Consejo de la Unión Europea

Bruselas, 14 de septiembre de 2017
(OR. en)

12209/17

DROIPEN 121
TELECOM 210
JAI 788
CYBER 130

NOTA DE TRANSMISIÓN

De:	secretario general de la Comisión Europea, firmado por D. Jordi AYET PUIGARNAU, director
Fecha de recepción:	13 de septiembre de 2017
A:	D. Jeppe TRANHOLM-MIKKELSEN, secretario general del Consejo de la Unión Europea
N.° doc. Ción.:	COM(2017) 474 final
Asunto:	INFORME DE LA COMISIÓN AL PARLAMENTO EUROPEO Y AL CONSEJO en el que se evalúa la medida en la que los Estados miembros han tomado las medidas necesarias para cumplir la Directiva 2013/40/UE relativa a los ataques contra los sistemas de información y por la que se sustituye la Decisión marco 2005/222/JAI del Consejo

Adjunto se remite a las Delegaciones el documento – COM(2017) 474 final.

Adj.: COM(2017) 474 final

COMISIÓN
EUROPEA

Bruselas, 13.9.2017
COM(2017) 474 final

INFORME DE LA COMISIÓN AL PARLAMENTO EUROPEO Y AL CONSEJO

en el que se evalúa la medida en la que los Estados miembros han tomado las medidas necesarias para cumplir la Directiva 2013/40/UE relativa a los ataques contra los sistemas de información y por la que se sustituye la Decisión marco 2005/222/JAI del Consejo

Índice

1. Introducción

Según la Evaluación de la amenaza de la delincuencia organizada en Internet (IOCTA) realizada por Europol en 2016, la ciberdelincuencia es un fenómeno cada vez más agresivo y conflictivo. Este hecho puede observarse en diversas formas de ciberdelincuencia entre las que se incluyen los ataques contra los sistemas de información[1]. Algunos de los ataques graves a los que hace referencia Europol son el empleo de programas informáticos malintencionados e ingeniería social para infiltrarse en un sistema de información, lograr el control del mismo o interceptar comunicaciones, así como los ataques informáticos a gran escala, por ejemplo, contra infraestructuras críticas. Estos ataques constituyen una amenaza importante para nuestra sociedad.

Habida cuenta de que cada vez hay más datos almacenados en nubes y que la información y los delincuentes gozan hoy de una gran movilidad, la cooperación transfronteriza entre las autoridades policiales se ha convertido en un elemento fundamental para la mayoría de las investigaciones de casos de ciberdelincuencia.

Para luchar contra estos delitos de una manera eficaz, los Estados miembros deben definir conjuntamente qué actos deben considerarse ataques contra los sistemas de información. Asimismo, deben fijar niveles de sanciones aproximados y disponer de los canales operativos para denunciar los delitos e intercambiar información entre las autoridades. Por consiguiente, el 12 de agosto de 2013, el Parlamento Europeo y el Consejo adoptaron la Directiva 2013/40/UE relativa a los ataques contra los sistemas de información y por la que se sustituye la Decisión marco 2005/222/JAI del Consejo (en lo sucesivo, «la Directiva»)[2].

1.1. Objetivos y alcance de la Directiva

Los objetivos de la Directiva son la aproximación del Derecho penal de los Estados miembros[3] en el ámbito de los ataques contra los sistemas de información y la mejora de la cooperación entre las autoridades competentes. Para ello, se fijan normas mínimas relativas a la definición de las infracciones penales y las sanciones correspondientes en el ámbito de los ataques contra los sistemas de información y se establece la obligatoriedad de que existan puntos de contacto operativos veinticuatro horas al día, siete días a la semana.

En cuanto a los términos aplicables, la Directiva recoge las siguientes **definiciones**:

- «Sistema de información», en el artículo 2, letra a)[4]. Esta definición es similar a la definición de «sistema informático» prevista en el artículo 1, letra a), del Convenio

[1] Europol, Evaluación de la amenaza de la delincuencia organizada en Internet (IOCTA) de 2016, disponible en: https://www.europol.europa.eu/sites/default/files/documents/europol_iocta_web_2016.pdf.

[2] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:218:0008:0014:es:PDF.

[3] En lo sucesivo, y a menos que se indique explícitamente lo contrario, las expresiones «los Estados miembros» o «todos los Estados miembros» se referirán a todos los Estados miembros sujetos a la Directiva, es decir, todos los Estados miembros de la UE excepto Dinamarca, que no participó en la adopción de la Directiva [de conformidad con lo previsto en los artículos 1 y 2 del Protocolo sobre la posición de Dinamarca que figura como anexo al Tratado de la Unión Europea y al Tratado de Funcionamiento de la Unión Europea (TFUE)]. De conformidad con el artículo 3 del Protocolo n.º 21 sobre la posición del Reino Unido y de Irlanda, ambos países participaron en la adopción de la Directiva y están sujetos a ella.

[4] A menos que se indique lo contrario, todos los artículos a los que se hace referencia se refieren a la Directiva.

sobre la Ciberdelincuencia del Consejo de Europa de 23 de noviembre de 2001 (en lo sucesivo, «el Convenio de Budapest»), con la excepción de que la Directiva también abarca explícitamente los datos informáticos.

