2024/2659

16.10.2024

RECOMENDACIÓN (UE) 2024/2659 DE LA COMISIÓN

de 11 de octubre de 2024

relativa a orientaciones sobre la exportación de productos de cibervigilancia con arreglo al artículo 5 del Reglamento (UE) 2021/821 del Parlamento Europeo y del Consejo

LA COMISIÓN EUROPEA,

Visto el Tratado de Funcionamiento de la Unión Europea, y en particular su artículo 292,

Considerando lo siguiente:

(1) El Reglamento (UE) 2021/821 del Parlamento Europeo y del Consejo ([1]) establece un régimen de la Unión de control de las exportaciones, el corretaje, la asistencia técnica, el tránsito y la transferencia de productos de doble uso.

(2) El Reglamento (UE) 2021/821 aborda el riesgo de que los productos de cibervigilancia se utilicen en relación con la represión interna o la comisión de graves violaciones de los derechos humanos y del Derecho internacional humanitario.

(3) De conformidad con el artículo 5, apartado 2, y el artículo 26, apartado 1, del Reglamento (UE) 2021/821, la Comisión y el Consejo han de facilitar a los exportadores orientaciones relativas a los productos de cibervigilancia no incluidos en la lista, habida cuenta de la necesidad de garantizar la eficacia del régimen de control de las exportaciones de la Unión en lo que respecta a la ciberseguridad, así como la aplicación coherente del Reglamento (UE) 2021/821.

(4) La presente Recomendación y las orientaciones adjuntas tienen por objeto apoyar a los exportadores en la aplicación de controles de productos de cibervigilancia que no figuran en la lista, incluidas, entre otras, medidas de diligencia debida para evaluar los riesgos relacionados con la exportación de dichos productos.

(5) Las orientaciones adjuntas a la presente Recomendación fueron objeto de amplias consultas en el Grupo de expertos en tecnología de vigilancia en 2022 y 2023 y tuvieron en cuenta las observaciones recibidas durante una consulta pública ([2]) que se celebró en el segundo trimestre de 2023.

(6) Cabe recordar que la presente Recomendación y las orientaciones adjuntas no son vinculantes. Por consiguiente, los exportadores deben seguir asumiendo la responsabilidad de cumplir las obligaciones que les incumben de conformidad con el Reglamento (UE) 2021/821, mientras que la Comisión debe velar por que la presente Recomendación siga siendo pertinente a lo largo del tiempo.

([1]) Reglamento (UE) 2021/821 del Parlamento Europeo y del Consejo, de 20 de mayo de 2021, por el que se establece un régimen de la Unión de control de las exportaciones, el corretaje, la asistencia técnica, el tránsito y la transferencia de productos de doble uso (DO L 206 de 11.6.2021, p. 1, ELI: http://data.europa.eu/eli/reg/2021/821/oj).

([2]) https://policy.trade.ec.europa.eu/consultations/guidelines-export-cyber-surveillance-items-under-article-5-regulation-eu-no-2021821_es.

HA ADOPTADO LA PRESENTE RECOMENDACIÓN:

Se recomienda que las autoridades competentes y los exportadores de los Estados miembros tengan en cuenta las orientaciones que figuran en el anexo de la presente Recomendación a fin de cumplir las obligaciones que les incumben de conformidad con el artículo 5, apartado 2, del Reglamento (UE) 2021/821.

Hecho en Bruselas, el 11 de octubre de 2024.

Por la Comisión
Valdis DOMBROVSKIS
Vicepresidente ejecutivo

ANEXO

ÍNDICE

INTRODUCCIÓN

El marco de control de las exportaciones de la Unión establecido por el Reglamento (UE) 2021/821 («el Reglamento») tiene por objeto garantizar el cumplimiento de las obligaciones y compromisos internacionales de la Unión y de sus Estados miembros, en particular en lo que respecta a la paz, la seguridad y la estabilidad regionales y al respeto de los derechos humanos y del Derecho internacional humanitario. Por consiguiente, la Unión y sus Estados miembros han aplicado las decisiones tomadas en los regímenes multilaterales de control de las exportaciones y han actualizado en consecuencia la lista de control de la Unión que figura en el anexo I del Reglamento ([1]). Además, antes de que fuera aplicable el artículo 5 del Reglamento, las autoridades competentes de los Estados miembros ya habían controlado la exportación de determinados productos incluidos en la lista que podían tener aplicaciones de vigilancia ([2]), teniendo en cuenta los riesgos de uso indebido en determinadas circunstancias específicas. En casos de circunstancias excepcionalmente graves, la Unión ha impuesto sanciones que restringen la exportación de determinados equipos de vigilancia ([3]).

El Reglamento refleja el compromiso de la Unión de abordar el riesgo de que los productos de cibervigilancia se utilicen en relación con la represión interna o la comisión de graves violaciones de los derechos humanos y del Derecho internacional humanitario. En particular, el Reglamento introduce nuevas disposiciones para el control de las exportaciones de productos de cibervigilancia que no figuran en la lista, incluida la obligación de que los exportadores notifiquen a la autoridad competente cuando tengan conocimiento, basándose en sus averiguaciones de diligencia debida, de que los productos de cibervigilancia no incluidos en la lista que los exportadores proponen exportar están destinados, total o parcialmente, a un uso relacionado con la represión interna o la comisión de graves violaciones de los derechos humanos y del Derecho internacional humanitario. En el Reglamento se solicita además a la Comisión y al Consejo que faciliten orientaciones a los exportadores para respaldar la aplicación eficaz de los nuevos controles de los productos de cibervigilancia no incluidos en la lista.

Por lo tanto, estas orientaciones tienen por objeto apoyar a los exportadores en la aplicación de controles de productos de cibervigilancia que no figuran en la lista, incluidas, entre otras, medidas de diligencia debida para evaluar los riesgos relacionados con la exportación de dichos productos a usuarios finales y para usos finales con arreglo a las nuevas disposiciones del Reglamento.

1. DISPOSICIONES JURÍDICAS PERTINENTES, DEFINICIONES Y CONCEPTOS CLAVE

1.1. Resumen de las disposiciones jurídicas pertinentes

El Reglamento introduce nuevas disposiciones específicas sobre los controles de las exportaciones de productos de cibervigilancia no incluidos en la lista del anexo I del Reglamento que estén destinados o puedan destinarse, total o parcialmente, a un uso relacionado con la represión interna o la comisión de graves violaciones de los derechos humanos y del Derecho internacional humanitario. Los considerandos y artículos pertinentes son los siguientes:

a) el considerando 8: «Con el fin de abordar el riesgo de que determinados productos de cibervigilancia no enumerados y exportados desde el territorio aduanero de la Unión puedan ser usados indebidamente por cómplices o responsables de dirigir o cometer violaciones graves de los derechos humanos o del Derecho internacional humanitario, conviene someter a control la exportación de dichos productos. Los riesgos asociados se refieren, en particular, a los casos en que los productos de cibervigilancia estén diseñados especialmente para permitir la intrusión o la inspección profunda

([1]) Véanse, en particular, los controles relativos a los sistemas de interceptación de telecomunicaciones (5A001.f), los sistemas de vigilancia de internet (5A001.j), los programas informáticos de intrusión (4A005, 4D004 y controles conexos con arreglo a los subartículos 4E001.a y 4E001.c) y los programas informáticos de vigilancia para hacer cumplir la legislación (5D001.e). Véanse, además, sobre la base de una evaluación caso por caso, los controles relativos a determinadas herramientas forenses o de investigación (5A004.b, 5D002.a.3.b y 5D002.c.3.b).

