Consejo de la
Unión Europea

Bruselas, 16 de mayo de 2019
(OR. en)

7299/19

LIMITE

CORLX 106
CFSP/PESC 191
RELEX 235
CYBER 81
JAI 264
FIN 216

ACTOS LEGISLATIVOS Y OTROS INSTRUMENTOS

Asunto:	DECISIÓN DEL CONSEJO relativa a medidas restrictivas contra los ciberataques que amenacen a la Unión o a sus Estados miembros

DECISIÓN (PESC) 2019/… DEL CONSEJO

de …

relativa a medidas restrictivas
contra los ciberataques que amenacen a la Unión o a sus Estados miembros

EL CONSEJO DE LA UNIÓN EUROPEA,

Visto el Tratado de la Unión Europea, y en particular su artículo 29,

Vista la propuesta de la Alta Representante de la Unión para Asuntos Exteriores y Política de Seguridad,

Considerando lo siguiente:

(1) El 19 de junio de 2017, el Consejo adoptó unas conclusiones sobre un marco para una respuesta diplomática conjunta a las actividades cibernéticas malintencionadas (en lo sucesivo, «conjunto de instrumentos de ciberdiplomacia»), en las que el Consejo manifestaba su preocupación por la capacidad y disposición crecientes de agentes estatales y no estatales de perseguir sus objetivos mediante actividades cibernéticas malintencionadas y afirmaba que existe una creciente necesidad de proteger la integridad y la seguridad de la Unión, sus Estados miembros y sus ciudadanos frente a las ciberamenazas y las actividades cibernéticas malintencionadas.

(2) El Consejo subrayó que comunicar claramente las posibles consecuencias de una respuesta diplomática conjunta de la Unión a dichas actividades cibernéticas malintencionadas tiene influencia en el comportamiento de los agresores potenciales en el ciberespacio, reforzando así la seguridad de la Unión y de sus Estados miembros. También afirmó que las medidas adoptadas en el marco de la política exterior y de seguridad común (PESC), incluidas, si procede, las medidas restrictivas, adoptadas con arreglo a las correspondientes disposiciones de los Tratados, son aptas de cara a un marco para una respuesta diplomática conjunta de la Unión a las actividades cibernéticas malintencionadas, con el objetivo de fomentar la cooperación, facilitar la lucha contra las amenazas inmediatas y a largo plazo, e influir en el comportamiento de los agresores potenciales a largo plazo.

(3) El 11 de octubre de 2017 el Comité Político y de Seguridad aprobó las directrices de aplicación del conjunto de instrumentos de ciberdiplomacia, que hacen referencia a cinco categorías de medidas, incluidas las medidas restrictivas, dentro de dicho conjunto de instrumentos, así como el proceso para recurrir a ellas.

(4) Las conclusiones del Consejo adoptadas el 16 de abril de 2018 sobre actividades cibernéticas malintencionadas condenaban firmemente el uso malintencionado de las tecnologías de la información y la comunicación (TIC) y hacen hincapié en que la utilización de las TIC con fines malintencionados es inaceptable, ya que menoscaba la estabilidad, la seguridad y los beneficios que ofrecen internet y el uso de las TIC. El Consejo recordaba que el conjunto de instrumentos de ciberdiplomacia contribuye a la prevención de conflictos, la cooperación y la estabilidad en el ciberespacio al establecer medidas enmarcadas en la PESC, incluidas medidas restrictivas, que pueden utilizarse para prevenir las actividades cibernéticas malintencionadas y responder a ellas. Afirmaba que la Unión seguirá sosteniendo firmemente que el Derecho internacional es aplicable al ciberespacio y hacía hincapié en que el respeto del Derecho internacional vigente, en particular la Carta de las Naciones Unidas, es esencial para mantener la paz y la estabilidad. El Consejo subrayaba también que los Estados no deben recurrir a intermediarios para cometer hechos internacionalmente ilícitos utilizando las TIC, y deben tratar de garantizar que su territorio no sea utilizado por agentes no estatales para cometer tales hechos, como se indica en el informe de 2015 del Grupo de Expertos Gubernamentales de las Naciones Unidas sobre los Avances en la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional.

5) El 28 de junio de 2018, el Consejo Europeo adoptó unas conclusiones en las que destacaba la necesidad de reforzar las capacidades contra las amenazas en materia de ciberseguridad procedentes de fuera de la Unión. El Consejo Europeo pidió a las instituciones y a los Estados miembros que pusieran en marcha las medidas indicadas en la comunicación conjunta de la Comisión y la Alta Representante de la Unión para Asuntos Exteriores y Política de Seguridad, de 13 de junio de 2018, titulada «Aumentar la resiliencia y desarrollar las capacidades para hacer frente a las amenazas híbridas», incluido el uso práctico del conjunto de instrumentos de ciberdiplomacia.

