REVISTA CHILENA
DE DERECHO Y TECNOLOGÍA

VOL. 8 NÚM. 2 (2019) • PÁGS. 111-137 • DOI 10.5354/0719-2584.2019.53447
RECIBIDO: 31/5/2019 • APROBADO: 9/12/2019 • PUBLICADO: 31/12/2019

DOCTRINA

La ciberseguridad en los Tratados de Libre Comercio

The cybersecurity in Free Trade Agreements

Anahiby Becerril
Universidad Nacional Autónoma de México

RESUMEN Las preocupaciones en torno a la seguridad y las políticas de comercio no son algo nuevo. Sin embargo, dado el carácter electrónico de las transacciones comerciales, la temática ha adquirido un nuevo y urgente relieve. El ciberespacio es un espacio de flujos, un espacio virtual que se acrecienta diariamente con las interacciones que se desarrollan con el empleo de las tecnologías de la información y la comunicación. Los gobiernos de muchos países han comenzado a desarrollar estrategias de ciberseguridad, mientras tratan de promover los beneficios de un mundo hiperconectado y ciberhabilitado. Respecto del comercio electrónico, se debe buscar que una estrategia de ciberseguridad no se convierta en obstáculo o barrera para estas transacciones electrónicas. La protección del ciberespacio se debe llevar a cabo con un enfoque *multistakeholder*. Estos temas también son de interés público, toda vez que las amenazas al ciberespacio pueden afectar a países y sociedades completas.

PALABRAS CLAVE Ciberseguridad, comercio electrónico, tratados.

ABSTRACT Concerns about security and trade policies are not new. However, given the electronic nature of the commercial transactions, the subject has acquired a new and urgent importance. Cyberspace is a space of flows, a virtual space that grows daily with the interactions that are made with the use of ICT. Governments in many countries have begun to develop cybersecurity strategies, while trying to promote the benefits of a hyperconnected and cyber-enabled world. In relation to electronic commerce, it should be sought that a cybersecurity strategy does not become an obstacle or barrier to these electronic transactions. The protection of cyberspace must be carried out in a multistakeholder approach. These issues are also of public interest since threats to cyberspace can affect countries and entire societies.

KEYWORDS Cybersecurity, ecommerce, treaties.

Introducción

> Si crees que la tecnología puede resolver tus problemas de seguridad, entonces no comprendes los problemas y no comprendes la tecnología (Schneier, 2004).

Nos encontramos ante una era digital caracterizada por los flujos constantes de bienes y servicios, activos,[1] ideas, personas y comunicación, todo gracias a la información. Si bien este flujo global no es algo nuevo, sí lo es su crecimiento exponencial en los últimos años, como resultado del surgimiento de la economía digital, caracterizada por la difusión masiva de las tecnologías de la información (TIC) y la comunicación, junto con internet.

La capacidad de vincular al mundo físico y cada acto de la actividad humana con sensores y redes para obtener conocimiento[2] a través de análisis avanzados está —y sin duda continuará— transformando nuestras vidas diarias, así como a la economía y la sociedad. La digitalización constituye uno de los grandes fenómenos de los últimos años. El traducir todo (documentos, música, imágenes, mapas, redes sociales) a *bits* transforma la manera en que interactuamos con el mundo (Becerril y Ortigoza, 2018).

La economía mundial se encuentra cada vez más conectada, y la digitalización se ha extendido a tal punto que hoy es también una economía digital. Ésta se nutre en gran medida de la masificación del cómputo en la nube (*cloud computing*), así como el *big data* y los avances del internet de las cosas, la inteligencia artificial, el aprendizaje automático y, en un futuro, del cómputo cuántico.

Con la reducción de costos y la conectividad, las plataformas TIC han permitido que a través del comercio electrónico fluyan bienes y servicios; en algunos casos la economía de las mercancías se encuentra superada por la de la información e ideas. Para el año 2017, la producción mundial de bienes y servicios TIC representaba alrededor de 6,5% del producto interno bruto mundial (UNCTAD, 2017). En el año 2015, las ventas mundiales de comercio electrónico alcanzaron un estimado de US$ 25.300 millones,[3] cifra que continúa aumentando diariamente. Se estima que para el año 2021 el comercio minorista mundial que se desarrolle a través del comercio electróni-

1. Como el caso los activos virtuales, entendidos como «la representación de valor registrada electrónicamente y utilizada entre el público como medio de pago para todo tipo de actos jurídicos y cuya transferencia únicamente puede llevarse a cabo a través de medios electrónicos». «Ley Para Regular las Instituciones de Tecnología Financiera», Cámara de Diputados de México, disponible en https://bit.ly/34yB2gr.

2. Caracterizado por el modelo DIKW (*data*, *information*, *knowledge*, *wisdom*).

3. Kimberley Botwright y Sean Doherty, «5 ways to make global e-commerce easier for everyone», World Economic Forum, 11 de diciembre de 2017, disponible en http://bit.ly/2Z6iK4X.

co alcanzará los US$ 4.479 millones.[4] Estas transacciones comerciales que se reflejan en el uso de información circulan de manera libre por este «metaespacio que es el ciberespacio»,[5] sin que se tengan que radicar físicamente en ningún lugar determinado, lo que permite una mayor deslocalización de los mercados.

A pesar de los potenciales beneficios que trae consigo el comercio electrónico, éste tiene también una serie de riesgos asociados, que deben ser identificados, evaluados y gestionados para minimizar su impacto. El aumento en las transacciones dentro del ciberespacio ha traído consigo un incremento en las amenazas e incidentes de seguridad, lo que ha tenido importantes consecuencias económicas y sociales para las organizaciones públicas y privadas, así como para las personas. Algunos ejemplos incluyen la interrupción de las operaciones —por ejemplo, por denegación de servicios (*distributed denial of service* o DDoS) o sabotaje—, pérdida financiera directa, demandas legales, daños a la reputación, disminución de competitividad —por ejemplo, en caso de robo de secreto comercial—, así como pérdida de la confianza de los usuarios o consumidores. Estos cambios y nuevos retos crean confusión e incertidumbre y pueden llevar a la creación de estrategias y políticas que se conviertan en barreras para el *ecommerce* y la economía digital, las cuales, al considerar el carácter transnacional de este tipo de comercio, pueden afectar las relaciones comerciales entre países.

Derivado de la importancia de la economía y mercado digital global, en vez de ser tratados como problemas técnicos que requieren soluciones técnicas, los riesgos en el ciberespacio deben abordarse como riesgos económicos. Es por lo que en este artículo analizaremos la importancia de la ciberseguridad para el fomento del *ecommerce*, en el marco de los tratados de libre comercio; cómo, a través de las políticas de ciberseguridad, se debe buscar el fomento al comercio electrónico, estudiando la forma en que la protección del ciberespacio, así como de las infraestructuras de las que depende, no constituyan un obstáculo para el mismo. Para ello, primero analizaremos el desarrollo del comercio electrónico como propulsor de la economía digital, con referencia a los habilitadores y tecnologías que se encuentran impulsando su desarrollo, y considerando que un conocimiento de estos habilitadores digitales ayudará a contextualizar algunos de los riesgos y amenazas que su uso conlleva. Con posterioridad, analizaremos al ciberespacio en el entorno de la ciberseguridad, para conocer cuáles son los esfuerzos que se han llevado a cabo para su protección. A través del conocimiento del ciberespacio y la ciberseguridad, se desarrollará el marco de la ciberseguridad en torno a los países que conforman el Tratado Integral y Pro-

4. «Worldwide retail and ecommerce sales: eMarketer's estimates for 2016-2021», eMarketer, 18 de julio de 2017, disponible en http://bit.ly/35zrtiA.

5. Concepto obtenido de Emilio Suñé Llinás, «Declaración de derechos del ciberespacio», Observatorio Iberoamericano de Protección de Datos, 21 de abril de 2013, disponible en http://bit.ly/2PB9Au9.

gresista de Asociación Transpacífico (CPTPP, por sus siglas en inglés), así como en el marco de las renegociaciones del tratado de libre comercio de América del Norte. Por último, se brindará una serie de consideraciones finales.

El comercio electrónico en la economía digital global

La nueva economía es global, pero también digital, y se desarrolla en tiempo real, sin fronteras. La economía se encuentra inmersa en una conversación global, o interacción digital. Pareciera que el mundo está ahora unido en un solo mercado electrónico, a un clic de distancia. La base del comercio que se desarrolla dentro del ciberespacio es la conectividad. Internet, por su propia naturaleza, ha derribado las fronteras geopolíticas que el comercio tradicional no había logrado.

