ANATEL Agência Nacional de Telecomunicações

ANÁLISE DE IMPACTO REGULATÓRIO

Segurança das redes de telecomunicações

JUNHO/2018

ANÁLISE DE IMPACTO REGULATÓRIO

Segurança das redes de telecomunicações

ELABORADO POR:

ANDRÉ MOTA DE ABREU IWASA – CPRP/SCP

DAVID SANTANA E SILVA BARRETO – GR08/SFI

DAVISON GONZAGA DA SILVA – ORCN/SOR

EDUARDO KRUEL MILANO DO CANTO – COQL/SCO

JEFERSON FUED NACIF - AIN

JOÃO ALEXANDRE MONCAIO ZANON – PRRE/SPR

PATRICIA LEAL COUTINHO – COQL/SCO

RAFAEL ANDRADE REIS DE ARAÚJO – PRRE/SPR

RENATA BLANDO MORAIS DA SILVA – PRRE/SPR

RENATO BIGLIAZZI – SRC

STEFAN RAFAEL LEANDRO MACHADO – ORCN/SOR

VANESSA COPETTI CRAVO – GR05/SFI

Nota Importante:

Esse Relatório de Análise de Impacto Regulatório é um instrumento de análise técnica, cujas informações e conclusões são fundamentadas nas análises promovidas pelo grupo de trabalho responsável pelo tema e assim não reflete necessariamente a posição final e oficial da Agência, que somente se firma pela deliberação do Conselho Diretor da Anatel.

ÍNDICE

INTRODUÇÃO

O presente Relatório de Análise de Impacto Regulatório – AIR tem como objetivo refletir sobre os atuais desafios relativos à segurança das redes de telecomunicações e analisar acerca da necessidade de atualizar a regulamentação setorial a respeito do tema.

O projeto está previsto no item nº 58 da Agenda Regulatória para o biênio 2017-2018, aprovada pela Portaria nº 491, de 10 de abril de 2017, e alterada pela Portaria nº 1, de 2 de janeiro de 2018, ambas do Conselho Diretor, sob o título de "Análise sobre a regulamentação de segurança das redes de telecomunicações" e apresenta seguinte descrição:

> "Elaboração de análises e estudos sobre a necessidade ou não de regulamentação que possibilite a implementação de medidas de proteção e segurança das redes e serviços das operadoras de telecomunicações. A segurança das redes é hoje um dos grandes problemas da nova economia digital. São diversos os países que vem enfrentando os problemas relacionados à segurança cibernética e realizando grandes investimentos na busca da disponibilidade, confidencialidade e integridade das informações no ambiente cibernético. Como os dados trafegam em redes de telecomunicações cabe à Anatel atuar dentro de suas competências a fim de garantir e fiscalizar a proteção dessa primeira linha de frente, a exemplo de outros reguladores como FCC (EUA), Anacom (Portugal), KISA (Coréia do Sul), Ofcom (Reino Unido) que atualizam constantemente suas diretrizes."

O projeto busca abordar um tema sempre presente nas discussões acerca do futuro da internet e das redes de telecomunicações. Com o advento da Internet das Coisas (IoT), o tema ganha ainda mais relevância devido à ubiquidade dos dispositivos conectados à rede.

Ainda, tal ação vai ao encontro das recentes diretivas de políticas públicas. A Estratégia Brasileira para a Transformação Digital (E-Digital), fruto do Grupo de Trabalho Interministerial, instituído pela Portaria nº 842, de 17 de fevereiro de 2017, do Ministério da Ciência, Tecnologia, Inovações e Comunicações (MCTIC), estabelece como um de seus eixos temáticos a "Confiança no Ambiente Digital" que é subdividido nos temas "Proteção de Direitos e Privacidade" e "Defesa e Segurança no Ambiente Digital".

A E-Digital foi instituída pelo Decreto nº 9.319, de 21 de março de 2018, e como ações estratégicas do eixo temático "Confiança no Ambiente Digital" destacam-se[1]:

> Estimular a definição e adoção de padrões e certificação de *privacy by design and default e security by design and default* (Categoria de Proteção de Diretos e Privacidade).
>
> Elaborar planos nacional e subnacionais de prevenção, resposta a incidentes e mitigação de ameaças cibernéticas, inclusive no âmbito de infraestruturas críticas.