(6) El 18 de octubre de 2018, el Consejo Europeo adoptó unas conclusiones en las que pedía que se impulsaran los trabajos sobre la capacidad para responder a los ciberataques, y disuadir de que estos se cometan, con medidas restrictivas de la Unión, con arreglo a las conclusiones del Consejo de 19 de junio de 2017.

(7) En este contexto, la presente Decisión establece un marco para unas medidas restrictivas específicas destinadas a impedir y contrarrestar los ciberataques con un efecto significativo que constituyan una amenaza externa para la Unión o sus Estados miembros. Cuando se estimen necesarias para el cumplimiento de los objetivos de la PESC en las disposiciones pertinentes del artículo 21 del Tratado de la Unión Europea, la presente Decisión también permite que se apliquen medidas restrictivas en respuesta a ciberataques con un efecto significativo contra terceros Estados u organizaciones internacionales.

(8) Para que tengan un efecto preventivo y disuasorio, las medidas restrictivas específicas deben centrarse en los ciberataques contemplados en el ámbito de aplicación de la presente Decisión que se hayan llevado a cabo deliberadamente.

(9) Hay que diferenciar las medidas restrictivas específicas de la imputación de responsabilidad por los ciberataques a un tercer Estado. La aplicación de medidas restrictivas específicas no implica tal imputación, que constituye una decisión política soberana adoptada en función de cada caso. Cada Estado miembro es libre de adoptar su propia determinación con respecto a la imputación de ciberataques a un tercer Estado.

(10) Es necesario que la Unión vuelva a actuar con el fin de aplicar determinadas medidas.

HA ADOPTADO LA PRESENTE DECISIÓN:

Artículo 1

1. La presente Decisión se aplica a los ciberataques con un efecto significativo, incluidas las tentativas de ciberataque con un efecto significativo potencial, que constituyan una amenaza externa para la Unión o para sus Estados miembros.

2. Entre los ciberataques que constituyen una amenaza externa se incluyen aquellos que:

   a) se originen, o se cometan, desde el exterior de la Unión;

   b) utilicen infraestructura fuera de la Unión;

   c) hayan sido cometidos por una persona física o jurídica, una entidad o un organismo establecidos o que tengan actividad fuera de la Unión; o

   d) hayan sido cometidos con el apoyo, bajo la dirección o bajo el control de una persona física o jurídica que tenga actividad fuera de la Unión.

3. A tal fin, los ciberataques son acciones que implican cualesquiera de los siguientes elementos:

   a) acceso a sistemas de información;

   b) intromisión en sistemas de información;

   c) intromisión en datos; o

   d) interceptación de datos,

cuando dichas acciones no estén debidamente autorizadas por el propietario o por otro titular de derechos del sistema o de datos o de parte del mismo, o no estén permitidas por el Derecho de la Unión o de un Estado miembro.

4. Entre los ciberataques que constituyen una amenaza para los Estados miembros se incluyen los que afecten a los sistemas de información relacionados, entre otros aspectos, con:

   a) las infraestructuras críticas, incluidos los cables submarinos y los objetos lanzados al espacio ultraterrestre, que resulten esenciales para el mantenimiento de funciones vitales de la sociedad, o para la salud, la seguridad, la protección y el bienestar económico o social de las personas;

   b) los servicios necesarios para el mantenimiento de actividades sociales o económicas esenciales, especialmente en los sectores de la energía (electricidad, petróleo y gas); el transporte (aéreo, ferroviario, fluvial o marítimo y por carretera); la actividad bancaria; las infraestructuras de los mercados financieros; el sector sanitario (proveedores de asistencia sanitaria, hospitales y clínicas privadas); el suministro y la distribución de agua potable; las infraestructuras digitales; o cualquier otro sector que resulte esencial para el Estado miembro de que se trate;

   c) las funciones vitales del Estado, en particular en los ámbitos de la defensa, la gobernanza y el funcionamiento de las instituciones, incluido en el caso de las elecciones públicas o los procesos electorales, el funcionamiento de las infraestructuras económicas y civiles, la seguridad interior, y las relaciones exteriores, también a través de las misiones diplomáticas;

d) el almacenamiento o el tratamiento de información clasificada; o

e) los equipos de respuesta de emergencia del Estado.

5. Los ciberataques que constituyen una amenaza para la Unión incluirán los cometidos contra sus instituciones, órganos y organismos, sus delegaciones en terceros países o ante organizaciones internacionales, sus operaciones y misiones de la política común de seguridad y defensa (PCSD) y sus representantes especiales.