Para la Organización Mundial del Comercio (OMC), el *ecommerce* o comercio electrónico constituye «la producción, distribución, comercialización, venta o entrega de bienes y servicios por medios electrónicos».[6] Mientras que para la OCDE esta modalidad de comercio constituye «la venta o compra de bienes o servicios, realizada por computadora redes por métodos diseñados específicamente para recibir o colocar pedidos».[7]

En 1996, para cumplir con su labor de establecer relaciones económicas internacionales amistosas, la Comisión de Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI), publicó la Ley Modelo sobre Comercio Electrónico, con la Guía para su Incorporación en el Derecho Interno. Mediante este instrumento, la Comisión buscó dar certeza jurídica y unificar criterios en las transacciones que se desarrollaban vía mensajes de datos, con la finalidad de la armonización y unificación progresivas del derecho mercantil internacional. En su preámbulo, la Ley Modelo hace referencia a las «transacciones comerciales internacionales que se realizan por medio del intercambio electrónico de datos y por otros medios de comunicación», en los que «se usan métodos de comunicación y almacenamiento de información sustitutos de los que utilizan papel».[8]

Las anteriores definiciones, además de destacar la importancia que tiene el comercio electrónico, abarcan toda clase de transacciones electrónicas comerciales, incluyendo las transferencias electrónicas de fondos y pagos con tarjeta de crédito.

6. «WT/L/274, Work programme on electronic Commerce», Organización Mundial de Comercio, disponible en http://bit.ly/2SboB4A.

7. «Glossary of statistical terms: Electronic commerce», OECD, 17 de enero de 2013, disponible en http://bit.ly/2M8PrcG.

8. Si bien destaca que muchas de las discusiones se encuentran limitadas a internet, al ser el medio con el que principalmente se asocia, la Ley Modelo de Comercio Electrónico distingue seis instrumentos principales a través de los cuales se puede llevar a cabo: el teléfono, el fax, la televisión, los pagos electrónicos, los sistemas de trasferencias de fondos, e internet.

Empero, aunque son amplias en su definición, resultan de alguna manera obsoletas al no reconocer nuevas formas de comercio electrónico, como son las efectuadas a través de internet (redes abiertas), limitándose a las transacciones electrónicas en sí mismas, sin referirse al espíritu de esta clase de negocios (ciberespacio, mercado virtual, entre otros). Por ello, consideramos la siguiente definición, más amplia:

> El comercio electrónico incluye el conjunto de transacciones comerciales realizadas por medios electrónicos o digitales de comunicación, ya sea por redes abiertas o cerradas, que se despliega dentro de un sistema global, utilizando redes informáticas y de telecomunicaciones (principalmente internet), que permiten crear mercados virtuales, dentro del ciberespacio, de todo tipo de productos, bienes y servicios (Castrillón y Luna y Becerril, 2015).

La economía que se lleva a cabo dentro del ciberespacio agrupa a las empresas en grandes redes de relaciones de interdependencia, en cuyo seno comparten actividades e intereses (Rifkin, 2013). La empresa industrial ha cedido su lugar a la empresa técnico-científica y a empresas red transnacionales. En la actualidad, todas las empresas son empresas de software. En algunos casos se han convertido en empresas de tiempo real, adaptándose de forma continua e inmediata a las cambiantes condiciones de un nuevo entorno digital o híbrido, condicionado por la inmediatez de la información.

De esta forma, la organización empresarial se ha reestructurado para adecuarse y obtener el máximo provecho de las TIC. Si bien antes el uso adecuado de internet dentro de las empresas se traducía en una fuente de competitividad y productividad, en la actualidad, una estrategia digital es parte fundamental del plan de negocios empresarial.

El comercio electrónico no solo favorece el comercio de empresa a consumidor (*business to consumer*, B2C), o de empresa a empresa (*business to business*, B2B), sino que ha fortalecido el de consumidor a consumidor (*consumer to consumer*, C2C). Plataformas como eBay, Mercado Libre y Amazon, entre muchas otras, han permitido a los pequeños empresarios y a cualquier persona ser un partícipe en el comercio internacional.

Otra de las características de esta economía digital es el cambio de papel «tradicional» entre los productores y consumidores. Al cambiar de un internet de consumo a uno de consumo y producción, nos hemos convertido en «prosumidores».[9] Al convertirnos en partícipes en el proceso de producción, con nuestro conocimiento, información e ideas, solicitando o diseñando artículos a la medida, o incluso subiendo contenidos a la red, la brecha entre consumidores y productores se ha difuminado.

9. «El cambio del modelo ha empoderado a los usuarios para convertirse en productores y, a la vez, consumidores de información, servicios y medios, lo que les permite convertirse en proveedores y cocreadores» (Becerril y Ortigoza, 2018: 17).

Si la década anterior nos había traído un internet de la información, en la actualidad estamos presenciando el surgimiento del internet del valor, el cual nos permite, a través de sus herramientas, una participación más activa en los procesos de servicios y productos.

La rapidez con que se desenvuelve esta economía digital es resultado de las tecnologías y las innovaciones que impulsan la cuarta revolución industrial. Múltiples organizaciones han elaborado clasificaciones de las tecnologías que se encuentran impulsando a esta nueva revolución industrial. Sin embargo, si reflexionamos en que todas estas nuevas tecnologías y desarrollos tienen como característica común el aprovechamiento del poder generado por la digitalización de todas las cosas y las TIC, deberíamos cuestionarnos por su seguridad y resiliencia, para su protección y continuidad. Estos habilitadores tecnológicos claves de la economía digital son:[10] la digitalización de todo y la creciente cantidad de información disponible, la inteligencia artificial, el big data, el internet de todas las cosas y el cómputo en la nube.

La digitalización de todo y la creciente cantidad de información disponible

En la economía digital cada dato tiene un valor. La generación de datos por las empresas para ser procesados y vendidos a terceros es un negocio creciente; de esta forma, los datos e información que surgen de la digitalización de las cosas se han convertido en la materia prima de los negocios y empresas, en un activo vital capaz de crear una nueva forma de valor económico (Mayer-Schönberger y Cukier, 2013). La implementación del modelo DIKW para la gestión del conocimiento y la extracción de valor de datos (datos materia prima) solo puede optimizarse dentro de un ecosistema de datos coherente que incluya a las empresas de software, las pymes, los sectores en datos (privados y públicos), los investigadores, las instituciones académicas y los proveedores de capital. Este ecosistema de datos apoyará la intensificación de la cooperación entre los diversos grupos de partes interesadas para que trabajen hacia el logro de objetivos que se refuercen mutuamente.

10. La CNUDMI reconoce a la robótica avanzada, la inteligencia artificial, el internet de las cosas, el cómputo en la nube, el análisis de macrodatos y la impresión tridimensional (UNCTAD, 2017: 2). Por su parte, la OCDE hace referencia a «la impresión 3D, el internet de las cosas, robótica avanzada, nuevos materiales (basados en "bio" o "nano" tecnología), así como a nuevos procesos (producción impulsada por datos, inteligencia artificial, biología sintética)» (OCDE, 2017: 14). Para el Foro Económico Mundial, las «megatendencias» y los motores tecnológicos de la cuarta revolución industrial son: físicos (vehículos autónomos, impresión 3D, robótica avanzada, nuevos materiales), digitales (internet de las cosas, *blockchain*) y biológicos (biología sintética) (Schwab, 2016: 17 y ss.).

La economía de los datos[11] mide la repercusión global del mercado de los datos —es decir, el mercado en que se intercambian datos digitales como productos o servicios derivados de los datos brutos— en el conjunto de la economía. Para la Unión Europea, esta economía de los datos implica la generación, recolección, almacenamiento, procesamiento, distribución, análisis, elaboración, entrega y explotación de los datos que hacen posibles las tecnologías digitales.[12]

Una economía libre de mercado se construye en gran medida con la filosofía fundamental a favor del fomento a la innovación empresarial, con una regulación que establece ciertas excepciones, lo que permite a las compañías una amplia libertad para experimentar. Sin embargo, las empresas y los Estados deben considerar que el mal uso de la información personal tiene consecuencias para su titular. Más allá del impacto en el ámbito financiero o económico, los datos personales son un reflejo de la vida y sustento de sus titulares; de ahí que su potencial para afectar la esfera del titular, en caso de su mal empleo, pueda afectarlo de forma potencial.

> En mayo del año 2017, el *ransomware* WannaCry impactó a 150 países y cientos de miles de sistemas, paralizando la atención médica, las instalaciones de producción y las telecomunicaciones. En el año 2018 se expusieron nuevas debilidades del hardware y se sumaron violaciones masivas de datos: en India, Aadhaar, considerado el sistema de identificación biométrica más grande del mundo, sufrió violaciones que comprometieron los datos de los 1.100 millones de ciudadanos registrados; en septiembre, Facebook notificó a sus usuarios la violación masiva de datos más grande que ha sufrido, la cual afectaría a más de 50 millones de personas. Y este año 2019 lo iniciamos con el «peor ataque de piratería informática» que ha sufrido Alemania; documentos y mensajes personales, números telefónicos móviles, información de tarjetas de crédito, direcciones, correos (entre otros), se encuentran dentro de esta große Datenleck, algunas de las víctimas son la canciller alemana, el presidente alemán Frank-Walter Steinmeier, así como partidos políticos, periodistas y artistas entre otros (Becerril, 2019).

El uso indebido de datos en esta era moderna digitalizada e hiperconectada ha alcanzado niveles críticos, sin que el público en general conozca el alcance real de los datos que producen. En la actualidad no transcurre más de un mes sin que salga a la luz alguna vulneración de bases de datos o incidentes exitosos contra los sistemas que los contienen, lo que no solo tiene costos e impactos negativos en la reputación de las empresas y países, sino en la vida de los millones de usuarios que son víctimas de estas vulneraciones.