[1] Disponível em: http://www.mctic.gov.br/mctic/export/sites/institucional/estrategiadigital.pdf. Acesso em 15/05/2018.

Estabelecer mecanismos de cooperação entre entes governamentais, entes federados e setor privado com vistas à adoção de melhores práticas, compartilhamento de informações, adoção de padrões adequados de segurança, coordenação de resposta a incidentes e proteção da infraestrutura crítica.

Treinar agentes públicos em segurança e mitigação de riscos cibernéticos e desenvolver parcerias para o treinamento de recursos humanos do setor privado.

Realizar campanhas educacionais amplas para expandir a conscientização da população sobre o tema da segurança da informação. (Categoria de Defesa e Segurança no Ambiente Digital).

Cumpre ressaltar que a E-Digital salienta que a Política Nacional de Segurança de Informação (PNSI) está sendo finalizada e será apresentada na forma de projeto de lei ao Congresso Nacional.

No mesmo sentido, o "Relatório do plano de ação - Iniciativas e Projetos Mobilizadores", um dos produtos do estudo "Internet das Coisas: um plano de ação para o Brasil", liderado pelo Banco Nacional de Desenvolvimento Econômico e Social (BNDES), em parceria com o Ministério da Ciência, Tecnologia, Inovações e Comunicações (MCTIC), reconhece o destaque da temática de segurança relacionada à IoT e apresenta os seguintes encaminhamentos[2]:

Cooperação internacional

- Aprimorar os mecanismos de cooperação internacional para a prevenção e tratamento de incidentes de segurança da informação como pela adesão a Acordos de Troca e Proteção Mútua de Informações Classificadas;
- Incentivar a adoção de padrões internacionais na temática de segurança da informação pela iniciativa privada.

Arranjo institucional brasileiro

- Estruturar governança baseada em modelo multissetorial, com a criação ou designação de estrutura específica para a coordenação de atividades baseadas em segurança da informação, na forma de conselho permanente, órgão/entidade pública ou agência reguladora independente. A entidade criada ou designada poderia apoiar a elaboração de políticas nacionais, criação de mecanismos de resposta a incidentes, dentre outras atribuições;
- Estimular a cooperação e interação entre o Poder Público, sociedade civil, iniciativa privada e academia, com o fim de promover medidas de conscientização e fomento da segurança da informação.

Incentivo à adoção de certificação voluntária de dispositivos

[2] Disponível em: http://www.mctic.gov.br/mctic/export/sites/institucional/tecnologia/SEPOD/politicasDigitais/arquivos/arquivos_estudo_iot/fase-3-9.pdf. Acesso em 15/05/2018.

- Incentivar a criação de sistema de certificação de segurança da informação em dispositivos em Internet das Coisas, baseada em modelo de autorregulação pela iniciativa privada. O modelo poderia ser baseado em auto avaliação voluntária, com a adoção de selo/sinalização de conformidade ao consumidor, o que evitaria alto custo de entrada;
- Mediante a consolidação do modelo de certificação voluntária, estruturar modelo de corregulação ou regulação híbrida para a certificação de dispositivos Internet das Coisas, com a participação de conselho multissetorial ou agência pública focada em segurança da informação.

Segurança da informação em infraestruturas críticas

- Fortalecer a estrutura institucional dedicada à segurança de infraestruturas críticas no âmbito da Administração Pública Federal, e incentivar os setores regulados a respeitarem aspectos mínimos de segurança da informação, em particular em setores de infraestrutura crítica.

A menção à IoT não é aleatória. A estimativa de custo anual dos crimes cibernéticos para a economia global é de mais de 445 bilhões de dólares, variando de uma visão mais conservadora de 375 bilhões até 575 bilhões[3]. A previsão com 200 bilhões de dispositivos IoT conectados à rede é que o custo alcance de 6 trilhões em 2021[4].Especificamente no Brasil, a previsão é de que o mercado de segurança cibernética cresça para 7,29 bilhões de dólares em 2019[5].