- «Datos informáticos», en el artículo 2, letra b). La definición se ajusta a la del artículo 1, letra b), del Convenio de Budapest, pero se refiere a un sistema de información en lugar de a un sistema informático.
- «Persona jurídica», en el artículo 2, letra c). Esta definición tiene por objeto garantizar la responsabilidad tanto de las personas físicas como jurídicas, excluyendo a los Estados, los organismos públicos y las organizaciones internacionales públicas.
- «Sin autorización», en el artículo 2, letra d). Esta definición está relacionada con un principio general del Derecho penal y tiene por objeto evitar la responsabilidad penal de una persona que actúe de la forma autorizada por el Derecho nacional o con la autorización del propietario u otro titular del derecho sobre el sistema de información o parte del mismo.

Se definen las siguientes **infracciones penales específicas**:

- El acceso ilegal a los sistemas de información como tal (artículo 3).
- La interferencia ilegal en los sistemas de información (artículo 4), que incluye todo acceso ilegal a un sistema de información que conlleve una obstaculización o una interrupción significativa de su funcionamiento.
- La interferencia ilegal en los datos (artículo 5) que se refiere a toda interferencia ilícita con los datos informáticos que, como tal, dañe su integridad o su disponibilidad.
- La interceptación ilegal (artículo 6) de transmisiones no públicas de datos informáticos y emisiones electromagnéticas desde un sistema de información que contenga dichos datos.
- La facilitación ilegal de los instrumentos utilizados para cometer las infracciones anteriormente señaladas (artículo 7). En este contexto, se consideran instrumentos un programa informático, una contraseña informática o cualquier otro dato que permita el acceso a un sistema de información.

Además, la Directiva **amplía la responsabilidad penal** a la inducción y complicidad en la comisión o la tentativa de comisión de las infracciones señaladas por parte de personas físicas o jurídicas (artículo 8). Si bien la inducción y la complicidad se aplican a todas las infracciones a las que se hace referencia en los artículos 3 a 7, la tentativa únicamente se refiere a los artículos 4 y 5.

En el artículo 9 se fijan niveles mínimos para las **sanciones** máximas aplicables a las infracciones a las que se hace referencia en la Directiva:

- Como base de referencia, se fija una sanción máxima de privación de libertad igual o superior a dos años para todas las infracciones, excepto para las recogidas en el artículo 8 (artículo 9, apartado 2).
- Se establece una sanción máxima de al menos tres años de privación de libertad para las infracciones recogidas en los artículos 4 y 5, siempre que hayan afectado a un número significativo de sistemas de información (conocidas generalmente como «infracciones botnet», artículo 9, apartado 3).
- Se fija una sanción máxima de al menos cinco años de privación de libertad para las infracciones a las que se refieren los artículos 4 y 5 que hayan sido cometidas por una organización delictiva [artículo 9, apartado 4, letra a)], que causen daños graves

[artículo 9, apartado 4, letra b)] o que se cometan contra el sistema de información de una infraestructura crítica [artículo 9, apartado 4, letra c)].
- En aquellos casos en los que una de las infracciones a las que se refieren los artículos 4 y 5 sea cometida utilizando ilícitamente datos de carácter personal de otra persona, los Estados miembros deben garantizar que ello pueda ser considerado circunstancia agravante, a menos que tal circunstancia ya esté contemplada en otra infracción (artículo 9, apartado 5).

En los artículos siguientes se establecen las condiciones mínimas de la **responsabilidad de las personas jurídicas** (artículo 10) y se facilita una lista de ejemplos de sanciones que podrían aplicárseles (artículo 11).

Reconociendo que las infracciones anteriormente mencionadas pueden cometerse (en el sentido de «ser ejecutadas») en el lugar en el que el infractor realmente actúa, mientras que sus efectos sobre el sistema de información atacado pueden producirse en un lugar diferente, el artículo 12 impone obligaciones de establecer la **competencia**, diferenciando entre:

- el lugar en el que el autor se encuentra físicamente presente al cometer la infracción;
- la ubicación del sistema de información afectado;
- la nacionalidad del autor;
- el lugar de residencia habitual del autor; y
- el lugar de establecimiento de la persona jurídica en cuyo beneficio se comete la infracción.

En cuanto al intercambio de información, el artículo 13, apartado 1, exige que los Estados miembros garanticen la existencia de un **punto de contacto** nacional operativo disponible veinticuatro horas al día, siete días a la semana, con el fin de poder responder a cualquier solicitud extranjera urgente en un plazo de ocho horas.

Además, los Estados miembros deben tomar las medidas necesarias para **facilitar la información** sobre las infracciones anteriormente mencionadas a las autoridades nacionales competentes (artículo 13, apartado 3), así como para recabar e intercambiar una cantidad mínima de **datos estadísticos** sobre dichas infracciones (artículo 14).

1.2 Finalidad y metodología del informe

El artículo 16 de la Directiva estipula que los Estados miembros deben poner en vigor las disposiciones legales, reglamentarias y administrativas necesarias para dar cumplimiento a lo que en ella se establece antes del 4 de septiembre de 2015 y comunicarlo a la Comisión.

