10.18800/themis.202001.031

CIBERSEGURIDAD Y ARBITRAJE INTERNACIONAL: EL PROTOCOLO DE CIBERSEGURIDAD EN ARBITRAJE INTERNACIONAL DEL ICCA, EL NYC BAR Y EL CPR (EDICIÓN 2020)

CYBERSECURITY AND INTERNATIONAL ARBITRATION: ICCA — NYC BAR — CPR PROTOCOL ON CYBERSECURITY IN INTERNATIONAL ARBITRATION (2020 EDITION)

Javier Fernández-Samaniego[*]
Samaniego Law
Gonzalo Hierro Viéitez[**]
Samaniego Law
Yaiza Araque Moreno[***]
Samaniego Law

The Protocol on Cybersecurity in International Arbitration constitutes an innovative proposal providing a rigorous approach aimed towards raising awareness on cybersecurity risks in arbitration for its participants. Likewise, it seeks to be a guide to which the parties and arbitrators can recur in order to determine which cybersecurity measures can reasonably be adopted. The Protocol is a soft-law instrument that acknowledges cybersecurity measures may vary for each particular case.

In this article, the authors evaluate the innovations proposed in the Protocol's 2020 edition. Thus, they address its evolution, reviewing the newest types of cyber threats, previous regulatory efforts and, in greater detail, the principles and schedules proposed in this document. Finally, the authors also reflect on the opportunities that the Protocol provides in a global emergency situation due to the COVID-19 pandemic.

Keywords: Protocol on Cybersecurity in International Arbitration; cybersecurity threats; privacy in international Arbitration; cyber incidents; virtual hearings.

El Protocolo sobre Ciberseguridad en el Arbitraje Internacional constituye una innovadora propuesta que recoge un enfoque riguroso con el propósito de incrementar la conciencia de los riesgos de ciberseguridad en el arbitraje para los participantes. Asimismo, busca proporcionar una guía que las partes y los árbitros sean capaces de consultar, a fin de determinar cuáles medidas de ciberseguridad es razonable adoptar. El Protocolo se configura como una norma de soft-law y reconoce que las medidas de ciberseguridad pueden variar caso a caso.

En el presente artículo, los autores evalúan las innovaciones propuestas por la edición 2020 del Protocolo. Así, abordan su evolución, repasando los incipientes tipos de ciberamenazas, los esfuerzos normativos previos y, con mayor detalle, los principios y schedules propuestos en este documento. Finalmente, los autores reflexionan también acerca de la oportunidad que el Protocolo representa ante una situación de emergencia global a causa de la pandemia producida por la COVID-19.

Palabras clave: Protocolo de Ciberseguridad en Arbitraje internacional; amenazas de ciberseguridad; privacidad en el Arbitraje internacional; incidentes cibernéticos; audiencias virtuales.

[*] Abogado. Socio fundador y director de Samaniego Law (Madrid, España). Contacto: javier.samaniego@samaniegolaw.com.

[**] Abogado. Máster en Acceso a la Abogacía y en International Law, Foreign Trade and International Relations por la Universidad Carlos III de Madrid y el ISDE y Master of Laws (LL.M.) en Banking, Corporate and Finance e Information Technology por la Fordham University de Nueva York. Asociado de Samaniego Law (Madrid, España). Contacto: gonzalo.hierro@samaniegolaw.com.

[***] Abogada. Máster de Acceso a la Profesión de Abogado y doctoranda por la Universidad Complutense de Madrid y máster en Derecho Comercial Internacional por la Universidad de La Rioja. Asociada de Samaniego Law (Madrid, España). Contacto: yaiza.araque@samaniegolaw.com.

Nota del Editor: El presente artículo fue recibido por el Consejo Ejecutivo de THĒMIS-Revista de Derecho el 11 de marzo de 2020, y aceptado por el mismo el 17 de julio de 2020.

I. INTRODUCCIÓN

El arbitraje internacional ha evolucionado de forma drástica y continua en las últimas décadas. En efecto, no solo se han presentado modificaciones en el ámbito legislativo o jurisprudencial; sino que dichos cambios se han ido implementando mediante factores de gran relevancia práctica, como es el uso de la tecnología. Asimismo, la situación provocada por la pandemia generada por la COVID-19 ha acelerado exponencialmente dicha tendencia.

De hecho, el 2018 International Arbitration Survey: The Evolution of International Arbitration, elaborado conjuntamente por White & Case y Queen Mary University of London, así lo reconoce cuando establece que la tecnología "is widely used in international arbitration, and an overwhelming majority of respondents favor the greater use in the future of hearing room technologies, […] cloud-based storage, videoconferencing, AI [Artificial Intelligence] and virtual hearing rooms"[1] (2018, p. 28).

No obstante, debemos tener en cuenta el panorama actual y, a su vez, ser conscientes de que el número de vulneraciones de datos personales e incidentes cibernéticos se ha incrementado considerablemente en los últimos años. En efecto, como expusimos en un artículo previo[2], un claro ejemplo de ello (en el ámbito empresarial) fue la filtración de las bases de datos de informes de crédito de Equifax en el año 2017, la cual conllevó a la exposición de información personal de más de 145.5 millones de personas. Para conocer los motivos que habían ocasionado dicha filtración, la Oficina General de Cuentas del Gobierno de Estados Unidos (GAO, por sus siglas en inglés) publicó un exhaustivo informe en agosto del año 2018 en el que se resumían los principales errores que se habían producido, tales como la falta de controles internos y exámenes de seguridad rutinarios (Fernández-Samaniego & Hierro Viéitez, 2019, pp. 1-2).

Ese mismo año, la base de datos de Aadhar se vio comprometida al permitir el acceso no autorizado por parte de terceros a información privada de 1.100 millones de residentes hindúes (incluyendo datos como nombres y apellidos, números de identificación de 12 dígitos o cuentas bancarias). Asimismo, otras muchas compañías, como Uber, Verizon[3] o Facebook[4] también se han visto afectadas por este tipo de incidentes (2019, p. 2).

