Documento
Opinión

143/2020 10 de noviembre de 2020

*Margarita Robles Carrillo**

Sanciones contra ciberataques:
la acción de la Unión Europea

Sanciones contra ciberataques: la acción de la Unión Europea

Resumen

La Unión Europea y sus Estados miembros han aprobado, en julio de 2020, las primeras medidas sancionadoras contra actividades maliciosas en el ciberespacio. Los destinatarios son personas físicas y jurídicas de nacionalidad china, rusa y norcoreana. El proceso seguido para su adopción ha sido largo y complejo como consecuencia del singular modelo sancionador previsto en el marco de la Unión y de las particularidades de la actividad cibernética. El régimen jurídico de las sanciones incluye la identificación de los destinatarios, la naturaleza y las víctimas de los ciberataques, las modalidades y el alcance de las medidas restrictivas y las salvaguardas, controles y garantías jurídicas requeridas para garantizar la conformidad a derecho de las medidas adoptadas por el Consejo.

Palabras clave

Sanciones, ciberataques, Estados, Unión Europea.

Sanctions against cyber-attacks: European Union action

Abstract

In July 2020, the European Union and its Member States have approved the first sanctions against malicious activities in cyberspace. These measures are directed against natural and legal persons of Chinese, Russian and North Korean nationality. The process followed for their adoption has been long and complex because of the singular sanctioning model provided for in the framework of the Union and the particularities of cyber activity. The legal regime for sanctions includes the identification of the intended subjects, the nature and victims of cyber-attacks, the modalities and scope of the restrictive measures and the safeguards, controls and legal guarantees required to ensure the legality of the measures adopted by the Council.

Keywords

Sanctions, cyberattacks, states, European Union.

Introducción

Wannacry, NotPetya o EternalPetya, Cloud Hopper y la acción, en grado de tentativa, dirigida a piratear la red wifi de la Organización para la Prohibición de las Armas Químicas (OPAQ), en los Países Bajos, son algunos de los numerosos ciberataques que se han conocido en los últimos años. Siendo diferentes en sus objetivos, medios, fechas, autores y destinatarios, tienen en común el hecho de haberse convertido en el objetivo de la primera acción sancionadora de la Unión Europea (UE) frente a actividades maliciosas en el ciberespacio.

Dos nacionales de China —Gao Qiang y Zhang Shilong—, cuatro nacionales rusos —Alexey Valeryevich Minin, Aleksei Sergeyvich Morenets, Evgenii Mikhaylovich Serebriakov y Oleg Mikhaylovich Sotnikov—, una empresa china —Tianjin Huaying Haitai Science and Technology Development Co. Ltd—, una empresa norcoreana —Chosen Expo; Korea Export Joint Venture— y el Centro Principal de Tecnologías Especiales (GTsST) del Mando Principal del Estado Mayor de la Defensa de las Fuerzas Armadas de la Federación Rusa (GU/GRU) son los destinatarios de las medidas sancionadoras aprobadas en la UE el 30 de julio de 2020.

Con esa finalidad, el Consejo adopta dos actos: por una parte, la Decisión (PESC) 2020/1127 por la que se modifica la Decisión (PESC) 2019/797 relativa a medidas restrictivas contra los ciberataques que amenacen a la Unión o a sus Estados miembros[1]; y, junto con ella, el Reglamento de Ejecución (UE) 2020/1125 por el que se aplica el Reglamento (UE) 2019/796 relativo a medidas restrictivas contra los ciberataques que amenacen a la Unión o a sus Estados miembros[2]. Este entramado normativo se explica porque la Decisión y el Reglamento de 2019 establecen el régimen jurídico general de las sanciones frente a actividades maliciosas en el ciberespacio, mientras que la Decisión y el Reglamento de Ejecución de 2020 incluyen el listado concreto de los destinatarios de estas y su motivación.

[1] DOUE, L 246, de 30/7/2020, p. 12.
[2] DOUE, L 246, de 30/7/2020, p. 4.

La adopción de estas medidas en el marco de la UE es el resultado de un proceso largo y complejo. Ello es debido, en gran medida, al propio modelo de adopción y ejecución de sanciones diseñado como consecuencia del sistema de distribución de competencias existente entre la Unión y sus Estados miembros. La comprensión de dicho modelo es básica para entender el alcance y la naturaleza de las medidas adoptadas, así como sus modalidades de ejecución práctica. Por ese motivo, en primer lugar, se explica el contexto jurídico en el que se desarrolla esta actividad sancionadora que difiere de la que puedan realizar individualmente el resto de los Estados y, a continuación, se analiza el régimen jurídico establecido en la Decisión (PESC) 2020/1127 y en el Reglamento de Ejecución (UE) 2020/1125, que resulta implementado finalmente en 2020.

Contexto jurídico

La actividad desarrollada en materia de sanciones por la UE es el resultado de una compleja construcción jurídica derivada del sistema de distribución de competencias entre los Estados y la Unión establecido en los tratados desde la constitución misma de la UE. Aunque se trata de una práctica iniciada antes con las CCEE[3], el modelo de sanciones se formaliza jurídicamente en el art. 228A del Tratado de Maastricht[4]. Esa disposición se encuentra ahora recogida básicamente en el art. 215 del Tratado de Funcionamiento de la UE (TFUE) adoptado en Lisboa.

Las disposiciones del Tratado

El modelo previsto en el art. 215 del TFUE es original y distinto de los procedimientos seguidos en cualquier otro contexto porque está específicamente diseñado para conciliar las competencias atribuidas a la UE con aquellas que mantienen los Estados miembros en materia de política exterior cuando se trata de imponer sanciones a terceros. En términos básicos, si quiere adoptar sanciones, cualquier Estado dispone de las competencias políticas para adoptar esa decisión, así como de las competencias

[3] Sobre la utilidad de estas medidas, puede verse COHEN, H.G. *Nations and Markets*. Research Paper Series. University of Georgia, School of Law 2020.
[4] Este sistema se explica en ROBLES CARRILLO, M. «La posición del TJUE en el Tratado de la Unión Europea: alcance y consecuencias de los artículos C y L». *Revista de Instituciones Europeas*, Vol. 21, N.º 3. 1994, pp. 828-830.

económicas, comerciales, financieras o de otra índole para materializar esa decisión[5] que, incluso, puede delegarse en un determinado organismo o agencia[6].

