Regulación de la ciberseguridad en el sector de telecomunicaciones de Brasil: un balance de incentivos en un contexto de neutralidad tecnológica

Revista Latinoamericana de Economía y Sociedad Digital

Issue 2, agosto 2021

Autores: Ronaldo Neves de Moura Filho, Luciano Charlita de Freitas, Egon Cervieri Guterres, Leonardo Euler de Morais, Mariana Almeida de Sousa Talouki

DOI: 10.53857/KMFK7888

Publicado: 25 agosto, 2021

Recibido: 21 marzo, 2021

Cita sugerida: De Moura Filho, Ronaldo Neves; Charlita de Freitas, Luciano; Cervieri Guterres, Egon; Euler de Morais, Leonardo & Almeida de Sousa Talouki, Mariana (2021) "Regulación de la ciberseguridad en el sector de telecomunicaciones de Brasil: un balance de incentivos en un contexto de neutralidad tecnológica", en Revista Latinoamericana de Economía y Sociedad Digital, Issue 2

Tipo: Estado del arte

Palabras clave: Brasil, Ciberseguridad, Reglamentación, Regulación, Telecomunicaciones

---

Resumen

El artículo explora la justificación que apoyó la redacción de la normativa de ciberseguridad en el sector de las telecomunicaciones brasileño, y que tendrá un impacto directo en su implementación. El trabajo parte de un repaso sobre la evolución de la temática y el contexto actual en el que el regulador nacional actuó para producir su intervención normativa, a partir de la postura técnica frente al escenario geopolítico y el reconocimiento de la transformación tecnológica en curso. Los pilares de la normativa se analizan desde la perspectiva de la gestión de riesgos, la asimetría regulatoria y la construcción de un nuevo modelo de gobernanza multilateral y progresiva. Las consideraciones pretenden ir más allá de un enfoque puramente descriptivo, y buscar identificar los puntos de atención que

estarán presentes en la implementación de la regulación en los próximos años.

Abstract

The paper explores the justification that supported the writing of the cybersecurity regulations in the area of Brazilian telecommunications and will have a direct impact in its implementation. It starts reviewing the evolution of the subject and the current context in which the national regulatory authority helped to produce its regulatory intervention, from a technical point of view and facing a geopolitical scenario and acknowledging the current technological transformation. The foundations of the regulations are analyzed from the perspective of the risk management, regulatory asymmetry and the construction of a new model of multilateral and progressive governance. The considerations pretend to go beyond a descriptive approach and look for the identification of the focal points that will be present in the implementation of the regulation in the following years.

Resumo

Este artigo explora o racional que subsidiou a elaboração da regulamentação sobre cibersegurança no setor de telecomunicações brasileiro, e que terá reflexos diretos em sua implementação. O trabalho parte de um apanhado sobre a evolução do tema e do atual contexto no qual o regulador nacional atuou para produzir sua intervenção normativa, pautando-se na postura técnica a respeito do cenário geopolítico e no reconhecimento da transformação tecnológica em curso. São analisados os pilares do regulamento sob as perspectivas de gestão de riscos, de assimetria regulatória e de construção de um novo modelo de governança multilateral e progressiva. Tais ponderações pretendem ir além de uma abordagem meramente descritiva, e buscam identificar os pontos de atenção que estarão presentes na implementação da regulamentação nos próximos anos.

1. Introducción

Las telecomunicaciones son de esencial importancia para la integralidad del sistema de infraestructuras críticas y el ciberespacio brasileño. Por un lado, el sector opera como un agente autónomo en el marco de las infraestructuras de comunicación y, por el otro, es un elemento integrador de otras infraestructuras nacionales esenciales, de carácter intra e intersectorial.

En las últimas décadas, el sector ha sido progresivamente utilizado para perpetrar actividades maliciosas que causan o tienen el potencial de causar daños a los usuarios y derechos propios de este entorno, con dimensiones políticas, económicas y militares (INÁCIO, 2016). Con la inminente llegada de una nueva generación tecnológica (5G), que

permitirá cambios de paradigma en la conectividad de las personas y las actividades productivas, las amenazas se amplifican. Después de todo, mayores superficies de redes asociadas a una mayor dependencia de la conectividad naturalmente aumentan los riesgos y efectos de posibles fallas y ataques (AHMAD et al, 2018). Esto representa una renovación del debate sobre la seguridad.

Es en ese contexto en el que se inserta el presente estudio. El objetivo es dar a conocer el razonamiento en el que se basa el recientemente publicado Reglamento de Seguridad Cibernética (R-Ciber) en el marco de las telecomunicaciones brasileñas. En este sentido, se parte de un historial del contexto normativo brasileño con relación a la ciberseguridad y una revisión de las definiciones y bases principiológicas que apoyaron la búsqueda de un equilibrio eficiente en la promoción de la integridad de la infraestructura crítica del Estado brasileño, los intereses de mercado y la preservación de los derechos fundamentales de los ciudadanos.

El estudio también presenta elementos económicos y de conducta subyacentes a la comprensión de los incentivos, las asimetrías y las externalidades que justifican la intervención regulatoria sobre el tema. Dichos fundamentos orientaron la opción del regulador por una vertiente técnica neutral, con la atribución de responsabilidades y la adopción de instrumentos flexibles para promover la transparencia, con énfasis en aquellos orientados a la divulgación de información y una gobernanza multilateral.

El informe se encarga, finalmente, de documentar los aspectos subyacentes al diseño de la normativa en Brasil y, de esa manera, no solo crear una referencia histórica sobre el desarrollo del tema y una presentación de su situación actual, sino también poner en evidencia los principales debates que su aplicación sin duda provocará en los próximos años.