---

11. Si consideramos que el 70% de la información la generamos nosotros, en cuanto usuarios de diversos dispositivos electrónicos, lo anterior equivaldría a la «mercantilización del yo».

12. «SMART 2013/0063. Study on a "European data market" and related services», Comisión Europea, 23 de julio de 2013, disponible en http://bit.ly/2sKeYlC.

La inteligencia artificial

En 2017, Facebook anunció la cancelación de uno de sus proyectos que empleaba inteligencia artificial, debido a que dos computadoras habrían desarrollado lenguaje propio para comunicarse entre ellas, creando así un nuevo idioma. Misma situación había sucedido unos meses antes con una inteligencia artificial de traducción de Google. En ambos casos, la cancelación se justificó debido a la «incomprensión» de dicho lenguaje —es decir, el desarrollo de un lenguaje del cual solo las computadoras conocieran conllevaría perder el control sobre ellas— y no a cuestiones de seguridad, o por lo menos ésas fueron las declaraciones de las empresas.

En años recientes, el interés por la inteligencia artificial ha crecido de forma exponencial. Gran parte de este crecimiento ha sido impulsado por los altos márgenes de ganancia que se le atribuyen: por ejemplo, según el estudio elaborado por Price Waterhouse Coopers, para el año 2030 el PIB mundial será 14% más alto como consecuencia de la inteligencia artificial, lo que equivaldría a US$ 15.700 millones,[13] un mercado del que sin duda nadie quiere quedarse atrás. Sin embargo, poco se ha explorado sobre lo que es y cómo funciona en realidad, lo que no ha evitado el creciente interés por regular y establecer pautas éticas en su empleo.

La inteligencia artificial se encuentra caracterizada por el aprendizaje automático basado en datos y la toma de decisiones automatizada. En términos amplios, constituye un término colectivo para identificar a «sistemas informáticos que pueden sentir su entorno, pensar, aprender y actuar en respuesta de lo que perciben y sus objetivos» (Becerril y Ortigoza, 2018).

Una de las áreas en las cuales se emplea inteligencia artificial dentro del *ecommerce* constituye el uso de las técnicas de creación de perfiles y la toma de decisiones automatizadas. Como usuarios, cada vez más nos enfrentamos a las decisiones basadas en procesamientos automatizados, alimentados por herramientas de inteligencia artificial y algoritmos; algunas de éstas pueden resultar perjudiciales para las personas involucradas, por ejemplo, cuando se trata de decisiones relacionadas con la solvencia crediticia, la vivienda, el empleo o incluso la sospecha de comisión de un delito.

Para Stephen Hawking, el desarrollo «completo» de la inteligencia artificial «podría significar el fin de la raza humana». Al considerar las limitantes que tenemos como seres humanos, por la lenta evolución biológica, Hawking valoró que no podríamos competir y que, al final, seríamos reemplazados.[14] Tal vez esto sea cierto, si consideramos que los procesadores de las máquinas actuales son capaces de producir

13. «Sizing the prize: What's the real value of AI for your business and how can you capitalise?», Price Waterhouse Coopers, junio de 2017, disponible en https://pwc.to/36PHst2.

14. BBC News, «Stephen Hawking: "AI could spell the end of the human race"», video de Youtube, 2 de diciembre de 2014, disponible en https://youtu.be/fFLVyWBDTfo.

millones de operaciones por segundo sin cansarse, tal vez lleguemos a ser superados por las grandes habilidades de las máquinas que hemos creado.

Big data

Si tomamos en cuenta que cada día en el mundo se generan más de 2,5 *exabytes* (equivalentes a un millón de *terabytes*),[15] debemos considerar que, como consecuencia de la digitalización de todo, vivimos en un mundo de ingentes cantidades de datos. La cantidad no define al *big data*, solo es un exponencial de la cantidad de información que diariamente se genera; de esta forma, podemos entenderlo, desde un punto de vista tecnológico, como la información o grupo de datos que por su elevado volumen, diversidad y complejidad no pueden ser almacenados ni visualizados con herramientas tradicionales (Montero, 2015).

El *big data*[16] se ha desarrollado como una nueva frontera para la innovación, la competitividad y la productividad. Sin embargo, debemos considerar que el dato por sí solo no vale si no se convierte en información que se traduzca en conocimiento y nos genere sabiduría (modelo DIKW). Los datos deben llevar al desarrollo de acciones, procesos o incluso políticas públicas. El *big data* se presenta como un desafío, pero también brinda nuevas oportunidades para las empresas, y a la vez aumentan el riesgo a que una vulneración dentro de la información contenida y procesada por éstas pueda causar efectos en los titulares de dicha información.

Internet de todas las cosas

Con un valor de mercado estimado que supere los 1.000 millones de euros para el año 2020, la Comisión Europea (2014) identifica al internet de las cosas como el siguiente paso en la digitalización de la sociedad y economía, en el que las personas y objetos estarán interconectados a través de redes de comunicación e informan sobre su estado y entorno. El internet de las cosas se conforma por un conjunto de sensores[17]

15. En términos de bytes, un gigabyte equivale a 109, es decir, 1.000.000.000 bytes.

16. Algo que aclarar acerca del uso del *big data*, es que el gran volumen de información no enseña a las computadoras o dispositivos a «pensar» como lo hacemos los seres humanos. Por el contrario, consiste en aplicar las matemáticas, en específico algoritmos, a estas ingentes cantidades de datos, para de ahí inferir probabilidades.

17. Se emplean identificadores de radio frecuencia (*radio frecuency identification*, RFID). Este sistema consiste en una etiqueta (*tag*) que contiene un microchip; a cada *tag* se le proporciona un código único denominado EPC (*electronic product code*). Además, contiene un lector —compuesto de una antena y un demodulador— que convierte la información analógica en información digital. La información es enviada por medio de la red a un centro de datos para ser tratada y, de esta forma, cruzar los datos en una computadora central. El EPC se conecta a internet mediante una dirección de IP y un nombre de dominio (Navarro y Clavijo, 2016).

que captan la información sobre lo que ocurre en su entorno. Debido a la naturaleza ubicua de los objetos conectados a la internet de las cosas, se estima que para el año 2020 cerca de 26.000 millones de dispositivos se conectarán a internet. Esta es una fuente de recolección de datos que crece de manera exponencial y, en consecuencia, adecuada para ser procesada mediante sistemas de *big data*.

Sin duda, el internet de las cosas aumentará de forma exponencial la conectividad, pero debemos tomar en consideración que en muchas ocasiones los sistemas, dispositivos o sensores no se encuentran preparados para afrontar los riesgos de ciberseguridad. En este caso, la vulnerabilidad de uno de los dispositivos puede poner en riesgo la integridad del sistema completo.

Cómputo en la nube

La *nube* es como se denomina al modelo que permite el acceso ubicuo, conveniente y bajo demanda de red a un conjunto de recursos informáticos configurables, el que puede ser rápidamente proveído con esfuerzos mínimos de administración o interacción con el proveedor de servicios. Este modelo promueve la disponibilidad, componiéndose de cinco características esenciales, tres modelos de servicios y cuatro modelos de implementación.[18] Las características esenciales, de acuerdo con el National Institute of Standards and Technology (NIST), son:

- Autoservicio a la carta: Esto permite al consumidor aprovisionar unilateralmente capacidades informáticas, atendiendo a sus necesidades, sin necesidad de interacción humana con cada proveedor de servicios.
- Amplio acceso a la red: Sus capacidades se encuentran disponibles en la red y son accesibles a través de mecanismos estándar que promueven el uso de plataformas heterogéneas tanto ligeras como pesadas.
- Puesta en común de recursos: Los recursos informáticos del proveedor sirven en común a múltiples consumidores (modelo de múltiples inquilinos), con distintos recursos tanto físicos como virtuales, mismos que se asignan y reasignan de forma dinámica, atendiendo a las necesidades del consumidor.
- Rapidez y elasticidad: Las capacidades se pueden aprovisionar y liberar elásticamente, en algunos casos de forma automática, para poder alcanzar de forma rápida el redimensionamiento correspondiente. Para el consumidor, las capa-

18. Los tres modelos de servicio son: software como servicio (*software as a service*); plataforma como servicio (*platform as a Service*); e infraestructura como servicio (*infrastructure as a service*). Por último, los modelos de implementación de la nube son: privada, comunitaria, pública e híbrida. «The NIST definition of cloud computing», National Institute of Standards and Technology, septiembre de 2011, disponible en https://bit.ly/2PDRSqd.

cidades disponibles para el aprovisionamiento a menudo parecen ilimitadas, pues se pueden adquirir en cualquier cantidad y momento.

- Servicio medido: Los sistemas en la nube controlan, monitorean, informan y optimizan de forma automática el uso de los recursos al aprovechar una capacidad de medición en algún nivel de abstracción adecuado al servicio de que se trate.

Se trata de un modelo de servicios de TIC en un ecosistema de recursos tecnológicos que ofrece servicios escalables, compartidos y bajo demanda en distintas modalidades y a diversos usuarios a través de internet.