La situación en la UE es diferente. Los Estados mantienen la competencia sobre política exterior para decidir soberanamente sobre la oportunidad de adoptar sanciones, pero los principales instrumentos comerciales, económicos o financieros para ejecutar esa decisión se encuentran en manos de la UE que tiene atribuidas la mayoría de esas competencias[7]. Ello implica que las sanciones han de aprobarse por los Estados miembros reunidos en el seno del Consejo en el marco de la PESC y después, en el plano operativo, siguiendo los procedimientos comunitarios dentro por la UE porque es preciso conciliar el poder de decisión política de los Estados con las competencias instrumentales de la Unión que permiten hacer efectiva esa decisión[8].

Tras la reforma del Tratado de Lisboa, el art. 215 del TFUE mantiene este sistema dual establecido originariamente en el Tratado de Maastricht. Según esa disposición, cuando se adopte en el marco de la PESC una decisión que prevea la interrupción o la reducción, total o parcial, de las relaciones económicas y financieras con uno o varios terceros países o contra personas físicas o jurídicas, grupos o entidades no estatales, el Consejo adoptará las medidas necesarias. Son precisos, en consecuencia, dos actos jurídicos diferentes siguiendo dos procedimientos distintos, aunque provengan ambos del Consejo. La decisión aprobada en el marco de la PESC requiere la unanimidad conforme a lo dispuesto en el art. 24 del TUE, mientras que el acto previsto en el art. 215 del TFUE,

[5] Puede verse el caso, como ejemplo, de la República de Corea en EBERT, H.; GROENENTAL, L. «Cyber Resilience and Diplomacy in the Republic of Korea: Prospects for EU Cooperation». *Digital Dialogue*. 2020, pp. 7-9.

[6] En el caso de EE. UU., sobre la base de la Orden Ejecutiva 13553 (Disponible en https://www.govinfo.gov/app/details/CFR-2011-title3-vol1/CFR-2011-title3-vol1-eo13553), la Oficina de Control de Activos Extranjeros (OFAC) en el Departamento del Tesoro es la encargada de la adopción de sanciones al Grupo APT39, a 45 individuos y a la empresa Rana Intelligence Computing Company a los que se asocia con el Gobierno de Irán (Disponible en https://home.treasury.gov/news/press-releases/sm1127), conforme a las investigaciones realizadas por el FBI (Disponible en https://www.ic3.gov/media/news/2020/200917-2.pdf).

[7] Sobre este modelo y la práctica, puede verse BARBOU DES COURIÈRES, C. «Between Supranationalism and Inter-Governmentalism in the European Union's Foreign Policy: A Principal Agent Approach of the Sanction Policy in the CFSP Framework». *Revista UNISCI*, N.º 43. 2017, pp. 13-15.

[8] Esa diferencia entre la práctica estatal y la acción de la UE es esencial para comprender la eficacia de la política sancionadora de la UE. Una perspectiva diferente, comparando la práctica de EE. UU. y la UE, puede verse en MESTRE-JORDÁ, J. «Análisis de la eficacia de las sanciones de EE. UU. y la UE a Rusia (2014-2017)». *Boletín del IEEE*, *Documento de Opinión* n.º 28/2018. 15 de marzo de 2018, pp. 1- 18. Una evaluación más acorde con la naturaleza de la UE puede verse en GIUMELLI, F.; IVAN, P. «The effectiveness of EU sanctions. An analysis of Iran, Belarus, Syria and Myanmar (Burma)». *EPC Issue Paper* N.º 76. 2013.

que puede tener la forma de un reglamento, se adopta por mayoría cualificada a propuesta conjunta de la Comisión y del alto representante de la Unión para Asuntos Exteriores y Política de Seguridad.

Los principios que informan esta actividad de la UE son cuatro: promover la paz y la seguridad internacional, prevenir conflictos, apoyar la democracia, el estado de derecho y los derechos humanos y defender los principios de derecho internacional[9]. La práctica europea en materia de sanciones se inicia y se desarrolla, manifestándose como un poderoso instrumento de política exterior, motivada por incumplimientos especialmente graves de la normativa internacional y teniendo como destinatarios principales a Estados terceros. Las sanciones dirigidas contra personas físicas y/o jurídicas aparecen con posterioridad y tienen una dinámica singular[10] en la que destaca su utilización principal para combatir el terrorismo internacional a partir de los ataques del 11S y su aplicación como consecuencia de los mandatos adoptados en el Consejo de Seguridad de Naciones Unidas[11]. El listado consolidado de personas, grupos o entidades sujetos a sanciones es considerablemente amplio[12].

La adopción de estas medidas en el ámbito cibernético supone la materialización del consenso que se ha ido generando entre los Estados miembros, en los últimos años, para ofrecer una respuesta diplomática conjunta frente a las actividades malintencionadas en el ciberespacio.

