CENTRO DE INVESTIGACIONES Y ESTUDIOS ESTRATÉGICOS
ANEPE.CL

ISSN 0719-4110

CUADERNO DE TRABAJO N°9-2019

INFRAESTRUCTURA CRÍTICA, USUARIOS Y CONTENIDO: ¿QUÉ SE BUSCA PROTEGER EN EL CIBERESPACIO?

CUADERNOS DE TRABAJO es una publicación orientada a abordar temas vinculados a la Seguridad y Defensa a fin de contribuir a la formación de opinión en estas materias.

Los cuadernos están principalmente dirigidos a tomadores de decisiones y asesores del ámbito de la Defensa, altos oficiales de las Fuerzas Armadas, académicos y personas relacionadas con la comunidad de defensa en general.

Estos cuadernos son elaborados por investigadores del CIEE de la ANEPE, pero sus páginas se encuentran abiertas a todos quienes quieran contribuir al pensamiento y debate de estos temas.

CUADERNO DE TRABAJO DEL CENTRO DE INVESTIGACIONES Y ESTUDIOS ESTRATÉGICOS es una publicación electrónica del Centro de Investigaciones y Estudios Estratégicos de la Academia Nacional de Estudios Políticos y Estratégicos y está registrada bajo el **ISSN 0719-4110 Cuad. Trab., - Cent. Estud. Estratég.**
Dirección postal: Avda. Eliodoro Yáñez 2760, Providencia, Santiago, Chile.
Sitio Web www.anepe.cl. Teléfonos (+56 2) 2598 1000, correo electrónico ciee@anepe.cl

INFRAESTRUCTURA CRÍTICA, USUARIOS Y CONTENIDO: ¿QUÉ SE BUSCA PROTEGER EN EL CIBERESPACIO?

Septiembre, 2019
Pía Martabit Tellechea*

RESUMEN

Los asuntos de ciberseguridad hoy se encuentran en una fase de definición de normas y límites de acción en el derecho nacional e internacional. Además, nos encontramos en la actualidad con la necesidad de comenzar a aplicar políticas destinadas a hacer de esta dimensión un lugar libre de amenazas. Para esto, este artículo tiene por objetivo definir lineamientos iniciales para generar debate sobre legislatura y políticas públicas a partir de la distinción sobre qué y a quienes se busca proteger en el ciberespacio de acuerdo con la estructura tecnológica, considerando por una parte la tensión manifiesta entre intereses de los diversos actores, y por otra, aplicando la teoría económica de bienes públicos y privados.

PALABRAS CLAVE: Seguridad internacional, Ciberseguridad, Infraestructura crítica, Bienes públicos

Introducción

El ciberespacio se ha desarrollado, en su breve historia, para constituirse en un espacio público universal, entorno donde diversos y complejos actores globales han volcado sus acciones utilizando la red hiperconectada del "Internet". Como consecuencia fenómenos sociales, políticos, económicos, etc., se han transferido, así como otros han mutado, y en múltiples casos han modificado conductas individuales y colectivas, a tal punto que las relaciones de poder entre actores se han reconfigurado. Por ejemplo, difícilmente podemos pensar en la ejecución y desarrollo de mercados económicos sin el uso de algún espacio del Internet, ni tampoco pensar que gran parte de los fenómenos sociopolíticos –de al menos 50% de la población mundial[1] – ocurren fuera o al margen de la red global informática.

* Docente del Instituto de Humanidades, Universidad del Desarrollo. Cientista político de la Universidad del Desarrollo y magíster en Periodismo Mención Prensa Escrita de la Pontificia Universidad Católica de Chile, con estudios de diplomado en Seguridad Internacional y Ciberseguridad de la Universidad de Chile. piajomte@gmail.com

[1] Nota del Autor: A marzo de 2019 la penetración de Internet, es decir cuánto de la población mundial tiene acceso a la red global, era de 56,8%. Entre el 2000 y el actual año esta cifra aumentó en un 1.114%. INTERNET WORLD STATS. World Internet Usage And Population Statistics March, 2019 - Updated [En línea]. [Fecha de consulta: 15 de mayo 2019] Disponible en:<https://www.internetworldstats.com/stats.htm>

De hecho, considerando los índices de penetración de Internet, a marzo de 2019 era de un 56,8% de la población mundial[2], más de la mitad del mundo podría o debería utilizar la "*web*" para acceder a algún bien o servicio, sea privado o público, y desde esta plataforma, infinitas posibilidades para continuar desarrollando todo tipo de interacciones.

Por otro lado, y a consecuencia de esta penetración, se percibe, por parte de los actores políticos, una aceptación general para hacer del ciberespacio un lugar seguro. Mientras los riesgos y amenazas cibernéticas avanzan en tanto la sociedad se hace cada vez más dependiente de las tecnologías de la información, generando focos de incertidumbre que alteran al colectivo social y sus diversos actores de manera transversal, de diferentes formas y disímiles alcances. En otras palabras, se instala la percepción de que en el Internet (o en relación a este) surgen numerosas y complejas fuentes de riesgo, ya sea por digitalización de amenazas tradicionales o por cambios paradigmáticos que sufren estas amenazas en este proceso de digitalización.

La conceptualización de ciberseguridad entonces toma peso, se torna un objetivo a alcanzar, pero el camino a ese lugar presenta divergencias por cuanto diferentes actores globales poseen intereses políticos, económicos y/o sociales contrapuestos, como también apreciaciones heterogéneas frente a qué y cómo se debe asegurar la red mundial por donde transita la información.

"Mientras los riesgos y amenazas cibernéticas avanzan en tanto la sociedad se hace cada vez más dependiente de las tecnologías de la información, generando focos de incertidumbre que alteran al colectivo social y sus diversos actores de manera transversal, de diferentes formas y disímiles alcances."

Para sortear las dificultades que se observan a la hora de analizar el ciberespacio en los términos descritos, se debe comenzar por comprender a cabalidad que el fenómeno comprende perspectivas de red global. En tanto, la "*web*" constituye parte fundamental de la comunicación social, y es utilizada como vehículo para el flujo de información, demostrando particularidades que la destacan por ser altamente eficiente e instantánea, atmósfera que posee fuerza para influenciar e incluso amenazar estructuras sociales tradicionales a nivel mundial.

Desde la perspectiva económica, "Internet" se presenta como mecanismo de comunicación financiera, pero a su vez como un servicio privado respaldado por empresas que mantienen infraestructuras críticas, y que propician un mercado completo de productos y servicios digitales. Desde la perspectiva de la política internacional, el ciberespacio se enmarca como fuente, multiplicadora o facilitadora, del desarrollo y/o generación de amenazas a la población, sus instituciones y el Estado. En síntesis, es el resultado de una dimensión donde las ventajas económicas del ciberespacio difieren de los intereses políticos y preocupaciones sociales. Las tensiones entre estos dos tipos de intereses, que no son exclusivos del Internet, van a construir discursos divergentes en relación a qué se debe proteger.

Pese a diversas perspectivas la pregunta es la misma cuando hablamos de ciberseguridad: ¿cómo asegurarnos y protegemos a la hora de utilizar y participar del ciberespacio? Pero antes

[2] Ibíd.

del "cómo", es necesario profundizar respecto del "qué". Para ello, se debe tener certeza y claridad del objeto que merece ser protegido para identificar con la misma precisión y nitidez la mejor forma de asegurar dicho elemento. Así como los actores poseen diferentes perspectivas sobre qué debe asegurarse, también hay partes del ciberespacio que son diferentes en naturaleza y que presentan también múltiples perspectivas de cómo deben ser protegidas y resguardadas.

La pregunta que la mayoría de los actores globales se hacen es: ¿qué se busca proteger? El problema del qué proteger resulta necesariamente fundamental para poder definir en primera medida los límites de la acción humana en la red global informática. Si el límite más universal que tenemos para la acción humana son los derechos humanos, ¿qué derechos, e incluso, obligaciones fundamentales podríamos determinar para regular las acciones en el escenario cibernético transfronterizo?