([2]) En particular, los sistemas de seguridad de la información.

([3]) Véanse el Reglamento (CE) n.º 765/2006 del Consejo, de 18 de mayo de 2006, relativo a la adopción de medidas restrictivas habida cuenta de la situación en Bielorrusia y la participación de este país en la agresión rusa contra Ucrania (DO L 134 de 20.5.2006, p. 1, ELI: http://data.europa.eu/eli/reg/2006/765/oj); el Reglamento (UE) n.º 359/2011 del Consejo, de 12 de abril de 2011, relativo a las medidas restrictivas dirigidas contra determinadas personas, entidades y organismos habida cuenta de la situación en Irán (DO L 100 de 14.4.2011, p. 1, ELI: http://data.europa.eu/eli/reg/2011/359/oj); el Reglamento (UE) n.º 36/2012 del Consejo, de 18 de enero de 2012, relativo a las medidas restrictivas habida cuenta de la situación en Siria y por el que se deroga el Reglamento (UE) n.º 442/2011 (DO L 16 de 19.1.2012, p. 1, ELI: http://data.europa.eu/eli/reg/2012/36/oj); el Reglamento (UE) n.º 401/2013 del Consejo, de 2 de mayo de 2013, relativo a medidas restrictivas habida cuenta de la situación en Myanmar/Birmania y por el que se deroga el Reglamento (CE) n.º 194/2008 (DO L 121 de 3.5.2013, p. 1, ELI: http://data.europa.eu/eli/reg/2013/401/oj); y el Reglamento (UE) 2017/2063 del Consejo, de 13 de noviembre de 2017, relativo a medidas restrictivas habida cuenta de la situación en Venezuela (DO L 295 de 14.11.2017, p. 21, ELI: http://data.europa.eu/eli/reg/2017/2063/oj).

de paquetes en sistemas de información y telecomunicaciones con el fin de llevar a cabo una vigilancia encubierta de las personas físicas mediante el seguimiento, la extracción, la recogida o el análisis de datos, incluidos datos biométricos, de dichos sistemas. Por lo general, los productos utilizados para aplicaciones puramente comerciales, como la facturación, la comercialización, los servicios de calidad, la satisfacción de los usuarios o la seguridad de la red, no se considera que conlleven tales riesgos»;

b) el considerando 9: «Con miras a reforzar el control eficaz de las exportaciones de productos de cibervigilancia no enumerados, es esencial armonizar en mayor medida la aplicación de controles universales en este ámbito. A tal fin, los Estados miembros se han comprometido a apoyar dichos controles compartiendo información entre sí y con la Comisión, en particular en lo que se refiere a los avances tecnológicos de los productos de cibervigilancia, y vigilando la aplicación de dichos controles para promover un intercambio a escala de la Unión»;

c) el artículo 2, punto 20, que establece la siguiente definición de «productos de cibervigilancia»: «productos de doble uso especialmente diseñados para permitir la vigilancia encubierta de personas físicas mediante el seguimiento, la extracción, la recogida o el análisis de datos procedentes de sistemas de información y telecomunicación»;

d) el artículo 5 introduce un requisito de autorización para la exportación de productos de cibervigilancia no incluidos en la lista cuando el exportador haya sido informado por la autoridad competente del Estado miembro de que se trata de productos destinados o que pueden destinarse, total o parcialmente, a un uso relacionado con la represión interna o la comisión de graves violaciones de los derechos humanos y del Derecho internacional humanitario (artículo 5, apartado 1); además, exige a los exportadores que informen a la autoridad competente cuando tengan conocimiento, basándose en sus averiguaciones de diligencia debida, de que los productos están destinados, total o parcialmente, a un uso relacionado con la represión interna o la comisión de graves violaciones de los derechos humanos y del Derecho internacional humanitario (artículo 5, apartado 2); esta última debe decidir si se ha de someter a autorización la exportación de que se trate; y

e) el artículo 5, apartado 2, establece además que «la Comisión y el Consejo facilitarán a los exportadores las orientaciones a que se refiere el artículo 26, apartado 1».

1.2. **Definiciones clave**

El Reglamento contiene determinados considerandos y disposiciones en los que se aclaran términos específicos pertinentes para los controles de las exportaciones de productos de cibervigilancia no incluidos en la lista, y que es importante que los exportadores entiendan con claridad de cara a llevar a cabo la diligencia debida y aplicar los controles de manera eficaz. Cabe destacar la definición precisa de «productos de cibervigilancia» que se establece en el artículo 2, punto 20: «productos de doble uso especialmente diseñados para permitir la vigilancia encubierta de personas físicas mediante el seguimiento, la extracción, la recogida o el análisis de datos procedentes de sistemas de información y telecomunicación».

A efectos de las presentes orientaciones, deben aclararse algunos aspectos específicos de dicha definición.

1.2.1. *«Diseñado especialmente»*

Un producto está diseñado para la vigilancia encubierta cuando sus características técnicas son adecuadas para la vigilancia encubierta de personas físicas y permiten objetivamente que se lleve a cabo. Por lo tanto, el término «diseñado especialmente» significa que la vigilancia encubierta de personas físicas tiene que haber sido el objetivo principal del desarrollo y diseño del producto. No obstante, este término no exige que el producto pueda utilizarse únicamente para la vigilancia encubierta de personas físicas.

Como se aclara en el considerando 8 del Reglamento, los productos utilizados para aplicaciones puramente comerciales, como la facturación, la comercialización, los servicios de calidad, la satisfacción de los usuarios o la seguridad de la red, no están diseñados especialmente para la vigilancia encubierta de personas físicas y, por consiguiente, no entran en la definición de los productos de cibervigilancia. Por ejemplo, si bien los productos destinados a vigilar los sistemas operativos en la industria o a realizar un seguimiento del tráfico de los usuarios pueden emplearse con fines de vigilancia, no se trata de productos de cibervigilancia contemplados en la definición, dado que no están diseñados especialmente para permitir la vigilancia encubierta de personas físicas.