El desarrollo normativo

La Estrategia de Ciberseguridad de la UE de 2013 subraya la importancia de conseguir una mayor coordinación dentro de la Unión mediante una política internacional coherente

[9] Disponible en https://ec.europa.eu/info/business-economy-euro/banking-and-finance/international-relations/sanctions_en.
[10] Sobre esta cuestión se recomienda: ECKES, C. *EU Counter-Terrorist Policies and Fundamental Rights The Case of Individual Sanctions*. Oxford University Press 2009; y «EU Restrictive Measures Against Natural and Legal Persons: From Counterterrorist to Third Country Sanctions». *Common Market Law Review*, 51. 2014, p. 869.
[11] Puede verse VAN DEN BROEK, M.; HAZELHORST, M.; DE ZANGER, W. «Asset Freezing: Smart Sanction or Criminal Charge? *Utrecht Journal of International and European Law*, Vol. 27, N.º 72, pp. 18-27.
[12] Listado disponible en https://ec.europa.eu/info/business-economy-euro/banking-and-finance/international-relations/sanctions_en.

del ciberespacio[13]. En el Marco Político de Ciberdefensa de la UE, adoptado en 2014 y actualizado en 2018, se reconoce que la ciberseguridad es una prioridad de la Estrategia Global sobre Política Exterior y de Seguridad de la Unión Europea y se subraya la necesidad de reforzar la Unión como una «comunidad de seguridad»[14]. Para ello, se cuenta con instrumentos propios de la UE como la Directiva sobre seguridad de las redes y sistemas de información[15] o el denominado Reglamento de Ciberseguridad[16], pero también es necesario reforzar la respuesta diplomática conjunta.

A esa idea responden las Conclusiones del Consejo sobre Ciberdiplomacia donde se insiste en el carácter esencial de un planteamiento común y global que, entre otros objetivos, contribuya a contrarrestar las amenazas, así como al respeto de la normativa internacional, en particular, en materia de responsabilidad por hechos ilícitos[17]. Con esa intención, en 2017, el Consejo adopta un conjunto de instrumentos de ciberdiplomacia en sus conclusiones relativas a un marco para una respuesta diplomática conjunta de la UE a las actividades informáticas malintencionadas[18].

En estas conclusiones, el Consejo reitera algunos de los principios básicos de la acción europea y establece el objetivo, la naturaleza, las medidas y los principios de la política diplomática conjunta de la UE. El «objetivo» es claramente político y disuasorio. Siguiendo literalmente el texto, la Unión afirma que el hecho de comunicar claramente las posibles consecuencias de una respuesta diplomática conjunta de la UE frente a las actividades informáticas malintencionadas «tendrá influencia en el comportamiento de los agresores potenciales en el ciberespacio, reforzando así la seguridad de la UE y de sus Estados miembros»[19].

La cuestión de la «naturaleza» de esta acción está claramente delimitada en los sucesivos actos del Consejo. La respuesta diplomática conjunta de la UE y de sus Estados miembros no constituye una «atribución» de autoría porque la atribución es una decisión política soberana que debe establecerse conforme a las reglas de derecho

[13] Disponible en https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52013JC0001&from=es.
[14] Disponible en https://data.consilium.europa.eu/doc/document/ST-14413-2018-INIT/es/pdf.
[15] Disponible en https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32016L1148.
[16] Disponible en https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32019R0881&from=EN.
[17] Disponible en https://data.consilium.europa.eu/doc/document/ST-6122-2015-INIT/es/pdf.
[18] Disponible en https://data.consilium.europa.eu/doc/document/ST-9916-2017-INIT/es/pdf.
[19] Disponible en https://data.consilium.europa.eu/doc/document/ST-9916-2017-INIT/es/pdf

internacional y que corresponde a los Estados[20]. Como regla, además, no todas las medidas de respuesta requieren atribución a un agente estatal o no estatal. Las únicas «medidas» a las que se hace referencia expresamente en las conclusiones del Consejo son «medidas restrictivas» adoptadas conforme a las disposiciones de los tratados y declaradas aptas de cara al marco para una respuesta diplomática conjunta de la UE.

Los «principios» rectores de este marco de respuesta diplomática son, básicamente, tres: proteger la integridad y seguridad de la UE, sus Estados y sus ciudadanos; cumplir los objetivos de la PESC; y respetar el derecho internacional y no vulnerar los derechos y libertades fundamentales. Junto con ellos, se incluyen dos principios de orden funcional: por una parte, tener en cuenta el contexto general de las relaciones de la UE con el país de que se trate y adoptar medidas proporcionadas a la actividad cibernética que las justifica en términos de alcance, escala, duración, intensidad, complejidad, sofisticación e impacto.

La aplicación de este conjunto de instrumentos de ciberdiplomacia se pone en marcha en 2018 haciendo mención explícita a los asuntos Wannacry y NotPetya.

La aplicación del modelo sancionador

El 16 abril de 2018, el Consejo adopta unas conclusiones sobre actividades informáticas malintencionadas en las que la UE condena firmemente el uso malintencionado de las TIC, señalando concretamente los casos Wannacry y NotPetya que han causado perjuicios y pérdidas económicas importantes tanto en la UE como fuera de ella. Tras ser declarados inaceptables y reconocer que se trata de incidentes que afectan a la estabilidad y a la seguridad, el Consejo confirma los principios básicos de la política de la UE en cuanto a la aplicación del derecho internacional al ciberespacio, el cumplimiento de las normas voluntarias y no vinculantes de comportamiento responsable de los Estados y el respeto del consenso alcanzado en el marco de los informes de los grupos de expertos gubernamentales reunidos en el marco de los trabajos de la Primera Comisión de la Asamblea General de Naciones Unidas[21].

[20] MINISTERE DES ARMEES. *Droit international appliqué aux opérations dans le cyberspace*. París: 2019, pp. 6-11.
[21] Disponible en https://data.consilium.europa.eu/doc/document/ST-7925-2018-INIT/es/pdf.

Prácticamente seis meses después, en su reunión de 18 de octubre de 2018, el Consejo Europeo condena el ciberataque hostil perpetrado contra la OPAQ y solicita la adopción de un abanico de medidas, incluidas las restrictivas, entre las que destaca luchar contra las actividades informáticas ilícitas y malintencionadas y fortalecer la ciberseguridad impulsando los trabajos sobre la capacidad de responder a ciberataques, conforme a las conclusiones del Consejo sobre el conjunto de instrumentos de ciberdiplomacia de 2017[22].

