽¹⁾ DO L 121 de 15.5.2009, p. 37.

parte esencial de un planteamiento global para contrarrestar eficazmente la ciberdelincuencia. Deben preverse unos niveles adecuados de protección contra las amenazas y vulnerabilidades que puedan identificarse de forma razonable, teniendo en cuenta los conocimientos más recientes sobre sectores específicos y las situaciones concretas de tratamiento de datos. El coste y la carga que representa dicha protección deben ser proporcionados a los daños probables que podría causar un ciberataque a las personas afectadas. Se alienta a los Estados miembros a que establezcan las medidas pertinentes que acarreen responsabilidades en el contexto de su Derecho nacional en aquellos casos en que una persona jurídica no haya previsto claramente un nivel apropiado de protección frente a ciberataques.

- (27) Las diferencias y divergencias significativas que existen entre las legislaciones y los procesos penales de los Estados miembros en este ámbito pueden dificultar la lucha contra la delincuencia organizada y el terrorismo y complicar la cooperación policial y judicial efectiva en este ámbito. La naturaleza transnacional y transfronteriza de los modernos sistemas de información significa que los ataques suelen revestir un carácter transfronterizo, lo que plantea la necesidad urgente de proseguir la aproximación del Derecho penal en este ámbito. Por otra parte, la coordinación del enjuiciamiento de los casos de ataques contra los sistemas de información debe facilitarse mediante la adecuada puesta en marcha y aplicación de la Decisión marco 2009/948/JAI del Consejo, de 30 de noviembre de 2009, sobre la prevención y resolución de conflictos de ejercicio de jurisdicción en los procesos penales ⁽¹⁾. Los Estados miembros, en cooperación con la Unión, deben intentar también mejorar la cooperación internacional en lo relativo a la seguridad de los sistemas de información, de las redes de ordenadores y de los datos que estos albergan. En los acuerdos internacionales relativos al intercambio de datos debe tomarse debidamente en consideración la seguridad de la transferencia de datos y del almacenamiento de los mismos.
- (28) Una mayor cooperación entre los servicios encargados de la aplicación de la ley y las autoridades judiciales competentes en la Unión es fundamental para combatir eficazmente la ciberdelincuencia. En este sentido, deben intensificarse los esfuerzos por ofrecer una adecuada formación a las autoridades competentes con vistas a mejorar la comprensión de la ciberdelincuencia y de sus repercusiones, y por promover la cooperación y el intercambio de las mejores prácticas a través, por ejemplo, de los organismos especializados competentes de la Unión. La formación debe estar dirigida, entre otras cosas, a sensibilizar más sobre los diferentes ordenamientos jurídicos nacionales, los posibles retos de tipo jurídico y técnico de las investigaciones penales y el reparto de competencias entre las autoridades nacionales competentes.
- (29) La presente Directiva respeta los derechos humanos y las libertades fundamentales y cumple los principios reconocidos, en particular, por la Carta de los Derechos Fundamentales de la Unión Europea y el Convenio Europeo

para la Protección de los Derechos Humanos y de las Libertades Fundamentales, incluida la protección de datos de carácter personal, el derecho a la privacidad, la libertad de expresión e información, el derecho a un juicio equitativo, la presunción de inocencia y los derechos de la defensa, así como los principios de legalidad y proporcionalidad de las infracciones penales y las sanciones. En especial, la presente Directiva tiene por objeto garantizar el pleno respeto de dichos derechos y principios y debe aplicarse en consecuencia.