El presente informe responde al requisito establecido en el artículo 17 de la Directiva, que prevé que la Comisión debe presentar un informe al Parlamento Europeo y al Consejo en el que se evalúe la medida en que los Estados miembros han adoptado las disposiciones necesarias para dar cumplimiento a la Directiva. Por consiguiente, el objetivo de este informe es ofrecer una visión de conjunto concisa pero informativa de las principales medidas de transposición adoptadas por los Estados miembros.

La transposición por parte de los Estados miembros supuso recopilar información sobre las disposiciones legislativas y administrativas pertinentes, analizarla, redactar nuevos actos

legislativos (o, en la mayoría de los casos, modificar los que ya existían), proceder a su promulgación y, por último, informar a la Comisión.

Al vencer el plazo de transposición, 22 Estados miembros habían notificado a la Comisión que habían concluido la transposición de la Directiva. En noviembre de 2015, la Comisión inició procedimientos de infracción por ausencia de notificación de las medidas nacionales de transposición nacional contra los cinco Estados miembros restantes: BE, BG, EL, IE y SI[5]. A 31 de mayo de 2017, aún no habían concluido los procedimientos de infracción por ausencia de notificación de las medidas nacionales de transposición contra BE, BG e IE[6].

La descripción y el análisis realizados en el presente informe se basan en los datos facilitados por los Estados miembros antes del 31 de mayo de 2017[7]. No se han tenido en cuenta las notificaciones recibidas después de esa fecha. Se tuvieron en cuenta todas las medidas notificadas relacionadas con las legislaciones nacionales, así como las decisiones judiciales y, cuando resultó apropiado, la doctrina jurídica consolidada. Además, durante el análisis, la Comisión se puso en contacto directamente con los Estados miembros cuando resultó necesario y apropiado para solicitar información adicional o aclaraciones. Para el análisis se tuvo en cuenta toda la información recabada.

Además de las cuestiones identificadas en este informe, pueden existir dificultades adicionales para la transposición y otras disposiciones no comunicadas a la Comisión, o cambios legislativos y no legislativos posteriores. Por lo tanto, este informe no es óbice para que la Comisión siga evaluando algunas disposiciones y apoyando a los Estados miembros en la transposición y la aplicación de la Directiva.

2. Medidas de transposición

2.1 Definiciones jurídicas (artículo 2 de la Directiva)

El artículo 2 de la Directiva recoge las definiciones jurídicas de «sistema de información» [letra a)], «datos informáticos» [letra b)], «persona jurídica» [letra c)] y «sin autorización» [letra d)]. Únicamente CY y UK (Gibraltar) han incorporado legislación que abarca todos los aspectos de estas definiciones. En concreto, la situación es la siguiente:

a) Sistema de información

La definición prevista en la Directiva se basa en la definición de «sistema informático» tal como se recoge en el artículo 1, letra a), del Convenio de Budapest, y añade los propios datos informáticos como parte del sistema de información. CY, EL, IE, FI, HR, MT, PT y UK (Gibraltar) han incorporado disposiciones legislativas que incluyen la definición de «sistema de información», mientras que los datos facilitados por DE, ES, FR, LU, LV, PL, SE y SK no fueron concluyentes. En cuanto a los demás Estados miembros, es decir, AT, BE, BG, CZ, EE, HU, IT, LT, NL, RO, SI y UK (excepto Gibraltar), las definiciones jurídicas correspondientes no se refieren explícitamente a los datos informáticos. Esto implica una

[5] En el presente documento, los Estados miembros aparecen abreviados conforme a los códigos que se recogen en: http://publications.europa.eu/code/es/es-5000600.htm.

[6] La información sobre las decisiones de la Comisión en lo relativo a los procedimientos de infracción se encuentra disponible en: http://ec.europa.eu/atwork/applying-eu-law/infringements-proceedings/infringement_decisions/?lang_code=es.

[7] IE notificó la transposición plena de la Directiva el 31 de mayo de 2017.

referencia al artículo 1, letra a), del Convenio de Budapest con un alcance idéntico para la definición de sistema informático.

b) Datos informáticos
Las disposiciones legislativas de AT, BG, CY, CZ, DE, EE, EL IE, FI, HR, LT, MT, NL, PT, RO y UK (Gibraltar) recogen el término «datos informáticos», mientras que la información facilitada por ES, FR, IT, LU, LV, PL, SE, SK y UK (excepto Gibraltar) no resultó concluyente. Sin embargo, en el caso de SE, la formulación específica de los artículos referentes hace que esta definición sea redundante. En cuanto al resto de Estados miembros, HU únicamente aplica la definición de «datos informáticos» a las infracciones descritas en los artículos 4 y 5 de la Directiva, mientras que ni BE ni SI incluyen los «programas que sirven para hacer que dicho sistema de información realice una función» en la definición de «datos informáticos».

c) Persona jurídica
Excepto en el caso de LU, que no facilitó información concluyente sobre la transposición del artículo 2, letra c), la transposición de la definición de «persona jurídica» no generó problemas. Esto se debe a que, por lo general, ya se recoge en el Derecho civil o mercantil de los Estados miembros. Únicamente CY cuenta con una disposición específica entre las medidas adoptadas para transponer la Directiva.

d) Sin autorización
En cuanto a la definición del término «sin autorización» recogida en el artículo 2, letra d), únicamente notificaron su transposición CY, IE, RO y UK (Gibraltar), lo que significa que 23 Estados miembros no han adoptado ninguna medida de transposición para esta definición. Sin embargo, cabe señalar que en todos los Estados miembros existe el principio general de ausencia de responsabilidad penal por cualquier acción que pueda tomarse si esta medida se realiza con autorización.