6. Cuando se estimen necesarias para el cumplimiento de los objetivos de la PESC en las disposiciones pertinentes del artículo 21 del Tratado de la Unión Europea, también podrán aplicarse medidas restrictivas con arreglo a la presente Decisión en respuesta a ciberataques que tengan un efecto significativo contra terceros Estados u organizaciones internacionales.

Artículo 2

A efectos de la presente Decisión, se entenderá por:

1) «Sistemas 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 digitales, así como los datos digitales almacenados, tratados, recuperados o transmitidos por dicho aparato o grupo de aparatos para su funcionamiento, utilización, protección y mantenimiento.

2) «Intromisión en sistemas de información»: obstaculización o interrupción del funcionamiento de un sistema de información introduciendo datos digitales, transmitiendo, dañando, borrando, deteriorando, alterando o suprimiendo tales datos, o haciéndolos inaccesibles.

3) «Intromisión en datos»: borrado, dañado, deterioro, alteración o supresión de los datos digitales en un sistema de información, o inutilización del acceso a estos datos. También incluirá el robo de datos, fondos, recursos económicos o propiedad intelectual.

4) «Interceptación de datos»: interceptación, por medios técnicos, de transmisiones no públicas de datos digitales con origen o destino en un sistema de información o realizadas en el interior de un sistema de información, incluidas las emisiones electromagnéticas de un sistema de información que contenga dichos datos digitales.

Artículo 3

Los factores que determinan si un ciberataque tiene un efecto significativo a que se refiere el artículo 1, apartado 1, incluirán cualesquiera de los siguientes elementos:

a) el alcance, la escala, la repercusión, o la gravedad de la perturbación ocasionada, incluido en las actividades económicas y sociales, los servicios esenciales, las funciones vitales del Estado, el orden público o la seguridad pública;

b) el número de personas físicas o jurídicas, entidades u organismos afectados;

c) el número de Estados miembros afectados;

d) el importe de las pérdidas económicas ocasionadas, por ejemplo mediante un robo a gran escala de fondos, recursos económicos o propiedad intelectual; e) los beneficios económicos obtenidos por el autor, para sí o para otros;

f) la cantidad o la naturaleza de los datos sustraídos o la magnitud de las violaciones de datos; o

g) la naturaleza de los datos comercialmente sensibles a los que se haya tenido acceso.

Artículo 4

1. Los Estados miembros adoptarán las medidas necesarias para impedir la entrada o tránsito por sus territorios de las personas físicas:

   a) las personas físicas que sean responsables de los ciberataques o intentos de ciberataques;

   b) las personas físicas que presten ayuda financiera, técnica o material o que estén implicadas de alguna otra forma en ciberataques o tentativas de ciberataque, en particular mediante la planificación, preparación, dirección o fomento de dichos ataques, así como la participación en ellos o la ayuda a su comisión [o la facilitación de su comisión por acción u omisión];

   c) las personas físicas asociadas a las personas contempladas en las letras a) y b);

   y que se enumeran en el anexo.

2. El apartado 1 no obliga a los Estados miembros a denegar la entrada en su territorio a sus propios nacionales.

3. El apartado 1 se entiende sin perjuicio de aquellos casos en los que un Estado miembro esté obligado por una disposición de Derecho internacional, a saber:

   a) como país anfitrión de una organización internacional intergubernamental;

   b) como país anfitrión de una conferencia internacional convocada o auspiciada por las Naciones Unidas;

   c) en virtud de un acuerdo multilateral que confiera privilegios e inmunidades; o

   d) en virtud del Concordato de 1929 (Pacto de Letrán) celebrado entre la Santa Sede (Estado de la Ciudad del Vaticano) e Italia.

4. El apartado 3 también se considerará aplicable cuando un Estado miembro sea país anfitrión de la Organización para la Seguridad y la Cooperación en Europa (OSCE).

5. Se informará debidamente al Consejo en todos los casos en que un Estado miembro conceda una exención de conformidad con los apartados 3 o 4.

6. Los Estados miembros podrán conceder exenciones de las medidas impuestas en el apartado 1 cuando el viaje esté justificado por razones humanitarias urgentes o en razón de la asistencia a reuniones intergubernamentales, a reuniones promovidas u organizadas por la Unión, u organizadas por un Estado miembro que ejerza la Presidencia de la OSCE, en las que se mantenga un diálogo político que fomente directamente los objetivos políticos de las medidas restrictivas, incluidas la seguridad y la estabilidad del ciberespacio.