- (30) La protección de los datos de carácter personal es un derecho fundamental conforme al artículo 16, apartado 1, del TFUE y al artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea. Por ello, todo tratamiento de datos de carácter personal efectuado en el contexto de la aplicación de la presente Directiva debe cumplir plenamente el Derecho de la Unión aplicable en materia de protección de datos.
- (31) De conformidad con el artículo 3 del Protocolo sobre la posición del Reino Unido y de Irlanda respecto del espacio de libertad, seguridad y justicia, anejo al Tratado de la Unión Europea y al Tratado de Funcionamiento de la Unión Europea, dichos Estados miembros han notificado su deseo de participar en la adopción y aplicación de la presente Directiva.
- (32) De conformidad con los artículos 1 y 2 del Protocolo sobre la posición de Dinamarca, anejo al Tratado de la Unión Europea y al Tratado de Funcionamiento de la Unión Europea, Dinamarca no participa en la adopción de la presente Directiva y no queda vinculada por ello ni sujeta a su aplicación.
- (33) Dado que los objetivos de la presente Directiva, a saber, garantizar que los ataques contra los sistemas de información sean castigados en todos los Estados miembros con penas efectivas, proporcionadas y disuasorias, y mejorar y fomentar la cooperación judicial entre las autoridades judiciales y otras autoridades competentes, no pueden ser alcanzados de manera suficiente por los Estados miembros, y que, por consiguiente, debido a sus dimensiones o efectos, pueden lograrse mejor a escala de la Unión, esta puede adoptar medidas, de acuerdo con el principio de subsidiariedad consagrado en el artículo 5 del Tratado de la Unión Europea. De conformidad con el principio de proporcionalidad enunciado en dicho artículo, la presente Directiva no excede de lo necesario para alcanzar dichos objetivos.
- (34) La presente Directiva tiene la finalidad de modificar y ampliar las disposiciones de la Decisión marco 2005/222/JAI del Consejo, de 24 de febrero de 2005, relativa a los ataques contra los sistemas de información ⁽²⁾. Dado que las modificaciones necesarias son importantes, tanto por número como por su naturaleza, la Decisión marco 2005/222/JAI debe, en aras de la claridad, ser sustituida en su totalidad en relación con los Estados miembros que participan en la adopción de la presente Directiva.

⁽¹⁾ DO L 328 de 15.12.2009, p. 42.

⁽²⁾ DO L 69 de 16.3.2005, p. 67.

HAN ADOPTADO LA PRESENTE DIRECTIVA:

Artículo 1

Objeto

La presente Directiva establece normas mínimas relativas a la definición de las infracciones penales y a las sanciones aplicables en el ámbito de los ataques contra los sistemas de información. También tiene por objeto facilitar la prevención de dichas infracciones y la mejora de la cooperación entre las autoridades judiciales y otras autoridades competentes.

Artículo 2

Definiciones

A efectos de la presente Directiva, se aplicarán las definiciones siguientes:

- a) «sistema de información»: todo aparato o grupo de aparatos interconectados o relacionados entre sí, uno o varios de los cuales realizan, mediante un programa, el tratamiento automático de datos informáticos, así como los datos informáticos almacenados, tratados, recuperados o transmitidos por dicho aparato o grupo de aparatos para su funcionamiento, utilización, protección y mantenimiento;
- b) «datos informáticos»: toda representación de hechos, informaciones o conceptos de una forma que permite su tratamiento por un sistema de información, incluidos los programas que sirven para hacer que dicho sistema de información realice una función;
- c) «persona jurídica»: toda entidad a la cual el derecho vigente reconoce este estatuto, salvo los Estados y otros organismos públicos que ejercen prerrogativas públicas y las organizaciones internacionales de carácter público;
- d) «sin autorización»: un comportamiento al que se refiere la presente Directiva, incluido el acceso, la interferencia o la interceptación, que no haya sido autorizado por el propietario u otro titular del derecho sobre el sistema o parte del mismo o no permitido por el Derecho nacional.

Artículo 3

Acceso ilegal a los sistemas de información

Los Estados miembros adoptarán las medidas necesarias para que, cuando haya sido realizado intencionalmente, el acceso sin autorización al conjunto o a una parte de un sistema de información sea sancionable como infracción penal cuando se haya cometido con violación de una medida de seguridad, al menos en los casos que no sean de menor gravedad.