Las tecnologías aquí referidas constituyen plataformas de innovación que pueden aplicarse de forma muy versátil y exitosa a infinidad de sectores, incluido el económico. Éstas son posibles, se alimentan, desarrollan y mejoran a través de la digitalización de todo. Al ser tecnologías impulsadas por datos (*data driven*), las cuestiones en torno a la privacidad, la protección de datos personales, la disponibilidad de la información y su seguridad están entre las principales preocupaciones en su adopción por parte de las organizaciones, empresas y gobiernos. Con la digitalización se generan enormes volúmenes de datos que constantemente alimentan al *big data*, el cual se encuentra almacenado en la nube,[19] por lo que ésta constituye una mina de oro potencial para ciberataques y ciberdelincuentes. No debemos olvidar que la información de gobiernos, empresas e individuos fluye por igual en ese espacio. De ahí la importancia de la ciberseguridad, la cual constituye el núcleo en la protección de los activos de información, incluidos los datos personales.

Debemos recordar que internet tuvo éxito no por la seguridad de su infraestructura, sino a pesar de su inseguridad inherente. Para la OCDE, la naturaleza de las vulnerabilidades técnicas de los sistemas de información interconectados a través de internet en gran medida no se ha modificado. Lo que ha cambiado, es que «la sociedad y la economía ahora dependen de este entorno fundamentalmente inseguro» (OCDE, 2012).

Además de los riesgos de ciberseguridad por ataques, las empresas, gobiernos e instituciones deben preocuparse por las vulnerabilidades asociadas al desconocimiento por incumplimiento de políticas de seguridad o demandas relacionadas con la violación de datos (*data breach*). Si no se tienen adecuados procesos, capacitación e innovación tecnológica en materia de ciberseguridad, estos actores pueden verse inmersos en varios problemas, pues además de la pérdida de la información finan-

19. El almacenamiento de información en la nube no excluye la responsabilidad de las organizaciones de proteger tanto su regulación como reputación. En general, a menudo es responsabilidad de las organizaciones de usuarios en la nube asegurarse de que los datos personales se encuentren protegidos y solo se utilicen de conformidad con la ley.

ciera, el daño a la marca y reputación y el incumplimiento a la ley (con las multas aparejadas), así como la pérdida de ventajas competitivas.

Del ciberespacio a la ciberseguridad

El ciberespacio es un espacio de flujos, un espacio virtual que se acrecienta diariamente con las interacciones mediante el empleo de las TIC. Denominado el quinto dominio —junto con la tierra, el mar, el aire y el espacio—, el ciberespacio constituye un ambiente virtual en el que cada día desarrollamos gran parte de nuestras actividades diarias. Pero, a diferencia de los otros cuatro dominios, éste necesita de la permanente atención y colaboración humana para su funcionamiento.

El ciberespacio es un mundo electrónico, un espacio común global en donde las personas se encuentran unidas para intercambiar ideas, servicios e incluso amistad;[20] representa además un sistema nervioso que controla a los países y la infraestructura crítica que los sostiene. Su funcionamiento saludable es esencial para la economía y la seguridad nacional.[21] Es un entono digital global constituido por redes informáticas y de telecomunicaciones, en el que se comunican e interactúan las personas, lo que permite el ejercicio de sus derechos y libertades, de la misma forma que lo hacen en el mundo físico.[22]

Técnicamente, la Organización Internacional de Normalización (ISO) señala que el ciberespacio es «un entorno complejo resultante de la interacción de personas, software y servicios en internet a través de dispositivos tecnológicos y redes conectadas a él, que no existe en ninguna forma física».[23] La definición que se otorgue respecto al ciberespacio atiende en gran medida al uso que se le otorgue; por ello, no existe un concepto consensuado.

Con independencia de su definición, el ciberespacio constituye la base a través de la cual se lleva a cabo el comercio electrónico, así como el fundamento de la economía digital. Consideremos el aumento diario en la creación de servicios y productos, además de tecnologías, que se desarrollan a través de este espacio. Ahora sumemos la información de todo tipo que manejamos a través de este flujo mundial virtual y los servicios que ya se encuentran conectados al él —incluyendo infraestructura crítica—. El resultado es una cada vez mayor dependencia a las TIC. En la medida en que aumenta nuestra dependencia de las nuevas tecnologías, nos hacemos más vulnerables ante ellas (Castrillón y Luna y Becerril, 2015). Poniendo en perspectiva

20. «Canada's cyber security strategy», Gobierno de Canadá, disponible en http://bit.ly/35Dcvbh.

21. «Cyberspace policy review: Assuring a trusted and resilient information and communications infrastructure», Office of the Chief Information Officer, disponible en http://bit.ly/2Z4Bz8Y.

22. «Estrategia nacional de ciberseguridad», Gobierno de México, 2017, disponible en https://bit.ly/36VkBMZ.

23. «ISO/IEC 25437:2012(en)», ISO Online Browsing Platform, disponible en http://bit.ly/2S7jQfi.

lo anterior, cabría preguntarse por qué preocuparnos sobre la seguridad del ciberespacio, y por qué resulta necesaria su incorporación en los tratados de libre comercio.

Sobre la primera cuestión, si en la actualidad la economía digital —de la misma forma que el comercio electrónico y múltiples actividades de nuestra vida diaria— se basan en el flujo de datos e información, debemos considerar la seguridad de toda la infraestructura que la contiene. Esta infraestructura crítica se encuentra cada vez más conectada a las redes que conforman dicho ciberespacio. Nuestras actividades diarias, desde la comunicación hasta acceder a información, trabajo, salud y educación, se desarrollan a cada instante en ese espacio. De esta forma, internet y las TIC se han vuelto recursos críticos en el desarrollo del comercio electrónico y de la economía digital, lo que tiene consecuencias en las políticas de ciberseguridad, entre las cuales una de las principales es la adopción de estrategias específicas en el tema.

¿Qué es la ciberseguridad? Se trata de la seguridad de este ciberespacio. Podemos interpretar el término atendiendo a los conceptos otorgados por la comunidad técnica, además de los empleados por los documentos nacionales de ciberseguridad. Sin embargo, consideramos que la definición que la Unión Internacional de Telecomunicaciones (UIT) emitió en su Recomendación ITU-T X.1209 (12/2019) resulta adecuada al explicar el concepto:[24]

> 3.2.5. Ciberseguridad [b-ITU-T X.1205]: El conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno.[25]

En este contexto, se identifican como *activos* a los «dispositivos informáticos conectados, los usuarios, los servicios/aplicaciones, los sistemas de comunicaciones, las comunicaciones multimedia», así como la totalidad de la información transmitida o almacenada en el ciberentorno. Se reconoce que la ciberseguridad garantiza que se alcancen y mantengan las propiedades de seguridad de los activos de la organización y los usuarios contra los riesgos de seguridad correspondientes en el ciberentorno. Las propiedades de la ciberseguridad son las siguientes: disponibilidad, integridad —que puede incluir la autenticidad y el no repudio— y la confidencialidad.

---

24. «Recommendation X.1209 (12/10)», Unión Internacional de Telecomunicaciones, 17 de diciembre de 2010, disponible en http://bit.ly/2PAootb.

25. La UIT no emplea el término ciberespacio. Sin embargo, hace referencia al ciberentorno para referirse a «los usuarios, redes, dispositivos, todo el software, procesos, información almacenada que circula, aplicaciones, servicios y sistemas que están conectados directa o indirectamente a redes». «Recomendación X.1205 (04/08)», Unión Internacional de Telecomunicaciones, 18 de abril de 2008, disponible en http://bit.ly/2PCGJWg.

Debido a su rápido crecimiento en número y sofisticación, los ciberataques se posicionan como una amenaza crítica a la seguridad nacional y uno de los mayores riesgos a los que se enfrentan las naciones en la actualidad. En su «Global risks report 2019», el Foro Económico Mundial ha reconocido el fraude o robo masivo de datos y a los ciberataques como dos de los cinco principales riesgos mundiales que perciben los países.[26] Mientras que, a nivel de Norteamérica, el riesgo a los ciberataques[27] ha superado a los ataques terroristas como el número uno de mayor preocupación al hacer negocios (FEM, 2018).

Consecuencia de lo anterior, los gobiernos de muchos países han comenzado a desarrollar estrategias o leyes y políticas nacionales de ciberseguridad para protegerse contra las amenazas cibernéticas, con una visión de gestión de riesgos que les permita conocer sus vulnerabilidades, mientras tratan de promover los beneficios de un mundo hiperconectado y ciberhabilitado. La elaboración de estrategias nacionales de ciberseguridad se ha convertido en una prioridad de política nacional en varios países (OCDE, 2012). El Centro de Excelencia de Ciberdefensa Cooperativa de la OTAN ha identificado más de 50 países que han publicado una estrategia de ciberseguridad o estrategia nacional de ciberseguridad, en la que definen «qué significa seguridad para sus futuras iniciativas de seguridad nacional y económica».[28]

Para la OCDE, las estrategias nacionales de ciberseguridad deben tener dos objetivos: impulsar la prosperidad económica y social, así como proteger las sociedades que dependen del ciberespacio contra las amenazas cibernéticas, lo que debe hacerse preservando la apertura de internet como plataforma de innovación y nuevas fuentes de crecimiento (OCDE, 2002).