Esta petición del Consejo Europeo recibe respuesta, el 17 de mayo de 2019, cuando el Consejo aprueba la Decisión (PESC) 2019/797 y el Reglamento (UE) 2019/796 relativos, ambos, a medidas restrictivas contra los ciberataques que amenacen a la Unión o a sus Estados miembros. La Decisión se basa en el art. 29 del TUE y se adopta sobre la base de la propuesta de la alta representante de la Unión para Asuntos Exteriores y Política de Seguridad. El Reglamento se fundamenta en el art. 215 del TFUE, en la propia Decisión (PESC) 2019/797 y en la propuesta conjunta de la alta representante y de la Comisión. Son dos actos aprobados por el Consejo sobre la base de distintas disposiciones de los tratados y con procedimientos también diferentes como consecuencia de la naturaleza dual del modelo sancionador de la UE. El contenido de ambos actos es básicamente coincidente, aunque hay algunas diferencias. El Reglamento desarrolla en mayor medida algunos de los aspectos que solo quedan reflejados genéricamente en la decisión o aborda aspectos de la regulación propios de la actividad de la Unión. El ámbito de aplicación territorial está previsto solo en el art. 18 del Reglamento. La competencia de los Estados para designar a las autoridades nacionales competentes y la función al respecto de la Comisión se establecen en su art. 17. Hay, sin embargo, algunos desajustes entre ambos actos, a los que se hace referencia en el siguiente apartado, que no se encuentran realmente justificados.

La Decisión y el Reglamento de 2019 cuentan con un anexo en blanco previsto para incluir el listado de destinatarios de las medidas sancionadoras. Los actos aprobados por el Consejo el 30 de julio de 2020 tienen como finalidad principal establecer ese listado. En esa fecha, el Consejo adopta dos nuevos actos: la Decisión (PESC) 2020/1127 por la que se modifica la Decisión (PESC) 2019/797, relativa a medidas restrictivas contra los ciberataques que amenacen a la Unión o a sus Estados miembros, y el Reglamento

[22] Disponible en https://www.consilium.europa.eu/media/36797/18-euco-final-conclusions-es.pdf.

de Ejecución (UE) 2020/1125 por el que se aplica el Reglamento (UE) 2019/796 también relativo a medidas restrictivas contra los ciberataques que amenacen a la Unión o a sus Estados miembros. Salvo en algún aspecto formal, el contenido de los actos adoptados en 2020 es igual. Es la respuesta a los ciberataques Wannacry, NotPetya o EternalPetya, Cloud Hopper y a la tentativa de ataque contra la OPAQ.

Régimen jurídico

Como ya se ha indicado, el régimen jurídico de las sanciones adoptadas en el marco de la UE frente a actividades maliciosas en el ciberespacio se encuentra recogido en la Decisión y el Reglamento de 2019 que establecen el marco normativo general, mientras que la Decisión y el Reglamento de Ejecución de 2020 explican los motivos y relacionan el listado de personas físicas y jurídicas, entidades y organismos, así como los ciberataques, frente a los cuales se adoptan las medidas. El análisis de estas normas permite identificar los componentes principales de su régimen jurídico: destinatarios, naturaleza y víctimas de los ciberataques objeto de las sanciones, modalidades y alcance de las medidas restrictivas, salvaguardas, controles y garantías jurídicas.

Destinatarios de las medidas restrictivas

La Decisión y el Reglamento de 2019 establecen que los destinatarios de las medidas restrictivas pueden ser personas físicas o jurídicas, entidades y organismos. La naturaleza de su participación permite distinguir entre tres categorías de sujetos: 1) responsables de los ciberataques o de los intentos de ciberataque; 2) prestadores de ayuda financiera, técnica o material o implicados de alguna forma en los mismos, incluida la facilitación de su comisión por acción o por omisión; y 3) asociados a los anteriores (arts. 4 de la Decisión y 3.3 del Reglamento).

Siguiendo el art. 7 de la Decisión y el 14 del Reglamento de 2019, en el anexo a los actos de adopción de las medidas restrictivas se incluirán los motivos que justifican la inscripción en la lista, así como, cuando se disponga de ella, la información necesaria para identificar a las personas, entidades u organismos relacionados en la misma. El art. 16 del mismo Reglamento atribuye a la Comisión la responsabilidad de llevar a cabo el tratamiento de datos personales.

Sobre esa base, la Decisión y el Reglamento de Ejecución de 2020 identifican tres acciones cibernéticas maliciosas en las que están implicadas seis personas físicas, dos empresas y un organismo público.

Los ciberataques que justifican la adopción de las medidas restrictivas tienen en común la calificacion de su «efecto significativo» para la UE y también para terceros Estados y su consideración como una amenaza externa para la Unión o sus miembros. En el caso de la OPAQ se entiende que el efecto fue «potencialmente significativo» por tratarse de una tentativa de ciberataque.

Cloud Hopper

La Operación Cloud Hopper se dirige contra los sistemas de información de empresas multinacionales de seis continentes, entre ellas empresas ubicadas en la Unión, obteniendo acceso no autorizado a datos sensibles y provocando importantes pérdidas económicas.

En este caso, los destinatarios de las medidas restrictivas son todos de nacionalidad china: Gao Qiang y Zhang Shilong y la empresa Tianjin Huaying Haitai Science and Technology Development Co. Ltd. La autoría del ciberataque corresponde al grupo conocido como APT10 (Advanced Persistent Threat 10) (alias Red Apollo, CVNX, Stone Panda, MenuPass y Potassium).

La empresa china se considera responsable de prestar apoyo financiero, técnico y material para el ciberataque y se relaciona, con una muy sucinta explicación, con el grupo APT10 y con los dos nacionales chinos porque los tuvo en nómina. A su vez, se conecta a Gao Qiang con el grupo APT10 por su relación con la infraestructura de mando y control de dicho grupo, por ser empleado de la empresa en cuestión y por tener vínculos con Zhang Shilong, ambos incluidos en la lista. Por su parte, Zhang Shilong se considera responsable del *software* malicioso que usó APT10, además de por estar relacionado con Gao Qiang y con la empresa china, que se incluyen en la lista. Este sistema de motivación recíproca no parece bien resuelto en la medida en que se apoya en las relaciones respectivas entre cada uno de los nacionales chino y respecto de la empresa.