Además de esta introducción, el artículo se divide en tres partes. La siguiente sección brinda una descripción detallada acerca de la evolución de las normativas relacionadas con la ciberseguridad en Brasil, y cómo se enmarca en ese contexto el Reglamento de Seguridad Cibernética aplicada al Sector de Telecomunicaciones.

Luego, se hacen consideraciones sobre el debate actual acerca de la ciberseguridad a la luz de las modernas tecnologías de telecomunicaciones. Se confiere un énfasis especial a la contextualización sobre el escenario geopolítico y de transformación tecnológica en curso.

La cuarta sección presenta reflexiones sobre las bases del reglamento desde las perspectivas de la gestión de riesgos, de la asimetría regulatoria y de la construcción de un nuevo modelo de gobernanza multilateral y progresiva. Tales consideraciones tienen como objetivo identificar los puntos de atención que estarán presentes en la implementación de la normativa. Les sigue una breve conclusión.

2. Evolución normativa sobre ciberseguridad en Brasil y renovación del debate

Brasil es escenario común de ataques cibernéticos y la preocupación por abordar el problema no es reciente. El primer reglamento relacionado con la ciberseguridad se remonta a la década de 1980 –Ley n° 7.232/1984 (BRASIL, 1984). Esta ley introdujo la Política Nacional de Informática e incluyó, entre sus principios, el de establecer mecanismos e instrumentos legales y técnicos para la protección de la confidencialidad de los datos, del interés de la privacidad y de la seguridad de las personas físicas y jurídicas, privadas y públicas.

Posteriormente, se publicó la primera Política de Seguridad de la Información, mediante el Decreto n° 3.505/2000 (BRASIL, 2020). Esta norma se centró en la Administración Pública Federal y se destaca su preocupación por la defensa de la soberanía nacional y la protección de derechos fundamentales, como la intimidad y la privacidad.

Después, a través del Decreto nº 4.801/2003 (BRASIL, 2003), se instituyó la Cámara de Relaciones Exteriores, órgano consultivo de la Presidencia de la República, que incluía entre sus objetivos la implementación de programas relacionados con la seguridad de la información y la seguridad cibernética[1].

En 2008, el Gabinete de Seguridad Institucional publicó la Instrucción Normativa nº 1/2008 (BRASIL, 2008), responsable por regular la Gestión de Seguridad de la Información y las Comunicaciones en la Administración Pública Federal. Además de las competencias establecidas en el ámbito de la administración pública, dicho documento trajo una lista de definiciones como la de disponibilidad, integridad, confidencialidad y autenticidad.

Hasta ese punto, es posible constatar que, en el ordenamiento jurídico y normativo brasileño, la ciberseguridad presenta distintas vertientes diferenciadas por su objeto y dependiendo del organismo responsable. En los casos en que el objeto es la protección de las infraestructuras críticas, con miras a garantizar la estabilidad política y económica, así como la protección de la sociedad y de los derechos e intereses de sus individuos, es el Gabinete de Seguridad Institucional el organismo a cargo. Como manifestación de ello, está la publicación por parte de la Presidencia de la República, en 2010, del Libro Verde sobre Seguridad Cibernética en Brasil (BRASIL, 2010).

En las situaciones en las que el objeto de la ciberseguridad es un bien de propiedad del Estado, con protagonismo de las infraestructuras críticas y con miras a la defensa y la soberanía nacional, o en casos de guerra cibernética, la competencia cabe al Ministerio de Defensa y las Fuerzas Armadas de Brasil, especialmente el Ejército brasileño. Como exponente de esta atribución, se encuentra el Libro Blanco de la Defensa Nacional, publicado por el Ministerio de Defensa en 2012 (BRASIL, 2012), que trata aspectos relacionados con las estrategias de guerra en el medio cibernético.

Lo que se puede notar al analizar los antecedentes normativos de la ciberseguridad en Brasil, es una preocupación por proteger bienes y derechos en el ámbito del ciberespacio. Sin embargo, pese a los pronósticos normativos y los avances institucionales, Brasil, a lo largo de estos casi 40 años, ha tenido un continuo aumento de la vulnerabilidad de sus redes de telecomunicaciones.

Prueba de ello es la alta incidencia de ciberataques en el país (UIT, 2018). Actualmente, Brasil ocupa la 70ª posición en el ranking *Global Cybersecurity Index*, indicador que mide el nivel de preparación de los países para enfrentar ataques cibernéticos (UIT, 2018).

La actual renovación del debate se debe en parte a un impulso relacionado con el sector privado ante las amenazas de seguridad. Se suman factores de índole económica y el interés en el uso de tecnologías de punta por parte del gobierno, empresas y particulares, cuyo ejemplo emblemático es el estándar de tecnología 5G (AHMAD et al, 2018).

Algunos aspectos de esta tecnología, en conjunto, contribuyen al recrudecimiento de las vulnerabilidades. Entre ellos, se destaca la transposición del uso de *hardware* a *software*, dificultando así la capacidad de inspección, control e higiene cibernética de los puntos de congestión. También como consecuencia de esa transposición está la virtualización en *software* de las funciones de red que antes eran ejecutadas por dispositivos físicos. Además, aunque es posible bloquear vulnerabilidades de *software* en la red, la misma también se gestiona a través de lo que se ha convenido denominar *AI-based softwares*, que favorecen la vulnerabilidad. Además al factor *software*, cabe destacar la difusión de dispositivos inteligentes, cuyo uso abarca desde aplicaciones domésticas hasta áreas de servicios esenciales, como hospitales, servicios de seguridad pública y transporte.

De hecho, la quinta generación de conectividad móvil de banda ancha se perfila como un catalizador de cambios de paradigma sobre la forma en la que Brasil aborda la ciberseguridad.

