Regulamentação da segurança cibernética das telecomunicações no Brasil: um balanço de incentivos em um contexto de neutralidade 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/TOJO8735

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: Segurança Cibernética; Regulação; Regulamentação; Telecomunicações

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. Introdução

As telecomunicações têm importância nuclear para a integralidade do sistema de infraestruturas críticas e o espaço cibernético brasileiro. Por um lado, o setor opera como agente autônomo no quadro de infraestruturas de comunicação e, por outro, é elemento integrador das demais infraestruturas nacionais essenciais, intra e intersetorial.

Ao longo das últimas décadas, o setor tem sido progressivamente utilizado para perpetração de atividades maliciosas que ocasionam ou tem o potencial de causar danos aos usuários e direitos inseridos nesse meio, com dimensões políticas, econômicas e militares (INÁCIO, 2016). Com a iminente chegada de uma nova geração tecnológica (5G), habilitadora de mudanças paradigmáticas na conectividade de pessoas e atividades produtivas, as ameaças

se amplificam. Afinal, maiores superfícies de redes associadas a uma maior dependência de conectividade naturalmente aumentam riscos e impactos de possíveis falhas e ataques (AHMAD et al, 2018). Isso representa uma renovação do debate sobre a segurança.

É nesse contexto que se insere o presente estudo. O objetivo é relatar o racional sobre o qual se apoia o recente editado Regulamento de Segurança Cibernética (R-Ciber) no âmbito das telecomunicações brasileiras. Nesse sentido, parte-se de um histórico do contexto normativo brasileiro em relação à cibersegurança e uma revisão das definições e bases principiológicas que subsidiaram a busca de um equilíbrio eficiente na promoção da integridade da infraestrutura crítica do Estado brasileiro, dos interesses mercadológicos e na preservação dos direitos fundamentais dos cidadãos.

O estudo também apresenta elementos econômicos e comportamentais subjacentes à compreensão dos incentivos, das assimetrias e das externalidades que justificam a intervenção regulatória sobre o tema. Tais fundamentos direcionaram a escolha do regulador por uma vertente técnica neutra, com a atribuição de responsabilidades e a adoção de instrumentos flexíveis de promoção da transparência, com destaque para aqueles voltados à divulgação de informações e uma governança multilateral.

Tal relato se presta, por fim, a documentar os aspectos subjacentes ao desenho da regulação no Brasil e, desse modo, criar não apenas uma referência histórica sobre o desenvolvimento do tema e uma apresentação de seu *status*, como também deixar evidenciados os principais debates que sua aplicação certamente levantará nos próximos anos.

Além dessa introdução, o artigo está dividido em três partes. A seção a seguir faz um apanhado circunstanciado sobre a evolução dos normativos afetos à segurança cibernética no Brasil, e como nela se encaixa o Regulamento de Segurança Cibernética aplicada ao Setor de Telecomunicações.

Em seguida, são feitas ponderações sobre o atual debate acerca da segurança cibernética à luz das modernas tecnologias de telecomunicações. Um destaque especial é atribuído à contextualização sobre o cenário geopolítico e de transformação tecnológica em curso.

A quarta seção apresenta reflexões sobre 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 estão voltadas à identificação dos pontos de atenção que estarão presentes na implementação da regulamentação. Segue-se uma breve conclusão.

2. Evolução normativa sobre segurança cibernética no

Brasil e renovação do debate

O Brasil é uma arena usual de ataques cibernéticos e a preocupação em endereçar o tema não é recente. Data da década de 1980 o primeiro normativo afeto à segurança cibernética, a Lei n° 7.232/1984 (BRASIL, 1984). Essa lei introduziu a Política Nacional de Informática e inscreveu, dentre os seus princípios, o de estabelecer mecanismos e instrumentos legais e técnicos para a proteção do sigilo de dados, do interesse da privacidade e da segurança de pessoas físicas e jurídicas, privadas e públicas.

Posteriormente, foi publicada a primeira Política de Segurança da Informação, mediante o Decreto n° 3.505/2000 (BRASIL, 2020). Tal norma tinha como foco a Administração Pública Federal e dela se destaca a preocupação com a defesa da soberania nacional e com a proteção de direitos fundamentais, tais como a intimidade e a privacidade.

Na sequência, por meio do Decreto n° 4.801/2003 (BRASIL, 2003), instituiu-se a Câmara de Relações Exteriores, órgão consultivo da Presidência da República que incluía entre suas finalidades a implementação de programas pertinentes à segurança da informação e à segurança cibernética[1].