2.2 Infracciones penales específicas (artículos 3 a 7 de la Directiva)

a) Acceso ilegal a los sistemas de información
En cuanto al acceso ilegal a los sistemas de información, el artículo 3 de la Directiva está incluido en la legislación nacional de AT, CY, CZ, EL, ES, IE, FI, FR, LT, LU, NL, PL, PT, SE y SK.

En el resto de los Estados miembros, es decir, BE, BG, DE, EE, HR, HU, IT, LV, MT, RO, SI y UK, la descripción nacional de esta infracción penal no establece diferencia entre si se logra el acceso a la totalidad o solo a una parte del sistema de información, incluso si la Directiva lo establece explícitamente. Además, la transposición de DE no incluye el mero acceso a los equipos informáticos, AT y LU han fijado requisitos adicionales relacionados con la existencia de una intención específica (intención de adquirir información, provocar una desventaja o fines fraudulentos) y LV sobre el hecho de que se causen daños sustanciales. En el caso de BE, BG, FR, HR, LU, MT, PT, RO, SI y UK, las disposiciones nacionales tienen un alcance superior al previsto en la Directiva, puesto que no requieren la elusión de medidas de seguridad para establecer la responsabilidad penal. El resto de Estados miembros se refieren literalmente al hecho de que la infracción se cometa transgrediendo medidas de seguridad (CY, EL y SK), o utilizan una terminología similar para describir esta cuestión (AT, CZ, DE, EE, ES, FI, HU, IT; LT, LV, NL, PL y SE).

b) Interferencia ilegal en los sistemas de información
El artículo 4 de la Directiva se refiere a la interferencia ilegal en los sistemas de información. La Directiva enumera ocho actos que podrían cometerse (introducir, transmitir, dañar, borrar, deteriorar, alterar, suprimir o hacer inaccesibles datos informáticos) y dos posibles resultados para cada acto (obstaculización o interrupción significativa del funcionamiento de un sistema de información). BE, CY, CZ, EL, IE, FR, HR, LU, MT, PT, SE y UK (excepto Gibraltar) han introducido las medidas legislativas correspondientes. BG únicamente se refiere a la introducción de un virus, y el resto de Estados miembros (AT, DE, EE, ES, HU, IT, LV, NL, PL, RO, SI, SK y UK) no hacen referencia específica a entre 1 y 4 de los posibles actos. En este contexto, puede observarse que la mayoría de los problemas planteados están relacionados con los términos «deteriorar» (ausente en 8 casos) y «hacer inaccesible» (ausente en 9 casos).

c) Interferencia ilegal en los datos
El artículo 5 de la Directiva se refiere a la interferencia ilegal en los datos y enumera los siguientes seis actos que podrían cometerse: borrar, dañar, deteriorar, alterar, suprimir o hacer inaccesibles datos informáticos. CY, EL, IE y MT han transpuesto esta disposición de manera literal; BE, CZ, LT, PT y SE emplearon términos más genéricos para cubrir todos los actos posibles. Las medidas de transposición de los demás Estados miembros no se refieren a todas las posibilidades, sino que únicamente cubren cinco alternativas (FI y SK) o menos (AT, BG, DE, EE, FR, HR, HU, IT, LU, NL, PL, RO, SI y UK). La mayoría de los problemas surgieron con los términos «dañar» (ausente en 8 casos), «deteriorar» (13 casos), «suprimir» (11 casos) y «hacer inaccesibles» (13 casos). Además de lo previsto en el texto de la Directiva, FI requiere «el propósito de causar daños o pérdidas financieras» para establecer la responsabilidad penal, mientras que LT y LV requieren que se cause un daño sustancial.

d) Interceptación ilegal
El artículo 6 se refiere a la interceptación ilegal de transmisiones no públicas de datos informáticos y emisiones electromagnéticas desde un sistema de información que contenga dichos datos. CY, CZ, DE, ES, IE, FI, HR, LV, MT, RO, SE, SK y UK (Gibraltar) han introducido legislación que cubre el artículo 6 en su totalidad. El alcance general de la Directiva en lo relativo a la interceptación de datos informáticos se limita a los mensajes (AT y BG), la observación de una persona (EE) o la correspondencia (FR y HU). Asimismo, las medidas de transposición de los siguientes Estados miembros no cubren la interceptación de emisiones electromagnéticas: BE, BG, EE, FR, HU, IT, LT, LU, NL, PL, PT, SI y UK (excepto Gibraltar). Además, algunos Estados miembros requieren una intención especial (por ejemplo, adquirir información, conseguir un beneficio económico o provocar una desventaja, véase AT, EL y HU), o actos adicionales específicos (por ejemplo, registrar o conocer el contenido interceptado, véase GB y HU).