El objetivo de este artículo no constituye proponer una carta de derechos fundamentales para el ciberespacio, sino que será identificar aquellos elementos esenciales que requieren protección en el ciberespacio, de qué forma y desde cuál perspectiva abordar, considerando convergencias y divergencias de los actores incumbentes. A partir de este registro, se buscará esquematizar aquellas posibles amenazas en las distintas capas que constituyen el ciberespacio, y así poder determinar elementos transversales de protección considerando la pluralidad cultural, ideológica y perceptiva de los participantes. De esta forma, no se pretende dar una solución universal, pero al menos constatar el grado de hiper-conectividad del escenario internacional desde la perspectiva de la ciberseguridad.

Internet en su complejidad técnica y social, requiere de una definición general y aproximaciones específicas para establecer qué elementos deberían estar regulados, cuáles podrían considerarse libres y cuáles merecerían ser analizados caso a caso, con la finalidad de generar políticas públicas eficientes, eficaces y de largo plazo, y así entregar de igual manera protección tanto para el Estado, para los agentes económicos, y para los ciudadanos de la sociedad global. Por esta razón, será imperativo determinar qué tipo de elementos requieren protección –incluidos los recursos–, de acuerdo a la función y rol de los actores.

"En este sentido, es necesario señalar que la noción de "seguridad" ha pasado de tener un enfoque exclusivamente militar a uno más multidisciplinario, contexto que incluye la variable económica."

Postulando que el concepto de ciberseguridad es la noción de un ciberespacio libre de amenazas, sería extrapolable a los paradigmas de los estudios de seguridad internacional. En este sentido, es necesario señalar que la noción de "seguridad" ha pasado de tener un enfoque exclusivamente militar[3] a uno más multidisciplinario, contexto que incluye la variable económica.

Sin embargo, esto ha hecho que el concepto se amplíe, por lo que Baldwin "formuló siete preguntas para reducir dicha conceptualización"[4]: "¿para quién?", "¿para qué valores?", "¿cuánta seguridad?", "¿para cuáles amenazas?", "¿por qué medios?", "¿a

[3] ENGERER, H. Security as a Public, Private or Club Good: Some fundamental Considerations. German Institute for Economic Research, Defence and Peace Economics, Vol. 22(2), abril 2011. [En línea] Disponible en:<https://www.tandfonline.com/doi/full/10.1080/10242694.2011.542333>

[4] ENGERER, H. Security as a Public, Private or Club Good: Some fundamental Considerations. German Institute for Economic Research, Defence and Peace Economics, Vol. 22(2), abril 2011. [En línea] Disponible en:<https://www.tandfonline.com/doi/full/10.1080/10242694.2011.542333>

qué costos?", "¿en qué periodo de tiempo?"[5]. Por otro lado, resulta importante establecer qué condición de seguridad comprende la ciberseguridad: ¿es pública o es privada?[6]. Este tipo de cuestionamiento genera otras preguntas como: ¿quién es responsable de esta, el Estado o el mercado? Esta interpelación es fundamental para el análisis ulterior, por tanto, el ciberespacio posee varios propietarios, sean estos privados y públicos.

Una forma de analizar la compleja dimensión de ciberseguridad es tomar en consideración lo señalado por algunos autores, que sitúan al dominio ciber y la seguridad en general como un bien público global. ¿Por qué el ciberespacio y su seguridad se podría considerar bien común público? ¿Y por qué esta condición importa a la hora de definir qué y cómo proteger los intereses de los actores incumbentes en las diferentes capas del ciberespacio? Las respuestas a estas interrogantes se abordarán desde la relevancia que representa aplicar la teoría económica al ciberespacio, principalmente porque tiene una utilidad analítica importante a la hora de definir estrategias de ciberseguridad multidisciplinarias y completas. Esta exigencia se explica inicialmente por dos razones.

La primera razón es que "Internet" se ofrece como un servicio, así como lo es el acceso a cualquier tecnología de la información y comunicación (televisión y la radio). Se transa como bien en el mercado, tanto los dispositivos necesarios como accesorios de acceso a la red misma. Es innegable que a fin de cuentas es un bien más, pero debido a que corresponde a una tecnología de comunicación masiva e innovadora de doble sentido, y a diferencia de otras tecnologías, sostiene un flujo de información elevadamente complejo que ha convertido el ciberespacio en una gran ágora mundial. Entonces, podemos señalar que es un bien (o servicio) y es de carácter global, pero habrá que distinguir si es público o privado.

"¿Por qué el ciberespacio y su seguridad se podría considerar bien común público? ¿Y por qué esta condición importa a la hora de definir qué y cómo proteger los intereses de los actores incumbentes en las diferentes capas del ciberespacio?"

La segunda razón se puede analizar desde la perspectiva de la teoría económica para definir quién debería asumir los costos por mantener la "carretera de información" libre de amenazas. Si postulamos a que constituyen "bienes públicos globales, como la capa de ozono, la ausencia de guerras, o los efectos de absorción del CO_2 de la vegetación del planeta, son bienes no rivales y no excluibles"[7], y por esto justificarían el rol regulador y supervisor del Estado en defensa de la protección de estos servicios.

Así las cosas, podría generarse una enorme brecha de desigualdad en los incentivos para diferentes actores incumbentes en el escenario internacional para otorgar la mejor seguridad en el ciberespacio, principalmente porque los mecanismos, las estrategias y aplicación de regulaciones involucran elevados presupuestos, y porque ciertos actores internacionales no perciben aún amenazas en su entorno, por lo cual no habría necesidad para realizar estas inversiones, ni destinar recursos para desarrollar una política pública.

[5] Ibíd.

[6] Ibíd.

[7] HANSEL, M. Cyber Security Governance and the Theory of Public Goods. E-International Relations (E-IR), 2013. [En línea]. Disponible en:<https://www.e-ir.info/2013/06/27/cyber-security-governance-and-the-theory-of-public-goods/>

Considerando el entorno descrito se analizará a continuación aquellas capas del ciberespacio que responden satisfactoriamente a la categoría del bien a proteger, de esta forma determinar inicialmente qué actor asumiría responsabilidades, tipo de costos y finalmente el vínculo con las amenazas.

Estructura del ciberespacio

Para identificar si el ciberespacio y su seguridad son bienes globales públicos o privados, se debe entender las diferentes partes de la red, que son diferentes en naturaleza. La estructura de Internet se compone de tres capas principales[8]:

1. Capa física[9]: Es aquel estrato compuesto por la infraestructura crítica de la red entendiéndose cualquier sistema que combina varias instalaciones y estructuras tangibles que habilitan ciertas actividades, como por ejemplo todos los ductos que transportan fluidos desde agua hasta petróleo. Hay una parte física compuesta por ordenadores, dispositivos, puertos, cables, etc., que compone la red del ciberespacio. Por otro lado, producto del desarrollo del ciberespacio, la infraestructura crítica de otros servicios (transporte y energía), se han automatizado, digitalizando y conectando el comando y control de estas con otros estadios.

En otras palabras, "en la era de la información, las infraestructuras tradicionales (físicas) se extienden al ciberespacio, transformándose en infraestructuras de información al incorporar computadores"[10], y en algunos casos, como los sistemas financieros, prácticamente utilizan plataformas digitales.

El fenómeno del "Internet de las Cosas" es parte de esta tendencia, entorno donde la automatización, digitalización e hiperconectividad de todo tipo de infraestructuras están conectados[11]. Las infraestructuras mencionadas se expanden de su maquinaria tangible a ser automatizada por medio de las otras capas no físicas de Internet. Estos sitios no físicos, en donde se establecen las partes automatizadas de otros servicios, son sostenidos en la realidad tangible de la capa física o infraestructura crítica del ciberespacio mismo; es decir, la infraestructura crítica de la red se transforma en la infraestructura crítica de otros servicios esenciales de la sociedad.

Este virtuosismo físico del ciberespacio es "la precondición básica para la existencia del ciberespacio"[12]. Sosteniendo esta premisa, esta capa necesariamente estaría sujeta bajo una autoridad estatal, condicionante dado por el carácter físico y tangible, situado en un territorio determinado[13], y por ende sujeto a la jurisprudencia de un país en particular. Con todo, la propiedad de la infraestructura crítica es, en su mayoría, privada, dejando al Estado como regulador de la operación.