Em 2008, foi publicada pelo Gabinete de Segurança Institucional a Instrução Normativa n° 1/2008 (BRASIL, 2008), responsável por disciplinar a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal. Para além das competências instituídas no âmbito da administração pública, o referido documento trouxe um rol de definições como os de disponibilidade, integridade, confidencialidade e autenticidade.

Até esse ponto, é possível constatar que, no ordenamento jurídico-normativo brasileiro, a segurança cibernética apresenta vertentes diferenciadas por seu objeto e pelo agente de tratamento. Nos casos em que o objeto é a proteção das infraestruturas críticas, com vistas a assegurar a estabilidade política e econômica, bem como a proteção da sociedade e dos direitos e interesses de seus indivíduos, é o Gabinete de Segurança Institucional o órgão responsável pelo tratamento. Como expressão disso, tem-se a publicação pela Presidência da República, em 2010, do Livro Verde de Segurança Cibernética no Brasil (BRASIL, 2010).

Nas situações em que o objeto da cibersegurança é um bem de titularidade estatal, com proeminência para as infraestruturas críticas e visando a defesa e a soberania nacional, ou em casos de guerra cibernética, a competência do seu tratamento está a cargo do Ministério da Defesa e das Forças Armadas Brasileiras, em especial o Exército Brasileiro. Como expoente dessa atribuição tem-se o Livro Branco de Defesa Nacional, publicado pelo Ministério da Defesa, em 2012 (BRASIL, 2012), que trata de aspectos relativos a estratégias de guerra no ambiente cibernético.

O que se percebe, ao analisar o histórico normativo de segurança cibernética do Brasil, é uma preocupação de se proteger bens e direitos no âmbito do ciberespaço. Contudo, malgrado as previsões normativas e avanços institucionais, o Brasil, ao longo desses quase

40 anos, teve sua vulnerabilidade de redes de telecomunicações continuamente aumentada.

Uma evidência disso é a alta incidência de ataques cibernéticos no país (UIT, 2018). Atualmente o Brasil ocupa a 70º posição no ranking *Global Cybersecurity Index*, indicador que mede o nível de preparo dos países para lidar com os ataques cibernéticos (UIT, 2018).

A atual renovação do debate se deve em parte por um impulso relacionado à iniciativa privada face às ameaças de segurança. Aliado a isso, tem-se fatores de ordem econômica e interesse na utilização de tecnologias de ponta por parte do governo, empresas e indivíduos, cujo exemplo emblemático é o padrão de tecnologia 5G (AHMAD et al, 2018).

Alguns aspectos dessa tecnologia, em conjunto, comungam para o recrudescimento das vulnerabilidades. Dentre eles, destaca-se a transposição da utilização de *hardware* para *software*, dificultando, assim, o potencial para inspeção, controle e ciberhigiene dos pontos de estrangulamento. Também consequência dessa transposição está a virtualização em *software* das funções de rede antes executadas por dispositivos físicos. Ademais, mesmo em sendo possível o bloqueio das vulnerabilidades de *software* na rede, esta é também gerenciada por o que se convencionou chamar *AI-based* softwares, que favorecem a vulnerabilidade. Aliado ao fator *software*, há que se destacar a difusão de dispositivos inteligentes, cujo emprego abrange aplicações domésticas a áreas de serviços essenciais, tais como hospitais, serviços de segurança pública e transporte.

Com efeito, a quinta geração para conectividade móvel em banda larga constitui-se um catalisador de mudança de paradigmas sobre a forma com a qual o Brasil lida com a segurança cibernética.

Nesse novo contexto, se insere a promulgação da mais recente Política Nacional de Segurança da Informação, por meio do Decreto n° 9.637/2018 (BRASIL, 2018), e a Estratégia Nacional de Segurança Cibernética, publicada através do Decreto n° 10.222/2020 (BRASIL, 2020). Resumidamente, o Decreto n° 10.222/20 apresenta a Estratégia Nacional de Cibersegurança e tem como metodologia o tratamento da segurança cibernética mediante contexto de governança de forma a harmonizar interesses e esforços por parte da administração pública, das empresas privadas, dos pesquisadores dessa área de conhecimento e da sociedade civil. A estratégia também é composta de ações e objetivos que, em comunhão, propõem o aperfeiçoamento da estrutura de cibersegurança a fim de promover a resiliência do país frente às ameaças no ambiente digital, assim como a sua confiabilidade no cenário internacional.