Internacionalmente, os problemas e desafios em matéria de segurança cibernética são um dos principais objetos de discussões nos mais importantes fóruns como Assembleia Geral das Nações Unidas (AGNU), União Internacional de Telecomunicações (UIT), Escritório das Nações Unidas sobre Drogas e Crime (UNODC), Fórum Econômico Mundial, G20, Organização para a Cooperação e Desenvolvimento Econômico (OCDE), Fórum de Governança da Internet (IGF), Corporação para da Internet para Atribuição de Nomes e Números (ICANN), entre outros.

Regionalmente, o assunto também é pauta na Organização dos Estados Americanos, principalmente no âmbito da Comissão Interamericana de Telecomunicações (CITEL) e no Comitê Interamericano contra o Terrorismo (CICTE), no Registro de Endereçamento da Internet para a América Latina e o Caribe (LACNIC), entre outros.

Além disso, a temática também é alvo de atuação bilateral, possuindo o Brasil acordos de cooperação com outros países.

No âmbito do tema, discute-se ainda sobre a existência de um arcabouço legislativo adequado e atualizado que possa prevenir e reprimir incidentes cibernéticos, prevendo, adicionalmente, sua tipificação

---

[3] Disponível em: https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/attachments/140609_McAfee_PDF.pdf. Acesso em 16/05/2018.

[4] Disponível em: https://cybersecurityventures.com/2015-wp/wp-content/uploads/2017/10/2017-Cybercrime-Report.pdf. Acesso em 15/05/2018.

[5] Disponível em: https://cybersecurityventures.com/cybersecurity-latin-america-q4-2015/. Acesso em 16/05/2018.

criminal. Tendo em vista a característica de transnacionalidade dos crimes cibernéticos, não é suficiente o enfrentamento nacional e isolado, exigindo uma atuação coordenada e cooperativa de todas as nações, uma vez que é possível envolver mais de uma centena de países em um único incidente.

Para enfrentar esse paradigma, no âmbito do Conselho da Europa foi gestada a Convenção sobre Crimes Cibernéticos (Council of Europe Convention on Cybercrime), Convenção nº 185, assinada em Budapeste, na Hungria, em 23 de novembro de 2001, também denominada de Convenção de Budapeste, contando com a adesão de 59 países, dos quais apenas 4 não a ratificaram[6]. Sua vigência iniciou em 1° de julho de 2004 com sua ratificação por 5 países, incluindo 3 países membros do Conselho da Europa. Além dos membros deste, outros países que não são membros assinaram a Convenção, quais sejam, África do Sul, Argentina, Austrália, Cabo Verde, Canadá, Chile, Costa Rica, Estados Unidos, Filipinas, Ilhas Maurício, Israel, Japão, Panamá, República Dominicana, Senegal, Sri Lanka e Tonga.

A Convenção, resultante de 4 anos de trabalho e 27 minutas, representa o maior esforço no âmbito regional e internacional para a repressão dos crimes cibernéticos. Sua importância não se limita às ratificações, uma vez que inúmeros países, ainda que não tenham aderido ao tratado, utilizaram o instrumento como inspiração para a elaboração e/ou atualização das suas legislações.

A Convenção é baseada nas seguintes premissas: necessidade de uma política criminal comum a fim de proteger a sociedade da criminalidade no ciberespaço; conscientização das profundas mudanças provocadas pela digitalização, pela convergência e pela globalização permanente das redes informáticas; preocupação com o risco de que as redes informáticas sejam utilizadas para a prática de infrações criminais, assim como de que as provas dessas infrações sejam por elas disseminadas; reconhecimento da necessidade de cooperação entre estados e o setor privado para o combate desse tipo de criminalidade, especialmente, destacando a imprescindibilidade de se preservar os interesses legítimos ligados ao uso e desenvolvimento das TICs; rápida e eficaz cooperação internacional em matéria penal como um imperativo para uma luta efetiva contra a criminalidade cibernética; necessidade da convenção para impedir atos contra a confidencialidade, integridade e disponibilidade de sistemas informáticos, de rede e dados informáticos, bem como sua utilização fraudulenta; necessidade de garantir um equilíbrio adequado entre os interesses de aplicação da lei e o respeito aos direitos fundamentais; esforços internacionais, notadamente da Organização das Nações Unidas (ONU), da Organização para a Cooperação e Desenvolvimento Econômico (OCDE) e do G8.

