LA LEY Mediación y Arbitraje nº 7, abril-junio 2021, Nº 7, 2 de abr. de 2021, Editorial Wolters Kluwer España

REGULACIÓN

La ciberseguridad: nuevo paradigma en el mundo del arbitraje

Cybersecurity: new paradigm in the world of arbitration

La ciberseguridad de la información, las redes, sistemas y datos se han convertido en una preocupación global que afecta de forma transversal a todas las actividades económicas o jurídicas, y en general a las sociedades e individuos en sus actividades más relevantes o más cotidianas. Los ataques e incidentes relacionados con la ciberseguridad de redes y sistemas, son una preocupación global no solo por el volumen e importancia que están alcanzando, sino por la velocidad a la que aumentan año tras año. Según Accenture, se estima que los costes directos e indirectos del cibercrimen a nivel mundial para el período 2019-2023 alcanzarán los 5.2 trillones de dólares. Según McAfee, en 2021 los costes de los ciberdelitos se incrementarán en un 50% con respecto al 2018 total y pasarán a representar ya el 1% de DDP global.

No obstante, esas cifras probablemente se verán superadas por los efectos de la pandemia de covid-19 que ha supuesto que las sociedades occidentales hayan iniciado procesos de trasformación digital masivos, acelerados e improvisados, de forma tal que se ha aumentado de forma exponencial la superficie de ataque a la misma velocidad que aumentábamos nuestra actividad digital en empresas y hogares. Entre las muchas consecuencias económicas, comerciales internacionales y sociales que ha traído la pandemia hay una indudable: existe una nueva percepción del riesgo en las sociedades occidentales. Se produce un cambio de paradigma que supone la búsqueda de seguridad y certezas. Las empresas y ciudadanos han percibido con claridad la total dependencia de las tecnologías digitales y las cuestiones relativas a la ciberseguridad se han convertido en centro de atención para la opinión pública: fraude online, phishing, desinformación, identidad digital, teletrabajo, reconocimiento facial, seguimiento digital, Inteligencia Artificial...

El Arbitraje nacional e internacional no es ajeno a esta tendencia, en un contexto en el que la pandemia covid-19 ha venido a aumentar la digitalización y tramitación en remoto de los procedimientos de arbitraje.

De ahí, que surjan regulaciones tendentes a asegurar dicha ciberseguridad así como protocolos y otras normas de *soft law* que buscan la aplicación del contenido de dichas regulaciones en el contexto de los procedimientos arbitrales.

Arbitraje, ciberseguridad de la información, procesos de transformación digital, inteligencia artificial.

The cybersecurity of information, networks, systems and data has become a global concern that transversally affects all economic or legal activities, and in general, societies and individuals in their most relevant or everyday activities. Attacks and incidents related to network and system cybersecurity are a global concern not only because of the volume and importance they are reaching, but also because of the speed at which they are increasing year after year.

However, these figures are likely to be surpassed by the effects of the covid-19 pandemic, which has meant that Western societies have embarked on massive, accelerated and improvised digital transformation processes, such that the attack surface has increased exponentially at the same rate as we have increased our digital activity in businesses and homes. Among the many economic, international trade and social consequences of the pandemic, one is undeniable: there is a new perception of risk in Western societies. There is a paradigm shift towards a search for security and certainty. Companies and citizens have clearly perceived the total dependence on digital technologies and cybersecurity issues have become the focus of public opinion: online fraud, phishing, disinformation, digital identity, teleworking, facial recognition, digital tracking, Artificial Intelligence...

National and international arbitration is no stranger to this trend, in a context in which the covid-19 pandemic has increased the digitisation and remote processing of arbitration proceedings.

Hence the emergence of regulations aimed at ensuring this cybersecurity, as well as protocols and other soft law rules that seek to apply the content of these regulations in the context of arbitration proceedings.

Arbitration, information cybersecurity, digital transformation processes, artificial intelligence.