1.2.2. *«Vigilancia encubierta»*

Se considera, en particular, que un producto permite llevar a cabo una vigilancia encubierta cuando la persona física afectada no puede percibir la vigilancia de manera obvia. Este sería el caso cuando las personas afectadas no tienen conocimiento de la presencia o la acción de productos de cibervigilancia y, por tanto, no tienen la oportunidad de ocultarse de dicha vigilancia o, al menos, de ajustar su comportamiento en consecuencia. Incluso si la vigilancia se lleva a cabo por medio de productos instalados o que funcionan en el espacio público, en determinados casos la adquisición de datos puede considerarse pertinente para la vigilancia encubierta; en particular, los datos recogidos pueden desviarse, evaluarse o tratarse para fines distintos de aquellos de los que la persona física en cuestión tenga conocimiento. En otras palabras, cuando una persona física no puede esperar objetivamente encontrarse bajo vigilancia, la vigilancia puede considerarse encubierta en el sentido del artículo 2, punto 20, del Reglamento.

1.2.3. *«Personas físicas»*

El término «personas físicas» se refiere a los seres humanos vivos, por oposición a las personas jurídicas o entidades, que, por consiguiente, no están sujetas a las disposiciones. El término no incluye la vigilancia de objetos, lugares o máquinas como tales.

1.2.4. *«Seguimiento, extracción, recogida, análisis de datos»*

Según el *Diccionario de la lengua española*, los verbos correspondientes a estas acciones, esto es, «seguir», «extraer», «recoger» y «analizar», tienen el significado lingüístico siguiente:

— «seguir»: observar atentamente el curso de un negocio o los movimientos de alguien o algo;

— «extraer»: sacar;

— «recoger»: juntar o congregar personas o cosas separadas o dispersas;

— «analizar»: someter algo a un análisis (definición de «análisis», según el mismo *Diccionario*: distinción y separación de las partes de algo para conocer su composición; estudio detallado de algo […]).

Estos términos implican que los productos utilizados para la vigilancia deben contar con capacidades técnicas precisas para el tratamiento de datos con el fin de llevar a cabo las acciones de seguimiento, recogida, extracción o análisis de los datos, como, por ejemplo, los siguientes productos:

a) productos utilizados para el seguimiento de los datos de sistemas de información y telecomunicación ([4]) (por ejemplo, el tamaño de los archivos o el tráfico de los paquetes de datos transmitidos en dicho sistema);

b) productos que extraen datos de sistemas de información y telecomunicación mediante intrusión y extracción (por ejemplo, programas informáticos de intrusión);

c) productos que permiten analizar los datos extraídos de sistemas de información y telecomunicación, incluidos los que pueden procesar imágenes de cámara almacenadas en dichos sistemas (por ejemplo, determinados tipos de tecnologías de análisis de datos utilizadas como parte de los sistemas de reconocimiento facial).

Los productos que se utilizan simplemente para el seguimiento de los sistemas de información o para observar a la población a través de cámaras de videovigilancia y que permiten captar conversaciones, intercambios de datos, movimientos y comportamientos individuales no entrarían en la definición de «productos de cibervigilancia» que establece el Reglamento, ya que no están diseñados especialmente para ese fin y tienen que trabajar con otras tecnologías, como las de la inteligencia artificial o los macrodatos. Sin embargo, el sistema en su integridad (trabajando conjuntamente con otras tecnologías como las de la inteligencia artificial o los macrodatos) podría ser un producto de cibervigilancia que entrase en la definición del artículo 2, punto 20, del Reglamento.

Es importante señalar que, aunque se ofrecen algunos ejemplos útiles a título ilustrativo, la definición y el alcance de los productos de cibervigilancia no se ven limitados por esos ejemplos, ya que el objetivo del artículo 5 es permitir un control eficaz de las exportaciones de productos no incluidos en la lista.

([4]) Véase la definición en el punto 1.2.5.

Como demuestra el uso de la conjunción «o» en la definición, las capacidades técnicas que se establecen han de considerarse alternativas, y no es necesario que un producto disponga de todas esas capacidades técnicas para llevar a cabo el seguimiento, la extracción, la recogida o el análisis de datos. En otras palabras, basta con que un producto tenga una de esas capacidades técnicas para entrar en la definición de «producto de cibervigilancia» que se establece en el artículo 2, punto 20.

1.2.5. *«De sistemas de información y telecomunicación»*

Estos términos se refieren a sistemas que procesan la información electrónicamente, por ejemplo, mediante programación o codificación, operaciones del sistema PC (*hardware*) y otras formas de administración de la información, incluida la tecnología de *software*, la tecnología web, la tecnología informática, la tecnología de almacenamiento, etc.; se refieren asimismo a algunos sistemas que transmiten información a distancia, por ejemplo, sistemas técnicos que transmiten sonidos, señales, texto, otros signos e imágenes a través de canales tanto alámbricos como inalámbricos, a través de fibras ópticas, radio y otros sistemas electromagnéticos. En conjunto, estos dos conceptos abarcan una amplia gama de sistemas de transmisión o tratamiento de la información. Cabe señalar que el término se refiere a sistemas y no a equipos.

1.2.6. *«Conocimiento» y «están destinados a»*

De conformidad con el artículo 5, apartado 2, del Reglamento, el exportador debe notificar a la autoridad competente cuando «tenga conocimiento de que los productos de cibervigilancia […] están destinados […] a un uso relacionado con la represión interna o la comisión de graves violaciones de los derechos humanos y del Derecho internacional humanitario».

El término «conocimiento» no constituye un nuevo concepto jurídico, sino que se ha utilizado en lo relativo a los requisitos de autorización relacionados con el uso final (los denominados controles «genéricos») con arreglo a los artículos 4, 6, 7 y 8 del Reglamento. Tener «conocimiento» implica que el exportador es efectivamente consciente del uso indebido previsto. La mera posibilidad de que tal riesgo exista no basta para demostrar el conocimiento. Sin embargo, el término «conocimiento» no puede asimilarse a la pasividad: exige que el exportador haya tomado medidas para obtener un conocimiento suficiente y adecuado de cara a evaluar los riesgos relacionados con la exportación y para garantizar el cumplimiento del Reglamento.

La indicación de que los productos deben «estar destinados a» un uso final sensible pertinente implica que el exportador debe evaluar el uso final caso por caso, teniendo en cuenta las circunstancias específicas del caso de que se trate. En cambio, un riesgo teórico, es decir, que no esté basado en una evaluación fáctica del caso, de que los productos puedan utilizarse de un modo que viole los derechos humanos no bastaría para suponer que «estén destinados a» un uso indebido específico con arreglo al artículo 5.

1.3. **Represión interna, graves violaciones de los derechos humanos y del Derecho internacional humanitario**

De conformidad con el artículo 15 del Reglamento, que establece las consideraciones para la evaluación de una autorización, los Estados miembros han de tener en cuenta todas las consideraciones pertinentes, incluidas las contempladas en la Posición Común 2008/944/PESC del Consejo ([5]).

El artículo 5 del Reglamento amplía los controles a la exportación de productos de cibervigilancia no incluidos en la lista, teniendo en cuenta el riesgo de que se utilicen en relación con la represión interna o la comisión de graves violaciones de los derechos humanos y del Derecho internacional humanitario. La Posición Común 2008/944/PESC y la Guía del Usuario para dicha Posición Común ([6]) proporcionan orientaciones útiles a este respecto.