OPAQ

Alexey Valeryevich Minin y Oleg Mikhaylovich Sotnikov —agentes auxiliares de inteligencia humana— y Aleksei Sergeyvich Morenets y Evgenii Mikhaylovich Serebriakov —informáticos especializados en ciberseguridad—, al servicio del Mando Principal del Estado Mayor de la Defensa de las Fuerzas Armadas de la Federación de Rusia (GU/GRU), son considerados responsables de participar en una tentativa de ciberataque contra la OPAQ en los Países Bajos, al formar parte de un equipo de agentes rusos de inteligencia militar que trató de obtener acceso no autorizado a la Wifi de esta organización, en abril de 2018, con el objetivo de piratearla.

Segú explican la Decisión y el Reglamento de Ejecución de 2020, en caso de haberlo conseguido, se habría puesto en peligro la seguridad de la red y de las investigaciones en curso en la misma. El ataque fue frustrado por el Servicio de Inteligencia y Seguridad de la Defensa de los Países Bajos (Militaire Inlichtingen —en Veiligheidsdienst— MIVD).

Wannacry, NotPetya o EternalPetya

Aunque expresamente se califica al grupo APT38 como responsable de Wannacry, los destinatarios de las medidas restrictivas son una empresa norcoreana y un organismo ruso.

La empresa norcoreana Chosen Expo, conocida como Korea Export Joint Venture, se relaciona con el grupo APT38 o Grupo Lazarus, entre otros motivos, por las cuentas utilizadas para los ciberataques. Chosen Expo es acusada de prestar apoyo financiero, técnico o material y facilitar la realización de diversos ciberataques, como WannaCry y los ataques contra la Autoridad de Supervisión Financiera de Polonia y Sony Pictures Entertainment, así como el ciberrobo al Banco de Bangladesh y la tentativa de ciberrobo al Banco Tien Phong de Vietnam. Wannacry es el ciberataque que centra la atención tanto por la descripción de sus consecuencias como por la identificación del Grupo APT39 o Grupo Lazarus como autor de dicho ataque.

El Centro Principal de Tecnologías Especiales (GTsST) del Mando Principal del Estado Mayor de la Defensa de las Fuerzas Armadas de la Federación Rusa (GU/GRU) es declarado expresamente responsable de diversos ataques entre los que se incluyen

NotPetya o EternalPetya y los ciberataques dirigidos contra una red eléctrica ucraniana en el invierno de 2015 y 2016.

Como se puede comprobar, en la motivación de dos de los ciberataques en la Decisión y el Reglamento de Ejecución de 2020 se hace referencia a grupos —el APT10 en la operación Cloud Hopper y el APT38 en Wannacry—, pero ninguno de ellos es destinatario de las medidas por la dificultad que implica identificarlos a esos efectos y por la carencia de personalidad jurídica de los mismos.

En cualquiera de los casos, la adopción de las medidas restrictivas no implica atribución en sentido jurídico-internacional porque, además de haberse excluido expresamente esa posibilidad en las conclusiones sobre un marco para una respuesta diplomática conjunta de la UE y en la propia Decisión (PESC) de 2019/797, por tratarse de una competencia soberana de los Estados, en derecho internacional, la atribución establece el vínculo entre el autor material de un hecho ilícito y el Estado al que se hace responsable del mismo. En los actos adoptados en 2010, se identifica a una serie de personas físicas y jurídicas y se explican los motivos por los cuales se encuentran vinculadas a una actividad cibernética maliciosa sin que se establezca una conexión jurídica formal entre sus actos y los de un Estado, más allá de la determinación de su nacionalidad. No hay atribución de responsabilidad a un Estado ni siquiera en el caso del Centro Principal de Tecnologías Especiales (GTsST) del Mando Principal del Estado Mayor de la Defensa de las Fuerzas Armadas de la Federación de Rusia (GU/GRU), también conocido por el código 74455, a quien se considera responsable de diversos ciberataques.

Naturaleza y víctimas de los ciberataques

Los ciberataques se definen como acciones que implican acceso a sistemas de información, intromisión en sistemas de información, intromisión en datos o 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 de este, o no estén permitidas por el Derecho de la Unión o de un Estado miembro (art. 1.3 de la Decisión y del Reglamento de 2019). Sobre la base de esta definición se delimitan los ciberataques susceptibles de ser objeto de las medidas sancionadoras de la UE.

Para empezar, conforme a los términos de la Decisión de 2019, solo se contemplan los ciberataques llevados a cabo deliberadamente y con un efecto significativo o las tentativas de ciberataque deliberadas y con un efecto potencialmente significativo (art. 1.1 de la Decisión y del Reglamento de 2019). Ello excluye cualquier tipo de ciberataque en el que no exista esa intencionalidad como posible objeto de medidas restrictivas. Cumplido ese requisito, los factores que determinan el efecto significativo o efecto significativo potencial se encuentran relacionados en el art. 3 de la Decisión y en el art. 2 del Reglamento de 2019[23].

El ciberataque ha de ser, además, «externo». Ello implica que solo comprende los ciberataques que se originen o se cometan desde el exterior de la Unión, que utilicen infraestructura fuera de la Unión, que hayan sido cometidos por una persona física o jurídica, una entidad o un organismo establecidos o que tengan actividad fuera de la Unión o que 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 (arts. 1.2 de la Decisión y del Reglamento).