2. Capa lógica o sintáctica: Es aquella que presenta los protocolos y reglas por los cuales

[8] ŽÁKOVÁ, G. Cyberspace: Global Public Goods?. Acta Oeconomica Pragensia, 2018, 26(2), 68-82 [En línea] Disponible en:<https://doi.org/10.18267/j.aop.602>

[9] TABANSKY, L. Critical Infrastructure Protection against Cyber Threats. Military and Strategic Affairs, Vol. 3, No. 2, november 2011.[En línea] Disponible en:<https://i-hls.com/wp-content/uploads/2013/03/Critical-Infrastructure-Protection-against-Cyber-Threats-Lior.pdf>

[10] Ibíd.

[11] BURGESS, M. What is the Internet of Things? WIRED explains. WIRED, 16 febrero de 2018. [En línea] Disponible en:<https://www.wired.co.uk/article/internet-of-things-what-is-explained-iot>

[12] ŽÁKOVÁ, Loc. Cit.

[13] Ibíd. Nota del Autor: Hay partes donde la infraestructura física no respondería necesariamente a alguna jurisprudencia de un Estado en particular. Esta parte sería el tramo del cableado submarino de fibra óptica cuando está en aguas internacionales.

se va a empaquetar la información para realizar el viaje. Una buena comparación para entender esta dimensión es entenderlo como el tradicional sistema de comunicación "masiva" de doble vía (correo postal). Los protocolos son entonces aquellos lenguajes creados para que el mensaje llegue a destino, es decir, el código postal.

Además de otros patrones informáticos para hacer que el mensaje llegue a destino de manera íntegra y segura. En palabras concretas, "está representado por reglas y límites a través de los cuales se puede procesar la información e incluye el software y las aplicaciones necesarias para el correcto funcionamiento del ciberespacio, como los protocolos del sistema y los nombres de dominio"[14]. Lenguajes principales como DNS (*Domain Name System*) e IP (*Internet Protocol*), son mantenidos por la organización Corporación de Internet para la Asignación de Nombres y Números (ICANN) que conecta organizaciones regionales alrededor del mundo en una plataforma global de múltiples "*stakeholders*"[15].

3.Capa semántica: Consiste en la información que es intercambiada, almacenada y procesada y que puede ser desplegada en varios formatos[16]. La información es al final el elemento que posee el valor para el emisor y receptor que pagan por el servicio de conectarse y poder entonces acceder a esta y hacer entrega de ella.

Ciberespacio: ¿Bien público global?

"Los bienes públicos son bienes que pueden ser utilizados por varios consumidores a la vez, sin afectar el uso de otros consumidores"[17]. La teoría desarrollada por Paul A. Samuelson en la década de 1950 define que los bienes públicos son no rivales y no excluibles. Por "no rivales" se entiende que son aquellos en donde su consumo no resulta en la reducción de la disponibilidad general, mientras que los bienes no excluibles son aquellos en donde es "prácticamente imposible excluir a cualquier actor de consumir el producto o el servicio"[18].

Por otro lado, mientras que algunos bienes son naturalmente globales, como el aire o la capa de ozono, el número de aquellos globalizados está creciendo[19]. Los bienes globales pueden identificarse en tres tipos: (1) bienes, como la radiación solar, donde es imposible o casi importable excluir el consumo; (2) aquellos diseñados como públicos, como la educación y el sistema legal; (3) bienes que se han hecho púbicos debido a la falta de conocimiento y previsión, como el adelgazamiento de la capa de ozono.

Los productos y servicios públicos presentan los mismos problemas de manejo de externalidades y asignación o distribución efectiva, y al estar disponible para todos sin costo, al no ser excluibles, los consumidores tienden a indicar un nivel más bajo de su utilidad (nivel de satisfacción) para disminuir el precio, generando distorsiones en el mercado y disponibilidad del bien. A nivel global estos problemas aumentan en negocios internos, el Estado puede a través de su autoridad regular y administrar estas externalidades, pero en el escenario global no hay autoridad central para eso. Esto se observa en bienes como la seguridad, el medio ambiente, la salud pública y otros esenciales para la sociedad. Entonces, cuando los Estados buscan

[14] Ibíd.
[15] ŽÁKOVÁ, Loc. Cit.
[16] Ibíd.
[17] Ibíd.
[18] HANSEL, Loc. Cit.
[18] ŽÁKOVÁ, Loc. Cit.

proveer seguridad, u otro bien público global, la solución habitual ha sido la cooperación a través de organismos internacionales y así minimizar estas externalidades[20].

También otros actores no gubernamentales se organizan en torno a minimizar dichas externalidades en estos bienes. Cuando hablamos a nivel estatal existen dos opciones de acción frente a estas externalidades, como también proveer de estos bienes globales a su población de manera unilateral o multilateralmente[21]. Desde el unilateralismo, se pueden concentrar los esfuerzos en fortalecer la parte de Internet, en este caso, que corresponde a la jurisprudencia y soberanía del Estado en cuestión; sin embargo, debido a la naturaleza global del ciberespacio que "tiende a ignorar barreras físicas, los esfuerzos unilaterales tienden a ser costosos o ineficientes"[22].

"Para países considerados democráticos y activos beneficiarios de la globalización, como es el caso de Chile, el aislacionismo no sería una opción, por lo que queda la cooperación y el multilateralismo para desarrollar y garantizar ciberseguridad."

En respuesta a esto, los Estados tienen la posibilidad también de cerrar sus fronteras informáticas, no obstante "esta opción casi seguramente implica altos costos económicos"[23]. Esto sería aplicable a escala global, a pesar de la existencia de un modelo de Internet cerrado que está en funcionamiento, y estaría bien encaminado (económicamente hablando). Este es el ciberespacio chino protegido por su "*Great Firewall*"[24].

Esta Gran Muralla informática corresponde a "esfuerzos conjuntos entre monitoreo gubernamental junto a empresas de tecnología y telecomunicaciones las que se encuentran obligadas a ejercer el control y reportar al Estado"[25]. Este tipo de espacio digital cerrado al demostrar su capacidad operativa (ya sea porque el tamaño de la población y economía China da para que funcione un ciberespacio relativamente independiente y aislado, o porque en términos generales y sin condiciones sería posible de igual manera) representa un modelo para otros Estados autoritarios que lo puedan replicar[26], con claras restricciones a libertades fundamentales del ciudadano.

Para países considerados democráticos y activos beneficiarios de la globalización, como es el caso de Chile, el aislacionismo no sería una opción, por lo que queda la cooperación y el multilateralismo para desarrollar y garantizar ciberseguridad[27]. Enmarcado en el contexto de la sociedad hiperconectada, el asunto se presenta de la siguiente manera: a falta de control fronterizo para enfrentar las amenazas

[20] Ibíd.

[21] HANSEL, Loc. Cit.

[22] Ibíd.

[23] Ibíd. Nota del Autor: El artículo citado señala el caso de Egipto 2011, en donde el gobierno intencionalmente bajó la conectividad, generando pérdidas entre 90 y 110 millones de dólares.

[24] BLOOMBERG NEWS. Analysis: The Great Firewall of China. BloombergQuickTake, The Washington Post, 5 de noviembre de 2018. [En línea] Disponible en:<https://www.washingtonpost.com/business/the-great-firewall-of-china/2018/11/05/5dc0f85a-e16d-11e8-ba30-a7ded04d8fac_story.html?utm_term=.0353f687dc8e>

[25] HANSEL. Loc. Cit.

[26] Ibíd.

[27] Ibíd.

globales, el multilateralismo se aplica para atender variados bienes públicos globales, como la seguridad, y específicamente en este caso se preocupa por la ciberseguridad.

Sin embargo, dado el carácter masivo de la hiperconectividad actual, pilar fundamental del proceso y fenómeno de la globalización, generada por el ciberespacio, resulta necesario concebir la seguridad y la ciberseguridad desde la perspectiva de la teoría económica de bien público global.

Por otro lado, existen los bienes de clubes globales que pertenecen a otro tipo de bienes impuros generales donde sería posible excluir a los clientes del consumo, empero la cantidad de estos no está limitada. La exclusividad propicia la facultad de imponer una tarifa al consumo[28].También participan los bienes comunes globales que están disponibles a nivel supranacional, éstos no son excluibles pero son rivales, es decir, hay una cantidad limitada y, por lo tanto, un consumo restrictivo de estos, como son océanos, la atmósfera, el universo o la Antártida[29].