Ante la gran relevancia de las vulneraciones cibernéticas, influyentes entidades del sector público y privado han elaborado informes sobre este riesgo cada vez más crítico. Entre ellos, podemos reseñar, en primer lugar, el realizado por la Online Trust Alliance, denominado Cyber Incident & Breach Trends Report[5]. En dicho informe se analizaron los diferentes incidentes cibernéticos acaecidos en el año 2018. En ese sentido, se mostró que los ataques de *ransomware* se habían multiplicado por cuatro entre los años 2015 y 2016; y, asimismo, que los archivos vulnerados se habían incrementado por cuatro en el año 2017.

El segundo informe que podemos destacar es el elaborado por el Gobierno del Reino Unido[6], cuya encuesta[7] del año 2018 identificó los siguientes aspectos: (i) más del 40% de las empresas habían sufrido un ataque en los doce meses anteriores; (ii) las cuestiones relativas a la ciberseguridad eran una alta prioridad para el 74% de los directores de empresas; y, (iii) solo el 27% de las compañías tenían una política formal o políticas que cubrían los riesgos de ciberseguridad (2018). Esta encuesta fue nuevamente realizada en marzo del año 2020 y en ella se subrayó, entre otras cuestiones de interés, que el número de empresas víctimas de ciberataques en los doce meses anteriores se había incrementado en un 46%[8].

Similares conclusiones se ratifican en el Data Breach Investigations Report que Verizon publica

---

1 Es ampliamente empleada en el arbitraje internacional, y una gran mayoría de los encuestados se encuentra a favor de que hacia el futuro se incremente el uso de las tecnologías en las salas de audiencias, […] el almacenamiento en la nube, las videoconferencias, la inteligencia artificial y las salas de audiencias virtuales [traducción libre].

2 Para mayor información, véase Fernández-Samaniego & Hierro Viéitez (2019). En dicho artículo, comentamos el Protocolo sobre Ciberseguridad en Arbitraje Internacional cuando todavía se encontraba en estado de borrador.

3 Verizon adquirió Yahoo en el año 2017. No obstante, esta adquisición se realizó por un importe menor del originalmente pactado, debido a dos ciberataques en los que se filtraron los nombres, fechas de nacimiento, números de teléfono y contraseñas de alrededor de un billón de usuarios de Yahoo.

4 Cobra vital importancia señalar, aunque sea de forma breve, que estos incidentes pueden provocar serios perjuicios económicos a las empresas, ya que pueden verse demandadas en procedimientos de reclamaciones monetarias. Tal es el caso, por ejemplo, de Facebook, empresa que ha sido demandada por el escándalo en el que está involucrada Cambridge Analytica. Para más información, véase Hern (2018); Cadwalladr & Graham-Harrison (2018).

5 Para mayor información, véase Online Trust Alliance (2019).

6 Para mayor información, véase United Kingdom Government, Department for Digital, Culture, Media & Sport (2020).

7 Para mayor información, véase United Kingdom Government, Department for Digital, Culture, Media & Sport (2018).

8 Para mayor información, véase United Kingdom Government (2017).

todos los años y que, para su edición de 2020, ha analizado 157.525 incidentes (Verizon, 2020). Sin embargo, dichas amenazas no se presentan únicamente en el mundo empresarial; sino que se encuentran presentes en otras instituciones también. En efecto, entre las organizaciones más afectadas por los ciberataques se encuentran los hospitales[9], despachos de abogados[10], e incluso instituciones y procedimientos arbitrales.

Ahora bien, centrándonos en el arbitraje internacional, no es controvertido afirmar que una de las grandes ventajas por las que los usuarios deciden dirimir sus controversias mediante este método alternativo es la confidencialidad que provee[11]. Este último aspecto es una de las piezas clave que diferencia al arbitraje de la litigación ante cortes nacionales. En ese sentido, para mantener esta diferencia, algunos despachos de abogados han adoptado su propio protocolo de ciberseguridad[12]. Sin embargo, dicha confidencialidad también se ha visto comprometida en varias ocasiones, a causa de la actuación de las diversas personalidades involucradas en los procedimientos arbitrales (empresas, despachos de abogados, Estados, entidades públicas, entre otras) y, asimismo, a causa de la presencia de datos sensibles y del impacto que el resultado de dichos procedimientos puede llegar a tener en el mercado financiero.

Prueba de este último aspecto, fue el hackeo en el año 2015 de la página web de la Corte Permanente de Arbitraje de La Haya (CPA). Dicho ataque se produjo durante la celebración de una audiencia entre los países de China y Filipinas sobre una delicada controversia fronteriza marítima. Este suceso provocó que los datos personales de todo aquel que accediera a la web estuvieran expuestos (Fernández-Samaniego & Hierro Viéitez, 2019, p. 5).

En ese mismo año se dio un suceso similar que involucraba al despacho de abogados Curtis, Mallet-Prevost, Colt & Mosle. Este interpuso una demanda en nombre de la República de Kazajistán tras conocer que las cuentas de correo electrónico y ordenadores de varios funcionarios del gobierno habían sido hackeadas mientras el despacho asesoraba a dicho Estado con respecto a un acuerdo con el consorcio dedicado a desarrollar el yacimiento de petróleo y gas de Kashagan[13].

Además, es común que un tribunal arbitral tenga que decidir, durante la tramitación del procedimiento, sobre la admisión de documentos que habían sido objeto de hackeos o filtraciones[14]. Tal es el caso, por ejemplo, de *Libananco Holdings Co. Limited c. Turquía*, en el cual el demandante presentó una solicitud informando al tribunal que había tenido conocimiento:

> [t]urkish court orders requested and obtained by [r]espondent in 2007 and 2008, expressly to conduct intercepts of emails and MSN instant messages not only sent by and to persons associated with [c]laimant, but also approximately 1,000 privileged, private and confidential emails sent by, to and between [c]laimant's counsel of record in connection with this arbitration over the past year[15] (*Libananco Holdings Co. Limited c. Turquía*, 2008, pár. 19).

En este caso en particular, el tribunal arbitral finalmente reconoció la importancia de la confi-

9 A modo de ejemplo, en el año 2017 se produjo un ciberataque que tuvo como objetivo las vulnerabilidades de los hospitales de Ontario y en el año 2016 otro ataque bloqueó el sistema informático del hospital de Ottawa (CBC News, 2017).