([5]) Posición Común 2008/944/PESC del Consejo, de 8 de diciembre de 2008, por la que se definen las normas comunes que rigen el control de las exportaciones de tecnología y equipos militares (DO L 335 de 13.12.2008, p. 99, ELI: http://data.europa.eu/eli/compos/2008/944/oj).

([6]) Véase la Guía del Usuario para la Posición Común 2008/944/PESC del Consejo, por la que se definen las normas comunes que rigen el control de las exportaciones de tecnología y equipos militares, https://data.consilium.europa.eu/doc/document/ST-12189-2019-INIT/es/pdf.

1.3.1. *Represión interna*

De conformidad con el artículo 2, apartado 2, de la Posición Común 2008/944/PESC, «[s]e considerará represión interna, entre otras cosas, la tortura y otros tratos o penas crueles, inhumanos y degradantes, las ejecuciones sumarias o arbitrarias, las desapariciones, las detenciones arbitrarias y toda violación grave de los derechos humanos y de las libertades fundamentales definidos en los instrumentos internacionales pertinentes de derechos humanos, incluida la Declaración Universal de los Derechos Humanos y el Pacto Internacional de Derechos Civiles y Políticos». La Guía del Usuario para la Posición Común 2008/944/PESC ofrece orientaciones sobre los elementos que deben tenerse en cuenta en la evaluación del exportador, incluidos los «antecedentes del usuario final propuesto en materia de derechos humanos y los del país receptor en general».

1.3.2. *Comisión de violación grave de los derechos humanos*

El uso indebido de productos de cibervigilancia no incluidos en la lista puede afectar negativamente a un amplio espectro de derechos humanos e interferir directamente en el derecho a la intimidad y a la protección de datos. La vigilancia arbitraria o ilegal también puede vulnerar otros derechos humanos, como el derecho a la libertad de expresión, asociación y reunión, la libertad de pensamiento, conciencia y religión, así como el derecho a la igualdad de trato o la prohibición de discriminación, y el derecho a unas elecciones libres, equitativas y secretas. En determinados casos, la vigilancia —incluido el seguimiento o la recogida de información— de las personas físicas, por ejemplo, de defensores de los derechos humanos, activistas, personalidades políticas, poblaciones vulnerables y periodistas, puede conducir a la intimidación, represión, detención arbitraria, tortura o incluso a ejecuciones extrajudiciales. Por lo tanto, los exportadores deben incluir en sus evaluaciones estos aspectos relacionados con violaciones graves de los derechos humanos.

La práctica internacional muestra que cualquier restricción de los derechos humanos debe ser «adecuada» y conforme a las normas internacionales en materia de derechos humanos. En la práctica, esto significa que existen garantías adecuadas para asegurar que las restricciones están establecidas por la ley y preservan la esencia de los derechos. Dentro del respeto del principio de proporcionalidad, solo pueden introducirse restricciones cuando sean necesarias y respondan efectivamente a un fin legítimo, como la seguridad nacional o pública, el orden público, la protección de la salud pública o la protección de los derechos y libertades de terceros.

Los productos de cibervigilancia pueden incluir herramientas legítimas y reglamentadas para hacer cumplir la legislación, por ejemplo, para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales, en particular en el ámbito de la lucha contra el terrorismo, o para la ejecución de sanciones penales. Al mismo tiempo, también puede realizarse un uso indebido de los productos de cibervigilancia para cometer graves violaciones de los derechos humanos y del Derecho internacional humanitario cuando se exportan a regímenes represivos o usuarios finales privados o a zonas de conflicto.

Esto requiere una evaluación individualizada de las circunstancias de cada caso, incluida la aplicación de la normativa pertinente a la luz de cualquier constatación realizada, por ejemplo, por los órganos competentes de las Naciones Unidas, la Unión o el Consejo de Europa en la que se hayan señalado graves violaciones de los derechos humanos. Un indicio de la «gravedad» de las violaciones de los derechos humanos puede ser el reconocimiento de dichas violaciones en la información publicada por los órganos competentes de las Naciones Unidas, por la Unión o por el Consejo de Europa. Tal reconocimiento explícito por parte de los organismos citados no se considera una condición absolutamente necesaria, pero constituye un factor importante para que se cumplan los criterios.

Según los términos del artículo 5, la violación de los derechos humanos ha de ser «grave». En la Guía del Usuario para la Posición Común 2008/944/PESC figuran orientaciones útiles para clasificar como «graves» posibles violaciones de los derechos humanos. Según dicha Guía, la naturaleza y las consecuencias de la violación son determinantes. Por lo general, las violaciones sistemáticas o generalizadas de los derechos humanos se consideran «graves», pero las violaciones que no sean sistemáticas o generalizadas también pueden considerarse «graves», por ejemplo, debido a la gravedad de la intervención para las personas afectadas.

El anexo II de la Guía del Usuario para la Posición Común 2008/944/PESC contiene una lista no exhaustiva de los principales instrumentos internacionales y regionales de derechos humanos, incluidos el Pacto Internacional de Derechos Civiles y Políticos, la Convención contra la Tortura y Otros Tratos o Penas Crueles, Inhumanos o Degradantes, el Convenio Europeo de Derechos Humanos (el Convenio) y la Carta de los Derechos Fundamentales (la Carta), que pueden proporcionar orientaciones importantes para la interpretación y aplicación de criterios que respalden evaluaciones sólidas en materia de derechos humanos. Tales instrumentos y sus respectivos protocolos adicionales representan las principales normas y pautas internacionales en el ámbito de los derechos humanos y las libertades fundamentales.

1.3.3. *Comisión de violación grave del Derecho internacional humanitario*

El Derecho internacional humanitario (también denominado «Derecho de Ginebra» o «Derecho aplicable a los conflictos armados») se ha desarrollado a través de un conjunto de tratados internacionales, de los cuales los más importantes son el Reglamento de La Haya, los Convenios de Ginebra y sus dos protocolos adicionales de 1977, y establece normas que, en tiempos de conflicto armado, sirven para proteger a las personas que no participan o han dejado de participar en las hostilidades (por ejemplo, civiles y combatientes heridos, enfermos o capturados) y para imponer limitaciones a las partes beligerantes en cuanto a los medios y métodos de guerra (Derecho de La Haya).

El uso de productos de cibervigilancia no incluidos en la lista debe ajustarse al Derecho internacional humanitario cuando se utilicen como medios y métodos de guerra en el contexto de un conflicto armado. En tales circunstancias, el riesgo de violación grave del Derecho internacional humanitario es un aspecto que debe considerarse con arreglo al Reglamento y, al igual que en el caso de la comisión de graves violaciones de los derechos humanos, debe evaluarse teniendo en cuenta el uso final previsto para los productos en el caso concreto. La Guía del Usuario para la Posición Común 2008/944/PESC ofrece orientaciones sobre los elementos que deben tenerse en cuenta, entre ellos, el comportamiento pasado y presente del receptor en materia de respeto del Derecho internacional humanitario, las intenciones expresadas por el receptor en compromisos oficiales y la capacidad del receptor para garantizar que los equipos o tecnología transferidos se utilicen con arreglo al Derecho internacional humanitario y que no se desvíen o transfieran a otros destinos donde puedan usarse para cometer violaciones graves de este Derecho.