Vicente Moret

Of Counsel de Andersen para el área de Derecho Procesal en la oficina de Madrid

Iñigo Rodríguez-Sastre

Socio de Andersen, responsable del área de Arbitraje

Elena Sevila

Socia de Andersen en el Área de Procesal y de Arbitraje Internaciona

I. LA CIBERSEGURIDAD Y SU MARCO REGULATORIO ACTUAL

En la actualidad, se están haciendo desde todas las instituciones ingentes esfuerzos por regular, como en el caso de los Estados o de la UE, o someter a regulación voluntaria, los riesgos derivados de la seguridad de redes y sistemas. Se trata de un esfuerzo global, intenso y novedoso que pretende sujetar de algún modo lo que ocurre en el ciberespacio a normas jurídica, con la dificultad que ello supone dadas las especiales características de la aplicación del Derecho en el ciberespacio (1) .

Si bien se puede decir que esa regulación está todavía en fase de conformación, lo cierto es que ya existe, especialmente en Europa un sólido marco regulador conformado ente otras por una serie de normas aprobadas en los últimos tres años. Ente otras normas se pueden citar:

- EU Cybersecurity Strategy. Dic 2020
- Reglamento UE 2019/881 relativo a ENISA y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación.
- Directiva 2019/713, de 17 de abril de 2019, sobre la lucha contra el fraude y la falsificación de medios de pago distintos del efectivo.
- Directiva UE 2016/1148 relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información. NIS
- Reglamento UE 2016/679 (RGPD) 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.
- Reglamento UE 910/2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior.

Ese cuadro va a quedar pronto desfasado ante el aluvión de normas que vienen desde Europa en los próximos meses: la nueva Directiva NIS2, el reglamento sobre Resiliencia de Entidades Financieras (DORA), el nuevo Reglamento eIDAS 2, el Convenio Budapest 2. O el Reglamento de resiliencia de infraestructuras críticas van a cambiar el entorno regulatorio de la ciberseguridad dentro de la UE.

II. EL ARBITRAJE, LA REGULACIÓN DE LA CIBERSEGURIDAD Y LA *SOFT LAW* APLICABLE AL ARBITRAJE

1. Especial referencia al Protocolo de ciberseguridad para arbitraje internacional de la ICCA-NCY Bar-CPR

Todo lo anterior motiva un necesario análisis del impacto de la ciberseguridad en unos de los ámbitos de aplicación del derecho más especiales que el del arbitraje internacional. Es indudable que este sector de actividad jurídica, dedicado a dirimir cuestiones relativas a disputa comerciales o económicas que afectan a sujetos muy relevantes y que implican también cantidades de dinero muy importantes, no quede exento del nuevo paradigma de gestión del riesgo digital.

En este sentido es especialmente relevante tener en cuenta que en 2020 se publica el Protocolo de ciberseguridad para arbitraje internacional de la ICCA-NCY Bar-CPR, como ejemplo de cuál es el camino a seguir para dotar a esa actividad arbitral de más garantías en cuanto a la ciberseguridad en sus actuaciones.

El protocolo es una buena muestra de cómo se puede contribuir a sentar las bases de una aproximación a la seguridad digital desde la óptica de la creación de estándares obligatorios para las partes pero que al mismo tiempo no constituyen una regulación formal de una materia. Se trata de unas recomendaciones para fomentar la adopción de normas en el ejercicio de la actividad arbitral por parte de la autoridad arbitral, las partes y la administración arbitral.

El protocolo, como *soft law*, es un código de comportamiento y de recomendaciones que se adaptan a la institución arbitral de forma que se deja margen de ajuste a los implicados en el arbitraje para graduar las obligaciones que se asumen. Esto significa que este protocolo es un documento orientativo y avalado por dos instituciones de prestigio en el ámbito del arbitraje.