Em se tratando do arcabouço regulatório atinente ao reforço da segurança cibernética paralelo aos preparativos para implantação do 5G, pode-se citar ainda duas iniciativas. A primeira, do Gabinete de Segurança Institucional, com a promulgação da Instrução Normativa n° 4/2020 (BRASIL, 2020) que estabelece requisitos mínimos de segurança cibernética para as redes de telecomunicações utilizadas pelo Governo Federal. Essa instrução se dirige à Administração Pública Federal direta e indireta e preconiza o

cumprimento de especificações técnicas e a diversificação de fornecedores, de forma a mitigar riscos decorrentes de dependência excessiva.

Por fim, é pertinente evidenciar a importância dada no conteúdo da estratégia ao papel das agências reguladoras no estímulo à adoção de procedimentos de segurança cibernética, por parte de seus regulados. No tocante ao setor das telecomunicações, essa incumbência tem respaldo na necessidade de participação da agência reguladora do setor – a Agência Nacional de Telecomunicações – Anatel – no tratamento da cibersegurança, de modo direto ou transversal, em cooperação com os demais *stakeholders*.

Para os agentes regulados do mercado, em dezembro de 2020, a Anatel publicou o Regulamento de Segurança Cibernética Aplicada ao Setor de Telecomunicações (R-Ciber), aprovado mediante a Resolução n° 740/2020 (ANATEL, 2020a). Sua gênese está na necessidade de cumprimento da Estratégia Nacional de Segurança Cibernética e da Agenda Regulatória da própria Agência (ANATEL, 2017). A publicação deste instrumento normativo reflete, ainda, a preocupação da Agência em fomentar uma Política de Segurança Cibernética para as prestadoras de serviços de telecomunicações, acompanhada pelo órgão regulador.

Com o histórico acima percebe-se que a abordagem normativa e institucional da segurança cibernética no Brasil evoluiu de um quadro amplo e associado à estratégia de defesa nacional até o ponto em que passa a permear regulações setoriais afins, no caso aquela voltada para as infraestruturas e a prestação de serviços de telecomunicações por entes privados, objeto das próximas seções.

3. O contexto geopolítico e tecnológico e as premissas da regulamentação de segurança cibernética para telecomunicações

Em linhas gerais, as boas práticas em atuação regulatória recomendam o estabelecimento de um arcabouço mínimo de intervenção, governança e confiança no tocante à prescrição de comportamentos para o setor de telecomunicações e deste com os demais setores da economia (OCDE, 2012).

Cumpre ao regulador observar elementos do debate e sobre eles se posicionar, promovendo soluções sustentáveis e adequadas à dinâmica de cada tema sob sua competência de atuação. Essa dimensão analítica abrange uma compreensão sobre temas tão diversos quanto a economia política e tecnopolítica de influência, as externalidades de rede e a interdependência nas relações de segurança cibernética e o dimensionamento da intervenção regulatória à luz de princípios de eficiência e resiliência.

Sobre o primeiro tema, é preciso reconhecer que o contexto em que o R-Ciber está inserido abrange um problema de ordem política. Em parte, os posicionamentos divergentes se

devem à abordagem multifacetada sobre o tema, cuja coordenação encontra-se fragmentada entre órgãos de estado, de governo e agentes privados. Desse modo, os países líderes no desenvolvimento tecnológico se amparam em perspectivas distintas sobre a natureza dos riscos do ciberespaço para elaborar sua estratégia de atuação e esforços de coordenação de políticas domésticas e internacionais (HILLER e RUSSELL, 2013).

Cabe ainda destacar que a rivalidade aflorada no debate sobre segurança cibernética não se resume a casos concretos. Ao contrário, ocorre na conjuntura de uma rivalidade histórica que molda debates estratégicos da geopolítica mundial em temas diversos (KASKA et al., 2019).

Quando transposta à dimensão tecnológica, a divergência se potencializa pelo fato de estar em jogo elementos de longo prazo cujos termos se fundamentam na definição de normas técnicas e nas chamadas tecnopolíticas de influência, subjacentes aos produtos e serviços digitais e cujo emprego transcende os limites das fronteiras territoriais. Nesse sentido, questões de desenvolvimento e uso de tecnologias escalam para tornarem-se objeto de debates políticos, pela defesa de valores e, ao cabo, de confirmação de influência mundial ou regional.

A despeito de sua inequívoca importância e efeitos sobre o setor, tal dimensão não foi objeto de exame pelo regulador setorial brasileiro que, em consonância com suas prerrogativas legais, ateve-se aos aspectos regulatórios afetos ao tema (ANATEL, 2020a, b).

No tocante às externalidades e à interdependência nas relações de segurança cibernética, cumpre observar que as ações e omissões de determinados agentes podem ter efeitos colaterais diversos sobre os demais. Tal condição se potencializa quando a interoperabilidade é a base de funcionamento de todo o sistema. A insegurança cria externalidades negativas. Nesse caso, um ponto da rede com segurança comprometida pode permitir brechas com efeitos amplos sobre as demais redes, serviços e usuários.