De conformidad con el artículo 5, la violación del Derecho internacional humanitario ha de ser «grave». Pueden encontrarse orientaciones en la Guía del Usuario para la Posición Común 2008/944/PESC, en la que se reconoce que «[l]os casos aislados de violaciones del Derecho internacional humanitario no son necesariamente indicativos de la actitud de un país determinado respecto del Derecho internacional humanitario», mientras que «[l]o que sí debe ser motivo de grave inquietud, en cambio, es la existencia de una constancia en esas violaciones o el hecho de que el país en cuestión no haya tomado las medidas necesarias para sancionarlas». El Comité Internacional de la Cruz Roja (CICR) ha proporcionado directrices con respecto a la evaluación de las violaciones del Derecho internacional humanitario a efectos del control de las exportaciones. Según el CICR, «las violaciones del Derecho internacional humanitario son graves si ponen en peligro a personas protegidas (por ejemplo, civiles, prisioneros de guerra, heridos o enfermos) o bienes protegidos (por ejemplo, bienes o infraestructuras civiles) o si infringen valores universales importantes». Los crímenes de guerra, por ejemplo, constituyen violaciones graves del Derecho internacional humanitario. El CICR menciona además algunos factores que deben considerarse similares a los que se citan en la Guía del Usuario para la Posición Común 2008/944/PESC, incluidos los compromisos formales de aplicar las normas del Derecho internacional humanitario, las medidas adecuadas para garantizar la obligación de rendir cuentas en caso de violación del Derecho internacional humanitario, la formación de los militares en materia de Derecho internacional humanitario y la prohibición de reclutar niños para las fuerzas armadas.

2. ÁMBITO DE APLICACIÓN TÉCNICO

2.1. Productos de cibervigilancia incluidos en la lista

El apéndice de estas orientaciones proporciona información sobre los productos de cibervigilancia incluidos en la lista del anexo I del Reglamento para ayudar a los exportadores a determinar posibles productos de cibervigilancia no incluidos en la lista.

2.2. Posibles productos de cibervigilancia no incluidos en la lista

Aunque, por definición, es imposible proporcionar una lista exhaustiva de los productos que pueden ser controlados como «productos no incluidos en la lista» con arreglo al artículo 5, los siguientes productos podrían tener un potencial de vigilancia y pueden justificar una vigilancia especial de conformidad con el Reglamento.

Como se aclara en el considerando 8 del Reglamento, por lo general, se considera que los productos utilizados para aplicaciones puramente comerciales, como la facturación, la comercialización, los servicios de calidad, la satisfacción de los usuarios o la seguridad de la red, no conllevan riesgos importantes de uso indebido en el marco de graves violaciones de los derechos humanos o del Derecho internacional humanitario y, por lo tanto, generalmente no están sujetos a los controles contemplados en el artículo 5. Muchos de estos productos cuentan con funcionalidades de seguridad de la información (criptográficas o incluso criptoanalíticas) que cumplen los parámetros de control establecidos en el texto sobre los controles, categoría 5, parte 2, del anexo I del Reglamento. Los equipos de redes de seguridad —incluidos los enrutadores, conmutadores o relés en los que la funcionalidad de seguridad de la información se limita a las tareas de «operación, administración o mantenimiento» que únicamente apliquen normas de cifrado comerciales o que hayan sido publicadas— tampoco están incluidos en la definición de «productos de cibervigilancia», pero los exportadores deben permanecer alerta, teniendo en cuenta que existen diversos informes sobre el uso indebido de este tipo de productos para cometer violaciones de los derechos humanos.

2.2.1. *Tecnología de reconocimiento facial y de emociones*

Las tecnologías de reconocimiento facial y de emociones tienen múltiples usos distintos de la cibervigilancia (por ejemplo, se emplean con fines de identificación o autenticación), por lo que no entrarían automáticamente en la definición. Sin embargo, en determinadas circunstancias, las tecnologías de reconocimiento facial y de emociones pueden entrar en la definición establecida en el artículo 2, punto 20, del Reglamento.

Las tecnologías de reconocimiento facial y de emociones que pueden utilizarse para realizar el seguimiento o el análisis de imágenes de vídeo almacenadas podrían entrar en el ámbito de la definición de «productos de cibervigilancia». Sin embargo, aunque se cumplan los criterios antes mencionados, ha de examinarse con detenimiento si el programa informático está diseñado especialmente para la vigilancia encubierta.

2.2.2. *Dispositivos de seguimiento de la ubicación*

Los dispositivos de seguimiento de la ubicación permiten rastrear la ubicación física de un dispositivo a lo largo del tiempo; las fuerzas y cuerpos de seguridad y los servicios de inteligencia emplean algunas tecnologías de seguimiento de la ubicación desde hace cierto tiempo. Su potencial para la vigilancia selectiva y masiva ha evolucionado considerablemente, ya que se han logrado avances en lo referente a las tecnologías de seguimiento —incluido el seguimiento de la ubicación por satélite, el seguimiento de la ubicación basándose en torres de telefonía móvil, los transceptores wifi y Bluetooth— y que los «dispositivos de seguimiento», como los teléfonos inteligentes y otros dispositivos electrónicos (por ejemplo, los sistemas integrados en los vehículos), se han generalizado.

Las fuerzas y cuerpos de seguridad y los servicios de inteligencia emplean dispositivos de seguimiento de la ubicación, por ejemplo, para recopilar pruebas en el curso de una investigación o para seguir a los sospechosos, pero las empresas también los utilizan con fines comerciales, tales como informar sobre patrones de movimiento agregados en las calles comerciales, realizar el seguimiento de los empleados que trabajan fuera de las instalaciones de la empresa u ofrecer publicidad basada en la ubicación.

2.2.3. *Sistemas de videovigilancia*

Con el fin de ayudar a los exportadores a detectar una posible cibervigilancia, cabe asimismo aclarar qué productos no entrarían en la definición. En este sentido, por ejemplo, los sistemas y las cámaras de videovigilancia, incluidas las cámaras de alta resolución, utilizados para grabar a personas en espacios públicos no entran en la definición de «productos de cibervigilancia», ya que no realizan un seguimiento ni recogen datos de sistemas de información y telecomunicación.

3. MEDIDAS DE DILIGENCIA DEBIDA

De conformidad con el considerando 7 del Reglamento, «[l]a contribución de los exportadores […] al objetivo general de los controles comerciales es crucial. Para que puedan actuar de conformidad con el presente Reglamento, la evaluación de los riesgos relacionados con las transacciones a que se refiere el presente Reglamento debe llevarse a cabo a través de medidas de comprobación de transacciones, también conocidas como el principio de diligencia debida, que formen parte de un programa interno de cumplimiento (PIC)».