Desde el punto de vista de su virtualidad tiene la gran ventaja de ser una herramienta válida para poder cubrir las dificultades que podrían generar los marcos de cumplimiento nacional o europeo en esta materia, al tratarse de normas que tienen un ámbito de validez limitado a la jurisdicción de los Estados de origen de esa normativa reguladora de la ciberseguidad. De esta forma mediante el Protocolo se fijan unos estándares y recomendaciones válidos para cualquier arbitraje internacional con independencia de la nacionalidad de las partes.

El propio protocolo señala que la necesidad de medidas razonables de seguridad de la información en los arbitrajes internacionales destaca por: el contexto litigioso del arbitraje, la naturaleza a menudo de alto valor y alto riesgo de las disputas, que aumenta el riesgo de incidentes de seguridad y la probabilidad de que esos incidentes causen pérdidas significativas.

Por otra parte, el intercambio de información que a menudo es información comercial confidencial y / o datos personales o de otro tipo regulados es otro factor de riesgo. En este contexto, la «confidencialidad» puede entenderse como un conjunto de reglas o restricciones que limitan el acceso a cierta información.

Por último, la naturaleza transfronteriza del proceso, que crea desafíos complejos para cumplir con los requisitos legales aplicables y agrava las consecuencias de un incidente de seguridad es señalada como otra razón de peso para proponer un protocolo que señale unas normas de obligado cumplimiento.

En cuanto al contenido, haya que decir que de sus análisis se extrae su acierto tanto en cuanto a la articulación de su aplicación como a las concretas recomendaciones y obligaciones que fija. Todas ellas están en línea con las recomendaciones y principios que las agencias (ENISA o NIST por ejemplo) y Estados han puesto en marcha a nivel europeo o nacional para aumentar el nivel de ciberseguridad.

Las finalidades del protocolo quedan claras desde el inicio:

1. Proporcionar un marco para determinar las medidas razonables de seguridad de la información para asuntos relativos a arbitraje individuales. Este marco incluye orientación práctica y de procedimiento para evaluar los riesgos de seguridad e identificar las medidas disponibles que pueden implementarse.

2. Aumentar la conciencia sobre la seguridad de la información en los arbitrajes internacionales. Esto incluye: los riesgos de seguridad de la información en el proceso arbitral, que incluyen tanto los riesgos de ciberseguridad como los de seguridad física.

Se considera por otra parte de vital importancia mantener la confianza del usuario en el régimen arbitral general y por ello se insiste en tener en cuenta los riesgos digitales.

> Las partes que brinden acceso a información arbitral cubierta por medidas de seguridad de la información a terceros deben asegurarse de que esos terceros estén al tanto de las medidas de seguridad aplicables

Asímismo, se adopta un enfoque centrado en la relevancia de las personas, del elemento humano que hace de este protocolo un documento en línea con lo que ahora es el nuevo paradigma de seguridad de la información señalado ya por la OTAN hace ya unos años y que se basa en una triple aproximación: tecnología, personas y procesos. En este caso el rol de las personas queda sufrientemente puesto de relieve ya que se considera que las personas involucradas en el arbitraje desempeñan un papel fundamental en la mitigación efectiva del riesgo. El protocolo señala que las partes, los árbitros y las instituciones administradoras contarán con empleados, abogados, asistentes legales, asistentes legales, aprendices, personal administrativo u otro personal de apoyo. Para mitigar el riesgo de incidentes de seguridad, la conciencia de la seguridad de la información debe permear las estructuras organizacionales y extenderse a esas personas, quienes deben conocer y cumplir con cualquier medida de seguridad de la información adoptada en el arbitraje.

Es más, se añade la obligación de tener en cuenta la ciberseguridad de terceros que de alguna manera sean suministradores de las partes, en línea con las nuevas preocupaciones que por ejemplo ha introducido la Comisión Europea en relación con DORA al fijar obligaciones muy detalladas en cuanto al control de los riesgos de terceros proveedores. Las partes que brinden acceso a información arbitral cubierta por medidas de seguridad de la información a dichos terceros deben asegurarse de que esos terceros estén al tanto de las medidas de seguridad aplicables, tengan las capacidades técnicas necesarias para cumplirlas. De esta forma el Protocolo pretende cerrar el proceso arbitral al riesgo procedente de terceros.