Uma outra modalidade de externalidade no caso em debate é a chamada segurança interdependente (KUNREUTHER e HEAL, 2003). Aqui, os investimentos em segurança podem ser complementos estratégicos e se operam quando um determinado indivíduo que toma medidas de proteção, cria externalidades positivas para os outros que, por sua vez, podem se sentir desencorajados a realizar seu próprio investimento. Trata-se do comportamento do tipo *free-riding* e se manifesta por induzir agentes a não se preocuparem em investir em segurança face à expectativa de que outros agentes estão protegendo suas redes.

O quadro posto exige um correto dimensionamento da intervenção regulatória. Isso porque as ameaças à segurança cibernética possuem características técnicas, partes interessadas e restrições legais distintas. Assim, para se alcançar efetividade, optou o regulador por estabelecer diretrizes de natureza principiológica, onde se concentram as barreiras econômicas que inibem a adesão de regras de segurança e a alocação de investimentos

necessários.

Ademais, a regulamentação em cibersegurança no setor de telecomunicações vai muito além da preocupação imediata com a implantação das redes 5G, dado seu escopo tecnologicamente neutro (ANATEL, 2017; ANATEL, 2020a,b) e não adotou um viés procedimental e estático de contenção de riscos e falhas. A estrutura corresponde a um conjunto composto por princípios e diretrizes objetivas de segurança no espaço cibernético, amparado em uma combinação de incentivos baseados nas regras competitivas de mercado e na supervisão regulatória.

Ainda na perspectiva principiológica, importa mencionar o racional expresso de proteção de dados pessoais de que se reveste o R-Ciber, decorrente da Lei n° 13.709/2018 (BRASIL, 2018), que centraliza as disposições gerais sobre o tema. Ao entender que a violação de dados pessoais pode constituir uma afronta a direitos fundamentais, tais como a privacidade e a intimidade, mostra-se indispensável a implementação de medidas cibersecuratórias tendentes a contornar riscos dessa natureza. Nesse sentido, para proteger a privacidade dos usuários, as empresas de telecomunicações estão incumbidas da responsabilidade de utilizar ferramentas adequadas para a proteção dos dados pessoais.

Sob o prisma do regulado, embora ele também se beneficie da ampliação do nível de segurança do espaço cibernético como um todo, é preciso considerar as implicações financeiro-econômicas sobre a exploração da atividade empresarial. A adoção de sistemas e mecanismos de proteção, preparação e resposta a incidentes de cibersegurança implica em custos. Por conseguinte, existe uma tensão entre eficiência e resiliência na composição das redes críticas de telecomunicações.

Assim, a decisão individual de um ente em reduzir seus custos operacionais visando eficiência pode implicar em risco de vulnerabilidade sistematizada de longo prazo. Nesse plano, os incentivos de curto prazo, para reduzir custos operacionais, conflitam com aqueles de longo prazo, orientados à promoção de resiliência.

Esse *trade-off* é revelador do dilema entre segurança e eficiência e serve para evidenciar o nível ótimo de intervenção, medida na qual os benefícios de operação eficiente superam qualquer redução no risco decorrente de medidas de segurança adicionais.

4. Regulamento: riscos, assimetrias e governança

A aplicação de princípios, diretrizes e boas práticas é essencial para uma política nacional de cibersegurança eficaz. Nesse sentido, o R-Ciber estabelece uma base principiológica que serve de guia para condutas e procedimentos que promovam a segurança cibernética nas redes e serviços de telecomunicações, a saber – autenticidade; confidencialidade; disponibilidade; diversidade; integridade; interoperabilidade; prioridade; responsabilidade; e transparência (ANATEL, 2020a,b).

Implementar e operacionalizar tais princípios e diretrizes em um ambiente tão complexo e dinâmico como o ecossistema das telecomunicações, requer abordagens e instrumentos regulatórios capazes de lidar com suas especificidades. Para endereçar esses desafios, o regulador elegeu um conjunto de diretivas e abordagens regulatórias em sua regulamentação técnica (ANATEL, 2017; ANATEL, 2020a,b), discutidas a seguir.

4.1 Regulação de riscos em infraestruturas críticas

Parte da infraestrutura crítica do Brasil opera em regimes autônomos tendo na conectividade seu elemento comum (CARVALHO e SANTOS, 2011). Esse padrão é revelador da essencialidade do setor de telecomunicações como agente autônomo no escopo das infraestruturas críticas e como agente integrador da infraestrutura nacional.