10 Recordemos que DLA Piper fue objeto de un ciberataque en el año 2017 que supuso la interrupción del trabajo por varios días. Asimismo, que la firma de abogados panameña Mossack Fonseca desapareció en julio del año 2016 por el incidente de los Papeles de Panamá. Este tipo de ataques fueron previstos en el año 2016 por el Federal Bureau of Investigation de los Estados Unidos, que emitió la "alerta 160304-001" en la que se advertía de posibles ciberataques a despachos de abogados. Dichos ataques tenían como objetivo principal la obtención de información no pública para realizar, posteriormente, ofertas en el mercado de valores y así obtener beneficios significativos. Para más información, véase Federal Bureau of Investigation, Cyber Division (2016).

11 En este sentido, el 2018 International Arbitration Survey: The Evolution of International Arbitration, elaborado por White & Case y Queen Mary University muestra cómo la confidencialidad y privacidad constituye una de las características más valiosas del arbitraje internacional (White & Case & Queen Mary University of London, 2018, p. 7).

12 Los despachos de abogados Debevoise & Plimpton LLP y Bryan Cave Leighton Paisner (BCLP) son algunos de ellos. En efecto, el BCLP publicó en el año 2019 su International Arbitration Survey: Don't be the weakest link. En ese sentido, véase Debevoise & Plimpton LLP (2017).

13 Para mayor información, véase el caso *Caratube International Oil Company LLP y Devincci Salah Hourani c. Kaz*. (2017).

14 En el presente artículo no se profundizará sobre qué criterios pueden adoptar los tribunales ordinarios o arbitrales sobre la admisión de documentos obtenidos ilícitamente por las partes. Para ello, véase Bertrou & Alekhin (2018).

15 Órdenes del tribunal judicial turco fueron solicitadas y obtenidas por la demandada en 2007 y 2008 expresamente para llevar a cabo la interceptación de correos electrónicos y mensajería instantánea de MSN tanto enviada por y hacia personas asociadas a la demandante, así como alrededor de mil mensajes de correo electrónico de carácter privilegiado, privado y confidencial que fueron enviados por, hacia y entre los representantes legales de la demandante vinculados a este arbitraje a lo largo del año pasado [traducción libre].

dencialidad de la información y decidió excluir del expediente todos los documentos e información privilegiados que se habían presentado[16].

No obstante, los tribunales arbitrales no siempre han mostrado una actitud negativa respecto de la aportación de documentos que previamente habían sido objeto de hackeo o filtración. Un ejemplo de ello es el caso *Caratube International Oil Company LLP y Devincci Salah Hourani c. Kazajistán* (2017). En este caso, los demandantes solicitaron la admisión de un total de once documentos que, a pesar de haber sido filtrados, estaban disponibles públicamente en una página web apodada KazakhLeaks[17].

En ese sentido, la parte demandada objetó la admisión de dichos documentos alegando que, además de haber sido filtrados, varios de ellos gozaban de una protección especial por estar sujetos al secreto profesional entre abogado y cliente. El tribunal arbitral emitió su decisión y autorizó lo siguiente: "the submission by the Claimants on the record of non-privileged leaked documents, but not of privileged leaked documents (namely privileged attorney-client communications)"[18] (*Caratube International Oil Company LLP y Devincci Salah Hourani c. Kazajistán*, 2017, pár. 156).

A pesar del aumento de este tipo de amenazas, cabe mencionar que en los últimos años también se han promulgado tres instrumentos legislativos en Europa con importantes efectos sobre la ciberseguridad: (i) el Reglamento General de Protección de Datos (en adelante, RGPD)[19]; (ii) la Directiva 2016/1148[20], relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión (en adelante, Directiva NIS por sus siglas en inglés); y, (iii) el Reglamento (UE) 2019/881[21] relativo a ENISA (Agencia de la Unión Europea para la Ciberseguridad) y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación (Reglamento sobre la Ciberseguridad).

El RGPD entró en vigor el año 2018; es decir, entro a regir más de seis años después de la propuesta sobre una nueva regulación que realizó la Comisión Europea el 25 de enero del año 2012. El RGPD aumenta los requisitos de ciberseguridad en su artículo 25, mediante el establecimiento de obligaciones de notificación de violaciones de seguridad a la autoridad de control y al propio afectado en determinados supuestos. Asimismo, establece una serie de medidas de responsabilidad activa entre las que se incluyen, entre sus artículos 37 a 39, la obligación en determinados supuestos de nombrar a un Delegado de Protección de Datos (DPO, por sus siglas en inglés).

Por su parte, la Directiva NIS supuso un importante impulso para la ciberseguridad en sectores vitales de la economía como el de la energía, transporte, agua, banca, infraestructuras del mercado financiero, sanidad e infraestructura digital (Fernández-Samaniego & Hierro Viéitez, 2019, p. 2). Asimismo, el recientemente aprobado Reglamento sobre la Ciberseguridad en Europa, además de reforzar el rol de la Agencia de la Unión Europea para la Ciberseguridad (ENISA), establece un marco para la creación de esquemas europeos de certificación de la ciberseguridad, con la finalidad de garantizar un nivel adecuado de ciberseguridad de los productos, servicios y procesos.

De forma independiente a los instrumentos legislativos mencionados, en los últimos años se han promulgado diferentes normas de *soft-law*, cuyo fin es informar a los usuarios sobre la importancia de la ciberseguridad y proporcionarles unas guías que pueden seguir para mitigar este tipo de ciberamenazas. Entre estas normas se encuentra el Protocolo de Ciberseguridad en Arbitraje Internacional (en adelante, el Protocolo). Este ha sido

16 Para mayor información, véase el caso *Libananco Holdings Co. Limited c. Turquía.* Otro caso similar en el que el tribunal arbitral examinó la ilicitud de las pruebas aportadas por las partes y finalmente rechazó su inclusión en el procedimiento; este es el caso *EDF ´Services´ Limited c.* Rumanía (2009).

17 El acceso público a estos documentos se debió al hackeo que sufrieron numerosos funcionarios del Gobierno de Kazajistán en sus cuentas de correo electrónico y, aproximadamente, el número de documentos filtrados ascendió a 60.000. Para mayor información, véase Ross (2015b).

18 La presentación en el expediente a cargo de los demandantes de documentos filtrados no privilegiados, mas no de documentos filtrados privilegiados (es decir, comunicaciones entre abogado-cliente de carácter privilegiado) [traducción libre].

19 Para mayor información, véase el Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, acerca de la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos).