Por otra parte, el propio Protocolo señala que, si bien ha sido concebido para ser aplicado en los

arbitrajes internacionales, aspira a ser aplicado también en los arbitrajes nacionales o a los arbitrajes entre inversores y Estados. Ahora bien, en su principio 4 establece con claridad un firme principio de no sustitución de las regulaciones en vigor en los distintos Estados señalando que no reemplaza la ley aplicable, las reglas de arbitraje, las obligaciones profesionales o éticas u otras obligaciones vinculantes. En este sentido y de forma muy acertada dada la posibilidad de conflictos de normativa aplicable, el Protocolo señala que cuando los participantes en el arbitraje se enfrentan a obligaciones legales diferentes o contradictorias, el tribunal puede necesitar determinar en consulta con las partes y cualquier institución administradora, cómo armonizar tales obligaciones, tomando en consideración las consecuencias del incumplimiento, los principios de proporcionalidad y debido proceso, así como el rol del tribunal en la administración de justicia.

En consonancia con lo anterior el Protocolo pretende facilitar el cumplimiento con los regímenes legales de protección de datos, como el RGPD e la Unión Europea. Sin embargo, y de forma muy acertada el Protocolo también recoge que su objetivo no es otro que, en un entorno tan complejo y difuso como el de los riesgos digitales, mitigar los riesgos de seguridad de la información y no lograr el cumplimiento de dichos regímenes.

Por otra parte, el Protocolo de Ciberseguridad proporciona un marco recomendado para todos los sujetos que participan en los arbitrajes; tribunales, partes e instituciones administradoras.

En este sentido se considera que la seguridad de la información efectiva en un arbitraje requiere que todos los custodios de la información relacionada con el arbitraje adopten prácticas razonables de seguridad de la información. Las partes, los árbitros y las instituciones administradoras deben asegurarse de que todas las personas directa o indirectamente involucradas en un arbitraje en su nombre conozcan y sigan las medidas de seguridad de la información adoptadas en un procedimiento.

En cuanto al nivel de exigencia y los umbrales a adoptar, el protocolo establece un enfoque realista y gradualista que atienda caso por caso a las circunstancias concretas de forma tal que se produzca una adaptación a cada situación en función del nivel de riesgo y los sujetos que intervienen o la información que se maneja. Así, al determinar qué medidas específicas de seguridad de la información son razonables para un arbitraje en particular, las partes y el tribunal deben considerar:

- El perfil de riesgo del arbitraje.
- Las prácticas, la infraestructura y las capacidades de seguridad de la información existentes de las partes, árbitros y cualquier institución administradora.
- Los costos y los recursos de las partes, árbitros y cualquier institución administradora.
- La proporcionalidad relativa al tamaño, valor y perfil de riesgo de la disputa.

De todo lo anterior se deduce una nueva tarea de las partes. Cuando se inicie el arbitraje estas deberán, según lo establecido en el protocolo, el nivel de exigencia que supongan las medidas concretas que las partes pacten entre ellas aplicar de mutuo acuerdo. Es decir, que una nueva serie

de obligaciones y procedimientos deben incluirse en las condiciones previas al procedimiento de arbitraje de forma tal que las partes acuerden el nivel de obligaciones a las cuales van a someterse. El propio protocolo añade que, en algunos casos, las obligaciones legales, contractuales o éticas pueden requerir que las partes, árbitros e instituciones se aseguren de que existan medidas razonables de seguridad de la información antes de compartir información relacionada con el arbitraje.