7. Los Estados miembros también podrán conceder exenciones respecto de las medidas impuestas en virtud del apartado 1 cuando la entrada o el tránsito sean necesarios para el desarrollo de un proceso judicial.

8. Todo Estado miembro que desee conceder las exenciones a que se refiere el apartado 6 o 7 lo notificará por escrito al Consejo. Se considerarán concedidas las exenciones a menos que uno o varios miembros del Consejo presenten objeciones por escrito antes de transcurridos dos días hábiles desde la recepción de la notificación de la exención propuesta. En caso de que algún miembro del Consejo formule una objeción, el Consejo, por mayoría cualificada, podrá decidir la concesión de la exención propuesta.

9. Cuando, en virtud de los apartados 3, 4, 6, 7 u 8, un Estado miembro autorice la entrada en su territorio o el tránsito por él de alguna de las personas enumeradas en el anexo, la autorización quedará estrictamente limitada a la finalidad para la cual fue concedida y a las personas a las que atañe directamente.

Artículo 5

1. Serán inmovilizados todos los fondos y recursos económicos cuya propiedad, titularidad, tenencia o control correspondan a:

   a) las personas físicas o jurídicas, entidades u organismos que sean responsables de los ciberataques o intentos de ciberataques;

   b) las personas físicas o jurídicas, entidades u organismos que presten ayuda financiera, técnica o material o que estén implicadas de alguna otra forma en ciberataques o tentativas de ciberataque, en particular mediante la planificación, preparación, participación en ellos, dirección, ayuda o fomento de dichos ataques, o la facilitación de su comisión por acción u omisión;

   c) las personas físicas o jurídicas, entidades u organismos asociadas con las personas físicas o jurídicas, entidades y organismos a que se refieren las letras a) y b),

   y que se enumeran en el anexo.

2. En ningún caso se pondrán fondos o recursos económicos a disposición directa o indirecta de las personas físicas o jurídicas, entidades u organismos enumerados en el anexo, ni se utilizarán en su beneficio.

3. Como excepción a lo dispuesto en los apartados 1 y 2, las autoridades competentes del Estado miembro podrán autorizar la liberación de ciertos fondos o recursos económicos inmovilizados, o la puesta a disposición de ciertos fondos o recursos económicos, en las condiciones que estimen oportunas, tras haber constatado que dichos fondos o recursos económicos:

a) son necesarios para satisfacer las necesidades básicas de las personas físicas enumeradas en el anexo y de los miembros de la familia que dependan de esas personas físicas, como el pago de alimentos, alquileres o hipotecas, medicamentos y tratamientos médicos, impuestos, primas de seguros y tasas de servicios públicos;

b) se destinan exclusivamente al pago de honorarios profesionales razonables o al reembolso de gastos correspondientes a la prestación de servicios jurídicos;

c) se destinan exclusivamente al pago de tasas o gastos ocasionados por servicios ordinarios de custodia o mantenimiento de fondos o recursos económicos inmovilizados;

d) son necesarios para sufragar gastos extraordinarios, siempre y cuando que la autoridad competente que corresponda haya notificado a las autoridades competentes de los demás Estados miembros y a la Comisión, al menos dos semanas antes de la autorización, los motivos por los cuales considera que debe concederse una autorización específica; o

e) se ingresan en la cuenta o se pagan con cargo a la cuenta de una misión diplomática o consular o de una organización internacional que goce de inmunidad con arreglo al Derecho internacional, en la medida en que dichos pagos estén destinados a ser utilizados para los fines oficiales de la misión diplomática o consular o de la organización internacional.

El Estado miembro de que se trate informará a los demás Estados miembros y a la Comisión de cualquier autorización concedida con arreglo al presente apartado.

4. Como excepción a lo dispuesto en el apartado 1, las autoridades competentes del Estado miembro podrán autorizar la liberación de determinados fondos o recursos económicos inmovilizados siempre que concurran las condiciones siguientes:

a) que los fondos o recursos económicos sean objeto de una resolución arbitral pronunciada antes de la fecha en que la persona física o jurídica, entidad u organismo a que se refiere el apartado 1 haya sido incluido en la lista del anexo, o de una resolución judicial o administrativa adoptada en la Unión, o de una resolución judicial con fuerza ejecutiva en el Estado miembro de que se trate, dictada antes o después de esa fecha;

b) que los fondos o recursos económicos vayan a utilizarse exclusivamente para satisfacer las demandas derivadas de tales resoluciones o reconocidas como válidas en ellas, en los límites establecidos por las disposiciones legales y reglamentarias aplicables a los derechos de las personas que presenten dichas demandas;

c) que la resolución no beneficie a ninguna de las personas físicas o jurídicas, entidades u organismos enumerados en el anexo; y

d) que el reconocimiento de la resolución no sea contrario al orden público en el Estado miembro de que se trate.