e) Instrumentos utilizados para cometer las infracciones
El artículo 7 tipifica como delito una serie de actos relacionados con el uso de instrumentos como los programas informáticos o los códigos de acceso para cometer las infracciones a las que se refieren los artículos 3 a 6: producción, venta, adquisición para el uso, importación, distribución u otra forma de puesta a disposición de dichos instrumentos. AT, BE, CY, DE, EL, IE y SK han introducido medidas legislativas nacionales correspondientes. Algunos Estados miembros no cubren todas las infracciones a las que se hace referencia (EE, IT, MT, PL y SI). Algunos no se refieren al autor del artículo 7 como a persona diferente del autor de las infracciones mencionadas en los artículos 3 a 6 (CZ y SI). Algunos requieren una intención específica (causar daños o actuar de manera fraudulenta, véase FI, IT y LU), un resultado concreto, como la violación del secreto (BG), o al menos un nivel de preparación de

las infracciones mencionadas (SE). Por último, existen discrepancias entre el artículo 7 y las medidas nacionales debido a la ausencia de transposición de todos los posibles actos enumerados. Este es, por ejemplo, el caso de BG, CZ, EE, ES, FR, HR, HU, IT, LT, LU, LV, PL, PT, RO, SI y UK. De estos países, la legislación de LU se refiere explícitamente a 5 de los 6 posibles actos enumerados en la Directiva, mientras que los demás Estados miembros únicamente se refieren explícitamente a solo 4 o menos.

Únicamente ES ha transpuesto la alternativa de adquisición para el uso.

2.3 Normas generales para las infracciones en cuestión (artículos 8 a 12 de la Directiva)

a) Inducción y complicidad

El artículo 8, apartado 1, exige a los Estados miembros garantizar que la inducción y la complicidad en la comisión de las infracciones mencionadas en los artículos 3 a 7 sean sancionables como infracciones penales. Todos los Estados miembros han transpuesto esta disposición.

b) Tentativa

En virtud de lo previsto en el artículo 8, apartado 2, la tentativa de cometer las infracciones a las que hacen referencia los artículos 4 y 5 debe ser sancionable como infracción penal. Si bien PT no cubre todos los tipos de tentativa de comisión de las infracciones a las que se refiere el artículo 4 y SE carece de responsabilidad penal para la tentativa de comisión de la infracción de «violación del secreto de las comunicaciones», el resto de Estados miembros disponen de legislación que transpone esta disposición.

c) Sanciones

aa) Disposiciones generales

El artículo 9, apartado 1, requiere que los Estados miembros, de manera general, prevean penas eficaces, proporcionadas y disuasorias para las infracciones cubiertas por la Directiva. Si bien casi todos los Estados miembros cumplen este requisito, AT, BE, BG, IT, PT, SE y SI no alcanzan los niveles mínimos para las sanciones máximas previstos en el artículo 9, apartado 2, en todos los casos (véase la sección 1.1). Esto afecta a la transposición del artículo 9, apartado 1, ya que cabe concluir que los requisitos mínimos del artículo 9, apartado 2, son el mínimo para garantizar una pena eficaz, proporcionada y disuasoria.

bb) Nivel mínimo general para la sanción máxima

El artículo 9, apartado 2, establece que el nivel mínimo para la sanción máxima aplicable a las infracciones generales mencionadas en los artículos 3 a 7 es una privación de libertad de al menos dos años. La mayoría de los Estados miembros cumplen esta disposición. Únicamente hay seis Estados miembros en los que se observan discrepancias: AT (privación de libertad de un máximo de 6 meses), BG (privación de libertad de un máximo de 1 año para todas las infracciones, excepto para la interceptación ilegal), IT [privación de libertad de un máximo de 1 año para la infracción a la que se refiere el artículo 7, letra b)], PT (privación de libertad de un máximo de 1 año para la infracción a la que se refiere el artículo 3), SE (privación de libertad de un máximo de 1 año para la infracción de «infligir daños») y SI (privación de libertad de un máximo de 1 año para las infracciones a las que se refieren los artículos 3, 6 y 7). En el caso de BE, únicamente se alcanza el nivel mínimo de la sanción máxima para los artículos 3, 6 y 7 cuando las infracciones se cometen con intención fraudulenta.

cc) Un número significativo de sistemas de información afectados

El artículo 9, apartado 3, prevé un aumento del nivel mínimo de las sanciones máximas a tres años de privación de libertad cuando se vea afectado un número significativo de sistemas de información como resultado de una de las infracciones mencionadas en los artículos 4 y 5. Por lo general, los Estados miembros han introducido las medidas legislativas correspondientes, si bien DE únicamente se refiere a los sistemas de información «que tienen una importancia sustancial para otro», FI requiere evaluar la infracción «en su totalidad» para aplicar la sanción más estricta y LV no se refiere a un número significativo de sistemas de información (o términos similares), sino únicamente a causar «un daño sustancial». La información facilitada por BG y SI no fue concluyente.

dd) Organizaciones delictivas

De conformidad con lo previsto en el artículo 9, apartado 4, letra a), se aplicará una sanción máxima de al menos cinco años de privación de libertad para las infracciones a las que se refieren los artículos 4 y 5 cuando sean cometidas por una organización delictiva según la definición de la Decisión marco 2008/841/JHA.