En este nuevo contexto se enmarca la promulgación de la más reciente Política Nacional de Seguridad de la Información, a través del Decreto nº 9.637/2018 (BRASIL, 2018), y la Estrategia Nacional de Seguridad Cibernética, publicada a través del Decreto nº 10.222/2020 (BRASIL, 2020). En síntesis, el Decreto nº 10.222/20 presenta la Estrategia Nacional de Ciberseguridad y tiene como metodología el tratamiento de la ciberseguridad a través de un contexto de gobernanza con el fin de armonizar intereses y esfuerzos por parte de la administración pública, empresas privadas, investigadores de esa área del conocimiento y de la sociedad civil. La estrategia también está compuesta por acciones y objetivos que, en conjunto, proponen el perfeccionamiento de la estructura de ciberseguridad con el fin de promover la resiliencia del país frente a las amenazas en el entorno digital, como también su confiabilidad en el escenario internacional.

En cuanto al marco regulatorio relacionado con el refuerzo de la ciberseguridad en paralelo a los preparativos para la implementación del 5G, también pueden mencionarse dos

iniciativas. La primera, del Gabinete de Seguridad Institucional, por medio de la promulgación de la Instrucción Normativa nº 4/2020 (BRASIL, 2020) que establece requisitos mínimos de ciberseguridad para las redes de telecomunicaciones utilizadas por el Gobierno Federal. Dicha instrucción está dirigida a la Administración Pública Federal directa e indirecta y aboga por el cumplimiento de especificaciones técnicas y la diversificación de proveedores, con el fin de mitigar los riesgos derivados de la dependencia excesiva.

Finalmente, es pertinente resaltar la importancia atribuida en el contenido de la estrategia al rol de los entes reguladores en el fomento de la adopción de procedimientos de ciberseguridad por parte de sus regulados. En lo que respecta al sector de las telecomunicaciones, dicha incumbencia se sustenta en la necesidad de participación del ente regulador del sector –la Agencia Nacional de Telecomunicaciones – Anatel– en el tratamiento de la ciberseguridad, de manera directa o transversal, en cooperación con los demás *stakeholders*.

Para los entes regulados del mercado, la Anatel publicó en diciembre de 2020 el Reglamento de Ciberseguridad Aplicada al Sector de Telecomunicaciones (R-Ciber), aprobado mediante la Resolución nº 740/2020 (ANATEL, 2020a). Su génesis radica en la necesidad de cumplir con la Estrategia Nacional de Ciberseguridad y la Agenda Regulatoria de la propia Agencia (ANATEL, 2017). La publicación de este instrumento normativo también refleja la preocupación de la Agencia por promover una Política de Ciberseguridad para los prestadores de servicios de telecomunicaciones, supervisada por el organismo regulador.

Vistos estos antecedentes, es claro que el enfoque normativo e institucional de la ciberseguridad en Brasil ha evolucionado desde un marco amplio asociado a la estrategia de defensa nacional hasta el punto en el que pasa a permear regulaciones sectoriales afines; en este caso, la que se refiere a las infraestructuras y la prestación de servicios de telecomunicaciones por parte de entes privados, objeto de las siguientes secciones.

3. El contexto geopolítico y tecnológico y las premisas de la regulación de la ciberseguridad para las telecomunicaciones

En términos generales, las buenas prácticas en la acción regulatoria recomiendan que se establezca un marco mínimo de intervención, gobernanza y confianza con respecto a la prescripción de comportamientos para el sector de telecomunicaciones y entre este y los demás sectores de la economía (OCDE, 2012).

Cabe al regulador observar los elementos del debate y emitir su posición acerca de ellos, promoviendo soluciones sostenibles y adecuadas a la dinámica de cada tema bajo su

competencia. Esta dimensión analítica abarca una comprensión sobre temas tan diversos como la economía política y la tecnopolítica de influencia, las externalidades de red y la interdependencia en las relaciones de ciberseguridad y el dimensionamiento de la intervención regulatoria a la luz de los principios de eficiencia y resiliencia.

Sobre el primer tema, es necesario reconocer que el contexto en el que se enmarca el R-Ciber engloba un problema de carácter político. En parte, las posiciones divergentes se deben al enfoque multifacético sobre el tema, cuya coordinación se encuentra fragmentada entre los órganos de Estado, de gobierno y entes privados. De esta manera, los países líderes en desarrollo tecnológico se apoyan en perspectivas distintas sobre la naturaleza de los riesgos del ciberespacio para elaborar su estrategia de acción y esfuerzos para la coordinación de políticas nacionales e internacionales (HILLER y RUSSELL, 2013).

También debe tenerse en cuenta que la rivalidad que surgió en el debate sobre la ciberseguridad no se limita a casos específicos. Por el contrario, se da en el contexto de una rivalidad histórica que moldea debates estratégicos de la geopolítica mundial en distintas temáticas (KASKA et al., 2019).

Cuando se transpone a la dimensión tecnológica, la divergencia se potencia por el hecho de que están en juego elementos de largo plazo cuyos términos se basan en la definición de normas técnicas y en las llamadas tecnopolíticas de influencia, subyacentes a los productos y servicios digitales y cuyo uso trasciende los límites de las fronteras territoriales. En ese sentido, cuestiones de desarrollo y uso de tecnologías pasan a convertirse en objeto de debates políticos, por la defensa de valores y, en definitiva, de confirmación de la influencia global o regional.

A pesar de su indudable importancia y efectos sobre el sector, tal dimensión no fue objeto de análisis por parte del regulador brasileño del sector que, en línea con sus prerrogativas legales, se limitó a los aspectos regulatorios relacionados con el tema (ANATEL, 2020a, b).

Con respecto a las externalidades y a la interdependencia en las relaciones de ciberseguridad, cabe señalar que las acciones y omisiones de ciertos agentes pueden tener distintos efectos colaterales sobre los demás. Tal condición se potencia cuando la interoperabilidad es la base para el funcionamiento de todo el sistema. La inseguridad crea externalidades negativas. En ese caso, un punto de la red cuya seguridad se encuentra comprometida puede permitir brechas con amplios efectos sobre las demás redes, servicios y usuarios.