Artículo 4

Interferencia ilegal en los sistemas de información

Los Estados miembros adoptarán las medidas necesarias para que la obstaculización o la interrupción significativas del funcionamiento de un sistema de información, introduciendo, transmitiendo, dañando, borrando, deteriorando, alterando, suprimiendo o haciendo inaccesibles datos informáticos, intencionalmente y sin autorización, sea sancionable como infracción penal, al menos en los casos que no sean de menor gravedad.

Artículo 5

Interferencia ilegal en los datos

Los Estados miembros adoptarán las medidas necesarias para que borrar, dañar, deteriorar, alterar, suprimir o hacer inaccesi-

bles datos informáticos contenidos en un sistema de información, intencionalmente y sin autorización, sea sancionable como infracción penal, al menos en los casos que no sean de menor gravedad.

Artículo 6

Interceptación ilegal

Los Estados miembros adoptarán las medidas necesarias para garantizar que la interceptación, por medios técnicos, de transmisiones no públicas de datos informáticos hacia, desde o dentro de un sistema de información, incluidas las emisiones electromagnéticas de un sistema de información que contenga dichos datos informáticos, intencionalmente y sin autorización, sea sancionable como infracción penal, al menos en los casos que no sean de menor gravedad.

Artículo 7

Instrumentos utilizados para cometer las infracciones

Los Estados miembros adoptarán las medidas necesarias para garantizar que la producción intencional, venta, adquisición para el uso, importación, distribución u otra forma de puesta a disposición de los siguientes instrumentos, sin autorización y con la intención de que sean utilizados con el fin de cometer cualquiera de las infracciones mencionadas en los artículos 3 a 6, sea sancionable como infracción penal, al menos en los casos que no sean de menor gravedad:

- a) un programa informático, concebido o adaptado principalmente para cometer una infracción de las mencionadas en los artículos 3 a 6;
- b) una contraseña de ordenador, un código de acceso o datos similares que permitan acceder a la totalidad o a una parte de un sistema de información.

Artículo 8

Inducción, complicidad y tentativa

1. Los Estados miembros garantizarán que la inducción y la complicidad en la comisión de las infracciones mencionadas en los artículos 3 a 7 sean sancionables como infracciones penales.
2. Los Estados miembros garantizarán que la tentativa de cometer las infracciones mencionadas en los artículos 4 y 5 sea sancionable como infracción penal.

Artículo 9

Sanciones

1. Los Estados miembros adoptarán las medidas necesarias para garantizar que las infracciones mencionadas en los artículos 3 a 8 se castiguen con penas efectivas, proporcionadas y disuasorias.
2. Los Estados miembros adoptará las medidas necesarias para garantizar que las infracciones mencionadas en los artículos 3 a 7 se castiguen con una sanción máxima de privación de libertad igual o superior a dos años, al menos en los casos que no sean de menor gravedad.
3. Los Estados miembros adoptarán las medidas necesarias para garantizar que, cuando se hayan cometido intencionalmente, siempre que hayan afectado a un número significativo de sistemas de información o cuando para cometerlas se haya

utilizado uno de los instrumentos a que se refiere el artículo 7, las infracciones mencionadas en los artículos 4 y 5, se castiguen con una sanción máxima de privación de libertad de al menos tres años.

4. Los Estados miembros adoptarán las medidas necesarias para garantizar que las infracciones mencionadas en los artículos 4 y 5 se castiguen con una sanción máxima de privación de libertad de al menos cinco años cuando:

- a) se cometan en el contexto de una organización delictiva con arreglo a la Decisión marco 2008/841/JAI, con independencia del nivel de la sanción que se establezca en la misma;
- b) causen daños graves, o
- c) se cometan contra el sistema de información de una infraestructura crítica.