Al considerar las medidas específicas de seguridad de la información que se aplicarán en un arbitraje, el protocolo propone atender a unas categorías de aspectos que deben formar parte del contenido del acuerdo al que lleguen las partes. Estas categorías, por otra parte, son las comunes que forman parte del contenido necesario de las políticas de seguridad de las organizaciones y empresas en cualquiera de los estándares nacionales o internacionales más comunes (ISO, ENISA, NIST entre otros). En este sentido, los aspectos a incluir en esa gestión adecuada de la ciberseguridad del arbitraje, deben comprender, entre otras, disposiciones que regulen:

- La gestión de activos.
- Los controles de acceso
- El cifrado de la información
- La seguridad de las comunicaciones
- La seguridad física y ambiental
- La seguridad de las operaciones;
- La gestión de incidentes de seguridad de la información

Por otra parte, el Protocolo también señala el modo en el cual el acuerdo de las partes para autoimponerse obligaciones debe articularse. Las partes deben intentar en primera instancia llegar a un acuerdo sobre medidas razonables de seguridad de la información. Y además señala que ese acuerdo debe ser una de las primeras disposiciones que acuerden las partes desde el mismo inicio del procedimiento arbitral. No obstante, en su Principio 11 señala con claridad que el tribunal arbitral tiene la autoridad para determinar las medidas de seguridad de la información aplicables al arbitraje. Ello es así, se deduce, si las partes no han alcanzado un acuerdo al respecto, o si han decidido obviar a cuestión o si la cuestión ha sido resuelta por las partes de un modo que no cumple con los estándares mínimos a juicio del tribunal arbitral.

Es más, el propio tribunal arbitral puede desviarse del acuerdo de las partes, entre otras razones, para proteger los intereses de terceros incluidos los intereses de los testigos u otras personas que puedan estar involucradas en el arbitraje. También si existe un interés propio del tribunal para proteger la legitimidad y la integridad del proceso arbitral, incluida la seguridad de sus propias comunicaciones y deliberaciones.

La relevancia de la ciberseguridad se estima tan decisiva que el propio Protocolo establece la posibilidad de introducir un arbitraje técnico dentro del arbitraje si el asunto tratado supone la resolución de problemas relacionados con la seguridad de la información, o utilizar el testimonio de un perito contradictorio para educar al tribunal arbitral.

Estas potestades arbitrales se ven reforzadas en el Principio 12, al reconocer al tribunal la capacidad de modificar las medidas previamente establecidas para el arbitraje, a solicitud de cualquiera de las partes o por propia iniciativa del tribunal, a la luz de la evolución de las circunstancias del caso.

No obstante, analizando los poderes conferidos a los árbitros por el Protocolo, llama la atención poderosamente la atribución de capacidades en el principio 13 que señala, sin lugar a dudas, que en caso de incumplimiento de las medidas de seguridad de la información adoptadas para un procedimiento de arbitraje o de un incidente de seguridad de la información, el tribunal arbitral podrá, a su criterio, o bien asignar a cada parte los costos generados, o bien imponer sanciones a las partes. Es sin duda una muestra de que el protocolo ha querido poner de relieve la relevancia de esta materia atribuyendo al árbitro la capacidad para aplicar un poder punitivo en forma de sanción en caso de que algunas de las partes no cumpa con las obligaciones contraídas y le sean además imputados los gastos generados por esa falta de diligencia debida.

El protocolo incluye una completa serie de anexos en los cuales se detallan las medidas concretas a adoptar, con un nivel de descripción técnica que dota al documento de una gran capacidad de ser aplicable de forma directa. Así, las partes pueden estipular sobre ese esquema de cumplimiento, ya que es una guía de contenido que las partes pueden seguir con la garantía de estar cumpliendo con lo estipulado en un protocolo ampliamente reconocido en la comunidad arbitral. Asimismo, esos anexos ofrecen parámetros para poder determinar con exactitud ante qué tipo de arbitraje nos encontramos desde el punto de vista de la ciberseguridad, pudiendo así graduar las medidas a adoptar en función del riesgo potencial.