A preocupação mundial justifica-se não só pelo impacto à economia global, mas também pelas características desses incidentes. Quando se fala em incidente de segurança cibernética, deve-se primeiramente reconhecer a inerente transnacionalidade, podendo envolver centenas de países e milhares ou mesmo milhões de usuários, impondo a necessidade de cooperação entre as diversas jurisdições envolvidas.

Ainda nesta esteira, a União Europeia, por meio da Diretiva nº 2016/1148 (*Network and Information Security – NIS – Directive),* estabeleceu uma série de medidas, a serem adotadas pelos

[6] Disponível em https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185. Acesso em 25/06/2018.

Estados-membros, destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União Europeia. Entre as medidas estão a adoção de uma estratégia nacional de segurança das redes e dos sistemas de informação; criação de um grupo de cooperação, envolvendo os Estados-membros, Comissão Europeia e a Agência Europeia para a Segurança das Redes e da Informação (ENISA); criação de uma rede de CSIRTs (*Computer Security Incident Response Team)* entre os Estados-membros; o estabelecimento de requisitos de segurança e de notificação para prestadores de serviços essenciais e serviços digitais; e designação de autoridades nacionais competente e pontos de contato. A diretiva entrou em vigor em agosto de 2016, tendo sido dado um prazo de 21 meses para a realização da transposição da diretiva, prazo este que se encerrou em 9 de maio de 2018[7].

A fim de reforçar a pertinência do tema, cita-se brevemente a seguir os principais incidentes recentes.

Em outubro de 2016, o *malware* Mirai foi o responsável por um dos maiores ataques distribuído de negação de serviço (*Distributed Denial of Service - DDoS*) da história, situação em que a rede sofre um ataque de volumetria e não consegue responder à demanda, utilizando-se de um exército de zumbis (*botnet*) - dispositivos conectados à rede, dispositivos de *Internet of Things* (IoT) como câmeras IP, impressoras, babás eletrônicas, entre outros. O Brasil foi identificado com um dos países com maior quantidade de dispositivos infectados[8]. Foram atacados os servidores da empresa Dyn retirando do ar Twitter, Amazon, Netflix e Paypal por algumas horas.

Em maio de 2017 a comunidade internacional foi afetada pelo WannaCry, um vírus que explorava vulnerabilidade do Sistema Operacional Windows e que atingiu mais de 200 mil computadores em mais de 150 países[9]. O *software* malicioso criptografava os arquivos e exigia pagamento de resgate (*ransomware*) em *bitcoins* para sua liberação.

Um mês após, tem-se o surgimento de outros *ransomwares*: Petya/NotPetya/GoldenEye[10], seguido pelo *Bad Rabbit*[11]. Já em 2018, no Brasil foi verificada alta incidência de casos de clonagem de contas no aplicativo *WhatsApp*[12].

Em relatório disponibilizado pela CISCO, em 2018, foi apontado como um dos principais desafios atuais a expansão dos dispositivos *IoT* (Internet das Coisas) e a utilização de serviços em nuvem. O relatório

---

[7] Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016L1148&from=EN. Acesso em 25/06/2018.

[8] Disponível em: https://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/. Acesso em 16/05/2018 e https://jhalderm.com/pub/papers/mirai-sec17.pdf. Acesso em 16/05/2018.

[9] Disponívem em: http://www.bbc.com/news/technology-39913630. Acesso em 16/05/2018.

[10] Disponível em: https://www.kaspersky.com/blog/new-ransomware-epidemics/17314/. Acesso em: 16/05/2018.

[11] Disponível em: http://www.ctir.gov.br/arquivos/alertas/2017/ALERTA_2017_07_RansomwareBadRabbit.pdf. Acesso em 16/05/2018.