20 Para mayor información, véase la Directiva 2016/1148 de la Unión Europea, de 6 de julio de 2016.

21 Para mayor información, véase el Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo relativo a ENISA (Agencia de la Unión Europea para la Ciberseguridad) y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación y por el que se deroga el Reglamento (UE) n. 526/2013 (Reglamento sobre la Ciberseguridad).

elaborado por la International Council for Commercial Arbitration (en adelante, ICCA), la New York City Bar Association (en adelante, NYC Bar) y el International Institute for Conflict Prevention and Resolution (en adelante, CPR).

II. EL PROTOCOLO DE CIBERSEGURIDAD EN ARBITRAJE INTERNACIONAL DEL ICCA, NYC BAR Y CPR (EDICIÓN 2020)

El 21 de noviembre del año 2019, el Protocolo[22] se dio a conocer en la *New York Arbitration Week*. Este ha sido elaborado por la ICCA, la NYC Bar y el CPR. Asimismo, representa el resultado de dos años de trabajo en el que participaron más de 240 personas procedentes tanto de instituciones arbitrales como de despachos de abogados, expertos en procedimientos arbitrales y organizaciones no gubernamentales; las cuales presentaron sus comentarios y sugerencias al borrador del Protocolo (en adelante, *Draft*) publicado en abril del año 2018[23].

Ahora bien, como su nombre indica *–2020 Edition–*, el Protocolo estará en continua revisión porque podrá recibir comentarios de los usuarios (por ejemplo, sobre su experiencia práctica al aplicarlo) y se adecuará a los cambios que se produzcan en el futuro en el sector de la tecnología.

En ese sentido, el Protocolo (2020) tiene dos objetivos principales señalados en su preámbulo. El primero es proporcionar un marco a través del cual se pueda determinar qué medidas de seguridad resulta razonable aplicar en cada arbitraje según los riesgos que existan en él. El segundo, concientizar a todos los usuarios sobre cuán importante es que la información proporcionada en un procedimiento arbitral esté segura, puesto que, como afirma Allen Waxman[24], "ensuring that proceedings in arbitration protect the security of the information at issue is critical to arbitration's continued vitality"[25] (International Institute for Conflict Prevention & Resolution [CPR], 2019).

Ahora bien, a diferencia del *Draft*, el Protocolo (International Council for Commercial Arbitration [ICCA], New York City Bar Association, & International Institute for Conflict Prevention & Resolution [CPR], 2020) está dividido en catorce principios complementados con comentarios y *schedules*[26]. Asimismo, a través de sus diferentes principios se muestra la relevancia de la ciberseguridad en el arbitraje internacional[27]. En efecto, como hemos visto, el arbitraje internacional y los procedimientos arbitrales también pueden ser víctimas de ciberataques y, por ello, podemos afirmar que su integridad depende del grado de protección que se proporcione a los datos y a la información intercambiada entre las partes, el tribunal arbitral y, en su caso, la institución arbitral.

En ese sentido, si bien debemos tener en cuenta que el Protocolo no pretende otorgar una solución única para todos los casos, los principios 1, 2 y 5 especifican que este debe adaptarse a las circunstancias del caso concreto y que tanto los árbitros como las partes[28] (y la institución arbitral, de haberla) deben considerar cuáles medidas de seguridad resultan razonablemente aplicables en su procedimiento. A su vez, tiene la finalidad de medir el impacto que tendrían en el mismo. Para ello, los principios 6 a 8 (así como el *schedule* B) son de gran ayuda al enumerar los factores y riesgos a tener en cuenta a la hora de determinar qué medidas se podrían adoptar.

Ahora bien, una de las cuestiones a considerar es el perfil del arbitraje y los riesgos que en él se puedan dar. Por ello, es relevante estudiar la naturaleza de la información que se va a aportar. Es decir, se debe saber si esta contiene datos confidenciales o sensibles y cómo será almacenada durante el procedimiento. Asimismo, se aconseja perfilar el objeto de la disputa para prever si es susceptible de ser víctima de algún tipo de ciberamenaza[29]. La identidad de las partes en el arbitraje también juega un papel relevante ya que el riesgo de amenaza se intensifica de las siguientes formas: (i) si

[22] Para mayor información, véase International Council for Commercial Arbitration [ICCA], New York City Bar Association, International Institute for Conflict Prevention & Resolution [CPR] (2020).

[23] Para mayor información, véase ICCA, New York City Bar Association y CPR (2018).

[24] Allen Waxman es presidente y *CEO* de CPR.

[25] Garantizar que los procedimientos arbitrales protejan la seguridad de la información en cuestión es crítico para la continua vitalidad del arbitraje [traducción libre].

[26] Para conocer cuáles son las principales diferencias entre el *Draft* y el Protocolo, véase ICCA, New York City Bar Association y CPR (2019).

[27] Si bien el Protocolo se ha redactado teniendo en mente al arbitraje comercial internacional, también se estipula en su preámbulo que puede ser una buena referencia para arbitrajes domésticos o de inversiones.

[28] El propio Protocolo (2020) menciona que con el término "partes" hace referencia tanto a las partes del procedimiento como a sus representantes legales. De igual modo, define "tribunal arbitral" como árbitro único o panel de árbitros.

[29] Para mayor información, véase el principio 6 (a) y (b); s*chedule* B. I y III del Protocolo (2020).

está involucrada una entidad que previamente ha sufrido un ciberataque o posee gran cantidad de información comercial confidencial; (ii) si está involucrada una figura pública, un funcionario o ejecutivo de alto rango o celebridad; o, (iii) si el asunto afecta a algún gobierno o involucra información gubernamental[30].

Otro extremo a tener en cuenta son los recursos de los que dispone cada una de las partes, los costos que puede ocasionarles la implementación de las medidas de seguridad y las consecuencias que se pueden derivar en el arbitraje en caso de no adoptarlas[31]. Por su parte, el contenido del *schedule* C es muy útil, puesto que, además de complementar los principios 7 y 8 del Protocolo, proporciona un listado no exhaustivo de ejemplos sobre las medidas y procedimientos de seguridad que se pueden adoptar atendiendo a las peculiaridades del arbitraje. En efecto, incide en que las medidas que se detallan no tienen que adoptarse en su integridad, puesto que algunas son alternativas o complementarias a otras, e incluso pueden quedar obsoletas con el transcurso del tiempo.