También en este caso, la mayoría de los Estados miembros cumplen lo previsto en el artículo 9, apartado 4, letra a). En el marco del Derecho penal de LU y SI, las disposiciones relativas a las infracciones cometidas por una organización delictiva no abarcan la ciberdelincuencia. La legislación de BE prevé un máximo de solamente tres años de privación de libertad para las infracciones a las que hace referencia el artículo 5, la legislación de DE no abarca a las personas físicas como víctimas de las infracciones, la legislación de FI requiere una evaluación adicional de la infracción «en su totalidad» y la legislación de SE prevé una sanción máxima de cuatro años de privación de libertad para los casos de «causa flagrante de daños».

ee) Daños graves

El artículo 9, apartado 4, letra b), prevé 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 se causen daños graves. Si bien no se especifica lo que debería entenderse por «daños graves», todos los Estados miembros, excepto BG, DE, FI, HU, LU y SE, han introducido medidas legislativas que se corresponden con lo previsto en la Directiva. La información facilitada por HU no fue concluyente. BG no alcanza el nivel mínimo de cinco años de sanción máxima, mientras que LU se refiere a una cláusula de sanción general para casos de daños graves que no abarca la ciberdelincuencia. Existen discrepancias poco significativas en DE (no se incluye a las personas jurídicas como víctimas de las infracciones), FI (una sanción mayor requiere una evaluación adicional de la infracción «en su totalidad») y SE (privación de libertad de un máximo de cuatro años por «causa flagrante de daños»).

ff) Sistemas de información de infraestructuras críticas

La implicación de sistemas de información de una infraestructura crítica en las infracciones a las que se refieren los artículos 4 y 5 también conlleva una privación de libertad de al menos cinco años como sanción máxima, de conformidad con lo previsto en el artículo 9, apartado 4, letra c).

Si bien la mayoría de los Estados miembros cumplen esta disposición, BG no ha facilitado información específica sobre la transposición. BE ha fijado una sanción máxima de tres años para las infracciones a las que se hace referencia en el artículo 5. DE no cubre a las personas físicas como víctimas. FI requiere una evaluación adicional de la infracción «en su totalidad», IT requiere que se cause «destrucción», PT requiere un ataque «de manera grave y duradera» y no incluye ninguna referencia al artículo 5, y SE únicamente cumple los requisitos de la Directiva en lo relativo a la infracción de «sabotaje flagrante».

gg) Usurpación de identidad y otras infracciones relacionadas con la identidad

El artículo 9, apartado 5, exige que los Estados miembros garanticen que, cuando las infracciones a que se refieren los artículos 4 y 5 sean cometidas utilizando indebidamente datos de carácter personal de otra persona con la finalidad de ganar la confianza de un tercero, causando así perjuicio al propietario legítimo de la identidad, ello pueda ser considerado como circunstancia agravante, a menos que tal circunstancia ya esté contemplada en otra infracción penal. El amplio margen de apreciación ha dado lugar a un amplio espectro de medidas de transposición entre los Estados miembros. BE y EL no han notificado ninguna transposición, y la legislación penal de CZ no incluye ninguna disposición específica. AT, CY, ES, IE, MT, PT y SE han adoptado el enfoque del agravante (SE hace referencia a la circunstancia de «planificación especial»), mientras que el resto de Estados miembros mencionan disposiciones adicionales para esta infracción penal específica. Entre quienes hacen referencia a disposiciones específicas, se han observado las siguientes cuestiones de transposición: BG y NL requieren una intención específica («recibir un beneficio» y «el objetivo de encubrir o utilizar indebidamente la identidad»), DE únicamente se refiere a «datos personales generalmente no accesibles», FR solo hace referencia al nombre de una persona, pero a ningún otro dato personal, LV requiere que se cause un «daño sustancial», y RO únicamente cubre el empleo de un documento y requiere que se cometa engaño.

d) Responsabilidad de las personas jurídicas

aa) En general

El artículo 10, apartado 1, requiere la acreditación de la responsabilidad de las personas jurídicas por las infracciones mencionadas en los artículos 3 a 8 cuando el autor tenga a) poder de representación de dicha persona jurídica, b) autoridad para tomar decisiones en nombre de dicha persona jurídica o c) autoridad para ejercer el control en el seno de dicha persona jurídica. Todos los Estados miembros han introducido medidas legislativas correspondientes a este artículo, con los siguientes problemas poco significativos: BG no cubre la infracción a la que hace referencia el artículo 6 y HR no incluye ninguna referencia al hecho de que el autor tenga autoridad para ejercer el control en el seno de la persona jurídica [artículo 10, apartado 1, letra c)].

bb) Por falta de supervisión o control

El artículo 10, apartado 2, exige que los Estados miembros introduzcan la responsabilidad de las personas jurídicas cuando la falta de supervisión o control por parte de alguna de las personas a que se refiere el artículo 10, apartado 1, haya permitido que se cometa una de las infracciones mencionadas en los artículos 3 a 8. Si bien casi todos los Estados miembros cumplen esta disposición, la información facilitada por LU no fue concluyente y BG carece de referencia a la comisión de una infracción prevista en el artículo 6.