A partir de ahí, la Decisión y el Reglamento de 2019 establecen una conexión entre la naturaleza y las víctimas de los ciberataques a efectos de justificar la adopción de medidas restrictivas porque se distinguen los supuestos en los que se dirigen contra los Estados miembros o la UE. Los ciberataques constituyen una «amenaza» para los Estados si afectan a las infraestructuras críticas, al mantenimiento de las actividades sociales o económicas esenciales, a las funciones vitales del Estado, al almacenamiento o tratamiento de información clasificada o a sus equipos de respuesta de emergencia (arts. 1.4 de la Decisión y del Reglamento de 2019). Constituyen una «amenaza» para la Unión los dirigidos contra sus instituciones y organismos, sus delegaciones, operaciones y misiones en el exterior y sus representantes especiales (arts. 1.5 de la Decisión y del Reglamento de 2019). También se contempla la posibilidad de adoptar

[23] Esos factores son: 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 fundamentales 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, de recursos económicos o de propiedad intelectual; e) los beneficios económicos obtenidos por el infractor, 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.

medidas contra ciberataques realizados contra terceros países y organizaciones cuando se estimen necesarias para el cumplimiento de los objetivos de la PESC.

Modalidades y alcance de las medidas restrictivas

Las medidas restrictivas consisten en la prohibición de entrada y tránsito en el territorio de los Estados miembros (art. 4 de la Decisión), la inmovilización de todos los fondos o recursos económicos a disposición directa o indirecta de los destinatarios de las sanciones (art. 5 de la Decisión y art. 3 del Reglamento) y la prohibición de participar consciente y deliberadamente en acciones cuyo objeto o efecto sea eludir aquella obligación de inmovilización (art. 9 del Reglamento).

Como se puede comprobar, una está prevista en la Decisión, otra en el Reglamento y otra en ambos. La primera se explica en la medida en que, al ser competencia de los Estados miembros, tiene su ubicación natural en la Decisión PESC, aunque se habría visto reforzada como obligación jurídica de haberse incluido también en el Reglamento que se define como «obligatorio en todos sus elementos y directamente aplicable en cada Estado miembro». También se habría visto reforzada y resultaría más coherente la inclusión en la Decisión de la disposición del Reglamento en virtud de la cual «queda prohibido participar de manera consciente y deliberada en acciones cuyo objeto o efecto sea eludir las medidas a que se refiere el artículo 3» relativo a la inmovilización de los fondos y recursos económicos. Más allá de estos desajustes, la situación resultante es la siguiente:

a) La prohibición de entrada o tránsito por el territorio concierne solo a las personas físicas, mientras que el resto de las medidas se aplica asimismo a las jurídicas, entidades y organismos responsables, prestadores de ayuda o asociados a ellos.

La prohibición de entrada o tránsito en el territorio de los Estados miembros incluye algunas excepciones y exenciones que estarán estrictamente limitadas a la finalidad para la que se hayan concedido y a las personas a las que afecte directamente (art. 4.9 de la Decisión). Como excepciones, esta prohibición no obliga a los Estados respecto de sus propios nacionales y se entiende sin perjuicio de los casos en los que el Estado está obligado en sentido contrario por una disposición de derecho internacional porque es anfitrión de una organización internacional o de una conferencia internacional convocada

por Naciones Unidas o en virtud de un acuerdo multilateral relativo a privilegios o inmunidades. También se aplica esta excepción respecto de la OSCE (art. 4.2 y 3 de la Decisión).

Las exenciones están justificadas por razones humanitarias urgentes, por ser necesarias para el desarrollo de un proceso judicial 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, con la precisión de que en ellas «se mantenga un diálogo político que fomente directamente los objetivos políticos de las medidas restrictivas, incluidas la seguridad y la estabilidad del ciberespacio» (art. 4.6 y 7 de la Decisión).

El procedimiento a seguir en el caso de las exenciones consiste en el envío por parte del Estado de una notificación por escrito al Consejo. Si en el plazo de dos días hábiles desde su recepción, no hay objeción por parte de alguno de sus miembros, se entenderán concedidas. Si hay alguna objeción, el Consejo decidirá sobre la exención por mayoría cualificada.

b) La obligación de inmovilización de todos los fondos o recursos económicos está recogida en el art. 5 de la Decisión y en el art. 3 del Reglamento de 2019 con algunas diferencias en la redacción, que podrían haberse evitado, porque parecen innecesarias. Esa obligación afecta a todos los fondos y recursos económicos cuya propiedad, titularidad, tenencia o control correspondan a las personas físicas o jurídicas, entidades u organismos que sean responsables de los ciberataques o de las tentativas de ataque, que presten ayuda financiera, técnica o material o estén implicados de alguna forma en los mismos o que estén asociados de alguna forma con cualquiera de los anteriores (art. 5.1 de la Decisión y art. 3 del Reglamento de 2019). En ningún caso se pondrán fondos o recursos económicos a disposición directa o indirecta de ninguno de ellos, ni se utilizarán en su beneficio.

Esta obligación contempla algunas excepciones. En primer lugar, las autoridades competentes podrán autorizar la liberación de determinados fondos o recursos con una finalidad concreta: satisfacer necesidades básicas o pagar honorarios profesionales, tasas o gastos relacionados con esos activos, gastos extraordinarios necesarios o vinculados a la cuenta de una misión diplomática o consular o de una organización internacional (art. 5.3 de la Decisión y art. 4.1 del Reglamento). En segundo lugar, las

autoridades competentes podrán autorizar la liberación de determinados fondos o recursos si son objeto de resolución arbitral, judicial o administrativa en función, en cada caso, de la fecha de adopción de la misma o si van a utilizarse para satisfacer demandas derivadas de dichas resoluciones, siempre que no resulten en beneficio de los sujetos sancionados y no sea contrario al orden público del Estado de que se trate (art. 5.4 de la Decisión y art. 5 del Reglamento). En tercer lugar, la obligación de inmovilización de esos activos económicos no impedirá la realización de pagos adeudados por contrato en las condiciones previstas por los arts. 5.5 de la Decisión y 6 del Reglamento, que tiene una redacción más extensa y precisa. Para terminar, dicha obligación no afectará al ingreso en las cuentas inmovilizadas de intereses, beneficios o pagos adeudados en virtud de contratos o resoluciones judiciales, administrativas o arbitrales siempre que respecto de ellos también se aplique la obligación de inmovilización (art. 5.6 de la Decisión y art. 7 del Reglamento). Los Estados deben informar de cualquier autorización de liberación de fondos a los demás Estados miembros y a la Comisión.