El Estado miembro de que se trate informará a los demás Estados miembros y a la Comisión de cualquier autorización concedida con arreglo al presente apartado.

5. El apartado 1 no impedirá que una persona física o jurídica, entidad u organismo incluido en el anexo pueda efectuar pagos adeudados en virtud de contratos suscritos antes de la fecha en que se haya incluido en el anexo a dicha persona física o jurídica, entidad u organismo, siempre y cuando el Estado miembro correspondiente haya considerado que el pago no es percibido directa ni indirectamente por una de las personas físicas o jurídicas, entidades u organismos a que se refiere el apartado 1.

6. El apartado 2 no se aplicará al ingreso en las cuentas inmovilizadas de:

a) intereses u otros beneficios correspondientes a dichas cuentas;

b) pagos en virtud de contratos o acuerdos celebrados u obligaciones contraídas antes de la fecha en que dichas cuentas hayan pasado a estar sujetas a las medidas reguladas en los apartados 1 y 2; o

c) pagos adeudados en virtud de una resolución judicial, administrativa o arbitral adoptada en la Unión, o que tenga fuerza ejecutiva en el Estado miembro de que se trate,

siempre que las medidas establecidas en el apartado 1 sigan siendo de aplicación a cualquiera de dichos intereses, otros beneficios y pagos.

Artículo 6

1. El Consejo, por unanimidad y a propuesta de un Estado miembro o de la Alta Representante de la Unión para Asuntos Exteriores y Política de Seguridad, establecerá y modificará la lista que figura en el anexo.

2. El Consejo comunicará la decisión a que se refiere el apartado 1, y los motivos de la inclusión en la lista, a la persona física o jurídica, entidad u organismo afectados, bien directamente, si se conoce su domicilio, o mediante la publicación de un anuncio, y ofrecerá a dicha persona física o jurídica, entidad u organismo la oportunidad de presentar observaciones al respecto.

3. Cuando se presenten observaciones o nuevas pruebas sustanciales, el Consejo reconsiderará la decisión a que se refiere el apartado 1 e informará en consecuencia a la persona física o jurídica, entidad u organismo afectados.

Artículo 7

1. El anexo incluirá los motivos de la inscripción en la lista de las personas físicas o jurídicas, entidades u organismos a que se refieren los artículos 4 y 5.

2. El anexo contendrá, cuando se disponga de ella, la información necesaria para identificar a las personas físicas o jurídicas, entidades u organismos de que se trate. Respecto de las personas físicas, esa información podrá incluir el nombre, apellidos y los alias, el lugar y fecha de nacimiento, la nacionalidad, el número de pasaporte o de documento de identidad, el sexo, la dirección, si se conoce, y el cargo o la profesión. En el caso de las personas jurídicas, entidades u organismos, la información podrá incluir el nombre, el lugar y la fecha de registro, el número de registro y el domicilio social.

Artículo 8

No se estimará demanda alguna relacionada con un contrato o transacción cuya ejecución se haya visto afectada, directa o indirectamente, total o parcialmente, por las medidas impuestas por la presente Decisión, incluidas las demandas de indemnización o cualquier otra pretensión de este tipo, tales como una demanda de compensación o una demanda a título de garantía, en particular cualquier demanda que tenga por objeto la prórroga o el pago de una fianza, una garantía o una indemnización, en particular financieras, independientemente de la forma que adopte, si la presentan:

a) personas físicas o jurídicas, entidades u organismos designados que figuren en la lista del anexo;

b) cualquier persona física o jurídica, entidad u organismo que actúe a través o en nombre de una de las personas físicas o jurídicas, entidades u organismos a que se refiere la letra a).

Artículo 9

Para que las medidas establecidas en la presente Decisión tengan el mayor impacto posible, la Unión animará a terceros Estados a que adopten medidas restrictivas similares a las establecidas en la presente Decisión.

Artículo 10

La presente Decisión será aplicable hasta el … [*un año después de la fecha de entrada en vigor de la presente Decisión*]y estará sujeta a revisión continua. Se prorrogará o modificará, según proceda, si el Consejo estima que no se han cumplido sus objetivos.

Artículo 11

La presente Decisión entrará en vigor el día siguiente al de su publicación en el *Diario Oficial de la Unión Europea.*

Hecho en Bruselas,

Por el Consejo
El Presidente

ANEXO

Lista de personas físicas o jurídicas, entidades y organismos a que se refieren los artículos 4 y 5

[…]