Las Estrategias de Ciberseguridad o Estrategias Nacionales de Ciberseguridad (ENCS) implican planes y acciones tomadas para facilitar la ventaja competitiva nacional respecto de la ciberseguridad. Constituyen un plan de acciones, basado en principios, valores y objetivos, diseñado para mejorar la seguridad y la capacidad de recuperación de las infraestructuras y servicios nacionales (resiliencia). En estos documentos se articula un acercamiento de la ciberseguridad adaptado a un contexto nacional o jurídico determinado. En este sentido, la implementación de las estrategias debe ir acompañado de una planeación en el desarrollo de tecnología e

26. En el cuarto y quinto lugar respectivamente, solo precedidos por riesgos climáticos (FEM, 2019).

27. Ciberataque entendido como un ataque que se perpetra a través del ciberespacio, dirigido al «uso de una empresa, del ciberespacio, con el fin de interrumpir, deshabilitar, destruir o controlar maliciosamente un entorno/infraestructura informática; o destruir la integridad de los datos o robar información controlada». «Glossary of key information security terms», National Institute of Standards and Technology, doi: 10.6028/NIST.IR.7298r2.

28. «NATO Cooperative Cyber Defense Centre of Excellence», CCDCOE, disponible en http://bit.ly/34LLzFl.

innovación, un presupuesto asignado, así como el desarrollo de habilidades y capital humano para trabajar por la misma.

Del mismo modo en que no existe una definición única para los términos ciberespacio y ciberseguridad, tampoco existe una estrategia única que se pueda seguir, dadas las características de cada país. Sin embargo, dentro de ellas podemos identificar temas comunes —lo que al final no nos hace tan diferentes—, entre los que destacan la cooperación (internacional y nacional); la protección de los derechos humanos de los usuarios/ciudadanos; así como la gestión de riesgos. Si bien su desarrollo e implementación constituyen un costo —el cual debe ser considerado como inversión—, el costo de la inacción es mayor.

La ciberseguridad en los tratados de libre comercio

Las preocupaciones en torno a la seguridad nacional y las políticas de comercio no son algo nuevo. Sin embargo, dado el carácter electrónico y transnacional de las transacciones comerciales, la temática ha adquirido un nuevo y urgente relieve, sobre todo en los países más desarrollados, debido al cada vez más creciente vínculo y dependencia de las TIC en sus servicios e infraestructura crítica.

Pasando ahora al contexto específico, si se considera que la mayoría de las economías desarrolladas y en desarrollo tienen leyes y regulaciones que restringen la inversión extranjera directa, sobre la base de preocupaciones relacionadas con la seguridad nacional o la pérdida de los recursos naturales de los países, ¿cuál sería el equivalente para desarrollar protecciones en el ciberespacio?

La seguridad económica trata el comercio, la producción y las finanzas (Albert y Buzan, 2011). No obstante que los países desarrollados y en desarrollo tienen diferentes puntos de vista[29] respecto de las amenazas de seguridad económica asociadas con la ciberseguridad, existen — como se refirió antes— problemas comunes y globales.

Con la rápida adopción de las tecnologías por parte de gobiernos, individuos y organizaciones, éstas son cada vez más relevantes en la ecuación de la economía y seguridad nacional. Las alegaciones relacionadas con la ciberseguridad han dado lugar a diversas barreras al comercio internacional y la inversión. Las barreras relacionadas con la ciberseguridad abarcan al menos las siguientes categorías de preocupaciones:

29. Para Kshetri (2016), a Estados Unidos les preocupa el robo de IP y otros problemas asociados con el espionaje económico. Los Estados BRICS (Brasil, Rusia, India, China y Sudáfrica), por otro lado, han argumentado que la dependencia de los países en desarrollo de las tecnologías occidentales es una amenaza para la seguridad económica.

espionaje político,[30] espionaje económico[31] y seguridad de la información de los países[32] y ciudadanos.[33]

Respecto del comercio electrónico, se debe buscar que una estrategia de ciberseguridad no se convierta en obstáculo o barrera para estas transacciones electrónicas. Es decir, así como existen barreras comerciales, las cuales constituyen restricciones impuestas al libre flujo de comercio e inversión, una barrera relacionada con la ciberseguridad para el comercio internacional y la inversión se define como «cualquier problema relacionado con los riesgos de seguridad reales y percibidos en el entorno cibernético que obstaculiza directa o indirectamente el crecimiento del comercio internacional y la inversión» (Kshetri, 2016).

Asociación de Naciones del Sudeste Asiático

En el caso de la Asociación de Naciones del Sudeste Asiático (ASEAN, por su nombre en inglés),[34] el capítulo 1 de su Carta[35] establece como uno de sus propósitos el «garantizar la seguridad y la estabilidad entre las naciones mediante la cooperación mutua». En 2013, la ASEAN firmó con Japón la «Declaración ministerial conjunta de la reunión de política ministerial de ASEAN y Japón sobre la cooperación en materia de ciberseguridad»,[36] en que además de reconocer la importancia del ciberespacio seguro como uno de los «principales propulsores de la innovación», éste resulta esencial para «promover las actividades sociales y económicas y fortalecer la conectividad de la ASEAN».

30. Si bien la práctica de espionaje entre Estados no es nueva, con las TIC se han facilitado, además de masificado. Recordemos las declaraciones de Edward Snowden respecto de las prácticas de vigilancia masiva, ilegal, llevada a cabo por el gobierno de Estados Unidos, situación que incluso derivó en la Recomendación de la ONU sobre «Privacidad en la era digital».

31. Por ejemplo, el robo de secretos industriales.

32. Relativo a la infraestructura crítica e información estratégica, de seguridad nacional o pública, entre otros.

33. Libertad de expresión, acceso a la información, privacidad y protección de datos personales, además del ejercicio de otros derechos humanos a través de internet.

34. Compuesto por Indonesia, Filipinas, Malasia, Singapur, Tailandia, Vietnam, Brunéi, Camboya, Laos y Myanmar. Papúa Nueva Guinea es observador.

35. La Carta entró en vigor el 15 de diciembre de 2008. Codifica las normas, leyes y valores de la ASEAN, además de crear un marco legal para las instituciones de la organización.

36. En esa ocasión se hizo referencia a que el concepto de «ciberseguridad» se entenderá de conformidad con lo establecido en la Recomendación ITU-T X.1205, la cual ha sido citada en este trabajo.

Del TPP al CPTPP

El Acuerdo Transpacífico de Cooperación Económica, mejor conocido por sus siglas TPP (Trans-Pacific Partnership),[37] abarcaba distintos aspectos encaminados a hacer el comercio más ágil y sencillo, reduciendo costos y tiempos para hacer negocios, contando siempre con la protección de reglas claras y precisas para todos. Para Sigmond, el TPP incorporó compromisos que no existían en los Tratados de Libre Comercio anteriores. Por ejemplo, refiere la autora, «las partes se comprometieron a tener protección para los consumidores y detener mensajes comerciales no solicitados. También se promovió el compromiso de ayudar a las pequeñas y medianas empresas» (Sigmond, 2018).

En enero de 2017, el gobierno de Estados Unidos decidió retirarse como signatario y de forma permanente de las negociaciones del TPP, en aras de buscar mejores condiciones para su país. En respuesta a esto, y en la búsqueda de darle vigencia al tratado, el 11 de noviembre de 2017, los representantes de comercio de los 11 países restantes[38] acordaron el Tratado Integral y Progresista de Asociación Transpacífico (CPTPP, por sus siglas en inglés).

El 23 de enero de 2018, los 11 países participantes en el Tratado alcanzaron un acuerdo en Tokio, Japón.[39] Éste incorpora algunas disposiciones contenidas del TPP, como un apartado sobre el comercio electrónico, en el que, además de reconocerlo como un motor para el crecimiento económico y de oportunidades, se reconoce la importancia de los marcos que promueven la confianza de los consumidores, así como la necesidad de evitar obstáculos para su uso y desarrollo (artículo 14.2.1).[40]

Como parte del logro de desarrollar un apartado sobre comercio electrónico en el Tratado, es el compromiso que adquieren los Estados parte de permitir que los consumidores dentro de sus territorios tengan la capacidad para el acceso, así como el uso de servicios y aplicaciones disponibles en internet. No obstante, la problemática surge del entorno de proveer contenidos exclusivos en algunos casos, lo que se considera una «administración razonable de la red», que puede conllevar un impacto negativo a su arquitectura.

Dentro de sus definiciones, el Tratado identifica como producto digital a los pro-

37. El TPP fue suscrito por 12 países el 4 de febrero de 2016.

38. Corresponde a Australia, Brunéi, Canadá, Chile, Japón, México, Nueva Zelanda, Malasia, Perú, Singapur y Vietnam.

39. «Tratado Integral y Progresista de Asociación Transpacífico: Qué es», Gobierno de México, disponible en http://bit.ly/35NXe7X.

40. En el tratado se hace referencia a la seguridad de los consumidores y establece la obligación de las partes de adoptar— o en su caso mantener— leyes en la materia, que prohíban prácticas comerciales fraudulentas y engañosas, que causen daño o potencial daño a los consumidores que participan en las actividades que se desarrollan en línea (artículo 14.7.2).

gramas de computador, textos, «imagen, grabación de sonido u otro producto codificado digitalmente, producido para venta o distribución comercial y que puede transmitirse electrónicamente».[41] Definición que, de conformidad con el texto del Tratado, no debe entenderse como «la opinión de una parte sobre si el comercio de productos digitales a través de la transmisión electrónica debe clasificarse como comercio de servicios o comercio de bienes».