En el artículo 2, punto 21, se define «programa interno de cumplimiento» o «PIC» como las «políticas y procedimientos en curso eficaces, adecuados y proporcionados, adoptados por los exportadores para facilitar el cumplimiento de las disposiciones y los objetivos del presente Reglamento y las condiciones de autorización aplicadas en virtud del presente Reglamento, incluidas, entre otras, medidas de diligencia debida para evaluar los riesgos relacionados con la exportación de los productos a usuarios finales y para usos finales».

La Recomendación (UE) 2019/1318 de la Comisión ([7]) ofrece un marco para ayudar a los exportadores a detectar, gestionar y mitigar los riesgos asociados a los controles del comercio de productos de doble uso y para garantizar el cumplimiento de las leyes y reglamentos pertinentes nacionales y de la Unión.

Estas orientaciones pueden ayudar a los exportadores en la puesta en marcha de medidas de comprobación de transacciones, también conocidas como «principio de diligencia debida», en el marco de un PIC.

Con arreglo al artículo 5, apartado 2, del Reglamento (UE) 2021/821, los exportadores de productos de cibervigilancia no incluidos en la lista deben actuar con la diligencia debida a través de medidas de comprobación de transacciones, es decir, adoptando medidas relativas a la clasificación de los productos y la evaluación del riesgo de las transacciones. En la práctica, se anima a los exportadores a revisar los aspectos siguientes:

([7]) Recomendación (UE) 2019/1318 de la Comisión, de 30 de julio de 2019, relativa a los programas internos de cumplimiento para los controles del comercio de productos de doble uso de conformidad con el Reglamento (CE) n.º 428/2009 (DO L 205 de 5.8.2019, p. 15, ELI: http://data.europa.eu/eli/reco/2019/1318/oj).

3.1. **Evaluar si el producto no incluido en la lista que se va a exportar puede ser un «producto de cibervigilancia», es decir, diseñado especialmente para permitir la vigilancia encubierta de personas físicas a través del seguimiento, la extracción, la recogida o el análisis de datos de sistemas de información y telecomunicación.**

Esta etapa se refiere a la determinación del producto con arreglo a las disposiciones aplicables a los productos de cibervigilancia. Esto incluye un examen de las características técnicas de los productos, sobre la base de los parámetros técnicos establecidos en el anexo I del Reglamento para los productos incluidos en la lista y a la luz de los términos y conceptos específicos que figuran en la definición de «productos de cibervigilancia» para los productos no incluidos en la lista, y la subsecuente clasificación del producto (bienes, tecnología o programas informáticos).

3.2. **Examinar las capacidades del producto en cuestión para determinar la posibilidad de un uso indebido relacionado con la represión interna o la comisión de graves violaciones de los derechos humanos y del Derecho internacional humanitario por parte de usuarios finales extranjeros.**

Los exportadores deben llevar a cabo una evaluación a fin de determinar si el producto podría utilizarse indebidamente para cometer actos de represión interna, violar o vulnerar los derechos humanos, entre ellos, el derecho a la vida, a no sufrir tortura ni tratos inhumanos y degradantes, el derecho a la intimidad, el derecho a la libertad de expresión, el derecho de asociación y reunión, el derecho a la libertad de pensamiento, de conciencia y de religión, el derecho a la igualdad de trato o la prohibición de la discriminación, o el derecho a unas elecciones libres, equitativas y secretas.

Asimismo, han de realizar una evaluación para determinar si el producto puede utilizarse como parte o componente de un sistema que podría dar lugar a las mismas violaciones o usos indebidos.

En su evaluación, los exportadores tienen que emplear las denominadas «señales de alerta», que hacen referencia a cualquier circunstancia anormal en una transacción que indique que la exportación puede estar destinada a un uso final, un usuario final o un destino inadecuados.

Señales de alerta:

a) el producto se comercializa con información relativa a la posibilidad de emplearlo con fines de vigilancia encubierta;

b) información que indique que se ha utilizado indebidamente un producto similar en relación con la represión interna o la comisión de graves violaciones de los derechos humanos y del Derecho internacional humanitario (véase la sección 1.3);

c) información que indique que el producto se ha utilizado ilegalmente en actividades de vigilancia dirigidas contra un Estado miembro o en relación con la vigilancia ilegal de un ciudadano de la UE;

d) información que indique que la transacción incluye productos que podrían utilizarse para establecer, personalizar o configurar un sistema que se sabe que se utiliza indebidamente en relación con la represión interna o la comisión de violaciones graves de los derechos humanos y del Derecho internacional humanitario (véase la sección 1.3);

e) el producto, o uno similar, figura en la lista publicada en la serie C del *Diario Oficial de la Unión Europea* de conformidad con el artículo 5, apartado 6, del Reglamento.

3.3. **Con el fin de apoyar a las autoridades competentes, examinar a las partes interesadas que participan en la transacción (incluidos los usuarios finales y los destinatarios, como distribuidores y revendedores).**

Para apoyar a las autoridades competentes, y en la medida de lo posible, los exportadores deberán:

a) antes y durante cualquier transacción, comprobar el modo en que los destinatarios o usuarios finales tienen previsto utilizar el producto o servicio, sobre la base de declaraciones de uso final;

b) familiarizarse con la situación en el lugar de destino en cuestión de los productos, especialmente con la situación general de los derechos humanos, ya que esto constituye un indicador importante del riesgo de violaciones graves de los derechos humanos y del Derecho internacional humanitario en el marco de una exportación;

c) evaluar los riesgos de que el producto o servicio se desvíe a otro usuario final no autorizado, sobre la base de las señales de alerta que se establecen a continuación.

Señales de alerta:

a) el usuario final tiene una relación evidente con un Gobierno extranjero que tiene un historial de represión interna o graves violaciones de los derechos humanos y del Derecho internacional humanitario;

b) el usuario final forma parte estructuralmente de las fuerzas armadas u otro grupo implicado en el pasado en un conflicto armado en el que se registraron medidas de represión interna o violaciones graves de los derechos humanos y del Derecho internacional humanitario;

c) el usuario final ha exportado en el pasado productos de cibervigilancia a países en los que su uso ha dado lugar a medidas de represión interna o graves violaciones de los derechos humanos y del Derecho internacional humanitario.