No obstante, surge la siguiente pregunta: ¿quién debe proponer y autorizar la adopción de estas medidas de seguridad? Y, sobre todo, ¿en qué momento? En este sentido se pronuncian los principios 9 a 13 del Protocolo. En efecto, las partes conocen el objeto del arbitraje y son las que se encuentran en mejor posición para saber sus implicancias y el impacto que el resultado puede tener en el mercado. Por ello, deben ser ellas las que tienen que intentar acordar las medidas o procedimientos de seguridad que podrán llevarse a cabo durante la tramitación del procedimiento.

Sin embargo, el Protocolo concede al tribunal arbitral[32] la potestad de autorizarlas y modificarlas. Es importante subrayar que, para ello, tendrá que tener en consideración las posiciones de las partes, los acuerdos que hayan podido alcanzar y la evolución de las circunstancias del caso. En ese sentido, resultarán de especial interés los casos en los que el tribunal arbitral tenga que decidir sobre la adopción de una medida especialmente onerosa o desproporcionada, puesto que en esos supuestos se dejan en el aire varias cuestiones como ¿quién deberá sufragar los costes? Si la respuesta es ambas partes, ¿en qué proporción? Y, ¿qué ocurriría si la institución arbitral o alguna de las partes, una vez adoptada la medida, no es capaz de llevarla a cabo?

Sin embargo, independientemente de quién adopte la medida (sea por acuerdo entre las partes o por decisión del tribunal arbitral) sobre lo que no hay que tener duda alguna es sobre el momento de su adopción. El Protocolo es claro al establecer, de forma lógica, que estas deben adoptarse "as early as practicable in the arbitration, which ordinarily **will not be later than the first case management conference**"[33] (2020, p. 3) [el énfasis es nuestro] y ello porque puede ponerse en riesgo y frustrarse el propósito de la medida de ciberseguridad.

Como puede apreciarse, el Protocolo aborda diversas cuestiones que son actualmente controvertidas. No obstante, en este no se menciona la responsabilidad en la que podrían incurrir las partes, los árbitros y la institución arbitral a causa de la adopción de este tipo de medidas. Por este motivo, sería conveniente añadir en las próximas ediciones del Protocolo un comentario sobre la conveniencia de que los árbitros, las partes y, en su caso, la institución arbitral consideren la contratación de un seguro de ciber-responsabilidad a la hora de decidir sobre la adopción de estas medidas de ciberseguridad.

III. EL PROTOCOLO COMO INSTRUMENTO DE *SOFT-LAW* Y OTRAS NORMAS SOBRE CIBERSEGURIDAD EN ARBITRAJE INTERNACIONAL

El número de normas *soft-law* en arbitraje internacional se ha visto incrementado considerablemente en los últimos años[34]. En efecto, dependiendo del enfoque que los autores quieran dar al texto, estas normas pueden aparecer bajo la forma de directrices, códigos, recomendaciones, reglas, no-

30 Para mayor información, véase el *schedule* B. II del Protocolo (2020).

31 Para mayor información, véase el principio 6 (c); *schedule* B. IV del Protocolo (2020).

32 Existe cierta controversia con respecto a la naturaleza de las medidas de ciberseguridad. En efecto, ¿tienen carácter procedimental o administrativo? La diferencia radica en que, si es procedimental, el órgano apropiado para su adopción será el tribunal; mientras que si es considerada como administrativa, podrá entenderse que la medida es capaz de ser adoptada por la institución arbitral que supervise el procedimiento. En este sentido, para mayor información véase Morel de Westgaver (2017; 2019).

33 Tan pronto como puedan ser aplicables en el arbitraje, lo que usualmente no excede la primera conferencia para el manejo de la causa [traducción libre].

34 Para más información sobre qué son las normas de *soft-law* en arbitraje internacional y cuál es su impacto, véase Erdem (2017).

tas, guía, entre otras. En ese sentido, su fin es proporcionar a las partes un estándar recomendado sobre una cuestión para que puedan adoptarlas voluntariamente o bien usarlas como orientación y adaptarlas a sus necesidades. Así ocurre, por ejemplo, con las Reglas de la International Bar Association (en adelante, IBA) sobre la Práctica de la Prueba en el Arbitraje Internacional[35].

Ahora bien, que el Protocolo sea un instrumento de *soft-law* es un gran acierto. En el arbitraje internacional, las partes están sujetas a una pluralidad de normas que originan, en ocasiones, potenciales conflictos de intereses. Por ello, es mucho más útil elaborar una norma de *soft-law* que un elenco de reglas estrictas que puedan provocar más problemas y cuestiones controvertidas que soluciones[36]. En efecto, con la finalidad de evitar este aspecto, el principio 4 dispone que el Protocolo no prevalecerá sobre las leyes aplicables, ni sobre cualquier otra ley que establezca obligaciones vinculantes (tales como aquellas reglas procedimentales a las que se hayan sometido las partes u obligaciones éticas o profesionales).

Asimismo, para garantizar su eficacia, el Protocolo declara la necesidad de que la medida de ciberseguridad adoptada en el seno de un procedimiento arbitral sea conocida y cumplida por todas las personas que estén involucradas en el arbitraje, ya sea directa o indirectamente. Se hace, de tal forma, referencia al término *weak link*, en el sentido de que todos los participantes son interdependientes entre sí y que el fallo en la custodia de la información que pueda cometer uno afecta a todos.

Además del Protocolo, no debemos olvidar que recientemente se han publicado otras normas de *soft-law* que abordan temas de ciberseguridad. Por un lado, la ICCA y la IBA han unido sus fuerzas y han creado un grupo de trabajo en Data Protection in International Arbitration[37]. Su objetivo es elaborar una guía práctica sobre el impacto que tienen los principios de protección de datos, en particular el RGPD, en los procedimientos de arbitraje internacional. Asimismo, posee la finalidad de ayudar a los usuarios a identificar y comprender las obligaciones de protección de datos y privacidad a las que pueden estar sujetos en un contexto de arbitraje internacional.

Por otro lado, la IBA publicó en el 2018 las Cybersecurity Guidelines[38] y son un excelente complemento para el Protocolo. Estas directrices se centran en analizar y explicar las mejores prácticas que los despachos de abogados pueden adoptar para prevenir la vulneración de datos y podrían ser útiles, *mutatis mutandis*, para todos los participantes de un procedimiento arbitral.