En definitiva, el Protocolo de ciberseguridad para arbitraje internacional de la ICCA-NCY Bar-CPR, publicado en 2020, es una disposición que refleja bien a las claras la necesidad de cubrir y mitigar riesgos asociados a ciberataques. Se trata de una propuesta de marco regulador en el cual las partes libremente deberán establecer las disposiciones concernientes a la protección de la información y del propio proceso arbitral frente a amenazas externas procedentes del ciberespacio.

Por otra parte, se inscribe de lleno en el nuevo paradigma de gestión de riesgo digital que se está introduciendo en las normas emanadas de la UE en esta materia, que pretende mitigar el riesgo y atribuir responsabilidades en caso de incumplimiento. Dadas las características y ventajas de atender a lo establecido en este protocolo, se considera necesario que árbitros, partes, e instituciones arbitrales, se adapten de forma inmediata a las disposiciones incluidas en este protocolo a efectos de incrementar la resiliencia frente a intrusiones, y de mitigar las posibles responsabilidades derivadas de un ciberincidente con efectos graves en el procedimiento arbitral. Incluso se considera recomendable extender la aplicación de sus disposiciones a los procedimientos arbitrales que no tengan componente internacional y que se ciñan al ámbito nacional, porque proveen con un estándar reconocido internacionalmente y específicamente adaptado al arbitraje.

2. Otras herramientas jurídicas en materia de arbitraje internacional y ciberseguridad

A este protocolo antes descrito, se suman otras reglas y protocolos de *soft law*, que dan cuenta de la importancia de la materia , como puedan ser el Protocolo de Seúl para videoconferencias en el arbitraje o la Nota de orientación de la Cámara de Comercio Internacional sobre posibles medidas destinadas a mitigar los efectos de la Pandemia COVID-19, ambos también emitidos durante el año 2020, o en fechas más recientes, la inclusión del artículo 2.2.e) de las reglas de la IBA sobre la práctica de la prueba en arbitraje internacional.

III. LAS OBLIGACIONES DE LOS INTERVINIENTES EN EL ARBITRAJE EN MATERIA DE CIBERSEGURIDAD: ¿SON SUFICIENTES LOS INSTRUMENTOS DE *SOFT LAW?*

Como ha dejado claro el Protocolo de ciberseguridad para arbitraje internacional de la ICCA-NCY Bar-CPR, y como se infiere de la regulación nacional y transnacional aludida (y cada vez más abundante), los actores que intervienen en el marco del arbitraje internacional son múltiples y todos ellos son sujetos obligados que deben garantizar en mayor o menor medida la ciberseguridad del procedimiento.

En efecto, las partes, los árbitros y las instituciones arbitrales, ya sea por la regulación a la que se encuentran sometidos (por ejemplo, en el caso de determinadas partes conforme a su regulación nacional o transnacional dependiendo de su volumen o el sector en el que operen), o por ser custodios de la información y documentación intercambiada, deben implementar las medidas a las que alude el mencionado Protocolo y la regulación aplicable, so pena de incurrir en responsabilidades y ser susceptibles de ser sancionados.

> Sorprende que las instituciones arbitrales no dispongan de mecanismos para garantizar que las medidas de ciberseguridad exigibles en el marco de la prestación de su servicio sean aplicadas

Por ello, surge la duda acerca de la conveniencia de dejar la regulación de dicha materia en el marco del arbitraje a la aplicación voluntaria de determinados instrumentos de *soft law* y ello a pesar de la idoneidad de la misma en procedimientos transnacionales.

En efecto, sorprende que, por ejemplo, las instituciones arbitrales no dispongan de mecanismos para garantizar que las medidas de ciberseguridad exigibles en el marco de la prestación de su servicio sean aplicadas y deban confiar en que los árbitros y las partes decidan pactar, en la conferencia de organización de la prueba, o mediante una orden procesal al principio del procedimiento, la adopción de un protocolo de ciberseguridad o la remisión a una serie de normas. Normas que además pueden no cubrir las obligaciones inherentes a la propia institución de arbitraje.