3.4. **Utilizar las averiguaciones de diligencia debida para elaborar planes destinados a prevenir y mitigar posibles efectos adversos en el futuro.**

Sobre la base de sus averiguaciones de diligencia debida, los exportadores deben interrumpir las actividades que causen o contribuyan a causar efectos adversos relacionados con los derechos humanos, así como elaborar y aplicar un plan de medidas correctoras. Dichas medidas podrán consistir en:

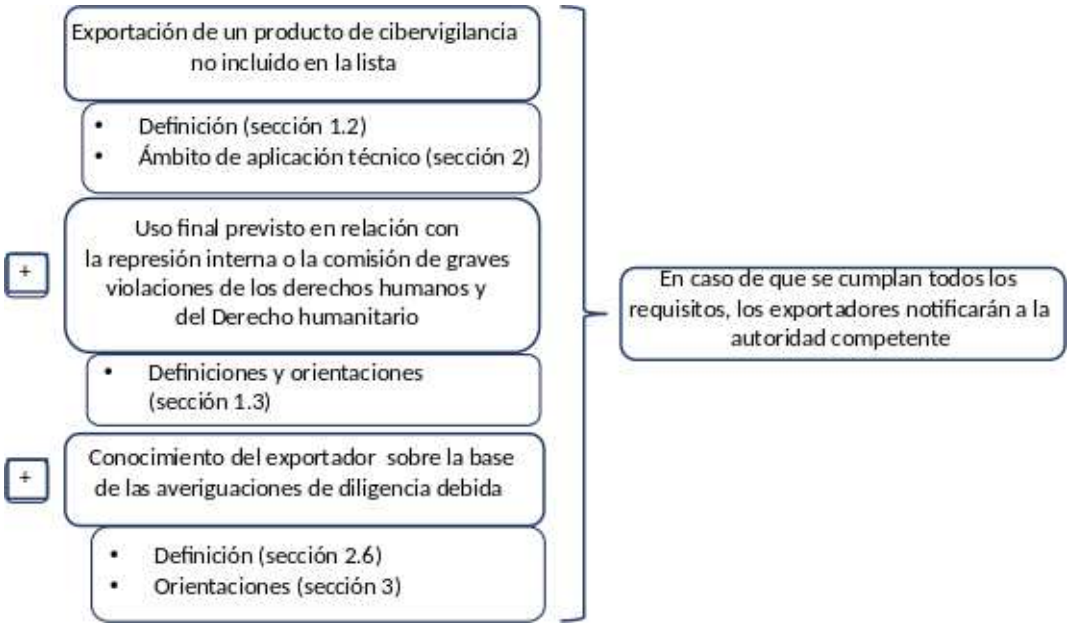
a) actualizar las políticas de la empresa para proporcionar directrices sobre el modo de evitar y tratar los efectos adversos en el futuro y garantizar la aplicación de dichas directrices;

b) aprovechar las conclusiones de la evaluación de riesgos para actualizar y reforzar los sistemas de gestión con vistas a realizar un mejor seguimiento de la información y señalar los riesgos antes de que se produzcan efectos adversos;

c) recopilar información para comprender los riesgos elevados de efectos adversos relacionados con el sector;

d) informar a las autoridades competentes de los Estados miembros de las averiguaciones de diligencia debida para facilitar el flujo de información en lo que respecta a determinados productos, usuarios finales y destinos.

Requisitos establecidos en el artículo 5, apartado 2, del Reglamento (UE) 2021/821



4. **APÉNDICE**

Productos de cibervigilancia incluidos en la lista como controlados con arreglo al anexo I del Reglamento (UE) 2021/821

— **Sistemas de interceptación de telecomunicaciones (5A001.f)**

En la mayoría de países, incluidos los Estados miembros, la confidencialidad de las comunicaciones está protegida por ley, pero existe un marco jurídico (denominado «interceptación legal») en el que la vigilancia electrónica encubierta de las comunicaciones por parte de las autoridades gubernamentales puede autorizarse. Sin embargo, la era digital ha supuesto la posibilidad de utilizar tecnologías de interceptación a gran escala. El uso de herramientas de interceptación por parte del régimen libio puso de relieve el potencial de utilización de estas tecnologías a gran escala e impulsó la introducción de controles de exportación de los sistemas de interceptación de telecomunicaciones en 2012.

Este control se aplica a los equipos diseñados para la extracción del contenido de una comunicación (voz o datos), así como a los identificadores de abonados u otros metadatos transmitidos por vía aérea a través de una comunicación inalámbrica, y a los equipos para el seguimiento de radiofrecuencias. Este control se aplica, por ejemplo, a los receptores de IMSI (identidad internacional de abonado móvil) que interceptan el tráfico de teléfonos móviles y hacen un seguimiento del movimiento de los usuarios de teléfonos móviles, o a los equipos que crean puntos de acceso wifi falsos que pueden extraer números IMSI de un teléfono, así como a determinados tipos de productos diseñados especialmente para permitir la «inspección profunda de paquetes» en los sistemas de telecomunicaciones. Los equipos de interferencia de telecomunicaciones móviles no entran en el ámbito de aplicación de los productos de cibervigilancia, ya que no recogen datos.

Si bien la tecnología de utilidad general puede emplearse para construir estos sistemas, sus capacidades de interceptación a gran escala dependen de determinadas piezas y componentes específicos, como programas informáticos específicos o circuitos integrados avanzados o específicos de una sola aplicación (por ejemplo, FPGA, ASIC, etc.) que permiten aumentar el número de paquetes o sesiones de comunicación que pueden procesarse por segundo.

— **Sistemas de vigilancia de internet (5A001.j)**

Aunque, por lo general, muchas comunicaciones basadas en internet se cifran actualmente por defecto, la interceptación de datos de tráfico (metadatos) relativos a las comunicaciones —como las direcciones IP y la frecuencia y el tamaño del intercambio de datos— puede seguir utilizándose para detectar vínculos entre personas y nombres de dominio. Los Gobiernos pueden utilizar estos sistemas de forma legal y con supervisión judicial para fines legítimos, como la identificación de personas que visiten dominios vinculados con contenidos delictivos o terroristas. Sin embargo, el seguimiento y el análisis del tráfico de internet sobre la base de una caracterización étnica, religiosa, política o social pueden dar lugar al establecimiento de una cartografía humana y social exhaustiva de un país para el control y la represión de la población, así como para otros fines, por ejemplo, identificar a disidentes políticos. Además de las cuestiones relativas a los derechos humanos y la represión interna, estos productos también pueden contribuir a mejorar las capacidades militares y de seguridad.

El control previsto en el subartículo 5A001.j se aplica a los sistemas de control de internet que operan en «red a través del IP de clase portadora (por ejemplo, el eje troncal IP de grado nacional)» para llevar a cabo el análisis, la extracción y la indexación del contenido de los metadatos transmitidos (voz, vídeo, mensajes, archivos adjuntos) sobre la base de «selectores rígidos» y cartografiar la red relacional de personas. Se trata de productos que permiten realizar una «vigilancia encubierta», dado que las personas objetivo no tienen conocimiento de la interceptación de sus comunicaciones. En cambio, los controles no van dirigidos a sistemas en los que exista una acción o una interacción con un usuario o un abonado; por ejemplo, no se aplican a las redes sociales o a los motores de búsqueda comerciales. Además, los controles se aplican a los sistemas que tratan datos procedentes de una red básica de proveedores de internet, y no a las redes sociales ni a los motores de búsqueda comerciales que tratan datos facilitados por los usuarios.