Inclusive existen varias instituciones arbitrales que, debido al incremento de estas ciberamenazas, han decidido incorporar en sus reglamentos de arbitraje referencias sobre ciberseguridad. Tal es el caso del reglamento de arbitraje del Hong Kong International Arbitration Centre (en adelante, HKIAC) cuyo artículo 3.1(e) dispone lo siguiente: "Any written communication pursuant to these Rules shall be deemed to be received by a party, arbitrator, emergency arbitrator or HKIAC if […] uploaded to any secured online repository that the parties have agreed to use"[39] (2018). Asimismo, la Corte de Arbitraje Internacional (en adelante, CCI) también ha dedicado varios apartados a cuestiones de ciberseguridad en su documento Note to parties and arbitral tribunals on the conduct of the arbitration under the ICC Rules of Arbitration (2019).

Sobre este último aspecto, los apartados 80 a 91 de esta nota aclaran que, al aceptar participar en un arbitraje de la ICC, todas las partes[40] involucradas aceptan que sus datos personales sean recopilados, transferidos, archivados y, según sea el caso, publicados. Además, se aconseja a los tribunales arbitrales que mencionen esta cuestión en los *Terms of Reference* y que tanto ellos como las partes se remitan cuando lo estimen necesario al Report on the Use of Information Technology in International Arbitration[41], documento elaborado por la Comisión de Arbitraje y ADR de la CCI para asegurar que las medidas de protección sobre estos datos se preservan durante todo el procedimiento arbitral.

35 Para mayor información, véase International Bar Association (IBA) (2010).

36 Para mayor información, véase Kaufmann-Kohler (2010).

37 Para mayor información, véase ICCA-IBA (2020).

38 Para mayor información, véase International Bar Association (IBA) (2018).

39 Cualquier comunicación escrita acorde a estas Reglas debe ser considerada como apta para ser recibida por las partes, árbitros, árbitros de emergencia o la HKIAC de ser […] subida a cualquier repositorio en línea seguro cuyo uso haya sido acordado por las partes [traducción libre].

40 Se hace así referencia a las partes, sus representantes, los árbitros (y, en su caso, el secretario administrativo), los testigos, los expertos y cualquier otra persona que pueda tener alguna implicación en el arbitraje.

41 Para mayor información, véase Corte Internacional de Arbitraje [CCI] (2017).

Como podemos apreciar, existe un elenco de normas que abordan, con mayor o menor detalle, temas de ciberseguridad y proporcionan a los usuarios las herramientas necesarias para intentar prevenir brechas en la seguridad o vulneraciones de datos. En lo que respecta al Protocolo, no es extraño pensar que, con el tiempo, este pueda convertirse en un código de buenas prácticas, tal y como ahora es, por ejemplo, el Código de Buenas Prácticas Arbitrales del Club Español del Arbitraje[42].

IV. INFLUENCIA DEL PROTOCOLO EN LAS NORMAS DE *SOFT-LAW* SOBRE AUDIENCIAS VIRTUALES ORIGINADAS POR LA PANDEMIA A CAUSA DE LA COVID-19

Desde que, a mediados de marzo del año 2020, la pandemia de la COVID-19 tomó dimensiones históricas, las principales instituciones arbitrales del mundo empezaron a adoptar instrumentos de *soft-law* para poder continuar sus procedimientos de forma telemática y guiar a los participantes en la conducción de audiencias en remoto o virtuales. Esta nueva realidad ha demostrado que el Protocolo es una guía imprescindible o *leading light* en esta materia.

Ahora bien, el Protocolo ha tenido en cuenta los siguientes instrumentos: (i) Nota de orientación de la CCI sobre Posibles Medidas Destinadas a Mitigar los Efectos de la Pandemia del COVID-19[43]; (ii) KCAB International's Seoul Protocol on Video Conferencing in International Arbitration[44]; (iii) Nota sobre organización de audiencias virtuales elaborado por la Corte de Arbitraje de Madrid[45]; (iv) CPR's Annotated Model Procedural Order for Remote Video Arbitration Proceedings[46]; (v) el artículo Draft Zoom Procedural Order[47]; (vi) AAA-ICDR's Best Practices Guide for Maintaining Cybersecurity and Privacy[48]; (vii) ClArb's Guidance Note on Remote Dispute Resolution Proceedings[49] y; (viii) African Arbitration Academy's Protocol on Virtual Hearings in Africa[50].

Asimismo, la propia administración de justicia como el Consejo General del Poder Judicial en España han referenciado al Protocolo en su Guía para la celebración de actuaciones judiciales telemáticas[51], lo que demuestra la importancia de este instrumento como ya vaticinamos cuando todavía se encontraba en fase de borrador.

V. CONCLUSIONES

Resultaba de vital importancia adoptar una norma de *soft-law* que estableciera el marco de actuación sobre la ciberseguridad en arbitraje internacional. En el actual contexto de implantación progresiva de actuaciones remotas y audiencias virtuales –acelerado por la pandemia originada por la COVID-19–, entendemos que este Protocolo puede ser útil no solo para el arbitraje (doméstico, comercial internacional o de inversiones), sino también para otras áreas del derecho.

En ese sentido, el Protocolo, sienta unas bases claras que permiten que se constituya como un documento completo y de referencia ante un panorama en el que las vulneraciones de datos y brechas en la ciberseguridad son comunes. Los comentarios y *schedules* que forman parte del Protocolo (y, por ello, complementan los principios) no solo aportan conciencia a los usuarios acerca de los riesgos que pueden darse en el arbitraje internacional; sino también les ofrece un marco que les sirve como guía y que pueden consultar para mitigar la producción de riesgos.

El Protocolo, asimismo, insiste en que el elenco de medidas sobre ciberseguridad que en este se detallan deben acogerse atendiendo a las circunstancias y peculiaridades del caso concreto. Sugiere también que los usuarios –en la medida de lo posible– tienen que garantizar el cumplimiento de dichas medidas.