Otra modalidad de externalidad en el caso en cuestión es la llamada seguridad interdependiente (KUNREUTHER y HEAL, 2003). Aquí, las inversiones en seguridad pueden ser complementos estratégicos y operan cuando un individuo en particular que toma medidas de protección crea externalidades positivas para los otros que, a su vez, pueden sentirse desalentados a realizar su propia inversión. Se trata del comportamiento del tipo *free-riding* y se manifiesta al inducir a los agentes a no preocuparse por la inversión en

seguridad ante la expectativa de que otros agentes estén protegiendo sus redes.

El cuadro expuesto requiere un correcto dimensionamiento de la intervención regulatoria. Esto se debe a que las amenazas a la ciberseguridad poseen características técnicas, partes interesadas y restricciones legales distintas. Así, para lograr efectividad, el regulador optó por establecer lineamientos de carácter principiológico, donde se concentren las barreras económicas que inhiben el establecimiento de normas de seguridad y la asignación de inversiones necesarias.

Asimismo, la regulación de la ciberseguridad en el sector de las telecomunicaciones va mucho más allá de la preocupación inmediata por la implementación de las redes 5G, dado su alcance tecnológicamente neutral (ANATEL, 2017; ANATEL, 2020a, b) y no ha adoptado un sesgo de procedimiento y estático de contención de riesgos y fallas. La estructura corresponde a un conjunto de principios y lineamientos objetivos de seguridad en el ciberespacio, respaldado por una combinación de incentivos basados en las reglas competitivas de mercado y en la supervisión regulatoria.

También desde la perspectiva principiológica, es importante mencionar la expresa protección de datos personales de la que se reviste el R-Ciber, resultante de la Ley nº 13.709/2018 (BRASIL, 2018), que centraliza las disposiciones generales en la materia. Al entender que la violación de datos personales puede constituir una afrenta a derechos fundamentales, como la privacidad y la intimidad, es fundamental implementar medidas de ciberseguridad tendientes a evitar riesgos de esa naturaleza. En este sentido, para proteger la privacidad de los usuarios, las empresas de telecomunicaciones deben utilizar herramientas adecuadas para la protección de los datos personales.

Desde la perspectiva del regulado, aunque este mismo también se beneficie del mayor nivel de seguridad del ciberespacio en su conjunto, es necesario considerar las implicaciones económico-financieras sobre la explotación de la actividad empresarial. La adopción de sistemas y mecanismos de protección, preparación y respuesta a incidentes de ciberseguridad conlleva costos. Por tanto, existe una tensión entre eficiencia y resiliencia en la composición de las redes críticas de telecomunicaciones.

En este sentido, la decisión individual de una entidad de reducir sus costos operativos con miras a una mayor eficiencia puede implicar un riesgo de vulnerabilidad sistematizada a largo plazo. En ese marco, los incentivos a corto plazo para reducir costos operativos generan conflicto con los de largo plazo, orientados a promover la resiliencia.

Ese *trade-off* revela el dilema entre seguridad y eficiencia y sirve para evidenciar el nivel óptimo de intervención, medida en la que los beneficios de la operación eficiente superan cualquier reducción en el riesgo resultante de medidas de seguridad adicionales.

4. Reglamento: riesgos, asimetrías y gobernanza

La aplicación de principios, directrices y buenas prácticas es fundamental para una política nacional de ciberseguridad eficaz. En este sentido, el R-Ciber establece una base principiológica que sirve de guía para las conductas y procedimientos que promueven la ciberseguridad en las redes y servicios de telecomunicaciones, a saber: autenticidad, confidencialidad, disponibilidad, diversidad, integridad, interoperabilidad, prioridad, responsabilidad y transparencia (ANATEL, 2020a, b).

Implementar y poner en funcionamiento estos principios y directrices en un entorno tan complejo y dinámico como el ecosistema de las telecomunicaciones requiere enfoques e instrumentos normativos capaces de abordar sus especificidades. Para enfrentar estos desafíos, el regulador ha elegido un conjunto de directivas y enfoques regulatorios en su reglamento técnico (ANATEL, 2017; ANATEL, 2020a, b), que se analizan a continuación.

4.1 Regulación de riesgos en infraestructuras críticas

Parte de la infraestructura crítica de Brasil opera en regímenes autónomos, con la conectividad como elemento común (CARVALHO y SANTOS, 2011). Este estándar revela la esencialidad del sector de las telecomunicaciones como agente autónomo en el ámbito de la infraestructura crítica y como agente integrador de la infraestructura nacional.

Los sistemas y dispositivos de las generaciones tecnológicas más recientes, que se basan principalmente en *softwares*, trajeron nuevos desafíos para la seguridad a nivel cibernético. En otras palabras, las innovaciones tecnológicas terminan por ampliar la superficie general sujeta a ciberataques –constantemente mejorados y en evolución para explotar nuevas vulnerabilidades–, lo cual, en consecuencia, exige reforzar la ciberseguridad (AHMDAD et. al, 2018).

La opción representada por el R-Ciber está orientada a los riesgos percibidos, en un enfoque panóptico y de vigilancia permanente, que contempla un híbrido de normativa de seguridad *ex ante* y la atribución de responsabilidades *ex post*. En la práctica, ese régimen permite, por un lado, establecer requisitos de seguridad a través de la certificación de equipos, concesión de licencias de estaciones y lineamientos de *compliance*, y, por otro lado, la identificación y atribución de responsabilidades de los agentes en la coordinación de las acciones de seguridad de la red.