e) Sanciones contra las personas jurídicas

aa) Sanciones obligatorias

El artículo 11, apartado 1, de la Directiva requiere que los Estados miembros prevean multas de carácter penal o de otro tipo como sanciones eficaces, proporcionadas y disuasorias. Todos los Estados miembros han notificado medidas nacionales conformes, excepto IE y UK. En estos dos países, todavía no se ha fijado la cuantía máxima de las posibles multas, debido a la ausencia de disposiciones legislativas específicas. Por consiguiente, no es posible evaluar la eficacia, la proporcionalidad ni el efecto disuasorio de las multas correspondientes.

bb) Sanciones opcionales

El artículo 11, apartado 1, continúa con una lista de posibles opciones de sanciones adicionales para las personas jurídicas. Estas sanciones son: exclusión del derecho a prestaciones o ayudas públicas (elegida por CY, CZ, EL, ES, HR, HU, LU, MT, PL, PT y SK), inhabilitación temporal o permanente para el ejercicio de actividades comerciales (AT, BE, CY, CZ, EL, ES FR, HR, HU, IT, LT, LV, MT, PL, PT, RO, SE, SI y SK), sometimiento a vigilancia judicial (CY, ES, FR, MT, PT y RO), liquidación judicial (CY, CZ, EL, ES, FR, HR, HU,LT, LU, LV, MT, PT, RO, SI y SK) y cierre temporal o definitivo de los establecimientos utilizados para cometer la infracción (BE, CY, WS, FR, LT, MT, PT y RO). De lo anterior se deduce que BG, DE, EE, IE, FI, NL y UK no han elegido ninguna de las opciones.

cc) Sanciones por omisión

Según lo previsto en el artículo 11, apartado 2, los Estados miembros deben 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 eficaces, proporcionadas y disuasorias. La información facilitada por LU no fue concluyente. Todos los demás Estados miembros, excepto IE y UK, han introducido las disposiciones legislativas correspondientes. En el caso de IE y UK, surgen los mismos problemas para el artículo 11, apartado 1: (véase el punto aa)).

f) Competencia

aa) Criterios de competencia obligatorios

El artículo 12, apartados 2 y 3, de la Directiva prevé que los Estados miembros establezcan sus propias competencias en relación con las infracciones contempladas en los artículos 3 a 8, cometidas total o parcialmente dentro de su territorio, tanto si el autor comete la infracción estando físicamente presente en él, como si la infracción se comete contra un sistema de información situado en el territorio del Estado miembro, o cuando la infracción la ha cometido en el extranjero uno de sus nacionales. La mayoría de los Estados miembros han introducido medidas legislativas nacionales correspondientes, pero la legislación de IT no determina la competencia en lo relativo a los nacionales que se encuentran en el extranjero en el caso de que se cometan infracciones básicas, las legislación de LV y SI incluyen disposiciones poco claras sobre aspectos territoriales, la competencia de MT en lo relativo a la comisión parcial en su territorio no es clara y UK se refiere a un sistema informático en lugar de a un sistema de información.

bb) Otros criterios de competencia

El artículo 12, apartado 3, establece que los Estados miembros informarán a la Comisión cuando decidan establecer competencias para casos en los que el autor tenga su residencia habitual en su territorio (a lo que optaron AT, CY, CZ, IE, FI, HR, LT, LV, NL, SE y SK), o en los que la infracción se cometa en beneficio de una persona jurídica establecida en su territorio (CY, CZ, LV, PT, RO y SK).

2.4 Cuestiones operativas (artículos 13 y 14 de la Directiva)

a) Disposición sobre los puntos de contacto nacionales

El artículo 13, apartado 1, exige que los Estados miembros establezcan puntos de contacto nacionales para el intercambio de información sobre las infracciones a las que hacen referencia los artículos 3 a 8. Sobre la base de dicha disposición, los Estados miembros deben garantizar que cuentan con procedimientos para que, en caso de solicitud de ayuda urgente, la autoridad competente pueda responder en un plazo máximo de ocho horas. Según la información facilitada, la mayoría de los Estados miembros han establecido la infraestructura necesaria. IE y RO señalaron que sus puntos de contacto respectivos únicamente están

disponibles durante un número limitado de horas al día, lo que impide que la autoridad pueda ofrecer una respuesta en un plazo de ocho horas a partir de la recepción de una solicitud en todos los casos. Varios Estados miembros indicaron que están empleando las redes de puntos de contacto operativos existentes creadas a través de la red G7 o en el marco del Convenio sobre la Ciberdelincuencia del Consejo de Europa.

b) Información sobre los puntos nacionales de contacto operativos existentes
Según lo previsto en el artículo 13, apartado 2, los Estados miembros deben facilitar las señas de sus puntos de contacto a la Comisión, quien la transmitirá a los demás Estados miembros. Todos los Estados miembros han facilitado la información necesaria.

c) Canales de información
El artículo 13, apartado 3, requiere que los Estados miembros garanticen la disponibilidad de canales de información adecuados para facilitar a las autoridades nacionales competentes información relativa a las infracciones a que se refieren los artículos 3 a 6. La información facilitada por HR, IT, IE y PT no fue concluyente. En los demás Estados miembros, parece que existen diferentes enfoques en lo relativo al establecimiento de los canales de información. La mayoría de los Estados miembros (BE, BG, CY, CZ, DE, EE, EL, FI, FR, HR, HU, IT, LT, LV, MT, NL, PL, PT, RO, SE, SI, SK y UK) han notificado medidas que contemplan canales destinados a facilitar el proceso de información para la persona o la organización que inicialmente denuncia una infracción, por ejemplo, la víctima de un ciberataque (LV no establece claramente los canales de información concretos). Sin embargo, otros Estados miembros (AT, ES y LU) han facilitado idéntica información sobre la aplicación del artículo 13, apartados 1 y 2, lo que parece indicar que sus medidas servirán principalmente para facilitar la comunicación entre las autoridades.