Os sistemas e dispositivos das gerações tecnológicas mais recentes, que são baseados preponderantemente em softwares, inauguraram novos desafios para a manutenção da segurança no plano cibernético. Em outras palavras, as inovações tecnológicas acabam por elastecer a superfície geral de ataques cibernéticos – constantemente aprimorados e evoluídos a fim de explorar novas vulnerabilidades –, o que, consequentemente, clama por um incremento na segurança cibernética (AHMDAD et. al, 2018).

A opção representada pelo R-Ciber é orientada aos riscos percebidos, em abordagem panóptica e de vigilância permanente, que contempla um híbrido de regulamentação de segurança *ex ante* e a atribuição de responsabilidades e*x post*. Na prática, esse regime permite, por um lado, estabelecer requisitos de segurança via certificação de equipamentos, licenciamento de estações e orientações de *compliance* e, por outro, a identificação e atribuição de responsabilidades dos agentes na coordenação das ações de segurança da rede.

A regulamentação de segurança *ex ante* trata de estabelecer os requisitos mínimos de segurança, aplicados na fase de certificação dos equipamentos, antes de sua homologação para ingresso no parque tecnológico que compõe a infraestrutura setorial. Trata-se de uma medida de prevenção, neutra em termos tecnológicos, e com os requisitos de salvaguardas necessários ao atendimento de requisitos de segurança.

Com destaque, o Regulamento prevê que os prestadores de serviços devem utilizar produtos e equipamentos de telecomunicações provenientes de fornecedores que possuam política de segurança cibernética compatíveis com os princípios e diretrizes de segurança cibernética definidos em regulamento. Esses componentes estariam, ainda, sujeitos a requisitos de conformidade aferidos em processos de auditoria independente periódicos (ANATEL, 2020a).

Tal designação pressupõe ações preliminares de auditoria técnica independente e a coordenação junto a um formato específico de governança colaborativa e multilateral, também constituído a partir do R-Ciber. Essa estratégia visa assegurar neutralidade e mostra-se compatível com a dinâmica tecnológica característica desse setor.

A abordagem *ex post* de responsabilização, complementa esse quadro ao estabelecer requisitos de governança integrada e fundamentos para imputação de falhas e consequências cabíveis à parte responsável. A expectativa do regulador foi pela dissuasão de comportamentos oportunistas e pela adesão às precauções necessárias para aumentar a resiliência da rede, sob pena de sancionamento que pode variar de advertência e multas a medidas mais severas como a perda da autorização para prestação de serviços (ANATEL, 2020a).

Nesse sentido, impõe-se aos regulados um sistema de compartilhamento de informações e notificação de incidentes relevantes, o qual abrange informações da causa e do impacto, bem como ações de mitigação adotadas, conforme o caso.

4.2. Assimetrias regulatórias, incentivos e custos de implementação

Uma vez que a maior parte das decisões relacionadas à segurança cibernética são tomadas pelos regulados em suas opções de investimento, de implementação de mecanismos e rotinas, e logo são descentralizadas, importa que os incentivos que se dirijam a elas estejam orientados a um nível de segurança ótimo e socialmente desejado (BAUER e EETEN, 2009).

No caso do R-Ciber, a regra geral de observância dos princípios e diretrizes regulamentares por todas as prestadoras dos serviços de telecomunicações, de interesse coletivo ou restrito, independentemente do porte, é apenas um ponto de partida para recortes mais claros e com efeitos diversos no cenário futuro.

Um eixo do Regulamento é sua incidência assimétrica sobre diferentes grupos de atores. As Prestadoras de Pequeno Porte (PPP), por exemplo, estão isentas do atendimento das obrigações, cabendo-lhes apenas a observância dos princípios e diretrizes elencados no R-Ciber. Prevê-se, contudo, que a Agência possa incluir ou dispensar de seu cumprimento – total ou parcialmente – outros atores como as citadas PPP, empresas detentoras de direito de exploração satelital e demais pessoas naturais ou jurídicas do ecossistema de telecomunicações envolvidos direta ou indiretamente na gestão ou no desenvolvimento das redes e serviços (ANATEL, 2020a).

Esse mecanismo garante uma flexibilidade para o regulador, que poderá agir, inclusive, de forma circunstancial e pontual a respeito de determinadas medidas que se façam necessárias sem que se justifique a imposição do regime regulamentar como um todo (ANATEL, 2020b). Ou seja, permite-se uma atuação sob medida, mais proporcional.