Las partes en el Tratado reconocen los beneficios económicos y sociales derivados de la protección de la información personal[42] de los usuarios de comercio electrónico, lo que también mejora la confianza en el consumidor (artículo 14.8.1). Para garantizar esta protección, cada parte se compromete a la adopción o mantenimiento de un marco legal que estimule la protección de la información personal de los usuarios, teniendo en cuenta los principios y directrices de los organismos pertinentes (artículo 14.8.2), lo que se pretende fomente un marco seguro que permita la transferencia transfronteriza de información —incluida la personal—, por medios electrónicos, cuando se trate de la celebración de negocios por parte de una «persona cubierta» (artículo 14.11.2). Considerando la disparidad de legislaciones en la materia entre los Estados parte, el punto para considerar será el desarrollo de estándares o principios generales que éstos se comprometan a cumplir para la protección de dicha información.

También hace referencia a la protección contra los mensajes electrónicos comerciales no solicitados. Además del deber de las partes de mantener un marco legal que gobierne las transacciones electrónicas consistente con los principios de la Ley Modelo de Comercio Electrónico de UNCITRAL o con la Convención de las Naciones Unidas para el uso de las Comunicaciones Electrónicas en los Contratos Internacionales (artículo 14.5.1.).

Respecto de las barreras al comercio electrónico, las partes acordaron esforzarse por: «a) Evitar cualquier carga regulatoria innecesaria en las transacciones electrónicas; b) facilitar el aporte de las personas interesadas en el desarrollo de su marco legal para las transacciones electrónicas» (artículo 14.5.2). Lo anterior implica, por un lado, el no aplicar barreras innecesarias (a las que antes se hacía mención) y, por otro, la cooperación en la conformación del marco legal de múltiples partes interesadas, lo que es acorde con el modelo *multistakeholder* de la gobernanza de internet.

En el mismo apartado se hace mención a las instalaciones informáticas,[43] dejando

41. «Chapter 14: Electronic Commerce», Gobierno de Nueva Zelanda, disponible en https://bit.ly/2tu2Up6.

42. Para efectos del CPTPP, la información personal constituye «cualquier información que incluye datos, relacionados a una persona física, identificada o identificable» (artículo 14.1).

43. Las instalaciones informáticas constituyen (para efectos del Tratado): servidores informáticos y dispositivos de almacenamiento para el procesamiento o almacenamiento de información para uso comercial (artículo 14.1).

al arbitrio de los Estados partes el establecer requisitos regulatorios propios sobre el uso de dichas instalaciones, incluyendo los que busquen mantener la seguridad y confidencialidad de las comunicaciones. Esto, al igual que la protección de la información personal, constituye un gran reto. Al considerar la disparidad en la protección a nivel nacional de las partes, el no contar con un estándar mínimo de seguridad puede aumentar el riesgo a que suceda un incidente exitoso.

La mayor parte de las naciones considera un compromiso u obligación internacional el cooperar con otras y contribuir a la ciberseguridad global. Cada vez más resulta más común escuchar, en discursos de todas partes del mundo, que la cooperación es primordial para mantener un ciberespacio seguro, lo que propiciará la seguridad nacional y la de todos los usuarios en general. Sin embargo, el discurso aún no se encuentra acorde con los hechos. No todos los países tienen dentro de sus prioridades la ciberseguridad.

Dentro del capítulo 14 destaca un apartado sobre la ciberseguridad, el cual va encaminado a fomentar la cooperación entre las partes contratantes. Además, se compromete al desarrollo de capacidades de las entidades nacionales responsables de la respuesta a incidentes de seguridad informática, así como a emplear los mecanismos de colaboración para la identificación y mitigación de intrusiones maliciosas o la diseminación de códigos maliciosos que afecten las redes electrónicas de las partes (artículo 14.16).

Aunque no hace una referencia única sobre el concepto de la ciberseguridad, la **tabla 1** muestra el marco en torno a los países que conforman el Tratado.

Aún existe una disparidad entre los Estados parte del Tratado en el desarrollo regulatorio y de políticas en torno a la ciberseguridad. El no contar con una definición consensuada es una muestra del estado del arte a nivel internacional. Las disparidades regulatorias y asimetrías en el desarrollo de capacidades sin duda tienen un impacto al momento de tomar decisiones sobre las medidas a adoptar o el rumbo a seguir.

El Tratado de Libre Comercio de América del Norte

Con la finalidad de establecer la base para un crecimiento económico fuerte y mayor prosperidad para los países que lo integra, en 1994 entró en vigor el Tratado de Libre Comercio de América del Norte (TLCAN), firmado por Canadá, Estados Unidos[44] y México. De esta forma, fue creada una de las zonas de libre comercio más grandes del mundo.

44. Para el año 2018 el CGI sitúa a Estados Unidos (0.926) en el segundo lugar, por debajo de Reino Unido (0.931). A nivel regional, el índice posiciona a Estados Unidos como el primero, mientras que Canadá se encuentra en el segundo lugar, seguido por Uruguay (0.681) y México (UIT, 2018).

Tabla 1. Legislación aplicable en materia de ciberseguridad, países miembros del CPTPP.

País y ranking en el IGC[1]	Documentos	Definición
Australia 10/0.890	• Strong and Secure. A Strategy for Australia's National Security (2013). • 2016 Defence White Paper.	«Medidas relacionadas con la confidencialidad, disponibilidad e integridad de la información que se procesa, almacena y comunica por medios electrónicos o similares» (Australia, 2013).
Brunéi 64/0.624	• Computer Misuse Act (2007)	Aún se encuentra desarrollando un marco en materia de ciberseguridad
Canadá 9/0.892	• Canada's Cyber Security Strategy. For a Stronger and More Prosperous Canada (2010) • Action Plan 2010-2015 for Canada's Cyber Security Strategy (2013) • Action Plan for Critical Infrastructures 2014-2017 (2014) • National cyber security strategy: Canada's vision for security and prosperity in the digital age (P. S. Canada 2018)	Dentro de su estrategia, se hace referencia al ciberespacio: «El ciberespacio es el mundo electrónico creado por redes interconectadas de tecnología de la información y la información en esas redes. Es un bien común global donde más de 1.700 millones de personas están unidas para intercambiar ideas, servicios y amistad».
Chile 88/0.438	• Política Nacional de Ciberseguridad (2017)	«La ciberseguridad es una condición caracterizada por un mínimo de riesgos para el ciberespacio, entendido como el conjunto de infraestructuras físicas, lógicas y las interacciones humanas que allí ocurren».[2]
Japón 14/0.880	• Japan Defense (2015) • Cybersecurity Strategy: Toward a World-Leading, Resilient and Vigorous Cyberspace (2013) • International Strategy on Cybersecurity: j-Initiative for Cybersecurity (2013) • Basic Act on Cybersecurity (2014),[3] enmnendada por la Act 91 2018.[4] • Cybersecurity Strategy (2015) • Cybersecurity Strategy (2018)	«El objetivo de Japón es construir un ciberespacio "líder", "resistente" y "vigoroso" e incorporar este ciberespacio como sistema social para alcanzar una "nación de ciberseguridad" como una sociedad fuerte contra los ciberataques, llena de innovaciones y de lo cual su gente estará orgullosa».[5]
Malasia 8/0.893	• The National Cyber-Security Policy (NCSP)	«Vision: La infraestructura nacional de información crítica de Malasia será segura, resistente y autosuficiente. Infundido con una cultura de seguridad, promoverá la estabilidad, el bienestar social y la creación de riqueza».[6]
México 63/0.629[7]	• Estrategia Nacional de Ciberseguridad (2017)	«Conjunto de políticas, controles, procedimientos, métodos de gestión de riesgos y normas asociadas con la protección de la sociedad, gobierno, economía y seguridad nacional en el ciberespacio y las redes públicas de telecomunicación»
Nueva Zelanda 36/0.789[8]	• New Zealand National Security System (2011) • Defence White Paper (2010) • New Zealand's Cyber Security Strategy: A secure, resilient and prosperous online New Zealand (2015) • New Zealand's Cyber Security Strategy Action Plan (2015) • National Plan to Address Cybercrime (2015) • Refresh of New Zealand's Cyber Security Strategy and Action Plan 2018[9]	«La práctica de hacer que las redes que constituyen el ciberespacio sean lo más seguras posible contra las intrusiones, manteniendo la confidencialidad, disponibilidad e integridad de la información, detectando las intrusiones e incidentes que ocurren, y respondiendo y recuperándose de ellos» (New Zealand National Security System).