El modelo de aplicación de las medidas es descentralizado. El art. 15 del Reglamento dispone que los Estados deben establecer las normas sobre las sanciones aplicables a las infracciones de estas disposiciones, que deben ser efectivas, proporcionadas y disuasorias y notificarlas a la Comisión, así como adoptar todas las medidas necesarias para garantizar su aplicación. Existe, además, conforme al art. 12 del Reglamento, una obligación de comunicación mutua de las medidas adoptadas y de cualquier información relativa a la aplicación de esta normativa, en particular, sobre los fondos inmovilizados y sobre los problemas de violación del Reglamento, su ejecución y las sentencias dictadas por los tribunales nacionales.

Salvaguardas

La efectividad de las medidas restrictivas se encuentra reforzada por algunas disposiciones que cumplen una función de garantía: por una parte, una exclusión de responsabilidad prevista en el art. 10 del Reglamento en circunstancias justificadas; y, por otra, una salvaguarda respecto de posibles demandas en los arts. 8 de la Decisión y 11 del Reglamento de 2019.

a) El art. 10.1 del Reglamento dispone que la inmovilización de fondos y recursos económicos —o la negativa a facilitarlos— no dará origen a ningún tipo de

responsabilidad por parte de la persona física o jurídica, entidad u organismo que la ejecute, siempre que hayan sido realizadas de buena fe con la convicción de que dicha acción se atiene al Reglamento y a menos que se pruebe que los fondos o recursos económicos han sido inmovilizados o retenidos por motivo de negligencia. Conforme a su apartado 2º, las acciones emprendidas por personas físicas o jurídicas, entidades u organismos, no generarán responsabilidad de ninguna clase por su parte si no sabían, y no tenían ningún motivo razonable para sospechar, que sus acciones infringirían las medidas establecidas en el Reglamento.

b) El art. 8 de la Decisión de 2019 dispone que «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». Ello incluye las demandas de indemnización o cualquier otra pretensión de esta naturaleza si la presentan los destinatarios de las medidas restrictivas o cualquier persona física o jurídica, entidad u organismo que actúe a través o en nombre de los mismos. El art. 11 del Reglamento de 2019 recoge esa misma previsión incluyendo un apartado adicional relativo a la carga de la prueba y otro en el que se reconoce, como no podía ser de otra manera, el derecho de las personas físicas o jurídicas, entidades y organismos en cuestión a recurrir por la vía judicial la legalidad del incumplimiento de obligaciones contractuales de conformidad con el Reglamento.

Controles y garantías jurídicas

La adopción de medidas restrictivas frente a actividades maliciosas en el ciberespacio está sometida a determinados controles y garantías. Siguiendo su considerando 3.º, el Reglamento «respeta los derechos fundamentales y observa los principios reconocidos en la Carta de los Derechos Fundamentales de la Unión Europea» y, especialmente, el derecho a la tutela judicial efectiva y a un juez imparcial y el derecho a la protección de los datos de carácter personal. Por ello, debe aplicarse de conformidad con esos derechos.

Ello implica, por una parte, la obligación de motivar la inclusión en la lista/anexo que está prescrita en los arts. 7 de la Decisión y 14 del Reglamento de 2019. Por otra parte, el art. 6.3 de la Decisión y el art. 13.3 del Reglamento de 2019 prevén la posibilidad de que el Consejo reconsidere su decisión sobre las medidas restrictivas adoptadas cuando se

formulen observaciones o se presenten nuevas pruebas sustanciales en cuyo caso informará a los interesados. Además de este mecanismo, existe la posibilidad de un control judicial que es competencia del TJUE.

El art. 215 del TFUE, al regular las medidas restrictivas, dispone en su apartado 3.º que los actos adoptados sobre la base de este precepto incluirán las disposiciones necesarias en materia de garantías jurídicas. La Declaración n.º 25 relativa a los arts. 75 y 215, anexa al Tratado de Lisboa, recuerda que el respeto de los derechos y libertades fundamentales implica la protección y el respeto del derecho a disfrutar de las garantías jurídicas previstas en la ley. Por ello, y con la finalidad de garantizar un control jurisdiccional estricto de las decisiones por las que se imponen medidas restrictivas a personas físicas o jurídicas, dichas decisiones deberán basarse en criterios claros, precisos y ajustados a la especificidad de cada una de esas medidas.

La comprensión de esta disposición exige recordar que, conforme al art. 24 del TUE y 275 del TFUE, el Tribunal de Justicia de la UE (TJUE) no tiene competencia respecto de las disposiciones en materia de PESC, salvo en relación con el art. 40 —que permite verificar el respeto de la delimitación entre esferas de acción de la PESC y el resto de los ámbitos de actuación de la Unión— y para controlar determinadas decisiones contempladas en el art. 275.2 del TFUE. Esta disposición establece precisamente la posibilidad de un control de la legalidad de las decisiones del Consejo relativas a medidas restrictivas frente a personas físicas o jurídicas.

En este supuesto, el procedimiento a seguir viene determinado en el párrafo 4.º del art. 263 que regula el planteamiento del recurso de anulación por parte de personas físicas o jurídicas. Hay dos cuestiones importantes: por una parte, el recurso solo puede ser interpuesto por una persona física o jurídica contra actos de los que sea destinataria o que le afecten directa e individualmente o contra los actos reglamentarios que le afecten directamente y que no incluyan medidas de ejecución; por otra parte, no están legitimados para plantear este recurso los Estados miembros y el resto de las instituciones que, sin embargo, son conocidos como los demandantes privilegiados en esta vía de recurso. Los motivos que pueden justificar el planteamiento del recurso son incompetencia, vicios sustanciales de forma, violación de los tratados o de cualquier norma jurídica relativa a su aplicación o desviación de poder.