O desenho da assimetria, na produção da norma e em sua aplicação presente e futura, dado seu caráter flexível, acima descrito, é um produto de considerações associadas às externalidades de rede e do relacionamento interdependente entre prestadores (ANATEL, 2017). Há que se reconhecer que, em se tratando de segurança cibernética, deve haver um limite razoável de assimetria benéfica, com a isenção de imposição de deveres excessivamente onerosos e que beirem a constituição de barreiras de entrada, a determinados prestadores (como as PPP), para que não se comprometam os objetivos gerais

perseguidos (ANATEL, 2020b).

Dado o caráter da governança estabelecida e do fluxo contínuo previsto para fixação de novas medidas, a assimetria continuará sendo modulada ao longo do tempo de aplicação do R-Ciber (ANATEL, 2017). Logo, é possível antever a criação de diferentes disciplinas para prestadoras e para fornecedores, por exemplo.

O compromisso regulatório com uma reflexão aberta para assimetria a cada etapa traz em si um risco não desprezível de efeitos negativos decorrentes de captura no que tange à distribuição dos custos para consecução dos objetivos gerais entre os regulados. Isto porque o juízo de consecução de finalidades com uma diferença de perdas e ganhos para diferentes grupos de regulados, inerente à função do regulador (PELTZMAN, 1976), deixa de ocorrer apenas no momento de expedição do regulamento, mas será efetivado a cada medida de sua aplicação com esse matiz.

Outra perspectiva associada tanto à assimetria quanto à natureza principiológica do R-Ciber é a de possibilitar que as prestadoras, respeitados os patamares mínimos, desenvolvam modelos de negócios nos quais os níveis de proteção constituam variáveis intrínsecas das ofertas de serviços. Tal aspecto, na perspectiva do regulador, atuaria como incentivo na medida em que diferenciais de oferta melhor podem aumentar o nível de satisfação dos usuários, especialmente daqueles de nichos, reduzir custos e fomentar a competição (ANATEL, 2020b).

Outro aspecto relacionado aos incentivos que a regulamentação coloca aos administrados diz respeito aos custos para seu cumprimento. Tendo em vista que as atividades relacionadas ao tema não são triviais, envolvem tecnologia geralmente no estado da arte e podem produzir impactos em cadeia, essa variável está presente tanto no juízo interno dos regulados acerca do ônus de cumprir ou não as obrigações, quanto no debate sobre os aspectos e formas dessas últimas, que é levado a cabo progressivamente pelo GT-Ciber, grupo técnico criado pelo R-Ciber, que será abordado na seção seguinte.

O R-Ciber deixa expressa a responsabilidade integral pelos ônus decorrentes da adoção e execução da Política de Segurança Cibernética e demais condutas e procedimentos nele exigidos. Abrange, dentre outros, orientações quanto à configuração de equipamentos entregues em comodato aos usuários ou a realização de ciclos de avaliação de vulnerabilidades.

Ponto de atenção, contudo, cabe à hipótese de outras medidas a serem impostas pelo próprio regulador a partir do funcionamento do sistema previsto de governança[2] (ANATEL, 2020a, b). Quanto a tais medidas, o que está estabelecido é que sua determinação se dará de forma motivada. Considerando os enunciados regulamentares à luz dos princípios de razoabilidade e proporcionalidade que regem a Administração Pública e as peculiaridades de intervenção sobre a atividade econômica, o impacto dos custos deverá ser necessariamente objeto de reflexão na construção dessas futuras medidas, o que revela

mais um ponto de complexidade para a governança responsiva.

Nesse sentido, verifica-se uma postura neutra atribuída ao próprio regulador. A coerência com a linha do R-Ciber de implementação cooperativa e de tendência responsiva exigirão uma constante ponderação de meios e fins que não ocorreria em um modelo diverso, de esgotamento *ex ante* de exigências de conformidade.

Na medida em que formalmente influirão na construção da disciplina temática, pode ser aventado que os resultados produzidos já trarão em si um balanceamento prévio dos incentivos acerca do custo-benefício do cumprimento ou descumprimento das regras. Diante disso, pode haver uma tendência mais natural de adesão à norma.

O risco existente continua sendo o de captura em sentido *lato* (DAL BÓ, 2006)[3], pelas razões exploradas no tópico relativo à governança, a seguir. Em um cenário de assimetria, a imposição de regimes diferenciados para distintos grupos pode ser utilizado por um deles, caso seja bem sucedido em influenciar o regulador, para impor maiores ônus ao outro com reflexos em competição, por exemplo.

Isso demonstra que a efetividade do regime de incentivos pretendido passa pela melhor ponderação dos custos a serem assumidos pelos regulados e, diante da existência de assimetrias, em uma distribuição de ônus que evite distorções permissivas de comportamentos *free-riding*.