En este sentido, no se puede obviar que la institución arbitral no sólo se encuentra obligada por un contrato con las partes, sino que existe un contrato entre la misma y los árbitros. Ambos independientes el uno del otro.

Sorprende todavía más, si se tiene en cuenta que existen precedentes de graves ciberataques en el mundo del arbitraje como la correspondencia que fue ilegalmente interceptada en el arbitraje *Libananco v Republic of Turkey (ICSID ARB/o6/8)* o el ataque que sufrió la página web de la Corte Permanente de Arbitraje en una disputa entre Filipinas y China en materia de fronteras marítimas.

No se explica el motivo por el que las instituciones arbitrales no incorporan en sus reglamentos obligaciones claras que garanticen que tanto los árbitros designados como las propias partes deben cumplir con las exigencias de ciberseguridad correspondientes.

Tampoco es entendible que, a estas alturas, la mayoría de las instituciones arbitrales no hayan incorporado en sus reglamentos al menos una obligación de adoptar todas las medidas necesarias para garantizar la aplicación de los protocolos de ciberseguridad aludidos anteriormente. No obstante, algunas instituciones como la *London Court of Arbitration* en su artículo 30 A, o la *Hong Kong International Arbitration Center,* artículo 3.1 e) de sus respectivos reglamentos, han dado pasos en el sentido de imponer algunas obligaciones contenidas en el Protocolo de ciberseguridad para arbitraje internacional de la ICCA-NCY Bar-CPR.

Como mínimo, las instituciones arbitrales podrían dirigir expresamente a los árbitros y a las partes a la adopción del Protocolo de ciberseguridad para arbitraje internacional de la ICCA-NCY Bar-CPR o incluirlo en los códigos de conducta de los árbitros promulgados por cada institución.

Sin embargo, la falta de adopción de este tipo de medidas no sólo perjudica a las instituciones arbitrales, sino a las propias partes quienes, en última instancia han decidido someter su disputa a una institución arbitral y a un reglamento que no cumple con la regulación en materia de ciberseguridad que es exigible a dicha parte por la regulación nacional, europea e incluso internacional. En este sentido, a pesar de que la Parte, en su momento, decida pactar con el Árbitro o Tribunal Arbitral y la contraparte la sumisión a un protocolo como el Protocolo de ciberseguridad para arbitraje internacional de la ICCA-NCY Bar-CPR, ello no significará que dicho Protocolo sea aceptado por la institución arbitral ni que la misma deba someterse a sus disposiciones. En última instancia será la parte quién haya escogido una institución que no se encuentra obligada por unos estándares similares a los que son exigibles a las partes y, ello a pesar del contrato que la parte establece con la institución arbitral.

En definitiva, la ciberseguridad no sólo se ha convertido en un elemento ineludible en el mundo del arbitraje sino que la importancia del mismo es tal que tiene una influencia decisiva en las obligaciones y deberes de todos los intervinientes del arbitraje. Puede alterar los contratos en los que se sustenta toda la institución del arbitraje con efectos directos para todos los actores.

Por todo ello, la institución del arbitraje, como otros sectores de actividad economía o profesional, deben desarrollar herramientas, protocolos y una organización preparada para asegurar un

adecuado nivel de ciberseguridad, mediante el establecimiento de sólidos mecanismos de gobernanza de la ciberseguridad que proteja la información y los propios procedimientos de arbitraje.

.....

(1)

Según Accenture, se estima que los costes directos e indirectos del cibercrimen a nivel mundial para el período 2019-2023 alcanzarán los 5.2 trillones de dólares [<https://www.accenture.com/_acnmedia/pdf-96/accenture-2019-cost-of-cybercrime-study-final.pdf>]. Según McAfee, en 2021 los costes de los ciberdelitos se incrementarán en un 50% con respecto al 2018 total y pasarán a representar ya el 1% de DDP global [<https://www.mcafee.com/enterprise/en-us/about/newsroom/press-releases/press-release.html?news_id=6859bd8c-9304-4147-bdab-32b35457e629>].

Ver Texto