— **«Programas informáticos de intrusión» (4A005, 4D004 y controles conexos con arreglo a los subartículos 4E001.a y 4E001.c)**

Los programas informáticos de intrusión permiten a su operador obtener de forma encubierta acceso remoto a un dispositivo electrónico, como un teléfono inteligente, un ordenador portátil, un servidor o un dispositivo de internet de las cosas, obtener datos almacenados en el dispositivo, realizar una escucha informática a través de una cámara o un micrófono integrados o conectados al dispositivo, y utilizar el dispositivo como vía de acceso para llevar a cabo ataques contra el equipo al que se conecta el dispositivo o contra los contactos del usuario («pirateo informático a través de dispositivos de terceros»). Si bien los programas informáticos de intrusión tienen algunos usos legítimos ([8]), como es el caso de los «programas informáticos de acceso remoto» que los departamentos de informática emplean para prestar asistencia a distancia, el carácter encubierto de la vigilancia y la magnitud de la información que puede recogerse presentan un alto riesgo de violación del derecho a la intimidad y a la protección de los datos personales, y pueden vulnerar gravemente el derecho a la libertad de expresión.

([8]) En aras de la claridad, para exportar los productos de cibervigilancia incluidos en la lista como controlados con arreglo al anexo I del Reglamento sobre productos de doble uso a terceros países es necesaria una autorización, independientemente de si el uso del producto es legítimo.

El control con arreglo al artículo 4A005 *et al*. incluye los programas informáticos, así como los sistemas, equipos, componentes y la tecnología conexa, diseñados especialmente o modificados para la generación, el manejo mediante comandos y el control o la emisión de «programas informáticos de intrusión», pero no se aplica a los propios «programas informáticos de intrusión», tal como se definen en el anexo I del Reglamento. Estas herramientas cibernéticas se controlan teniendo en cuenta las posibles perturbaciones y daños que pueden causar si se utilizan y ejecutan con éxito, pero el objetivo de los controles no es afectar a la actividad de los investigadores y la industria del ámbito de la ciberseguridad, por ejemplo, ya que necesitan compartir información relativa a los programas informáticos de intrusión para poder desarrollar soluciones para sus productos y ponerlas en marcha antes de que se divulgue públicamente la existencia de una vulnerabilidad.

— **Programas informáticos de seguimiento de la comunicación (5D001.e)**

Estos programas informáticos están diseñados para que las fuerzas y cuerpos de seguridad autorizados realicen el seguimiento y el análisis de los datos recogidos a través de medidas de interceptación específicas solicitadas a un proveedor de servicios de comunicaciones. Permiten realizar búsquedas, sobre la base de «selectores rígidos», del contenido de las comunicaciones o de sus metadatos, utilizando una interfaz para la interceptación legal y cartografiando la red relacional o siguiendo el movimiento de personas concretas sobre la base de los resultados de las búsquedas. Estos programas informáticos están destinados a la «vigilancia encubierta», puesto que utilizan datos recogidos a partir de la interceptación de comunicaciones sin que las personas tengan conocimiento de ello. Además, «analizan» los datos recogidos a través de «sistemas de telecomunicaciones». Estos programas informáticos están instalados en la autoridad gubernamental (por ejemplo, la central de interceptación de las autoridades competentes), y el control no se aplica a los sistemas de conformidad de la interceptación legal (como los sistemas de gestión de la interceptación legal y los dispositivos de mediación) que se desarrollan comercialmente y se instalan en el espacio del proveedor de servicios de comunicaciones (por ejemplo, integrados en la red de comunicaciones), y que el proveedor de servicios opera y mantiene. Como se aclara en el texto sobre los controles, los controles no se aplican a los «programas informáticos» especialmente diseñados o modificados para fines puramente comerciales, como la facturación, la calidad del servicio de red (QoS), la calidad de la experiencia (QoE), los dispositivos de mediación o los pagos móviles o el uso bancario.

— **Productos utilizados para realizar criptoanálisis (5A004.a)**

Este control se aplica a productos diseñados para desactivar mecanismos criptográficos con el fin de derivar variables confidenciales o datos sensibles, incluyendo texto claro, contraseñas o claves criptográficas. La criptografía se emplea para preservar la confidencialidad de la información en tránsito y en reposo. El criptoanálisis se utiliza para desactivar esta confidencialidad, por lo que esta tecnología «permite» la vigilancia encubierta mediante el seguimiento, la extracción, la recogida o el análisis de datos de sistemas de información y telecomunicación.

— **Herramientas forenses o de investigación (5A004.b., 5D002.a.3.b. y 5D002.c.3.b.)**

Las herramientas forenses o de investigación están diseñadas para extraer datos brutos de un dispositivo (por ejemplo, de uno informático o de comunicación) de modo que los datos no se manipulen o corrompan y puedan utilizarse con fines judiciales, es decir, en una investigación judicial o ante un tribunal de justicia. Estos productos eluden los controles de «autenticación» o autorización de un dispositivo, de modo que los datos brutos puedan extraerse del dispositivo. El Gobierno y las fuerzas y cuerpos de seguridad, así como las fuerzas militares, emplean estos productos para extraer y analizar datos de los dispositivos incautados. Aunque tienen usos legítimos, pueden utilizarse indebidamente y, por tanto, suponer un riesgo para los datos sensibles o comerciales.

Sin embargo, las herramientas forenses o de investigación que no están «diseñadas especialmente» para la vigilancia encubierta no entran en la definición de «productos de cibervigilancia» del artículo 2, punto 20. Asimismo, las herramientas forenses o de investigación que solo extraen datos de los usuarios o en las que los datos no se encuentran protegidos en el dispositivo no están cubiertas por el texto sobre los controles del subartículo 5A004.b *et al*. Del mismo modo, los controles no se aplican a los equipos de producción o ensayo del fabricante, a las herramientas de administración de sistemas o a los productos destinados exclusivamente al sector del comercio al por menor, como es el caso de los productos para el desbloqueo de teléfonos móviles. Por lo tanto, teniendo en cuenta la variedad de estos tipos de tecnología, la aplicación de controles depende de una evaluación caso por caso de cada producto.

Por último, ha de tenerse en cuenta que hay otros productos relacionados con la vigilancia incluidos en la lista del anexo I del Reglamento que no deben considerarse incluidos en la definición de «productos de cibervigilancia», como los equipos de interferencia de telecomunicaciones móviles (5A001.f) diseñados para dañar o perturbar las comunicaciones o los sistemas, los programas informáticos de intrusión que modifican un sistema (4D004) y los equipos láser de detección acústica (6A005.g) que recogen datos de audio con un láser o permiten escuchar conversaciones a distancia (en ocasiones se les denomina «micrófonos láser»). Del mismo modo, el uso con fines de vigilancia de vehículos aéreos no tripulados incluidos en la lista no haría que estos productos entren en la definición de «productos de cibervigilancia».