Dos aspectos surgen de estas definiciones; en primer lugar, la provisión y protección de los bienes públicos constituye un interés de todos[30], ya que benefician al conjunto, como la seguridad; y en segundo lugar, es posible beneficiarse del bien sin participar de su generación, producción y/o protección, siendo estos las personas "*free-riders*" o polizones[31]. Ambos constituyen fundamentos razonables para sostener por qué los bienes públicos son poco provistos, y que la subproducción de ellos es muy común en el ámbito de las relaciones internacionales[32].

"Bajo el pensamiento pragmático, los incentivos para participar de una seguridad colectiva y enfrentar los costos de ésta en la dimensión del Internet presentan desafíos de cesión de soberanía en favor de prácticas y decisiones colectivas, que en muchos casos pueden ir en contra de otros objetivos propios del Estado..."

¿Por qué la subproducción de un bien público global como la seguridad internacional es común en relaciones internacionales? Si se reconoce que la seguridad es un bien público, entonces, estos tienden a ser insuficientemente provistos por actores privados, y por ende, el Estado es responsable de la provisión de seguridad[33].

En ambientes con gran número de consumidores, a escala global, da como resultado una mayor heterogeneidad, manifiestas diferencias culturales y distintos niveles de expectativas, entorno que complica la adopción de agendas para moderar las externalidades[34]. De acuerdo a la percepción con el cuál los realistas observan el escenario internacional anárquico y competitivo, la seguridad propia es el fin último del Estado.

Bajo el pensamiento pragmático, los incentivos para participar de una seguridad colectiva y enfrentar los costos de ésta en la dimensión

[28] ŽÁKOVÁ. Loc. Cit.

[29] Ibíd.

[30] HANSEL. Loc. Cit.

[31] Ibíd.

[32] Ibíd.

[33] KIRSHNER, J. Realist political economy. Routledge Handbook of International Political Economy (ed. Mark Blyth). Abingdon:Routledge,2009.[Enlínea]Disponibleen:<https://www.routledgehandbooks.com/doi/10.4324/9780203881569.ch2>

[34] ŽÁKOVÁ. Loc. Cit.

del Internet presentan desafíos de cesión de soberanía en favor de prácticas y decisiones colectivas, que en muchos casos pueden ir en contra de otros objetivos propios del Estado (diferencias de intereses, nivel de expectativas o nociones culturales), y además requiere de extraordinarios costos asociados a la negociación internacional.

Para sistematizar lo señalado nos preguntamos ¿Para qué participar de prácticas y tendencias de acción estatal en torno a la protección del medio ambiente si algunos Estados, que tienen la capacidad y desarrollo para no verse afectados en términos de poder y no sufren las consecuencias de igual manera? Situaciones como estas se evitan, en teoría, cuando un Estado o varios están dispuestos a llevar una carga adicional al hacer un esfuerzo extra, o se evita al establecer un régimen internacional que opere mecanismos de desincentivos para actitudes de "*free-riding*", al facilitar la identificación y castigo de los "*free-riders*"[35].

Bajo la óptica del realismo es parte de la supervivencia actuar siempre en términos de "egoísmo", siempre que no afecte mis intereses, no habría razones para destinar esfuerzos y recursos escasos para participar de la acción colectiva en torno a la seguridad internacional; aún más, cuando los Estados no asumen costos ni externalidades a consecuencia de la digitalización y penetración de internet.

Entonces, hablando específicamente sobre el aspecto de ciberseguridad, no todos los Estados presentan y evalúan sus inseguridades en el ciberespacio de igual manera porque no se ven afectados ecuánimemente. No todos los actores poseen igual penetración de Internet, ni el mismo avance de digitalización de sus servicios públicos y privados, como para promover las tendencias actuales en seguridad informática.

"La situación se complejiza debido al problema de atribución y territorialidad que presenta el ciberespacio. El problema de atribución es que difícilmente se puede identificar quién es el perpetrador de un ciberataque..."

China, bajo los intereses de su régimen particular, no vislumbra incentivos para practicar la ciberseguridad de la misma forma de los Estados europeos, por ejemplo. Esto quiere decir que en el aspecto del ciberespacio, no florece un consenso suficiente para desarrollar prácticas globales en favor de atender los costos y externalidades generados por la inseguridad, por lo que algunos actores harán esfuerzos mayores para generar regímenes de control sobre "*free-riders*" (o que se ven beneficiados de una debilidad en la institucionalidad cibernética), mientras que estos "*free-riders*" aplicarán medidas unilaterales que estén de acuerdo con sus propios intereses.

La situación se complejiza debido al problema de atribución y territorialidad que presenta el ciberespacio. El problema de atribución es que difícilmente se puede identificar quién es el perpetrador de un ciberataque[36] y por eso defensas cibernéticas débiles crean significativas externalidades para otros (que pueden ser consideradas como males públicos globales)[37], y enreda el panorama al aumentar incentivos para mantener dichas defensas bajas en países que no se ven directamente amenazados, pero que sus ciberespacios pueden ser utilizados para multiplicar ataques informáticos y así difuminar el origen de dichos ataques.

[35] HANSEL. Loc. Cit.

[36] HAY NEWMAN, L. Hacker Lexicon: What Is The Attribution Problem?. Security, WIRED, 24 de diciembre 2016. [En línea] Disponible en:<https://www.wired.com/2016/12/hacker-lexicon-attribution-problem/>

[37] HANSEL. Loc. Cit.

Por otro lado, se presenta un problema de territorialidad como consecuencia de la globalidad de la red, dimensión que podría emplazar a que las decisiones que se adopten unilateralmente sean poco eficientes y eficaces. Para lograr un moderado control de las entradas y salidas de información, en escenarios sin fronteras, debe desarrollarse cierta capacidad técnica que contribuya a ejercer vigilancia y autoridad sobre las acciones que se generen en el ciberespacio.

Podemos decir entonces que los Estados, dependiendo de sus necesidades e intereses, se pueden beneficiar de las defensas bajas (o mantención del *statu quo*) para perpetrar ciberataques, ocultando (*free-riding*) detrás del problema de atribución de territorialidad.

En resumen, y en los términos más específicos del concepto seguridad, si consideramos que constituye un bien privado puro, "el mercado ofrecerá un conjunto óptimo de medidas de protección con respecto a la composición, el alcance y la durabilidad"[38]. Por otro lado, "si la seguridad es un bien público, entonces se advierte un peligro por falta de provisión"[39]. Finalmente, "la seguridad como bien del club proporciona beneficios solo para sus miembros y efectos de desbordamiento potencialmente positivos para los forasteros"[40].

De acuerdo a lo expresado por Hella Engerer, la seguridad será un bien público, privado o club, dependiendo de la materia que se está "asegurando" y en qué contexto. Varios ejemplos son exhibidos, y muchos pueden ser aplicados al ciberespacio. Ante esta realidad es necesario clarificar qué se busca proteger, en el vasto y complejo ciberespacio, y a qué tipo de bien corresponde, luego se podrá identificar quiénes son responsables en los diferentes niveles de ciberseguridad.

¿Qué buscamos proteger?

Es una pregunta que no tiene una única respuesta. Hay, como mencionamos, tres capas que son diferentes en naturaleza y responden a distintas partes de la web. En estas capas, diferentes y múltiples actores internacionales y nacionales, son titulares propietarios de lo que posee valor político, económico y social, y por ende, representa la dimensión de lo que se busca proteger.

Retomando las preguntas de Baldwin, es importante aplicarlas y responderlas ya que para otorgar respuestas acertadas dependerá si la seguridad en este marco es un "*commodity*" privado, un bien público, o un bien club[41]. Estas preguntas se enmarcan en:

(1) ¿Quién es responsable de la seguridad, el Estado o el mercado?

(2) *¿Cuál (es) preocupaciones de seguridad deben tratarse públicamente, y cuáles deben de ser jerarquizadas en privado?*[42]

Engerer replantea lo señalado, y presenta otras interrogantes más relevantes para este análisis:

a) ¿Qué valores deben ser protegidos? ¿Cuáles deben ser de manera privada y cuáles de manera pública?[43]

Estas preguntas dependen si la seguridad es un bien privado o uno público[44]. A diferencia de

[38] ENGERER. Loc. Cit.

[39] Ibíd.

[40] Ibíd.

[41] ENGERER. Loc. Cit.

[42] BALDWIN. Loc. Cit. En: ENGERER. Loc. Cit.

[43] Ibíd.

la seguridad en términos genéricos, en donde se observa la presunción de que es un bien público pero que es atendido de manera pública y privada, la ciberseguridad debe ser planteada en sus propios términos.