Perú 95/0.401	• Política de Seguridad y Defensa Nacional (2017)[10] • Decreto Supremo 066-2011-PCM: Agenda Digital Peruana 2.0 • Decreto Legislativo 1.141, Decreto de Fortalecimiento y Modernización del Sistema de Inteligencia Nacional (SINA) y la Dirección Nacional de Inteligencia (DINI)	«La seguridad digital en el ámbito nacional es el estado de confianza en el entorno digital que resulta de la gestión y aplicación de un conjunto de medidas proactivas y reactivas frente a los riesgos que afectan la seguridad de las personas, la prosperidad económica y social, la seguridad y los objetivos nacionales en dicho entorno. Se sustenta en la articulación con actores del sector público, sector privado y otros quienes apoyan en la implementación de controles, acciones y medidas» (Política de Seguridad y Defensa Nacional).
Singapur 6/0.898[11]	• National Cyber Security Masterplan 2018 • Factsheet on National Cyber Security Masterplan 2018 • Cyber Security Strategy (2016) • Cybersecurity Bill (2017)	«[Ciberseguridad] significa la seguridad de una computadora o sistema informático contra el acceso o ataque no autorizado, para preservar la disponibilidad e integridad de la computadora o sistema informático, o la confidencialidad de la información almacenada o procesada en la misma» (Cybersecurity Bill).
República Socialista de Vietnam 50/0.693	• Law on Network Information Security (2016)	«Seguridad de la información de red significa la protección de la información de red y los sistemas de información contra cualquier acceso, uso, divulgación, interrupción, enmienda o sabotaje ilegal, a fin de garantizar la integridad, la confidencialidad y la disponibilidad de la información»

Notas: **1.** Ranking global/puntuación. El Índice Global de Ciberseguridad (GCI) preparado por la Unión Internacional de Telecomunicaciones (UIT), en el marco de la Agenda Global de Ciberseguridad (GCA), mide el grado de compromiso de cada país con la ciberseguridad, utilizando una serie de indicadores individuales sobre aspectos legales, técnicos y organizativos, medidas, fomento de la capacidad y esfuerzos de cooperación internacional. Los indicadores se preparan sobre la base de una encuesta que revisa las leyes, regulaciones, equipos de respuesta a incidentes de seguridad informática (CSIRT), políticas y estrategias nacionales, estándares, certificaciones, capacitación vocacional, concientización y alianzas. **2.** Dentro del concepto se hace referencia que, en seguimiento a los estándares internacionales, los atributos claves a proteger son «la confidencialidad, integridad y disponibilidad de la información», lo que a nuestro parecer coincide con la definición de la UIT sobre ciberseguridad (Gobierno de Chile, 2017). **3.** La Basic Act on Cybersecurity, promulgada el 6 de noviembre de 2014, proporcionó una posición legal para el concepto de ciberseguridad y aclaró las responsabilidades de los distintos stakeholders. Fue creada como una política básica sobre medidas relacionadas con la ciberseguridad para desarrollarse en un período de tres años (Gobierno de Japón, 2018). **4.** La enmienda apunta a garantizar la ciberseguridad, mientras que Japón alberga los Juegos Olímpicos y Paralímpicos de Tokio en 2020. «Global legal monitor», Library of Congress, 26 de diciembre de 2018, disponible en http://bit.ly/35L2Mjy. **5.** Tim Maurer y Robert Morgus, «Compilation of existing cybersecurity and information security related definitions», New America, 5 de noviembre de 2014, disponible en http://bit.ly/2Q5yjWq. **6.** «National Cyber Security», Ministry of Science, Technology and Innovation de Malasia, disponible en https://bit.ly/35GoJQu. **7.** En el año 2017 se situaba en el lugar 38 (0.660). **8.** Para el año 2018 Nueva Zelanda no respondió el cuestionario del Índice. Sin embargo, en el año 2017 se situaba en el lugar 19 con 0.718. **9.** En abril de 2018, el Departamento del Primer Ministro y el Gabinete (DPMC, por sus siglas en inglés) publicó dos documentos relacionados con la actualización de la Estrategia de Seguridad Cibernética y el Plan de Acción de Nueva Zelanda. **10.** Este documento cuenta con un apartado denominado 4.2.14, «Infraestructura para enfrentar ataques a los sistemas de información: Ciberseguridad», en el que se destaca el compromiso con el desarrollo de habilidades militares y policiales, con la finalidad de «garantizar la paz internacional y el orden interno, a través de la integración de sistemas relacionados con la seguridad para disuadir, enfrentar, combatir eficazmente y eliminar a las organizaciones terroristas y de narcotraficantes». **11.** Para el año 2017 el IGC situaba a Singapur en el número 1 con 0.925.

El 13 de agosto de 2017 iniciaron las rondas de renegociaciones del TLCAN. Más allá de las declaraciones del gobierno de Estados Unidos en torno al tratado, los tres países están de acuerdo en que necesita modernizarse. El TLCAN original no contiene disposiciones sobre comercio electrónico ni sobre ciberseguridad. Por ello, estamos presenciando un nuevo capítulo respecto del flujo comercial entre las tres naciones, así como nuevos acuerdos en torno a la seguridad, pero esta vez, para salvaguardar el ciberespacio, el cual es común y global.

Ahora dentro del nuevo Tratado de México, Estados Unidos y Canadá (T-MEC) se ha incorporado —entre otras disposiciones—, el capítulo 19 relativo al comercio digital, en el que entre diversas cuestiones se abordan: los principios sobre acceso y uso de internet para el comercio digital (artículo 19.10), así como la protección de datos personales y el flujo transfronterizo de información por medios electrónicos (artículo 19.11).

Respecto de la ciberseguridad, la cual se aborda en el mismo capítulo, ésta se enfoca en la cooperación internacional y en el desarrollo de capacidades entre los tres países. Tanto en el CPTPP como el T-MEC, existen similitudes en cuanto a los compromisos establecidos en materia de ciberseguridad entre las partes contratantes. En el CPTPP:

- Destaca un apartado relacionado con la ciberseguridad, el cual va encaminado a fomentar la cooperación entre las partes contratantes.
- Las partes contratantes se comprometen al desarrollo de capacidades de las entidades nacionales responsables de la respuesta a incidentes de seguridad informática, así como a emplear los mecanismos de colaboración para la identificación y mitigación de intrusiones maliciosas o la diseminación de códigos maliciosos que afecten las redes electrónicas de las partes (artículo 14.16).

En el T-MEC:

- En el artículo 19.15 referente a la ciberseguridad, el compromiso entre los tres países se enfocará también al desarrollo de capacidades de las entidades responsables de la respuesta a incidentes de ciberseguridad.
- Además, se busca fortalecer los mecanismos de colaboración existentes para identificar y mitigar las intrusiones malintencionadas o la difusión de códigos maliciosos que afecten a las redes electrónicas y utilizar esos mecanismos para abordar de manera rápida los incidentes de ciberseguridad, así como el intercambio de información para el conocimiento y las mejores prácticas.

En este sentido, podemos apreciar que para el desarrollo del mercado digital que se encuentra contenidos en los referidos instrumentos, aparece ya un apartado específico para el ámbito de la ciberseguridad, lo que refleja la importancia de la temática

en la materia. No obstante, como se desprende de sus estrategias o políticas nacionales en la materia, existen disparidades en la definición, en ambos casos los instrumentos son omisos en establecer un término consensuado para «ciberseguridad».

En los últimos años, la creación de estrategias nacionales de ciberseguridad ha aumentado. Sin embargo, lo que es bueno en una primera visión puede no serlo en realidad. Las leyes y políticas de ciberseguridad tienen un impacto directo en los derechos humanos, en particular el derecho a la privacidad, la libertad de expresión y el libre flujo de información. Los responsables políticos han creado varias políticas nacionales con la intención de proteger internet y otras TIC contra actores maliciosos. Sin embargo, muchas de estas políticas son demasiado amplias y están mal definidas, y carecen de controles y equilibrios claros u otros mecanismos democráticos de *accountability*, que pueden conducir a abusos de los derechos humanos e ir contra la innovación.

También se aprecia que dentro de los compromisos adquiridos se encuentran la colaboración y el desarrollo de habilidades. Gran parte de la desconfianza existente en el empleo de las TIC para mantener la paz, estabilidad y seguridad internacional, constituye la disparidad que tienen los países en el desarrollo de habilidades en la materia. Un paso a favor de la confianza será la colaboración en el desarrollo de capacidades. Sin embargo, esto puede volverse también en contra si consideramos las distintas visiones que países más desarrollados tienen sobre el uso del ciberespacio. Por tomar un ejemplo, la National Cyber Strategy de Estados Unidos de 2018, destaca no solo por la defensa de sus redes, sistemas, funciones y datos, sino por mantener el liderazgo en el desarrollo de tecnologías emergentes y por la búsqueda de la hegemonía en el ciberespacio; distinta a la de la administración anterior, en que el entonces presidente Obama hacía referencia a la importancia de la colaboración y apoyo entre los países para disuadir el uso malicioso del ciberespacio (2016).

Más importante constituye el hecho de que en algunos casos, con la entrada de nuevos gobiernos, cambian las prioridades y las políticas a seguir. En ocasiones la creación y publicación de las ENCS resultan ser poco coherentes y estar acordes no con necesidades de los Estados, sino con los intereses de los gobiernos en curso, lo que impacta en: i) la falta de continuidad con las estrategias antes desarrolladas e implementadas, lo que genera incertidumbre; ii) la falta de confianza de los *stakeholders*; y iii) el desperdicio de tiempo con el que no se cuenta al volvernos más vulnerables ante las amenazas y riesgos, por no tener un punto claro de acción.