[12] Disponível em: http://www.ctir.gov.br/arquivos/alertas/2018/ALERTA_2018_02_whatsapp.pdf. Acesso em 16/05/2018.

aponta que *IoT botnets (*redes de dispositivos infectados) estão em crescimento, permitindo a ocorrência de ataques DDoS (ataque distribuído de negação de serviço) mais sofisticados[13].

Importa também ao debate assentar a competência da Agência relacionada à segurança das redes de telecomunicações. A Lei nº 9.472, de 16 de julho de 1997, Lei Geral de Telecomunicações (LGT) dispõe no art. 1º que compete à União, por intermédio da Agência, organizar a exploração dos serviços de telecomunicações, o que inclui "*o disciplinamento e a fiscalização da execução, comercialização e uso dos serviços e da implantação e funcionamento de redes de telecomunicações, bem como da utilização dos recursos de órbita e espectro de radiofrequências*". Nesse sentido, especifica o art. 19:

> Art. 19. À Agência compete adotar as medidas necessárias para o atendimento do interesse público e para o desenvolvimento das telecomunicações brasileiras, atuando com independência, imparcialidade, legalidade, impessoalidade e publicidade, e especialmente:
>
> (...)
>
> II - representar o Brasil nos organismos internacionais de telecomunicações, sob a coordenação do Poder Executivo;
>
> (...)
>
> IV - expedir normas quanto à outorga, prestação e fruição dos serviços de telecomunicações no regime público;
>
> (...)
>
> X - expedir normas sobre prestação de serviços de telecomunicações no regime privado;
>
> (...)
>
> XII - expedir normas e padrões a serem cumpridos pelas prestadoras de serviços de telecomunicações quanto aos equipamentos que utilizarem;
>
> XIII - expedir ou reconhecer a certificação de produtos, observados os padrões e normas por ela estabelecidos;

Assim, os dispositivos legais acima dão à Agência a competência em matéria de segurança das redes de telecomunicações[14]. Complementarmente, cumpre relembrar que existem outros foros que podem recomendar, de maneira complementar às competências da Anatel, requisitos técnicos sobre questões afetas à segurança de redes, como é o caso do CGI.br para questões de padrões de segurança e sigilo dos registros, dados pessoais e comunicações privadas, nos termos do §1º do artigo 13 do Decreto nº 8.771, de 11 de maio de 2016.

---

[13] Disponível em https://www.cisco.com/c/m/en_au/products/security/offers/cybersecurity-reports.html. Acesso em 25/06/2018. Relatório em anexo ao processo 53500.078752/2017-68.

[14] Disponível em http://www.anatel.gov.br/legislacao/leis/2-lei-9472

Ressalta-se que como a Agência representa o Brasil nos organismos internacionais de telecomunicações, sob coordenação do Poder Executivo (art. 19, II, da LGT), precisa ter condições e conhecimento para representar o país, repisando-se que o tema de segurança cibernética é um dos assuntos de maior relevância e controvérsia na agenda desses órgãos (talvez seja até mesmo o assunto mais importante no momento e no futuro das discussões nestes fóruns).

Ademais, a importância do assunto e o papel de representação nesses órgãos exigem que a Anatel tenha capacidade de internacionalizar as discussões exteriores com os diversos órgãos e entidades que internamente tem competência e interesse no tema, assim como auxiliar na coordenação dos interesses brasileiros a serem defendidos nesses fóruns.

Ainda sobre competência, a regulamentação do Marco Civil da Internet (Lei nº 12.965, de 23 de abril de 2014), feita por meio do Decreto nº 8.771, de 11 de maio de 2016, determinou, em seu art. 5º, § 2º, que cabe à Anatel a fiscalização e apuração das infrações quanto aos requisitos técnicos indispensáveis que permitiriam a discriminação ou degradação de tráfego (exceções à neutralidade), os quais também decorrem de tratamento de questões de segurança de redes, tais como restrição ao envio de mensagens em massa (*spam*) e controle de ataques de negação de serviço. Nesse sentido, a Anatel expressamente passou a ser competente para fiscalizar e realizar o acompanhamento e controle das regras de neutralidade, precisando ter condições e recursos humanos e técnicos de avaliar se a quebra da neutralidade estaria amparada, pois decorreria da gestão de segurança das redes.