Es importante recurrir a la historia del ciberespacio brevemente para entender su naturaleza tanto pública como privada. "Internet" comenzó como ARPANET en 1969, una red de investigación académica financiado por la agencia militar de los Estados Unidos, *Advances Research Projects Agency* (ARPA, hoy DARPA)[45].

Una razón fundamental de la creación de este espacio virtual fue la necesidad de fortalecer las comunicaciones, haciéndolas resilientes ante la posibilidad de un ataque nuclear de la Unión Soviética, en contexto de la Guerra Fría[46]. Hasta 1980 se crearon los protocolos y estándares esenciales como TCP/IP, y en dicha década el "Internet" se desplazó desde la agencia militar al *National Science Foundation*, oficina gubernamental de ciencia e ingeniería de los Estados Unidos, que se encargó de financiar la infraestructura crítica fundamental del ciberespacio hasta 1994[47]. Para ese año, la administración estatal tomó control de la troncal de la "*web"* y se la entregó al sector privado, y desde entonces es operada y financiada por este sector[48]. Dicho esto, queda claro que el objetivo inicial, y la mentalidad que estaba presente en el desarrollo de las formas fundamentales del ciberespacio, era de carácter público y que con la administración Clinton se privatiza.

¿Qué buscamos proteger? La respuesta más obvia debería situarse en torno a mantener alejadas las amenazas o bien reducidas al mínimo en las tres capas del ciberespacio, estratos que son, en su naturaleza y características, muy diferentes.

La capa física del ciberespacio

La capa física o la infraestructura crítica de la red es quizás una de las primeras y más fundamentales áreas por proteger. Una vulnerabilidad en este nivel podría provocar que los principales servicios básicos (agua, energía, transporte, etc.), que se han digitalizado y desplazado hacia la capa lógica y semántica sean dañados. Esta capa es gobernada, en su gran mayoría, por empresas privadas.

Esta circunstancia instala a la capa física como un bien excluible, ya que cobra dinero por la conexión[49]. Entonces, preliminarmente, constituye un bien global club, es decir, un usuario de los servicios de internet paga por el acceso al "club del ciberespacio", y una vez adentro, está facultado para hacer uso y consumir toda la información disponible. Si aplicamos las preguntas de Baldwin y Engerer en la capa física sobre esta materia, ¿qué podremos responder?

(1) ¿Quién es responsable de la seguridad, el Estado o el mercado?

En el caso de la capa física, existen numerosos propietarios y dueños de las diferentes partes. Los consumidores, individuos y ciudadanos, son propietarios de los dispositivos en donde almacenan y acceden a la información disponible en la red. En este caso, la exigencia

[44] Ibíd.

[45] LEE, T.B. The Internet, explained. VOX, 14 de mayo 2015. [En línea] Disponible en:<https://www.vox.com/2014/6/16/18076282/the-internet>

[46] HISTORY.COM EDITORS. The Invention of the Internet. History.com, 21 de agosto de 2018. [En línea] Disponible en:<https://www.history.com/topics/inventions/invention-of-the-internet>

[47] LEE. Loc. Cit.

[48] Ibíd.

[49] ŽÁKOVÁ. Loc. Cit.

de responsabilizar a los clientes sobre las fallas en la seguridad de sus dispositivos es altamente complejo, principalmente porque estos aparatos se utilizan sin la educación y capacidad técnica necesaria para que los usuarios se hagan cargo de la seguridad de sus teléfonos y computadoras. Políticas públicas destinadas a esta área específica del ciberespacio deberían constituir un marco de la educación informática, proceso y entrega de resultados que son de largo plazo.

Por otro lado, las empresas de telecomunicaciones, y en algunos casos el Estado dependiendo de cada país, son propietarios de la red troncal que conecta los ordenadores. A pesar de que el objeto que se busca proteger es privado, componen la columna vertebral del sistema, condición necesaria para que exista el ciberespacio.

"La protección de la información ha dominado la discusión pública, pero es necesario otorgarle especial atención a la infraestructura física del ciberespacio. "

Debido al Internet de las Cosas (IoT) y la creciente tendencia global de digitalizar y automatizar las infraestructuras críticas de servicios, surge la necesidad de otorgarle mayor responsabilidad al Estado en su rol de regulador y proveedor de seguridad. Dicho esto, las reglas de mercado han funcionado relativamente bien, al menos en Chile, en proteger la red troncal del ciberespacio. Sin embargo, no está libre de la necesidad de que el Estado aplique más y mejores exigencias e incentivos para hacer más resiliente el sistema, como por ejemplo la instalación de diversos cables submarinos que se enlacen con diversos puertos de conexión mundial.

El Estado, sin embargo, pierde control cuando los cables submarinos entran en aguas internacionales. En ese caso, rige la Convención de las Naciones Unidas sobre el Derecho del Mar (CDM, CONVEMAR, CNUDM, o UNCLOS, por sus siglas en inglés), que por su parte tiene "importantes vacíos en relación a recopilación de inteligencia en áreas marítimas"[50], es decir, sería posible, aunque altamente complejo, interceptar estas redes en aguas internacionales. Edward Snowden desclasificó información en relación a este escenario, corroborando que tanto los Estados Unidos como el Reino Unido habían interceptado algunos cables[51]. La protección de la información ha dominado la discusión pública, pero es necesario otorgarle especial atención a la infraestructura física del ciberespacio.

De acuerdo al análisis del derecho internacional de Tara Davenport de la Escuela de Derecho de la Universidad de Yale, "los cables submarinos son vulnerables a dos desafíos: interferencia intencional con los sistemas de cableado submarino por Estados y/o actores no estatales, así como herramientas de recopilación de inteligencia"[52].

De acuerdo a su investigación, "el actual sistema legal es deficiente en asegurar la protección de los cables", a pesar que para "la UNCLOS, las leyes de guerra y convenciones de terrorismo son capaces de atender algunos aspectos de la protección de las redes, pero seguramente infraestructura comunicacional crítica como dichos cables merecen un régimen legal más exhaustivo y holístico"[53]. En este caso es necesario que los Estados y no el mercado asuman la responsabilidad de esta parte de la capa física debido a la falta de soberanía

[50] DAVENPORT, T. Submarine Cables, Cybersecurity and International Law: An intersectional Analysis. Catholic University Journal of Law & Technology, Vol. 24, Issue 1, Article 4, 2015. [En línea] Disponible en:<http://scholarship .law.edu/jlt/vol24/iss1/4>

[51] Ibíd.

[52] Ibíd.

[53] Ibíd.

que se cierne en las aguas de alta mar, y de acuerdo normas del derecho internacional, esta medida debería abordarse con noción del multilateralismo. Por otro lado, la infraestructura crítica dentro del territorio soberano debería constituir un objetivo a ser protegido, de allí que sus esfuerzos corresponden a la legislatura y políticas públicas nacionales. Impulsos en esta materia deben ser aplicados lo antes posible, en tanto los costos son menores que las redes de cables submarinos.

(2) ¿Cuál (es) preocupaciones de seguridad deben tratarse públicamente, y cuáles deben de ser organizadas en privado?

En el caso de la infraestructura crítica del ciberespacio es necesario que las preocupaciones, y por ende las estrategias de seguridad, deban tratarse en privado con incentivos y regulaciones públicas para reducir las externalidades de malas prácticas de seguridad, ya sea por los usuarios individuales o bien colectivamente, como por las empresas dueñas de los terminales y cableados que componen esta capa. El Estado debería exigir estándares de seguridad mínimos, así como exige pautas meticulosas de calidad a otras infraestructuras fundamentales para la sociedad. Para esto, Chile debería generar una ley que aborde infraestructuras críticas con sentido de protección, con énfasis sobre el proceso de digitalización y por ende de la red troncal cibernética.

Así las cosas, es posible determinar que, desde la dimensión de ciberseguridad, en esta capa, se observa a la provisión de seguridad como bien un privado; sin embargo, tomando en consideración lo anteriormente señalado sería necesario determinarlo como un bien público, sobre todo si consideramos al estrato físico como una especie de "meta" en la infraestructura crítica, donde las tradicionales dependen finalmente de ésta.