La normativa de seguridad *ex ante* busca establecer los requisitos mínimos de seguridad, aplicados en la fase de certificación de los equipos, antes de su aprobación para el ingreso al parque tecnológico que conforma la infraestructura sectorial. Se trata de una medida preventiva, neutral en términos tecnológicos, y con las salvaguardas necesarias para cumplir con los requisitos de seguridad.

El Reglamento establece, particularmente, que los prestadores de servicios deben utilizar

productos y equipos de telecomunicaciones de proveedores que tengan una política de ciberseguridad compatible con los principios y lineamientos de ciberseguridad definidos en el reglamento correspondiente. Estos componentes también estarían sujetos al cumplimiento de requisitos de conformidad evaluados en procesos de auditoría independiente periódicos (ANATEL, 2020a).

Dicha directiva presupone acciones preliminares de auditoría técnica independiente y la coordinación con respecto a un formato específico de gobernanza colaborativa y multilateral, también constituido a partir del R-Ciber. Esa estrategia busca garantizar la neutralidad y es compatible con la dinámica tecnológica característica de este sector.

El enfoque *ex post* de responsabilidad complementa ese marco al establecer requisitos de gobernanza integrada y fundamentos para la atribución de fallas y consecuencias apropiadas aplicadas a la parte responsable. La expectativa del regulador fue la de disuadir comportamientos oportunistas y adherir a las precauciones necesarias para aumentar la resiliencia de la red, bajo pena de sanciones que pueden variar desde advertencias y multas hasta medidas más severas como la pérdida de la autorización para la prestación de servicios (ANATEL, 2020a).

En este sentido, se impone a los regulados un sistema de intercambio de informaciones y notificación de incidentes relevantes, que abarca informaciones sobre la causa y el impacto, así como las acciones de mitigación adoptadas, según el caso.

4.2. Asimetrías regulatorias, incentivos y costos de implementación

Dado que la mayoría de las decisiones relacionadas con la ciberseguridad son tomadas por los regulados en sus opciones de inversión, de implementación de mecanismos y rutinas, y son luego descentralizadas, es importante que los incentivos dirigidos a las mismas estén orientados a un nivel de seguridad óptimo y socialmente deseado (BAUER y EETEN, 2009).

En el caso del R-Ciber, la regla general de observancia de los principios y lineamientos regulatorios por parte de todos los prestadores de servicios de telecomunicaciones, de interés colectivo o restringido, independientemente de su porte, es solo un punto de partida para enfoques más claros y con diferentes efectos en el escenario futuro.

Un eje del Reglamento es su incidencia asimétrica sobre diferentes grupos de actores. Los Prestadores de Pequeño Porte (PPP), por ejemplo, están exentos de cumplir con las obligaciones, y solo son responsables por observar los principios y lineamientos enumerados en el R-Ciber. Se espera, sin embargo, que la Agencia pueda incluir o eximir de su cumplimiento –total o parcialmente– a otros actores como los mencionados PPPs, empresas con derechos de explotación satelital y demás personas físicas o jurídicas del ecosistema de telecomunicaciones involucradas directa o indirectamente en la gestión o en el desarrollo de las redes y servicios (ANATEL, 2020a).

Este mecanismo garantiza una flexibilidad para el regulador, que incluso podrá actuar de

manera circunstancial y puntual respecto de determinadas medidas que resulten necesarias sin que se justifique la imposición del régimen regulatorio en su conjunto (ANATEL, 2020b). En otras palabras, se permite una intervención hecha a medida, más proporcional.

El diseño de la asimetría en la elaboración de la normativa y en su aplicación presente y futura, dado su carácter flexible mencionado anteriormente, es producto de consideraciones asociadas a las externalidades de red y de la relación de interdependencia entre prestadores (ANATEL, 2017). Hay que reconocer que, en materia de ciberseguridad, debe existir un límite razonable de asimetría beneficiosa, dispensándose la imposición de deberes excesivamente onerosos y evitando la creación de barreras de entrada, para determinados prestadores (como los PPPs), de manera que los objetivos generales a lo que se apunta no se vean comprometidos (ANATEL, 2020b).

Dada la naturaleza de la gobernanza establecida y el flujo continuo previsto para el establecimiento de nuevas medidas, la asimetría se seguirá modulando durante el tiempo de aplicación del R-Ciber (ANATEL, 2017). Por tanto, es posible prever la creación de diferentes directivas para prestadores y para proveedores, por ejemplo.

El compromiso regulatorio con una reflexión abierta para lograr la asimetría en cada etapa trae consigo un riesgo no menor de efectos negativos derivados de eventual captura, en lo que respecta a la distribución de costos para lograr los objetivos generales entre los regulados. Esto se debe a que el sistema de consecución de propósitos con diferencia de pérdidas y beneficios para diferentes grupos de regulados, inherente al rol del regulador (PELTZMAN, 1976), solo deja de ocurrir en el momento en que se emite el reglamento, pero se efectivizará a cada medida aplicada con ese matiz.

Otra perspectiva asociada tanto a la asimetría como a la naturaleza principiológica del R-Ciber es la de permitir que los prestadores, respetándose los niveles mínimos, desarrollen modelos de negocio en los que los niveles de protección constituyan variables intrínsecas de las ofertas de servicios. Este aspecto, desde la perspectiva del regulador, actuaría como un incentivo, puesto que diferenciales de oferta mejores pueden incrementar el nivel de satisfacción de los usuarios, especialmente de los nichos, además de reducir costos y fomentar la competencia (ANATEL, 2020b).

Otro aspecto relacionado con los incentivos que la normativa impone a los administrados se refiere a los costos para lograr su cumplimiento. Teniendo en cuenta que las actividades relacionadas con el tema no son triviales, involucran tecnología generalmente de última generación y puede producir impactos en cadena, esta variable está presente tanto en el juicio interno de los regulados acerca del costo de cumplir o no con las obligaciones como en el debate sobre los aspectos y formas de esas obligaciones, lo cual es llevado a cabo progresivamente por el GT-Ciber, grupo técnico creado por el R-Ciber, que se tratará en la siguiente sección.