4.3. Governança colaborativa

A tutela de um aspecto como a segurança cibernética pelo regulador possui um diferencial em relação a outras vertentes de sua atuação tais como aquelas relacionadas à proteção de direitos consumeristas dos usuários ou cumprimento de metas de expansão de infraestrutura. Para a segurança, pelas razões acima mencionadas, o *compliance* individual dos atores é significativo, mas é insuficiente dados os impactos transversais diretos e potencialmente negativos que as condutas de cada um deles podem ter sobre o ecossistema inteiro.

Põe-se ao regulador um desafio para engajamento coletivo dos entes privados, no sentido não só da observância de patamares técnicos mínimos, em práticas preventivas e corretivas, mas também de um fluxo constante de troca de informações, materializado no funcionamento de sistema de notificação e compartilhamento de dados sobre incidentes. Esse determinante do sucesso da regulação temática, pressupõe o estabelecimento de incentivos jurídicos e econômicos e aí se insere a constituição de grupo de governança multi-institucional, que pretende servir como plataforma para acomodar o diálogo multilateral.

Essa perspectiva de governança ocorre à luz de elementos históricos[4] recorrentes para o endereçamento do tema (RUTKOWSKI, 2011) e de experiências internacionais, a exemplo dos Centros de Compartilhamento e Análise de Informações (ISACs) na União Européia

(ENISA, 2018). Essas organizações foram constituídas para facilitar o compartilhamento de informações entre os setores público e privado, bem como para coletar informações sobre ameaças cibernéticas. Eles visam construir confiança por meio do compartilhamento de experiência, conhecimento e análise, especialmente sobre as causas raízes, incidentes e ameaças. Aspectos positivos que foram absorvidos no modelo brasileiro.

A constituição desse modelo permite, a um só tempo, a composição de um acervo de dados; a construção de canais permanentes de informação que facilitem reações instantâneas e sistêmicas a incidentes, com redução de danos; e a elaboração célere de novos patamares mínimos exigíveis para a conduta dos regulados.

Sob o viés jurídico-formal o Grupo Técnico de Segurança Cibernética e Gestão de Riscos de Infraestruturas Críticas (GT-Ciber), coordenado por autoridade do órgão regulador, é um foro de participação impositiva para prestadoras com poder de mercado significativo (PMS). Representantes de outras prestadoras, associações, órgãos e entidades poderão ter participação franqueada na discussão de seus temas de interesse. Sua gama de atribuições passa por atividades de observação e assessoramento interno, mas têm proeminência seu funcionamento como instância de proposição de requisitos técnicos e medidas específicas relativas a redes e de disposição sobre aspectos e formas de atendimento das obrigações relacionadas às políticas de segurança e avaliação de vulnerabilidades dos entes privados (ANATEL, 2020a).

O incentivo a uma participação efetiva dos prestadores decorre menos da imposição do que da possibilidade de materialização de seus próprios interesses em disposições que podem vir a ser cogentes para todo o ecossistema. Nesse ambiente expressamente pautado pelo diálogo e consenso, mas cuja decisão cabe à autoridade regulatória (ANATEL, 2020a), a persecução de soluções mais céleres quando comparadas com o rito administrativo tradicional, também pode resultar em maior razoabilidade para os resultados (ANATEL, 2017, ANATEL, 2020b).

Em um cenário onde esse mecanismo contempla obrigações para calibrá-las, não é difícil prever a constituição de arenas paralelas onde se verifique uma competição entre diferentes grupos para influenciar o regulador, em arranjos mais complexos do que uma vitória ou derrota total para os objetivos em jogo (BECKER, 1983). Isto porque as perspectivas entre grupos acerca dos deveres e correspondentes ônus a serem assumidos varia consideravelmente. Exemplo disso seria um movimento dos maiores prestadores por uma menor assimetria em relação aos PPP, de modo a retirar de si a assunção pela garantia da higidez do ecossistema como um todo.

Isso revela o desafio que esse modelo de governança impõe para os participantes e para o regulador. Diante de sua natureza, é possível que a ele se apliquem as considerações do modelo identificado como teoria do ciclo de vida das agências reguladoras (MARTIMORT, 1999) a título de reflexão.

Em linhas gerais, assume-se que a nova estrutura receba maior atenção institucional e passe por maior escrutínio na sequência de sua instalação. Com o passar do tempo, esse tipo de pressão tende a se reduzir, enquanto a pressão dos grupos de interesse das firmas permanece constante, a um tempo em que a burocratização das atividades também se mostraria crescente. Para que se evite tal risco, a supervisão regular do GT-Ciber por outras instâncias da Anatel, por órgãos de controle e pela sociedade, mostra-se recomendável.