A pesar de que Internet funciona como bien club, conforme al cobro de una tarifa, en términos generales, este grupo es demasiado amplio, masivo y profundamente sustancial para el desarrollo estructural del país, por ende, debe ser tratado como bien público, pero asignando un balance de responsabilidades entre los privados que lo administran y generan utilidades, y el espacio público que requiere y necesita profundamente de este bien.

"El Estado debería exigir estándares de seguridad mínimos, así como exige pautas meticulosas de calidad a otras infraestructuras fundamentales para la sociedad."

b) ¿Qué valores deben ser protegidos? ¿Cuáles de manera privada y cuáles de manera pública?

Los valores que deben ser protegidos son principalmente los de resiliencia y privacidad de las comunicaciones. La idea es evitar la posibilidad de espionaje estatal, tal como han sido acusados los gobiernos de Estados Unidos y Reino Unido, administraciones que habrían actuado sobre la parte de la capa física que corresponde al cableado submarino.

Es necesario tener en consideración que tanto "amigos" como "enemigos" de un Estado podrían llevar a cabo este tipo de intromisiones. Cuando hablamos del cableado submarino se requiere de acuerdos internacionales ya que sería importante abrir el debate acerca del espionaje y la supervigilancia en tiempos de

paz, algo que poco se ha discutido en el ámbito del derecho internacional[54]. Sin embargo, como estrategia política, se puede deducir que una falta de normas del derecho internacional en esta materia sería una maniobra para evitar una pérdida de capacidad para los Estados de acceder a información.

Independientemente de eso, resulta importante entonces que los esfuerzos se destinen a generar mayor resiliencia de las comunicaciones, es decir, invertir en diversificar cables submarinos para distribuir la difusión de información, y con eso, reducir la dependencia de un solo sistema. La resiliencia en este caso, traducida en una diversificación del sistema de salida del territorio chileno, requeriría de esfuerzos conjuntos entre lo público y lo privado, principalmente porque los tipos de actores invirtiendo en el tendido de redes submarinas ha ido aumentando y cambiando.

Empresas como Google, Facebook, Microsoft y Amazon se han incorporado a la lista de inversionistas proveedores y propietarias del cableado submarino, desplazando a las que se dedicaban exclusivamente a participar del mercado de la red troncal[55]. En otras palabras, aquellos actores que no participaban en el rol de agentes económicos en esta capa, como aquellos creadores de contenido en el ciberespacio, luego del incremento de la demanda han comenzado a invertir en la red troncal de Internet. Aun cuando en Latinoamérica esta tendencia no está tan fuertemente desarrollada, la región lidera en el monto de inversiones en cableado submarino entre 2015 y 2020[56]. Para regular y proteger se requiere contar con una política definida y clara que contenga medidas y estándares de seguridad y privacidad de las comunicaciones que el Estado de Chile debiese aplicar a los nuevos actores, principalmente para evitar la concentración de la propiedad sobre la infraestructura crítica[57].

Un aspecto polémico se posesiona en esta materia y su origen se encuentra determinado cuando el valor a proteger es la privacidad. Esta fricción ocurre entre la variable privacidad y control, especialmente cuando la discusión se centra en el cibercrimen. Es necesario entonces determinar equilibrios entre mecanismos de control destinados a combatir el delito cibernético sin caer en un exceso de vigilancia, generando institucionalidad de control transparente y con especial respeto a dicha privacidad. Esta aclaración ya se encuentra incorporada en la Política Nacional de Ciberseguridad[58].

La seguridad de la infraestructura crítica o capa física del ciberespacio, entonces, requiere de acciones conjuntas entre el sector privado, propietario mayoritario de la red troncal interna y externa del país, y el público mediante la aplicación de políticas públicas para generar un balance entre seguridad, privacidad, y resiliencia. Así las cosas, el sector privado que provee servicios, se aplican las reglas del mercado, pero el Estado debe implementar incentivos para que la práctica y lucro de la capa física no genere externalidades que vulneren la seguridad, calidad, distribución del servicio, y potenciales abusos del uso de datos personales. Por otro lado, frente a los usuarios que son

[54] DAVENPORT. Loc. Cit.

[55] TELEGEOGRAPHY. Submarine Cable Map 2019. [En línea] Disponible en:<https://submarine-cable-map-2019.telegeography.com/>

[56] Ibíd.

[57] Nota del Autor: Las investigaciones realizada por el programa de Netflix, Patriot Act with Hasan Minhaj, señalan diferentes problemáticas con la concentración de propiedad, y por ende de poder, que empresas como Amazon tienen sobre el ciberespacio.

[58] GOBIERNO DE CHILE. Política Nacional de Ciberseguridad 2017-2022. Comité Interministerial sobre Ciberseguridad. [En línea] Disponible en:<https://www.ciberseguridad.gob.cl/media/2018/06/PNCS_Chile_ES_FEA.pdf>

propietarios de sus dispositivos electrónicos por donde acceden al ciberespacio, es necesario generar lineamientos de derechos y obligaciones, como también una forma de educación cívica cibernética, para generar consciencia sobre prácticas que afectan los valores y la seguridad de la capa física, aun cuando están relacionadas con actitudes que afectan otras capas del ciberespacio.

En síntesis, la capa física actúa como un bien club, pero dada su creciente importancia y exponencial dependencia en el uso del ciberespacio para las otras infraestructuras críticas, el Estado debería adoptar medidas para atender la generación de las externalidades señaladas.

“Así las cosas, el sector privado que provee servicios, se aplican las reglas del mercado, pero el Estado debe implementar incentivos para que la práctica y lucro de la capa física no genere externalidades que vulneren la seguridad, calidad, distribución del servicio, y potenciales abusos del uso de datos personales.”

La capa lógica del ciberespacio

Es aquella que corresponde en su aspecto más amplio desde los protocolos principales para la comunicación hasta complejos programas computacionales. Se puede decir que al menos el sistema de dirección IP opera globalmente y es gobernado por ICANN, que funciona como una organización de múltiples “stakeholders”, y otros softwares como los navegadores que son proporcionados sin costos. Se puede entender entonces como bienes públicos globales, aun cuando no son entregados por el Estado[59].

En 1998, el Departamento de Justicia de los Estados Unidos demandó a Microsoft por cargos de monopolio porque sus ordenadores venían con un navegador predeterminado gratuito, “Internet Explorer”, afectando las posibilidades de competencia en el mercado de otro navegador “Netscape”. Un caso similar fue que el año pasado cuando el Comité Europeo realizó una demanda contra Google por los mismos cargos de acciones monopólicas[60].

La capa física es, en consecuencia, un bien público global al considerarse no rival y no excluible[61], pero al ser propiedad de actores privados, empresas de telecomunicaciones principalmente, es necesario que el Estado también aplique control sobre ellas, especialmente frente a prácticas que incentiven concentración del mercado y también frente a bajos niveles de seguridad en la administración de los datos (la capa semántica).

Por otra parte, bancos, hospitales, departamentos gubernamentales, y otras instituciones que proveen servicios básicos, son titulares administradores y/o almacenadores de enormes bases de datos que son sensibles y pertenecen a dicha capa semántica. En muchos casos no existen los suficientes incentivos para proteger dicha información, al menos que ocurran casos como el ciberataque que fue objeto el Banco de Chile el año 2018, instancia que exhortó a las autoridades a generar conciencia en favor de normas de ciberseguridad, sin embargo tienden a ser esfuerzos reactivos y no proactivos.

[59] ŽÁKOVÁ. Loc. Cit.

[60] BRANDOM, R. Google’s European fine is a flashback to Microsoft’s ugly antitrust battle. Editorial, The Verge, 18 de julio 2018. [En línea] Disponible en:<https://www.theverge.com/2018/7/18/17587620/google-european-commission-billion-fine-microsoft-antitrust>

[61] ŽÁKOVÁ. Loc. Cit.

(1) ¿Quién es responsable de la seguridad, el Estado o el mercado?

Al ser una capa que es principalmente propiedad de privados o instituciones no gubernamentales, la responsabilidad se asume desde el mercado. Sin embargo, las empresas propietarias de aplicaciones y plataformas donde se almacena, despliega y distribuye la información, se han visto envueltas en polémicas frente a la falta de protección de datos personales, por venta y abuso de dichos datos, por lo que organismos gubernamentales como la Comisión Europea han tenido que interferir para limitar dichos abusos y falta de protocolos en ciberseguridad[63].