Siguiendo la jurisprudencia del TJUE en la materia, recordada en su sentencia de 9 de julio de 2020 en el asunto Haswani relativo a la legalidad de medidas restrictivas adoptadas en el ámbito de la PESC, en materia de garantías jurídicas son de aplicación el conjunto de disposiciones del TUE y la Carta de los Derechos Fundamentales de la Unión Europea. Conforme al artículo 52.1 de la misma, cualquier limitación del ejercicio de los derechos y libertades reconocidos por la Carta deberá ser establecida por la ley y respetar el contenido esencial de dichos derechos y libertades dentro del respeto del principio de proporcionalidad. Este principio exige que los medios adoptados sean idóneos para alcanzar el objetivo legítimo perseguido por la normativa de que se trate y no vayan más allá de lo necesario para alcanzarlo. Sobre el control judicial del respeto de ese principio, el TJUE ha reconocido «una amplia facultad discrecional al legislador de la Unión en ámbitos en los que deba tomar decisiones de naturaleza política, económica y social, y realizar apreciaciones complejas». Ello implica que «solo el carácter manifiestamente inadecuado de una medida adoptada en tales ámbitos, con relación al objetivo que tiene previsto conseguir la institución competente, puede afectar a la legalidad de tal medida»[24].

Conclusiones

El modelo sancionador europeo se ha definido como un instrumento esencial de la política exterior que permite intervenir a la Unión aplicando sus principios y políticas en materia de promoción de la paz y la seguridad internacional, la prevención de conflictos y la defensa del derecho internacional, el estado de derecho, la democracia y los derechos humanos. Esos objetivos justifican también la adopción de medidas para combatir las actividades maliciosas en el ciberespacio.

La aplicación del modelo sancionador europeo en relación con las actividades cibernéticas malintencionadas se caracteriza por unos parámetros básicos. El primero es la persistente invocación y defensa de la aplicabilidad del derecho internacional al ciberespacio, así como de las normas de comportamiento responsable de los Estados, siguiendo los compromisos asumidos en el marco de los trabajos y de los informes de los grupos de expertos gubernamentales de la Primera Comisión de la Asamblea General

[24] Sentencia del TJUE de 9 de julio de 2020, Asunto C-241/19 P, Haswani, considerandos 98 a 100.

de Naciones Unidas. En los sucesivos actos adoptados se reitera el principio defendido por la UE y sus Estados miembros de que el respeto del derecho internacional vigente es esencial para mantener la paz y la estabilidad. En particular, 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 Naciones Unidas.

En segundo lugar, la adopción de medidas restrictivas en el marco de la UE no implica atribución en el sentido dado a esta operación en derecho internacional, porque no se trata de establecer un vínculo entre un hecho realizado por un agente y un Estado, ni tampoco en sentido general se considera una «atribución» de autoría. Siguiendo la práctica de sus Estados en esta materia, significativamente Francia, en los sucesivos actos adoptados se reconoce que la atribución es una decisión política soberana que debe establecerse conforme a las reglas de derecho internacional y que corresponde exclusivamente a los Estados.

En tercer lugar, a pesar de dirigir las sanciones contra nacionales chinos, norcoreanos y rusos y, en este caso, contra el Centro Principal de Tecnologías Especiales del Mando Principal del Estado Mayor de la Defensa de las Fuerzas Armadas de la Federación Rusa, no hay asignación de responsabilidad a ninguno de los países de su nacionalidad. Irán y China son, sin embargo, directamente asociados a las actividades maliciosas en el ciberespacio en la práctica del FBI[25]. La ausencia de referencia a Estados en el caso europeo puede ser consecuencia de la concepción de la atribución como una potestad soberana, pero también podría explicarse por la falta de acuerdo al respecto entre los miembros de la UE o, desde otra perspectiva, como seguimiento de los compromisos asumidos en el marco de los grupos de expertos gubernamentales en relación con los criterios para la atribución de responsabilidad a los Estados.

En cuarto lugar, las medidas restrictivas se concretan en la prohibición de entrada y tránsito por el territorio de la UE y en la inmovilización de activos económicos que, habiendo demostrado su efectividad en otros supuestos, tienen el alcance que supone su aplicación en el conjunto de la UE y la posibilidad de que tengan mayor impacto si,

[25] Disponible en https://www.ic3.gov/media/news/default.aspx.

como contempla el art. 9 de la Decisión de 2019, la UE anima a su adopción por parte de terceros Estados.

En quinto lugar, los controles y garantías jurídicas en cuanto a la conformidad a derecho de estas medidas parecen suficientes en la medida en que contemplan la posibilidad de revisión de la decisión por parte del Consejo si se presentan observaciones o nuevas pruebas sustanciales y, en cualquier caso, el control judicial del TJUE que constituye la garantía última del respeto del derecho a la tutela judicial efectiva.

Todos estos elementos que caracterizan la primera acción sancionadora de la UE frente a actividades maliciosas en el ciberespacio constituyen un modelo de acción singular y diferente del seguido por otros Estados no solo por su funcionamiento sino, también y, sobre todo, por su contenido. Aunque podría modificarse para hacer más transparente y comprensible su funcionamiento, eliminando duplicidades y desajustes normativos, las carencias de esa naturaleza no son suficientes para eclipsar sus resultados. Los principios, las normas invocadas, el procedimiento y las garantías de este modelo sancionador responden a una impronta europea, que no es la primera vez que se manifiesta, en la que se advierten dos signos distintivos: la defensa de un ciberespacio global, abierto, estable, pacífico y seguro y la aplicación de la normativa internacional y de los compromisos asumidos a esos efectos en el marco de Naciones Unidas.

*Margarita Robles Carrillo**
Profesora titular de Derecho Internacional Público y RR. II.
Network Engineering & Security Group NESG-TIC233
Universidad de Granada