d) Recogida de datos estadísticos
Según lo previsto en el artículo 14, apartados 1 y 2, los Estados miembros deben garantizar la existencia de un sistema para la recogida, la elaboración y el suministro de datos estadísticos, al menos sobre el número de infracciones mencionadas en los artículos 3 a 7 registradas por los Estados miembros y sobre el número de personas procesadas y condenadas por dichas infracciones. En base a las notificaciones obtenidas, la mayoría de los Estados miembros parecen haber puesto en marcha medidas tanto legislativas como administrativas para garantizar la recogida de información, normalmente a partir de un sistema electrónico nacional general. La información de varios Estados miembros no fue concluyente (EL, IE y UK (Gibraltar, Irlanda del Norte y Escocia)). Uno de los motivos fue que no resultó posible recabar por separado información sobre las infracciones concretas a las que hace referencia la Directiva (BE, DE y SE) o que la información recabada podía no cubrir todas las infracciones a las que hace referencia la Directiva (RO).

e) Transmisión de datos estadísticos a la Comisión
El artículo 14, apartado 3, requiere que los Estados miembros transmitan a la Comisión los datos estadísticos correspondientes. Todos los Estados miembros que notificaron medidas, excepto UK (Gibraltar, Irlanda del Norte y Escocia) y HU, han confirmado la aplicación de medidas legales, administrativas o de ambos tipos para garantizar el cumplimiento de esta obligación. La información facilitada por EL, ES, LU y SI no fue concluyente.

3. Conclusión y próximas etapas

La Directiva ha conllevado un progreso significativo en la tipificación como delito de los ciberataques a un nivel comparable entre los Estados miembros, lo que facilita la cooperación transfronteriza entre las autoridades policiales que investigan este tipo de infracciones. Los

Estados miembros han modificado los códigos penales y otra legislación pertinente, han racionalizado los procedimientos y han creado sistemas de cooperación o mejorado los existentes. La Comisión reconoce los grandes esfuerzos realizados por los Estados miembros para transponer la Directiva.

Sin embargo, la Directiva no alcanzará todo su potencial hasta que se consiga la aplicación plena de todas sus disposiciones por parte de los Estados miembros. El análisis llevado a cabo hasta la fecha sugiere que una de las mejoras más importantes que lograrán los Estados miembros es el empleo de definiciones (artículo 2), lo que tiene repercusiones en el alcance de las infracciones definidas en el Derecho nacional en virtud de lo previsto en la Directiva. Además, parece que los Estados miembros han tenido dificultades para incluir todas las posibilidades al definir las acciones relacionadas con las infracciones (artículos 3 a 7) y al fijar niveles comunes para las sanciones impuestas a los ciberataques (artículo 9). Otros de los problemas que han surgido parecen estar relacionados con la aplicación de disposiciones administrativas sobre los canales de información adecuados (artículo 13, apartado 3) y con el seguimiento y las estadísticas de las infracciones a que se refiere la Directiva (artículo 14).

La Comisión seguirá facilitando apoyo a los Estados miembros para la aplicación de la Directiva. Habida cuenta de su posible contribución a la cooperación transfronteriza, este apoyo se refiere especialmente a las disposiciones operativas de la Directiva relativas al intercambio de información (artículo 13, apartados 1 y 2), los canales de información (artículo 13, apartado 3) y el seguimiento y las estadísticas (artículo 14). Para ello, la Comisión ofrecerá oportunidades adicionales para que los Estados miembros identifiquen e intercambien mejores prácticas durante el segundo semestre de 2017.

En estos momentos, la Comisión no ve la necesidad de proponer enmiendas a la Directiva. En este contexto, con el fin asimismo de apoyar las investigaciones penales sobre ataques contra sistemas de información, delitos facilitados por el medio cibernético y otros tipos de delitos, la Comisión está considerando medidas para mejorar el acceso transfronterizo a pruebas electrónicas relativas a investigaciones penales, incluso proponiendo, a principios de 2018, posibles medidas legislativas[8]. La Comisión también está estudiando la función de cifrado en las investigaciones penales, e informará sobre sus conclusiones antes de octubre de 2017[9].

La Comisión se compromete a garantizar que se complete la transposición en toda la UE y que las disposiciones se apliquen correctamente. Para ello, realizará un seguimiento para verificar que las medidas nacionales respetan las disposiciones correspondientes de la Directiva. En caso necesario, la Comisión recurrirá a las competencias ejecutivas que le confieren los Tratados a través de procedimientos de infracción.

[8] Evaluación inicial de impacto sobre la mejora del acceso transfronterizo a las pruebas electrónicas, de 4 de agosto de 2017, disponible en ec.europa.eu.

[9] Comunicación sobre el octavo informe de situación relativo a una Unión de la Seguridad genuina y efectiva (COM(2017) 354 final).