Conclusões

A segurança cibernética no setor de telecomunicações sintetiza as vertentes mais sofisticadas do tema entre os setores de infraestrutura. Além disso, a nova geração tecnológica das redes móveis surge como um impulso transformador, destino de investimentos e de possibilidades extraordinárias no uso de serviços e aplicações de alto valor agregado, porém traz a reboque novas ameaças, riscos e preocupações em relação à segurança do espaço cibernético.

As referências sumarizadas neste artigo evidenciam a complexidade do tema e a necessidade do contínuo e aprofundado estudo sobre as possíveis soluções normativas e administrativas, delas decorrentes, que auxiliem na contenção do problema.

Diante dos novos desafios, o regulador de telecomunicações optou por uma intervenção técnica assimétrica e colaborativa, mais flexível, e atuação regulatória orientada aos riscos percebidos, em abordagens *ex ante* e *ex post*. Ademais, o foco na identificação dos incentivos é revelador da natureza econômica do tema e sua compreensão auxiliou o tomador de decisão na modulação do grau de intervenção regulatória. Desse modo, o produto da regulação contemplou, além dos aspectos técnicos e legais, a busca pelo alinhamento de incentivos das partes interessadas, a implementação colaborativa do novo arcabouço regulatório e a adoção de remédios orientados a corrigir falhas intrínsecas a esse mercado, cujos efeitos são definidores da postura dos agentes no tocante à segurança cibernética.

Uma vez que o caminho regulatório escolhido e que se começa a trilhar com a edição do Regulamento de Segurança Cibernética prevê a existência de um foro permanente de interações entre regulador e regulados para especificação de regras e construção de novas medidas é essencial que o juízo acerca da construção de incentivos seja igualmente duradouro e evite comportamentos nocivos para o ecossistema como um todo, tanto no tocante à cibersegurança quanto à competição.

Referências

– 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: Brasília.

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

– 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: Brasília.

– 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]. Disponível em 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*. Congresso Nacional: Brasília.

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

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

– 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 Segurança Institucional, Presidência da República: Brasília.

– BRASIL. 2010. *Livro Verde: Segurança Cibernética no Brasil.* Presidência da República, Gabinete de Segurança Institucional. Departamento de Segurança da Informação e Comunicações: Brasília.

– BRASIL. 2012. *Livro Branco de Defesa Nacional*. Presidência da República, Gabinete de Segurança Institucional. Departamento de Segurança da Informação e Comunicações: Brasília.

– 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*. Presidência da República: Brasília.

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

– BRASIL, 2020. *Decreto nº 10.222/2020: Aprova a Estratégia Nacional de Segurança Cibernética*. Presidência da República: Brasília.

– BRASIL, 2020. *Instrução Normativa nº 4/2020: Dispõe sobre os requisitos mínimos de Segurança Cibernética que devem ser adotados no estabelecimento das redes 5G*. Ministério de Estado do Gabinete de Segurança Institucional da Presidência da República: Brasília.

– CARVALHO, B.E.F.C., SANTOS, D.B.M. 2011. *Segurança de infraestruturas críticas no Brasil.* Conference Paper, XIX Simpósio Brasileiro 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. [Consult. 28 dez. 2020].

– INÁCIO, André – *Tecnologias de informação e segurança pública: um equilíbrio instável*. In: CIJIC. Revista Científica sobre *Cyberlaw*. Lisboa, n.1, 2016, p. 9. [Consult. 28 dez. 2020]. Disponível em: 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. [Consult. 31 dez. 2020]. Disponível em 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. Disponível online em: 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 Atualizado em 17/12/20, 23:07.

– UNIÃO INTERNACIONAL DE TELECOMUNICAÇÕES. 2018. *Global Cybersecurity Index V3*. Disponível em: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf

Sobre os 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 Em que pese a posterior revogação desse decreto, as previsões de ordem protetiva à segurança permaneceram inalteradas.

↑2 Por estar limitado a suas competências legais, não caberia ao regulador endereçar ou, à guisa de exemplo, isentar os regulados de ônus decorrentes de normativos e outras medidas expedidas por outros órgãos.

↑3 Para esse autor, em sentido lato, a captura regulatória vem a ser o processo pelo qual interesses específicos afetam a intervenção estatal em alguma de suas formas.

↑4 O elemento colaborativo vem sendo um dos pilares da construção do regime de regulação da segurança cibernética que pode ser rastreado desde suas origens, na Convenção de Dresden 1850 (RUTKOWSKI, 2011), em um crescendo que se inicia na associação entre administrações e reguladores nacionais distintos e começa a abarcar outros entes, sobretudo privados.