5. Los Estados miembros tomarán las medidas necesarias para garantizar que, cuando las infracciones a que se refieren los artículos 4 y 5 sean cometidas utilizando ilícitamente datos de carácter personal de otra persona con la finalidad de ganar la confianza de un tercero, causando así daños al propietario legítimo de la identidad, ello pueda ser considerado, de conformidad con el Derecho nacional, como circunstancia agravante, a menos que tal circunstancia ya esté contemplada en otra infracción que sea sancionable con arreglo al Derecho nacional.

Artículo 10

Responsabilidad de las personas jurídicas

1. Los Estados miembros adoptarán las medidas necesarias para garantizar que las personas jurídicas puedan ser consideradas responsables de las infracciones mencionadas en los artículos 3 a 8 cuando estas infracciones sean cometidas en su beneficio por cualquier persona que, actuando a título particular o como parte de un órgano de la persona jurídica, ostente un cargo directivo en el seno de dicha persona jurídica, basado en:

- a) el poder de representación de dicha persona jurídica, o
- b) la capacidad para tomar decisiones en nombre de dicha persona jurídica, o
- c) la capacidad para ejercer un control en el seno de dicha persona jurídica.

2. Los Estados miembros adoptarán las medidas necesarias para garantizar que las personas jurídicas puedan ser consideradas responsables cuando la falta de supervisión o control por parte de alguna de las personas a que se refiere el apartado 1 haya permitido que una persona sometida a su autoridad cometa una de las infracciones mencionadas en los artículos 3 a 8 en beneficio de esa persona jurídica.

3. La responsabilidad de las personas jurídicas en virtud de los apartados 1 y 2 no excluirá la incoación de acciones penales contra las personas físicas que sean autoras, inductoras o cómplices de las infracciones mencionadas en los artículos 3 a 8.

Artículo 11

Sanciones contra las personas jurídicas

1. Los Estados miembros adoptarán las medidas necesarias para garantizar que a la persona jurídica considerada responsable en virtud de lo dispuesto en el artículo 10, apartado 1, le sean impuestas sanciones efectivas, proporcionadas y disuasorias, que incluirán multas de carácter penal o de otro tipo, y entre las que podrán incluir otras sanciones como:

- a) exclusión del disfrute de ventajas o ayudas públicas;
- b) inhabilitación temporal o permanente para el ejercicio de actividades comerciales;
- c) vigilancia judicial;
- d) medida judicial de liquidación;
- e) cierre temporal o definitivo de los establecimientos utilizados para cometer la infracción.

2. Los Estados miembros adoptarán las medidas necesarias para garantizar que a la persona jurídica considerada responsable en virtud de lo dispuesto en el artículo 10, apartado 2, le sean impuestas sanciones o medidas efectivas, proporcionadas y disuasorias.

Artículo 12

Competencia

1. Los Estados miembros establecerán su competencia respecto de las infracciones mencionadas en los artículos 3 a 8, cuando la infracción se haya cometido:

- a) total o parcialmente en su territorio, o
- b) por uno de sus nacionales, al menos cuando el acto constituya una infracción penal en el lugar en el que fue cometido.

2. Al establecer su competencia de acuerdo con el apartado 1, letra a), cada Estado miembro garantizará que se incluyan en la misma los casos en que:

- a) el autor cometa la infracción estando físicamente presente en su territorio, independientemente de que la infracción se cometa o no contra un sistema de información situado en su territorio, o
- b) la infracción se cometa contra un sistema de información situado en su territorio, independientemente de que el autor cometa o no la infracción estando físicamente presente en su territorio.

3. Los Estados miembros informarán a la Comisión cuando decidan establecer competencias en relación con infracciones contempladas en los artículos 3 a 8 y cometidas fuera de su territorio, incluyendo cuando:

- a) el autor tenga su residencia habitual en su territorio, o
- b) la infracción se cometa en beneficio de una persona jurídica establecida en su territorio.