El R-Ciber pone de manifiesto la responsabilidad integral por los costos derivados de la

adopción y ejecución de la Política de Seguridad Cibernética y demás conductas y procedimientos exigidos en la misma. Abarca, entre otros, lineamientos sobre la configuración de equipos entregados en comodato a los usuarios o la realización de ciclos de evaluación de vulnerabilidades.

Un punto de atención, sin embargo, es la hipótesis de que el propio regulador imponga otras medidas a partir del funcionamiento del sistema previsto de gobernanza[2] (ANATEL, 2020a, b). En cuanto a esas medidas, lo que se establece es que se determinarán de forma motivada. Considerando los planteos normativos a la luz de los principios de razonabilidad y proporcionalidad que rigen la Administración Pública y las peculiaridades de la intervención sobre la actividad económica, el impacto de los costos debe ser necesariamente objeto de reflexión en la construcción de esas futuras medidas, lo cual revela otro punto de complejidad para una gobernanza receptiva.

En este sentido, se verifica una postura neutral atribuida al propio regulador. La coherencia respecto de la línea del R-Ciber de implementación cooperativa y la tendencia receptiva requerirán una ponderación constante de medios y fines que no ocurriría en otro tipo de modelo, de agotamiento *ex ante* de requisitos para la conformidad.

En la medida en que incidirán formalmente en la construcción de la directiva temática, se puede considerar que los resultados producidos ya traerán en sí mismos un balance previo de incentivos en cuanto al costo-beneficio del cumplimiento o incumplimiento de las normativas. Por lo tanto, puede haber una tendencia más natural a adherirse a la norma.

El riesgo existente sigue siendo el de captura en sentido *lato* (DAL BÓ, 2006)[3], por las razones exploradas en el tema relacionado con la gobernanza, que se expone a continuación. En un escenario de asimetría, la imposición de regímenes diferenciados para distintos grupos puede ser utilizada por uno de ellos, si logra influir en el regulador, para imponer mayores cargas al otro, con consecuencias sobre la competencia, por ejemplo.

Esto demuestra que la efectividad del régimen de incentivos pretendido depende de la óptima ponderación de costos que asumirán los regulados y, ante la existencia de asimetrías, de una distribución de cargas que evite distorsiones que permitan el comportamiento *free-riding*.

4.3. Gobernanza colaborativa

El tratamiento de un aspecto como la ciberseguridad por parte del regulador tiene un diferencial con relación a otros aspectos de su desempeño, como los relacionados con la protección de los derechos del consumidor aplicada a los usuarios o el cumplimiento de metas de expansión de infraestructura. Para la seguridad, por las razones mencionadas anteriormente, el *compliance* individual de los actores es significativo pero insuficiente, en virtud de los impactos transversales directos y potencialmente negativos que la conducta de cada uno de ellos puede tener sobre el ecosistema como un conjunto.

El regulador enfrenta un desafío para lograr el compromiso colectivo de las entidades privadas, no solo en el sentido del cumplimiento de estándares técnicos mínimos, en prácticas preventivas y correctivas, sino también de un flujo constante de intercambio de información, materializado en el funcionamiento de un sistema de notificación y difusión de datos sobre incidentes. Este determinante del éxito de la regulación temática presupone el establecimiento de incentivos legales y económicos y es allí donde se enmarca la constitución de un grupo de gobernanza multiinstitucional, que pretende servir como plataforma para albergar el diálogo multilateral.

Esta perspectiva de gobernanza se da a la luz de elementos históricos[4] recurrentes en el abordaje del tema (RUTKOWSKI, 2011) y de experiencias internacionales, a ejemplo de los Centros de Intercambio y Análisis de Información (ISACs) en la Unión Europea (ENISA, 2018). Estas organizaciones fueron constituidas para facilitar el intercambio de información entre los sectores público y privado, como también para recopilar información sobre amenazas cibernéticas. Su objetivo es generar confianza mediante el intercambio de experiencias, conocimientos y análisis, especialmente sobre las causas raíces, incidentes y amenazas. Aspectos positivos que fueron absorbidos en el modelo brasileño.

La constitución de este modelo permite, al mismo tiempo, la composición de un acervo de datos; la construcción de canales permanentes de información que faciliten reacciones instantáneas y sistémicas ante incidentes, con reducción de daños; y la rápida elaboración de nuevos niveles mínimos requeridos para la conducta de los regulados.

Bajo la perspectiva jurídica formal, el Grupo Técnico de Seguridad Cibernética y Gestión de Riesgos de Infraestructuras Críticas (GT-Ciber), coordinado por autoridades del organismo regulador, es un foro de participación obligatoria para prestadores con poder de mercado significativo (PMS). Representantes de otros prestadores, asociaciones, organismos y entidades podrán tener participación libre en la discusión de sus temas de interés. Su rango de atribuciones incluye actividades de observación y asesoramiento interno, pero prevalece su funcionamiento como instancia para proponer requisitos técnicos y medidas específicas relacionadas con las redes y de disposiciones sobre aspectos y formas de cumplimiento de las obligaciones relacionadas con las políticas de seguridad y evaluación de vulnerabilidades de los entes privados (ANATEL, 2020a).

El incentivo para la participación efectiva de los prestadores resulta menos de la imposición que de la posibilidad de materializar sus propios intereses en disposiciones que pueden llegar a ser indispensables para todo el ecosistema. En este entorno expresamente pautado por el diálogo y el consenso, pero cuya decisión corresponde a la autoridad reguladora (ANATEL, 2020a), la búsqueda de soluciones más rápidas comparadas al procedimiento administrativo tradicional también puede resultar en un mayor discernimiento para obtener los resultados (ANATEL, 2017, ANATEL, 2020b).