Consideraciones finales

Los países cada vez dependen más de internet para mantener sus servicios, infraestructura y economías en el ciberespacio. Por tanto, deben ser los más preocupados en mantenerlo seguro. De esta forma, los encargados de la formulación de políti-

cas públicas enfrentan una inmensa tarea para seguir el rápido ritmo del cambio tecnológico en medio de una gran incertidumbre sobre la configuración del futuro (UNCTAD, 2017).

En el mundo físico no existe un sistema completamente seguro, lo que también aplica en el ciberespacio. Debemos considerar que cada día individuos, organizaciones, empresas, gobiernos y sociedades dependemos más de las TIC, y aunque el crear e implementar estrategias o políticas en materia de ciberseguridad tiene un costo económico, el costo de la inacción puede ser mayor. En este sentido, vale la pena estar preparados y ser resilientes.

Con independencia de su definición, la ciberseguridad debe ser implementada de manera holística, abarcando aspectos económicos, sociales, educativos, legales, policiales, técnicos, diplomáticos, militares y de inteligencia. Debe estar basada en la gestión de riesgos, respetando los derechos humanos y gestionada con un enfoque *multistakehol*der.

Se debe buscar que las preocupaciones relacionadas con la ciberseguridad no den lugar a barreras al comercio electrónico y la inversión extranjera. Si bien el desarrollo del comercio electrónico requiere un marco normativo que facilite la seguridad jurídica de las personas que opten por emplear medios electrónicos en lugar de los convencionales, estos marcos no pueden imponer barreras que eviten el desarrollo y crecimientos económicos que trae aparejado esta clase de comercio.

Para la OCDE (2002), las estrategias nacionales de ciberseguridad deben tener dos objetivos: impulsar la prosperidad económica y social, así como proteger las sociedades que dependen del ciberespacio contra las amenazas cibernéticas, lo que debe hacerse preservando la apertura de internet como plataforma de innovación y nuevas fuentes de crecimiento, y no a través de bloqueos arbitrarios o de decisiones que vayan en contra de su arquitectura o funcionamiento.

La forma en que la ciberseguridad se vincula a la seguridad económica nacional tiene nuevas maneras y contextos. Con el desarrollo de tecnologías que habilitan de la economía digital y fomentan el comercio electrónico, la seguridad económica asociada con la alta tecnología está siendo reconocida como una fuente sustancial de seguridad nacional.

Debemos poner atención en la forma en que la ciberseguridad se encuentra permeando dentro de los tratados de libre comercio, en especial en el ámbito del comercio electrónico. En ellos se encuentran contempladas obligaciones para las partes sobre la cooperación, así como el desarrollo de capacidades que permitan mantener la confianza y protección del comercio electrónico.

La responsabilidad en el uso ético de las tecnologías no solo concierne a los países, sino a las empresas comprometidas con el desarrollo, el respeto de los derechos humanos, la paz y la estabilidad internacional. Existen crecientes preocupaciones sobre el desarrollo y la venta de tecnología por parte de las empresas a los regímenes

gubernamentales que violan los derechos humanos; esto ha derivado en gran medida en las limitantes que algunos países presentan al momento de desarrollar habilidades en ciberseguridad, con gobiernos que, con el pretexto de la seguridad, emplean estas herramientas contra su sociedad. Estas herramientas hechas «por diseño» pueden causar daños y violar derechos y libertades fundamentales. Dentro de los tratados de libre comercio debería considerarse la responsabilidad y el uso ético de estas herramientas que pueden llegar a tener impactos en la estabilidad, la seguridad y la paz internacional, esto a través del compromiso entre los Estados parte de desarrollar e implementar sistemas robustos de *accountability* y transparencia.

Además de considerar cuestiones como la educación y el desarrollo de habilidades digitales, el mercado laboral, la ciencia e innovación, la competencia, el desarrollo de tecnología, así como el régimen de políticas comerciales e industriales, deben encargarse de la protección de las infraestructuras críticas, que depende de las políticas y prioridades nacionales. Pero también se debe llevar a cabo con la cooperación de las diversas partes interesadas (*stakeholders*), considerando que la mayor parte de prestadores del servicio son empresas particulares. Estos temas también son de interés público, toda vez que las amenazas al ciberespacio pueden afectar a países y sociedades completas.

Referencias

Albert, Mathias, y Barry Buzan (2011). «Securitization, sectors and functional differentiation». *Security Dialogue,* 42 (4-5): 413-425. Disponible en http://bit.ly/2PBRcBx.

Becerril, Anahiby (2019). «La ciberseguridad en la seguridad nacional: Amenazas y retos en el ciberespacio». *Ciberseguridad Nacional, Revista de Administración Pública*, 54 (1): 113-148.

Becerril, Anahiby y Samuel Ortigoza (2018). «Habilitadores tecnológicos y realidades del Derecho Informático Empresarial». *IUS Revista del Instituto de Ciencias Jurídicas de Puebla,* 12 (41): 11-44. Disponible en http://bit.ly/35EA5on.

Castrillón y Luna, Víctor Manuel y Anahiby Becerril (2015). *Contratación electrónica civil internacional: Globalización, internet y derecho.* Ciudad de México: Porrúa.

Comisión Europea (2014). *Definition of a research and innovation policy leveraging cloud computing and IoT combination*. Doi: 10.2759/38400.

eMarketer (2017). *Worldwide retail and ecommerce sales: eMarketer's estimates for 2016-2021*. Disponible en http://bit.ly/35zrtiA.

FEM, Foro Económico Mundial (2018). *Global risks report 2018*. Ginebra. Disponible en https://bit.ly/2EyoESX.

—. (2019). *Global risks report 2019*. Ginebra. Disponible en https://bit.ly/2PBuHwq.

Gobierno de Australia (2013). «Strong and secure: A strategy for Australia's national security». Disponible en https://bit.ly/2rU2KXV.

Gobierno de Chile (2017) «Política Nacional de Ciberseguridad». Disponible en https://bit.ly/2txYqoJ.

Gobierno de Japón (2018). «Cybersecurity strategy». Disponible en https://bit.ly/35FpXMo.

Kshetri, Nir (2016). *The quest to cyber superiority: Cybersecurity regulations, frameworks and strategies of major economies.* Amsterdam: Springer. DOI: 10.1007/978-3-319-40554-4.

Mayer-Schönberger, Viktor y Kenneth Cukier (2013). *Big data: La revolución de los datos masivos.* Madrid: Turner.

Montero, Javier Puyol (2015). *Aproximación jurídica y económica al big data.* Valencia: Tirant Lo Blanch.

Navarro, Susana Navas y Sandra Camacho Clavijo (2016). *Mercado digital: Principios y reglas jurídicas.* Valencia: Tirant Lo Blanch.

OCDE, Organización para la Cooperación y Desarrollo Económicos (2002). *Guidelines for the security of information systems and networks: Towards a culture of security*. París: OECD Publishing.

—. (2012). *Cybersecurity policy making at a turning point: Analysing a new generation of national cybersecurity strategies for the internet economy.* París: OECD Publishing.

—. (2017). *The next production revolution: Implications for governments and Business*. París: OECD Publishing.

Rifkin, Jeremy (2013). *La era del acceso: La revolución de la nueva economía.* Barcelona: Paidós.

Schneier, Bruce (2004). *Secrets & lies: Digital security in a networked world*. Indianápolis: Wiley.

Schwab, Klaus (2016). *The fourth industrial revolution*. Ginebra: World Economic Forum.

Sigmond, Karen (2018). «El comercio electrónico en los tratados de libre comercio de México». *IUS Revista del Instituto de Ciencias Jurídicas de Puebla,* 12 (41): 359-377. Disponible en http://bit.ly/2tsqZfZ.

UNCTAD, United Nations Conference on Trade and Development (2017). *Informe sobre la economía de la información 2017: Digitalización, comercio y desarrollo. Panorama general.* Nueva York: Organización de Naciones Unidas.

UIT, Unión Internacional de Telecomunicaciones (2018). *Global cybersecurity index*. Ginebra.

Sobre la autora

Anahiby Becerril es abogada. Licenciada en Derecho por la Universidad de las Américas, Puebla (UDLAP), México. Doctora en Derecho y Globalización por los Programas Nacionales de Posgrados de Calidad de Conacyt, México. Su correo electrónico es anahiby@hotmail.com. http://orcid.org/0000-0002-5726-5400.

REVISTA CHILENA DE DERECHO Y TECNOLOGÍA

La *Revista de Chilena de Derecho y Tecnología* es una publicación académica semestral del Centro de Estudios en Derecho Informático de la Facultad de Derecho de la Universidad de Chile, que tiene por objeto difundir en la comunidad jurídica los elementos necesarios para analizar y comprender los alcances y efectos que el desarrollo tecnológico y cultural han producido en la sociedad, especialmente su impacto en la ciencia jurídica.

EDITOR GENERAL

Daniel Álvarez Valenzuela
(dalvarez@derecho.uchile.cl)

SITIO WEB

rchdt.uchile.cl

CORREO ELECTRÓNICO

rchdt@derecho.uchile.cl

La edición de textos, el diseño editorial
y la conversión a formatos electrónicos de este artículo
estuvieron a cargo de Tipográfica
(www.tipografica.cl).