Finalmente, para que estas medidas no queden obsoletas, es encomiable que el Protocolo haya manifestado su seria intención de actualizarse acogiendo las mejores prácticas de ciberseguridad. Para ello, será vital observar diversos aspectos, tales como la evolución del sector tecnológi-

42 Para mayor información, véase el Club Español del Arbitraje (2019).

43 Para mayor información, véase la Corte Internacional de Arbitraje [CCI] (2020).

44 Para mayor información, véase KCAB International (2020).

45 Para mayor información, véase la Corte de Arbitraje de la Cámara de Comercio, Industria y Servicios de Madrid (2020).

46 Para mayor información, véase International Institute for Conflict Prevention & Resolution [CPR] (2020).

47 Para mayor información, véase Cohen (2020). Draft Zoom Hearing Procedural Order.

48 Para mayor información, véase American Arbitration Association (2020).

49 Para mayor information, véase Chartered Institute of Arbitrators (ClArb) (2020).

50 Para mayor información, véase African Arbitration Academy (2020).

51 Para mayor información, véase Consejo General del Poder Judicial de España (2020).

co, su regulación, los nuevos riesgos que podrían producirse en el seno de un procedimiento o las experiencias prácticas de los usuarios a la hora de aplicar el Protocolo.

REFERENCIAS

Bertrou, G., & Alekhin, S. (2018). The Admissibility of Unlawfully Obtained Evidence in International Arbitration: Does the End Justify the Means? *Les Cahiers de l'Arbitrage*, (4), 11-71.

Bienvenu, P., & Grant, B. (2019). Data protection and cyber risk issues in arbitration. En Rogers, J. (Ed.), *International Arbitration Report* (pp. 19-21). Norton Rose Fullbright. https://www.nortonrosefulbright.com/-/media/files/nrf/nrfweb/knowledge-pdfs/emea_15747_newsletter__international-arbitration-report-_issue-13.pdf?la=fr-ca&revision=

Bryan Cave Leighton Paisner (2019). *International Arbitration Survey: Don't be the weakest link*. Bryan Cave Leighton Paisner. https://www.bclplaw.com/images/content/1/6/v2/160089/Bryan-Cave-Leighton-Paisner-Arbitration-Survey-Report-2018.pdf

Cadwalladr, C., & Graham-Harrison, E. (17 de marzo de 2018). *Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach*. The Guardian. https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election

CBC News (14 de mayo de 2017). *Oshawa hospital among thousands of global 'ransomware' cyberattack victims*. https://www.cbc.ca/news/canada/toronto/oshawa-hospital-cyberattack-1.4114758

Cohen, S. (2020, en preparación). *Draft Zoom Hearing Procedural Order*. TDM. https://www.transnational-dispute-management.com/journal-advance-publication-article.asp?key=1815

Corte Internacional de Arbitraje [CCI] (2017) *Report on the Use of Information Technology in International Arbitration*. ICC Commission on Arbitration and ADR. https://iccwbo.org/publication/information-technology-international-arbitration-report-icc-commission-arbitration-adr/

Curtis, Mallet-Prevost, Colt y Mosle LLP (19 de enero de 2016). *Curtis Advises Kazakhstan on Amended Agreement for Kashagan Project*. Curtis. https://www.curtis.com/our-firm/news/curtis-advises-kazakhstan-on-amended-agreement-for-kashagan-project

Debevoise & Plimpton LLP (2017). *Protocol to Promote Cybersecurity in International Arbitration*. http://www.debevoise.com/~/media/files/capabilities/cybersecurity/protocol_cybersecurity_intl_arb_july2017.pdf

Erdem, M. (10 de marzo de 2017). *Turkey: Soft Law in International Arbitration*. Mondaq. https://www.mondaq.com/turkey/arbitration-dispute-resolution/575696/soft-law-in-international-arbitration

Federal Bureau of Investigation, Cyber Division (4 de marzo de 2016). *Criminal-Seeking-Hacker" Requests Network Breach for Insider Trading Operation* [Alerta]. FBI Bulletin. https://info.publicintelligence.net/FBI-Insider-TradingHacking.pdf

Fernández-Samaniego, J. & Hierro Viéitez, G. (2019). The Draft ICCA-CPR-New York City Bar Association Protocol for Cybersecurity in Arbitration: A Leading Light, at Least. *TDM*, (3). https://www.transnational-dispute-management.com/article.asp?key=2645

Fiegerman, S. (21 de febrero de 2017). *Verizon cuts Yahoo deal price by $350 million*. CNN Business. https://money.cnn.com/2017/02/21/technology/yahoo-verizon-deal/index.html

White & Case & Queen Mary University of London (2018). *2018 International Arbitration Survey: The Evolution of International Arbitration*. White & Case; Queen Mary University of London. http://www.arbitration.qmul.ac.uk/media/arbitration/docs/2018-International-Arbitration-Survey---The-Evolution-of-International-Arbitration-(2).PDF

Hern, A. (19 de diciembre de 2018). *Facebook: Washington DC sues tech giant over Cambridge Analytica data use*. The Guardian. https://www.theguardian.com/technology/2018/dec/19/facebook-cambridge-analytica-washington-dc-lawsuit-data

International Council for Commercial Arbitration [ICCA-IBA] (2020). The ICCA-IBA Roadmap to Data Protection in International Arbitration [Borrador para consulta pública]. *The ICCA Reports*, 7. https://www.arbitration-icca.org/media/14/18191123957287/roadmap_28.02.20.pdf

International Institute for Conflict Prevention & Resolution [CPR] (21 de noviembre de 2019). *Working Group Releases Cybersecurity Protocol for International Arbitration*. https://www.cpradr.org/news-publications/press-releases/2019-11-21-working-group-releases-cybersecurity-protocol-for-international-arbitration-2020

Kaufmann-Kohler, G. (2010). Soft Law in International Arbitration: Codification and Normativity. *Journal of International Dispute Settlement*, *2*(11), 1-17. https://doi.org/10.1093/jnlids/idq009

Morel de Westgaver, C. (6 de octubre de 2017). *Cybersecurity in International Arbitration – A Necessity And An Opportunity For Arbitral Institutions*. Kluwer Arbitration Blog. http://arbitrationblog.kluwerarbitration.com/2017/10/06/cyber-security/?doing_wp_cron=1596504328.3245139122009277343750

(15 de febrero de 2019). *Cybersecurity in International Arbitration: Don't be the Weakest Link*. Kluwer Arbitration Blog. http://arbitrationblog.kluwerarbitration.com/2019/02/15/cybersecurity-in-international-arbitration-dont-be-the-weakest-link/?doing_wp_cron=1596503920.9210839271545410156250