En un escenario donde este mecanismo contempla obligaciones para calibrarlas, no es difícil prever la constitución de escenarios paralelos donde se verifique una competencia entre

diferentes grupos para ejercer influencia sobre el regulador, de maneras más complejas que una victoria o derrota total para los objetivos en juego (BECKER, 1983). Esto se debe a que varían considerablemente las perspectivas entre grupos sobre los deberes y las cargas correspondientes que deben asumirse. Un ejemplo de esto sería un movimiento por parte de los principales prestadores en busca de una menor asimetría con relación a los PPPs, con el fin de quitarse la carga de tener que garantizar la salud del ecosistema como un todo.

Esto revela el desafío que este modelo de gobernanza impone a los participantes y al regulador. Dada su naturaleza, es posible que se le apliquen las consideraciones del modelo identificado como teoría del ciclo de vida de las agencias reguladoras (MARTIMORT, 1999) a título de reflexión.

En términos generales, se espera que la nueva estructura reciba una mayor atención institucional y pase por un mayor control tras su instalación. Con el tiempo, este tipo de presiones tiende a reducirse, mientras que la presión de los grupos de interés de las empresas se mantiene constante, al tiempo que la burocratización de las actividades también se mostraría creciente. Para evitar dicho riesgo, resulta aconsejable la supervisión periódica del GT-Ciber por parte de otras instancias de la Anatel, de organismos de control y de la sociedad.

Conclusiones

La ciberseguridad en el sector de las telecomunicaciones sintetiza los aspectos más sofisticados del tema entre los sectores de infraestructura. Igualmente, la nueva generación tecnológica de redes móviles surge como un impulso transformador, destino de inversiones y de posibilidades extraordinarias en el uso de servicios y aplicaciones de alto valor agregado, pero trae consigo nuevas amenazas, riesgos y preocupaciones en materia de seguridad del espacio cibernético.

Las referencias resumidas en este artículo evidencian la complejidad del tema y la necesidad de un estudio continuo y profundo de las posibles soluciones normativas y administrativas resultantes, que ayuden a contener el problema.

Ante los nuevos desafíos, el regulador de telecomunicaciones optó por una intervención técnica asimétrica y colaborativa, más flexible, además de una acción regulatoria orientada a los riesgos percibidos, en enfoques *ex ante* y *ex post*. Asimismo, el enfoque en la identificación de los incentivos revela la naturaleza económica del tema y su comprensión ayudó al tomador de decisiones a modular el grado de intervención regulatoria. Así, el producto de la normativa contempló, además de los aspectos técnicos y legales, la búsqueda de la alineación de incentivos de las partes interesadas, la implementación colaborativa del nuevo marco regulatorio y la adopción de soluciones dirigidas a corregir fallas intrínsecas a este mercado, cuyos efectos definen la postura de los agentes en lo que respecta a la ciberseguridad.

Visto que el camino regulatorio elegida, que empieza a ser recorrido con la edición del Reglamento de Seguridad Cibernética, prevé la existencia de un foro permanente de interacción entre el regulador y los regulados para la especificación de normas y construcción de nuevas medidas, es fundamental que el entendimiento acerca de la construcción de incentivos sea igualmente duradero y evite comportamientos perjudiciales para el ecosistema en su conjunto, tanto en términos de ciberseguridad como de competencia.

Referencias

– AHMAD, I., KUMAR, T., LIYANAGE, M. OKWUIBE, J., YLIANTTILA, M., GURTOV, A. *Overview of 5G Security Challenges and Solutions*, in *IEEE Communications Standards Magazine*, vol. 2, no. 1, pp. 36-43, 2018, doi: 10.1109/MCOMSTD.2018.1700063.

– ANATEL. 2017. Processo nº 53500.078752/2017-68. *Projeto de Análise sobre a regulamentação de segurança das redes de telecomunicações*. ANATEL: Brasilia.

– ANATEL. 2020a. *Resolução nº 740/2020: Aprova o Regulamento de Segurança Cibernética Aplicada ao Setor de Telecomunicações*. ANATEL: Brasilia.

– ANATEL. 2020b. *Voto nº 87/2020/PR: Proposta de reavaliação da regulamentação relacionada a serviços públicos de emergência e à segurança de redes de telecomunicações – Item nº 7 da Agenda Regulatória para biênio o 2019-2020.*. ANATEL: Brasilia.

– BAUER, Johannes M; EETEN, Michel J.G. van. *Cybersecurity: stakeholder, incentives, externalities and policy options*. Telecommunications Policy. (33) 10-11, p.p. 706-719, 2009. [Consult. 31 dez. 2020]. Disponible en Cybersecurity: Stakeholder incentives, externalities, and policy options – ScienceDirect.

– BECKER, G.S. 1983. *A Theory of Competition Among Pressure Groups for Political Influence*. The Quarterly Journal of Economics, Vol. 98, No. 3., p. 371-400.

– BRASIL, 1984. *Lei nº 7.232/1984: Dispõe sobre a Política Nacional de Informática, e dá outras providências*. Congreso Nacional: Brasilia.

– BRASIL. 2000. *Decreto nº 3.505/2000: Institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal*. Presidencia de la República: Brasilia.

– BRASIL. 2003. *Decreto nº 4.801/2003: Cria a Câmara de Relações Exteriores e Defesa Nacional, do Conselho de Governo*. Presidencia de la República: Brasilia.

– BRASIL. 2008. *Instrução Normativa GSI/PR nº 1/2008: Disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta, e dá outras providências*. Gabinete de Seguridad Institucional, Presidencia de la República: Brasilia.

– BRASIL. 2010. *Livro Verde: Segurança Cibernética no Brasil.* Presidencia de la República, Gabinete de Seguridad Institucional. Departamento de Seguridad de la Información y Comunicaciones: Brasilia.