Mientras las empresas sean los propietarios mayoritarios de la capa semántica y proporcionen servicios sin cobros por el uso de sus plataformas, el Estado debería en esta instancia generar marcos legales para que los proveedores no hagan abuso de los datos que recopilan de los usuarios, así como incentivar en medidas de protección de los mismos.

Casos de ciberataques como el sufrido por el Banco de Chile el año 2018[62] demuestran la necesidad que el Estado asuma un rol con mayor responsabilidad y en esta condición exigir estándares mínimos, así como distinción de obligaciones a los diversos actores. Como estamos hablando que esta capa se define como un bien público global, es responsabilidad entonces del Estado atender las externalidades insatisfechas por los privados que se producen en la cobertura y entrega de bienes públicos globales.

(2) ¿Cuáles preocupaciones de seguridad deben tratarse públicamente, y cuáles deben de ser organizadas en privado?

En la capa lógica, es necesario comprender que la ciberseguridad debe tratarse en privado con cumplimiento de estándares mínimos (que deben estar de acuerdo a las amenazas exigentes y posibles), que son determinados desde la esfera pública. Una analogía podría darse por las exigencias que el Estado de Chile impone al mercado automotriz al hacer obligatorio el uso de cinturón de seguridad. Sin este sistema de seguridad, los vehículos no pueden obtener permiso de circulación. Igualmente podría aplicarse esta lógica a dicha capa. El Estado entonces debe de exigir estándares mínimos de ciberseguridad a las empresas que operan en la gama lógica, para evitar abusos.

(A) ¿Qué valores deben ser protegidos? ¿Cuáles de manera privada y cuáles de manera pública?

Entre los valores que deben ser protegidos se encuentran los datos personales sensibles, como fichas médicas o actividad financiera. Los administradores de estos datos, sean instituciones públicas o privadas, deben considerar como responsabilidad prioritaria la protección de la información que poseen frente a actos de terceros. Por otro lado, el mal uso de dicha información afecta la libre competencia, cuestión que debiese ser evitado.

En este sentido, la libre competencia constituye un valor que tiene que ser protegido por las empresas e instituciones que participan del mercado en esta capa. Esto se sintetiza entonces en la necesidad de generar un marco regulatorio que proteja y defienda estos dos valores.

Si consideramos la creciente tendencia de empresas que operan en esta capa, es decir empresas con poder de manejo de contenidos como Google, Facebook o Amazon, por invertir

[62] CASAS, L. Robaron US$10 millones en ataque informático al Banco de Chile: virus fue un distractor. Biobiochile.cl, Nacional, 9 de junio 2018. [En línea] Disponible en:<https://www.biobiochile.cl/noticias/nacional/chile/2018/06/09/robaron-us10-millones-en-ataque-informatico-al-banco-de-chile-virus-fue-un-distractor.shtml>

[63] BRANDOM. Loc. Cit.

en este estrato, prontamente adquirirán un poder que harán valer en el ámbito de las relaciones internacionales, ante ello esfuerzos unilaterales y multilaterales son necesarios para que estos actores no estatales sean, al menos, regulados en su actuar.

Hoy las empresas de telecomunicaciones representan una categoría de industria transnacional poseedoras de grandes cuotas de poder en diferentes ámbitos internacionales, por ello el propender limitaciones en favor de la ciberseguridad y la protección de la información de los usuarios constituye un ambicioso y necesario objetivo. Casos como los de Google Analytica demuestran la capacidad que tienen estas empresas en este nivel para interferir e incluso afectar la institucionalidad democrática, como habría sido el caso de las elecciones de Estados Unidos[64], principalmente por el dominio que poseen como almacenadoras y/o distribuidoras de información de individuos.

Es responsabilidad de los Estados, entonces, nuevamente regular y disminuir las externalidades que se generan cuando entendemos que esta capa del ciberespacio obedece a criterios de bien público global con acceso y uso gratuito.

Es necesario aclara que muchos "*software*" y aplicaciones que almacenan, ordenan, distribuyen y procesan la información generada por otros no siempre responden a un carácter gratuito, ejemplo de este tipo de plataformas es Netflix. Sin embargo, en casos como el señalado, igualmente se deben aplicar los estándares y exigencias por abuso de datos.

En muchos procesos la separación entre la capa lógica y semántica tiende a difuminarse. Algunas plataformas y empresas pueden participar tanto como generadoras de contenido (capa semántica), administradores y distribuidoras de contenido (capa lógica) y también como propietarios de parte de la red troncal del ciberespacio (capa física), las consecuencias pueden ser múltiples y sus efectos extremadamente sensibles sobre los protocolos de seguridad que se utilizan en las demás capas.

"... empresas con poder de manejo de contenidos como Google, Facebook o Amazon, por invertir en este estrato, prontamente adquirirán un poder que harán valer en el ámbito de las relaciones internacionales, ante ello esfuerzos unilaterales y multilaterales son necesarios para que estos actores no estatales sean, al menos, regulados en su actuar. "

La capa semántica del ciberespacio

Finalmente, nos encontramos con la capa semántica que hace referencia al contenido, en síntesis, a la información que todos los actores generan, almacenan y/o comparten. En otras palabras, el "commodity" que le da la razón de ser, y por ende utilidad e importancia al ciberespacio. La información en gran medida es un bien público global, en tanto es naturalmente no rival, el consumo de una información no reduce su disponibilidad para otros, pero dependiendo de su alcance puede ser excluible. Si no fuera este el caso el ciberespionaje no sería una realidad. Por tanto, se crean dos espacios donde existe información pública, entendida como un bien público global, y otro donde se comparte información privada, entendida como un bien club global. Para

[64] BBC MUNDO. 5 claves para entender el escándalo de Cambridge Analytica que hizo que Facebook perdiera US$37.000 millones en un día. BBC MUNDO, 21 de marzo de 2018. [En línea] Disponible en:<https://www.bbc.com/mundo/noticias-43472797>

estos dos casos se aplican entonces diferentes respuestas a las preguntas de Balwdin y a la de Engerer.

(1) ¿Quién es responsable de la seguridad, el Estado o el mercado?

Cuando la información es pública, el mercado y los privados son responsables de la seguridad de dicha información, principalmente las empresas que la difunden, porque los individuos poseen capacidad limitada para asimilar la veracidad de la información que se publica. En términos concretos, es incumbencia de quién publica, sea un individuo o varios, responder por la autenticidad de lo trasmitido. Por ejemplo, no debería ser responsabilidad de Facebook que una información publicada en su plataforma sea falsa, sino más bien quién la publicó, sobre todo si aceptamos estas plataformas bajo la analogía que hace Hasan Minhaj, en su programa Patriot Act, al explicar la afectación a la neutralidad de la red[65].

¿Quién es responsable de la información que se publica en Internet? El usuario y no la plataforma que la hospeda. Aquí se genera un debate importante, si se percibe a plataformas de intercambio de información como aquellas vinculadas a redes sociales de forma similar a medios de comunicación tradicionales, a sabiendas que estos últimos son responsables de lo que publican y difunden, entonces son igualmente responsables de la información que administra su plataforma. Esta definición es importante a la hora de generar normas para proteger esta capa del ciberespacio.

Con todo, es responsabilidad de los Estados generar marcos que protejan los derechos fundamentales de libertad de expresión en Internet. Cuando hablamos de información pública, la neutralidad de la red está en línea con dicha protección y, por tanto, debe generarse un marco regulatorio para resguardar dicha neutralidad, además de la custodia de la integridad y/o modificación no autorizada de los contenidos publicados.

Esta misma protección debe de aplicarse para la información que no es pública, es decir la protección a la integridad del contenido, independientemente de si es una comunicación abierta o cerrada. Que un correo enviado por servicio como “Gmail” o una publicación abierta en “Instagram” sea modificado por un tercero, es responsabilidad de las políticas de seguridad de los proveedores, es decir “Google y Facebook”, respectivamente, dueños de las plataformas señaladas; sin embargo, la veracidad o la legalidad que podría subyacer en el contenido mismo (noticias falsas o difamación), es responsabilidad de quien difundió esa información en dichas plataformas.

Cuando hablamos de información pública, es importante proteger a los individuos frente a las empresas editoras, para que los derechos de expresión de las personas no se vean afectados, evitando que se generen conductas que restrinjan la libre competencia entre los actores formuladores de contenidos.