Naish, V. (25 de noviembre de 2018). *Cybersecurity in Arbitral Proceedings: How to Kick-Start the Conversation about Protecting your Clients'*. Kluwer Arbitration Blog. http://arbitrationblog.kluwerarbitration.com/2018/11/25/cybersecurity-in-arbitral-proceedings-how-to-kick-start-the-conversation-about-protecting-your-clients-data/?doing_wp_cron=1596504680.5694000720977783203125

Online Trust Alliance (2019). *2018 Cyber Incident & Breach Trends Report. Review and Analysis of 2018 Cyber Incidents and Key Trends to Address*. https://www.internetsociety.org/wp-content/uploads/2019/07/OTA-Incident-Breach-Trends-Report_2019.pdf

Pinsent Masons & Queen Mary University of London (2019). *International Arbitration Survey - Driving Efficiency in International Construction Disputes*. Pinsent Masons. https://www.pinsentmasons.com/-/media/pdfs/en-gb/special-reports/international-arbitration-survey-november-2019.pdf?la=en-gb&hash=2BF84CD21097CCBAD3C1A9DCD9263EBB

Ross, A. (2015a, 23 de julio). *Cybersecurity and confidentiality shocks for the PCA*. Global Arbitration Review. https://globalarbitrationreview.com/article/1034637/cybersecurity-and-confidentiality-shocks-for-the-pca

(2015b, 22 de septiembre). *Tribunal rules on admissibility of hacked Kazakh emails*. Global Arbitration Review. https://globalarbitrationreview.com/article/1034787/tribunal-rules-on-admissibility-of-hacked-kazakh-emails

Thompson, B. (6 de julio de 2017). *DLA Piper still struggling with Petya cyber-attack*. Financial Times. https://www.ft.com/content/1b5f863a-624c-11e7-91a7-502f7ee26895

United Kingdom Government (2017). *National Cyber Security Strategy 2016 to 2021*. https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021

United Kingdom Government, Department for Digital, Culture, Media & Sport (2018). *Cyber Security Breaches Survey 2018*. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/702074/Cyber_Security_Breaches_Survey_2018_-_Main_Report.pdf

(2020). *Cyber Security Breaches Survey 2020*. https://www.gov.uk/government/publications/cyber-security-breaches-survey-2020/cyber-security-breaches-survey-2020

U.S. Government Accountability Office [GAO]. (30 de Agosto de 2018). *Actions Taken by Equifax and Federal Agencies in Response to the 2017 Breach* [Reporte]. https://www.gao.gov/products/GAO-18-559

Verizon (2020). *2020 Data Breach Investigations Report*. https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf

LEGISLACIÓN, JURISPRUDENCIA Y OTROS DOCUMENTOS LEGALES

African Arbitration Academy (2020). *Protocol on Virtual Hearings in Africa.* https://www.africaarbitrationacademy.org/wp-content/uploads/2020/04/Africa-Arbitration-Academy-Protocol-on-Virtual-Hearings-in-Africa-2020.pdf

American Arbitration Association [AAA] (2020). AAA-ICDR Best Practices Guide for Maintaining Cybersecurity and Privacy. https://www.adr.org/sites/default/files/document_repository/AAA258_Best_Practices_Cybersecurity_Privacy.pdf

Caratube International Oil Company LLP y Devincci Salah Hourani c. Kaz, Caso CIADI ARB/13/13, Laudo 27 de septiembre de 2017. https://www.italaw.com/cases/2131

EDF 'Services' Limited c. Rum, Caso CIADI ARB/05/13, Laudo 8 de octubre de 2009. http://icsidfiles.worldbank.org/icsid/ICSIDBLOBS/OnlineAwards/C57/DC1215_En.pdf

Hong Kong International Arbitration Centre [HKIAC] (2018). *Administered Arbitration Rules*. https://www.hkiac.org/arbitration/rules-practice-notes/hkiac-administered-2018

International Bar Association [IBA] (2010). *IBA Rules on the Taking of Evidence in International Arbitration*. https://www.ibanet.org/Document/Default.aspx?DocumentUid=68336C49-4106-46BF-A1C6-A8F0880444DC

(2018). *Cyber Security Guidelines*. https://www.ibanet.org/LPRU/cybersecurity-guidelines.aspx

International Council for Commercial Arbitration [ICCA], New York City Bar Association, & International Institute for Conflict Prevention & Resolution (CPR) (2018). *Draft Cybersecurity Protocol for International Arbitration*. https://www.arbitration-icca.org/media/10/43322709923070/draft_cybersecurity_protocol_final_10_april.pdf

(2019). *Protocol Consultation Process*. https://www.arbitration-icca.org/media/14/44059883674056/protocol_consultation_process.pdf

(2020). *Protocol on Cybersecurity in International Arbitration (2020 Edition)*. http://documents.nycbar.org/files/ICCA-NYCBar-CPR-Cybersecurity-Protocol-for-International-Arbitration-Electronic-Version.pdf

International Institute for Conflict Prevention & Resolution [CPR] (2020). *Annotated Model Procedural Order for Remote Video Arbitration Proceedings*. https://www.cpradr.org/resource-center/protocols-guidelines/model-procedure-order-remote-video-arbitration-proceedings

KCAB International (2020). *Seoul Protocol on Video Conference in International Arbitration*. http://www.kcabinternational.or.kr/user/Board/comm_notice_view.do?BBS_NO=548&BD_NO=169&CURRENT_MENU_CODE=MENU0025&TOP_MENU_CODE=MENU0024

Libananco Holdings Co. Limited c. República de Turquía, Caso CIADI ARB/06/8, Decisión sobre cuestiones preliminares 23 de junio de 2008. https://www.italaw.com/cases/626

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos), 2016 O.J. (L 119), 1. https://www.boe.es/doue/2016/119/L00001-00088.pdf

Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo de 17 de abril de 2019 relativo a ENISA (Agencia de la Unión Europea para la Ciberseguridad) y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación y por el que se deroga el Reglamento (UE) n. 526/2013 (Reglamento sobre la Ciberseguridad), 2019 O.J. (L 151), 15. https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32019R0881&from=ES