– BRASIL. 2012. *Livro Branco de Defesa Nacional*. Presidencia de la República, Gabinete de Seguridad Institucional. Departamento de Seguridad de la Información y Comunicaciones: Brasilia.

– BRASIL, 2018. *Decreto nº 9.637/2018: Institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação e determina outras providências*. Presidencia de la República: Brasilia.

– BRASIL, 2018. *Lei nº 13.709/2018: Lei Geral de Proteção de Dados Pessoais (LGPD)*. Congreso Nacional: Brasilia.

– BRASIL, 2020. *Decreto nº 10.222/2020: Aprova a Estratégia Nacional de Segurança Cibernética*. Presidencia de la República: Brasilia.

– BRASIL, 2020. *Instrução Normativa nº 4/2020: Dispõe sobre os requisitos mínimos de Segurança Cibernética que devem ser adotados no estabelecimento das redes 5G*. Ministerio de Estado del Gabinete de Seguridad Institucional de la Presidencia de la República: Brasilia.

– CARVALHO, B.E.F.C., SANTOS, D.B.M. 2011. *Segurança de infraestruturas críticas no Brasil.* Conference Paper, XIX Simposio Brasileño de Recursos Hídricos. Maceió.

– DAL BÓ, E. 2006. *Regulatory Capture: A Review*. Oxford Review of Economic Policy, Volume 22, Issue 2, Summer , p. 203–225.

– ENISA. 2018. *Information Sharing and Analysis Centres (ISACs) Cooperative models*. ENISA: Creta.

– HILLER, J.S.; RUSSELL, R.S. *The challenge and imperative of private sector cybersecurity: an international comparison*. In: Computer Law & Security Review. Elsevier, 2013. [Consultado: 28 dic. 2020].

– INÁCIO, André – *Tecnologias de informação e segurança pública: um equilíbrio instável*. In: CIJIC. Revista Científica sobre *Cyberlaw*. Lisboa, n.1, 2016, p. 9. [Consultado: 28 dic. 2020]. Disponible en: http://www.cijic.org/wp-content/uploads/2016/01/ANDRE-INACIO.pdf

– KASKA, K., BECKVARD, H., MINÁRIK, T. 2019. *Huawei, 5G and China as a security threat*. CCDCOE – Nato Cooperative Cyber Defence Centre of Excellence. Tallinn, 2019. [Consultado: 31 dic. 2020]. Disponible en CCDCOE-Huawei-2019-03-28-FINAL.pdf

– KUNREUTHER, H., HEAL, G. 2003. Interdependent Security. Journal of Risk and Uncertainty, Vol. 26, No. 2/3, Special Issue on the Risks of Terrorisum, pp. 231-249.

– MARTIMORT, D. 1999. *The Life Cycle of Regulatory Agencies: Dynamic Capture and Transaction Costs*. Review of Economic Studies 66(4), 929-947.

– OECD. 2012. *Recommendation of the council on regulatory policy and governance*. Recommendation of the Council on Regulatory Policy and Governance, OECD Publishing, Paris. Disponible en línea en: http://dx.doi.org/10.1787/9789264209022-en

– PELTZMAN, S. 1976. Toward a More General Theory of Regulation. The Journal of Law & Economics, 19(2), 211-240. Retrieved March 17, 2021, from http://www.jstor.org/stable/725163

– RUTKOWSKI, Anthony. (2011), *Public international law of the international telecommunication instruments: cyber security treaty provisions since 1850*, info, Vol. 13 No. 1, pp. 13-31. https://doi.org/10.1108/14636691111101856.

– TELETIME. 2020. *Regulamento de segurança cibernética alcança fornecedores; operadoras pagarão pelas medidas necessárias*. Por Bruno Do Amaral E Samuel Possebon -17/12/20, 23:04. Actualizado el 17/12/20, 23:07.

– UNIÓN INTERNACIONAL DE TELECOMUNICACIONES. 2018. *Global Cybersecurity Index V3*. Disponible en: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf

Acerca de los Autores

Ronaldo Neves de Moura Filho é Especialista em Regulação e Mestrando em Administração Pública pelo Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa (IDP), Brasil.

Luciano Charlita de Freitas é Especialista em Regulação e Doutor em Políticas de Desenvolvimento pela Universidade de Hiroshima, Japão.

Egon Cervieri Guterres é Especialista em Regulação de Telecomunicações da Anatel e Especialista em Planejamento e Estratégias de Desenvolvimento pela Escola Nacional de Administração Pública, Brasil.

Mariana Almeida de Sousa Talouki é Analista Administrativo na Agência Nacional de Telecomunicações, Brasil, e Doutoranda em Direito pela Faculdade de Direito da Universidade do Porto, Portugal.

Leonardo Euler de Morais é Especialista em Regulação e Mestre de Economia pela Universidade de Brasília, Brasil.

Notas

↑1 Pese a la posterior derogación de este decreto, las disposiciones de protección de la seguridad se mantuvieron sin cambios.

↑2 Al estar limitado a sus competencias legales, no correspondería al regulador tratar o, a modo de ejemplo, eximir a los regulados de los costos derivados de normativas y otras medidas expedidas por otros organismos.

↑3 Para dicho autor, en sentido *lato*, la captura regulatoria es el proceso por el cual intereses específicos afectan la intervención estatal en alguna de sus formas.

↑4 El elemento colaborativo viene siendo uno de los pilares de la construcción del régimen de regulación de la ciberseguridad, el cual puede ser rastreado desde sus orígenes, en la Conferencia de Dresde de 1850 (RUTKOWSKI, 2011), en un crecimiento que comienza con la asociación entre diferentes administraciones nacionales y reguladores, y comienza a abarcar a otras entidades, especialmente privadas.