Artículo 13

Intercambio de información

1. A efectos del intercambio de información sobre las infracciones mencionadas en los artículos 3 a 8, los Estados miembros garantizarán que tienen un punto de contacto nacional operativo y harán uso de la red existente de puntos de contacto operativos disponibles veinticuatro horas al día, siete días a la semana. Los Estados miembros también se asegurarán de que cuentan con procedimientos para que, en caso de solicitud de ayuda urgente, la autoridad competente pueda indicar en un plazo máximo de ocho horas a partir de la recepción de la solicitud de ayuda si la misma será atendida, y la forma y el plazo aproximado en que lo será.

2. Los Estados miembros comunicarán a la Comisión su punto de contacto a que hace referencia el apartado 1. La Comisión transmitirá esta información a los demás Estados miembros y a los órganos y organismos especializados competentes de la Unión.

3. Los Estados miembros adoptarán las medidas necesarias para garantizar la disponibilidad de canales de información adecuados a fin de facilitar sin demora indebida a las autoridades nacionales competentes información relativa a las infracciones a que se refieren los artículos 3 a 6.

Artículo 14

Seguimiento y estadísticas

1. Los Estados miembros garantizarán el establecimiento de un sistema para la recogida, elaboración y suministro de datos estadísticos sobre las infracciones mencionadas en los artículos 3 a 7.

2. Los datos estadísticos mencionados en el apartado 1 se referirán, como mínimo, a los datos existentes sobre el número de infracciones mencionadas en los artículos 3 a 7 que han sido registrados por los Estados miembros y al número de personas procesadas y condenadas por las infracciones mencionadas en los artículos 3 a 7.

3. Los Estados miembros transmitirán a la Comisión los datos recogidos con arreglo al presente artículo. La Comisión garantizará la publicación de una revisión consolidada de sus informes estadísticos y su presentación a los órganos y organismos especializados competentes de la Unión.

Artículo 15

Sustitución de la Decisión marco 2005/222/JAI

Queda sustituida, en relación con los Estados miembros que participan en la adopción de la presente Directiva, la Decisión marco 2005/222/JAI, sin perjuicio de las obligaciones de los Estados miembros en lo que se refiere a los plazos de transposición de dicha Decisión marco al Derecho nacional.

En relación con los Estados miembros que participan en la adopción de la presente Directiva, las referencias a la Decisión marco 2005/222/JAI se entenderán hechas a la presente Directiva.

Artículo 16

Transposición

1. Los Estados miembros pondrán en vigor las disposiciones legales, reglamentarias y administrativas necesarias para dar

cumplimiento a lo establecido en la presente Directiva a más tardar el 4 de septiembre de 2015.

2. Los Estados miembros transmitirán a la Comisión el texto de las medidas por las que incorporen a su ordenamiento jurídico nacional las obligaciones que les impone la presente Directiva.

3. Cuando los Estados miembros adopten dichas medidas, estas harán referencia a la presente Directiva o irán acompañadas de dicha referencia en su publicación oficial. La forma en la que se haga dicha referencia la determinarán los Estados miembros.

Artículo 17

Informes

A más tardar el 4 de septiembre de 2017, la Comisión presentará al Parlamento Europeo y al Consejo un informe en el que evaluará en qué medida los Estados miembros han adoptado las medidas necesarias para dar cumplimiento a la presente Directiva, junto con las propuestas legislativas que resulten procedentes. La Comisión deberá también tener en cuenta el progreso técnico y jurídico en el ámbito de la ciberdelincuencia, especialmente en lo que se refiere al ámbito de aplicación de la presente Directiva.

Artículo 18

Entrada en vigor

La presente Directiva entrará en vigor a los veinte días de su publicación en el *Diario Oficial de la Unión Europea*.

Artículo 19

Destinatarios

Los destinatarios de la presente Directiva son los Estados miembros de conformidad con los Tratados.

Hecho en Bruselas, el 12 de agosto de 2013.

Por el Parlamento Europeo

El Presidente

M. SCHULZ

Por el Consejo

El Presidente

L. LINKEVIČIUS