(2) ¿Cuáles preocupaciones de seguridad deben tratarse públicamente, y cuáles deben ser organizadas en privado?

Cada persona con acceso a internet posee la capacidad de generar contenido, ya sea de manera individual o colectiva. En estos casos, necesariamente constituye una preocupación de seguridad que debe tratarse públicamente, y no de manera privada. Es una necesidad urgente y global generar políticas de seguridad,

[65] Nota del Autor: Hasan Minhaj es conductor del programa de Netflix, “Patriot Act with Hasan Minhaj”, que realiza, como ya se mencionó, varias investigaciones periodísticas y análisis sobre abusos de poder a nivel mundial, y concretamente la investigación en el capítulo “Content Moderation and Free Speech” desplegó el caso de violación de la neutralidad de la red, que quiere decir que las empresas e instituciones proveedoras de servicios de Internet no pueden generar incentivos, como velocidad de descarga, en favor de un tipo de contenido en desmedro de otro.

así como regular contenidos para que cumplan con estándares globales mínimos, evitando que cada plataforma determine, unilateralmente, los términos y condiciones de protección que le otorgará a la información. Obviamente aquí nos encontramos con aquellos regímenes políticos en que la protección del derecho de expresión no es protegida ni defendida, instalándose en este pináculo China.

La condición descrita presenta un desafío mayor que difícilmente se podrá resolver con gobernanza e institucionalidad internacional. Sin embargo, es necesario que un gran número de actores, a pesar de estas dificultades, generen protocolos de regulación sobre el uso de plataformas, igualmente se establezcan responsabilidades sobre los consumidores por el contenido publicado, evitando casos como la pornografía infantil, entre otros.

(A) ¿Qué valores deben ser protegidos? ¿Cuáles de manera privada y cuáles de manera pública? Los valores del derecho de expresión y neutralidad de la red son los que deben ser protegidos, además de los otros derechos que poseen las personas fuera del ciberespacio. El primero para limitar el poder del Estado frente a las libertades de expresión de sus ciudadanos, y la neutralidad de la red para frenar la capacidad de manipulación y control que pueden hacer las empresas privadas o plataformas frente a estas mismas libertades. Ambas de manera pública. Por otro lado, el individuo debe estar protegido por la acción de sus pares, precaviéndole de ser víctima de crímenes cibernéticos o de suplantación de identidad, atraerlo hacia plataformas de tráfico de pornografía infantil, etc. Estos casos son ejemplos esenciales para otorgar gobernanza de la ciberseguridad en la capa semántica.

Conclusión

Definir la ciberseguridad como un bien público global en términos generales es altamente simplista. Las distintas capas del ciberespacio son considerablemente diferentes por naturaleza como para ser tratadas de manera independiente. Los actores, por otro lado, poseen disímiles intereses y formas de enfrentar a las amenazas que puedan existir en la red global.

Sin duda que el Estado debe velar por la integridad de numerosas infraestructuras críticas y otorgar la respectiva seguridad, como también proteger a sus ciudadanos frente actitudes que amenacen sus libertades y derechos. Las empresas, por su parte, deben velar por la integridad de sus servicios que entregan.

Considerando que los atributos de la red global son inherentes a bienes globales, y que no son privados, requieren de protocolos y formalidades que la regulen; a su vez, se deben establecer restricciones para que el Estado no manipule a los individuos. Los consumidores, por otro lado, también deben ser sujetos de regulación, así como objeto de sanción, en caso de acciones delictuales, manteniendo el grado de protección a su privacidad y garantías fundamentales.

El Estado, entonces, debe destinar esfuerzos importantes para reducir las externalidades que se generan en la dimensión del ciberespacio, lugar de intercambio de información que es sustentado por empresas privadas, aun cuando ciertas capas del ciberespacio se comporten como bien público global o bien club global.

Bibliografía

BBC MUNDO. 5 claves para entender el escándalo de Cambridge Analytica que hizo que Facebook perdiera US$37.000 millones en un día. BBC MUNDO, 21 de marzo de 2018. [En línea] Disponible en:<https://www.bbc.com/mundo/noticias-43472797>

BLOOMBERG NEWS. Analysis: The Great Firewall of China. BloombergQuickTake, The Washington Post, 5 de noviembre de 2018. [En línea] Disponible en:<https://www.washingtonpost.com/business/the-great-firewall-of-china/2018/11/05/5dc0f85a-e16d-11e8-ba30-a7ded04d8fac_story.html?utm_term=.0353f687dc8e>

BRANDOM, R. Google's European fine is a flashback to Microsoft's ugly antitrust battle. Editorial, The Verge, 18 de julio 2018. [En línea] Disponible en:<https://www.theverge.com/2018/7/18/17587620/google-european-commission-billion-fine-microsoft-antitrust>

BURGESS, M. What is the Internet of Things? WIRED explains. WIRED, 16 febrero de 2018. [En línea] Disponible en:<https://www.wired.co.uk/article/internet-of-things-what-is-explained-iot>

CASAS, L. Robaron US$10 millones en ataque informático al Banco de Chile: virus fue un distractor. Biobiochile.cl, Nacional, 9 de junio 2018. [En línea] Disponible en:<https://www.biobiochile.cl/noticias/nacional/chile/2018/06/09/robaron-us10-millones-en-ataque-informatico-al-banco-de-chile-virus-fue-un-distractor.shtml>

DAVENPORT, T. Submarine Cables, Cybersecurity and International Law: An intersectional Analysis. Catholic University Journal of Law & Technology, Vol. 24, Issue 1, Article 4, 2015. [En línea] Disponible en:<http://scholarship .law.edu/jlt/vol24/iss1/4>

ENGERER, H. Security as a Public, Private or Club Good: Some fundamental Considerations. German Institute for Economic Research, Defence and Peace Economics, Vol. 22(2), Abril 2011.

GOBIERNO DE CHILE. Política Nacional de Ciberseguridad 2017-2022. Comité Interministerial sobre Ciberseguridad. [En línea] Disponible en:<https://www.ciberseguridad.gob.cl/media/2018/06/PNCS_Chile_ES_FEA.pdf>

HANSEL, M. Cyber Security Governance and the Theory of Public Goods. E-International Relations (E-IR), 2013. [En línea]. Disponible en:<https://www.e-ir.info/2013/06/27/cyber-security-governance-and-the-theory-of-public-goods/>

HAY NEWMAN, L. Hacker Lexicon: What Is The Attribution Problem?. Security, WIRED, 24 de diciembre 2016. [En línea] Disponible en:<https://www.wired.com/2016/12/hacker-lexicon-attribution-problem/>

HISTORY.COM EDITORS. The Invention of the Internet. History.com, 21 de agosto de 2018. [En línea] Disponible en:<https://www.history.com/topics/inventions/invention-of-the-internet>

INTERNET WORLD STATS. World Internet Usage And Population Statistics March, 2019 - Updated [En línea]. [Fecha de consulta: 15 de mayo 2019] Disponible en:<https://www.internetworldstats.com/stats.htm>

KIRSHNER, J. Realist political economy. Routledge Handbook of International Political Economy (ed. Mark Blyth). Abingdon: Routledge, 2009. [En línea] Disponible en:<https://www.routledgehandbooks.com/doi/10.4324/9780203881569.ch2>

LEE, T.B. The Internet, explained. VOX, 14 de mayo 2015. [En línea] Disponible en:<https://www.vox.com/2014/6/16/18076282/the-internet>

TABANSKY, L. Critical Infrastructure Protection against Cyber Threats. Military and Strategic Affairs, Vol. 3, No. 2, November 2011.[En línea] Disponible en:<https://i-hls.com/wp-content/uploads/2013/03/Critical-Infrastructure-Protection-against-Cyber-Threats-Lior.pdf>

TELEGEOGRAPHY. Submarine Cable Map 2019. [En línea] Disponible en:<https://submarine-cable-map-2019.telegeography.com/>

ŽÁKOVÁ, G. Cyberspace: Global Public Goods?. Acta Oeconomica Pragensia, 2018, 26(2), 68-82 [En línea] Disponible en:<https://doi.org/10.18267/j.aop.602>

DIRECCIÓN DEL CUADERNO

DIRECTOR

CONSEJO EDITORIAL


CENTRO DE INVESTIGACIONES Y ESTUDIOS ESTRATÉGICOS
ANEPE.CL