Um dos fóruns de maior atuação internacional da Agência é notadamente a UIT, agência especializada das Nações Unidas paras as Tecnologias de Informação e Comunicação (TICs), a qual é a moderadora/facilitadora líder da Linha de Ação C.5 do Plano de Ação de Genebra da 1º Fase da Cúpula Mundial sobre a Sociedade da Informação, que trata do Princípio de Criação de Confiança e Segurança na Utilização das TICs.

Em cumprimento ao seu mandato, a UIT tem desenvolvido diversas iniciativas relacionadas à segurança cibernética, envolvendo todos os setores da União, quais sejam, os setores de radiocomunicação (UIT-R), normalização (UIT-T) e desenvolvimento das telecomunicações (UIT-D)[15].

Em 2007 a UIT lançou a Agenda Global de Segurança Cibernética (AGSC)[16] como arcabouço que permite às múltiplas partes interessadas participar na cooperação internacional. Esse arcabouço está estruturado em cinco pilares estratégicos orientados à luta contra ameaças cibernéticas que incluem medidas legais; medidas técnicas e procedimentais; estrutura organizacional; capacitação e cooperação internacional.

A fim de verificar o grau de comprometimento dos Estados Membros e no intuito de aumentar a conscientização sobre Segurança Cibernética, a UIT lançou o Índice Global de Segurança Cibernética

[15] Informação sobre todas as atividades da UIT na matéria estão disponíveis em: https://www.itu.int/en/action/cybersecurity/Pages/default.aspx. Acesso em 16/05/2018.

[16] Informações sobre a AGSC disponível em: https://www.itu.int/en/action/cybersecurity/Pages/gca.aspx. Acesso em 16/05/2018.

(*Global Cybersecurity Index - GCI*), tendo como referência os cinco pilares da AGSC. Atualmente, o GCI encontra-se na sua terceira interação, na fase de resposta ao questionário.

O Brasil, representado pela Anatel, respondeu às duas interações anteriores, ficando na 38° posição geral, como país em que a segurança está em fase de maturação (as três categorias mencionadas são líderes, em maturação e iniciantes)[17] e em 5º lugar na Região das Américas, atrás dos Estados Unidos, Canadá, México e Uruguai.

Menciona-se ainda como iniciativas da UIT: Programa Nacional de Grupos de Segurança e Resposta a Incidentes (*Computer Incident Response Teams – CIRTs*), que envolve a avaliação, implantação e a condução de simulações de incidentes; Proteção das Crianças na Rede (*Child Online Protection - COP*); Repositório de Estratégias Nacionais de Segurança Cibernética; Questão de Estudo 3/2 da Comissão de Estudos 2 da UIT-D; Grupo de Estudos 17 da UIT-T; dentre diversas outras ações.

Tem pertinência ao presente trabalho o Relatório final da Questão de Estudos 22 da Comissão de Estudos 1 da UIT-D do ciclo de 2006-2010[18], uma vez que oferece aos administradores nacionais um arcabouço gerencial flexível para a abordagem da questão da segurança cibernética no âmbito interno, sendo dividido em cinco partes, as quais versam sobre o desenvolvimento e a obtenção de um consenso acerca da estratégia nacional de segurança cibernética; o estabelecimento de colaboração nacional entre governo e indústria; o combate aos crimes cibernéticos; a criação de capacidade de gerenciamento nacional de incidentes; e a promoção de uma cultura nacional de segurança cibernética. Em cada uma das partes existe uma explanação dos objetivos a serem atingidos e de passos específicos para alcançá-los.

Tratamento internacional

Após essa breve visão da atuação da UIT na temática, relata-se atuação de órgãos reguladores de telecomunicações em outros países.

Estados Unidos – *Federal Communications Commission* (FCC)

Segurança cibernética é uma das mais altas prioridades da FCC[19], que fiscaliza as redes de comunicação privadas como um dos componentes de um esforço maior para proteção das infraestruturas críticas de comunicação e dos cidadãos contra atores criminosos.

A atuação da FCC inclui a obrigação de que os provedores de serviço adotem medidas para proteger a sua rede, uma vez que os provedores tem a obrigação de proteger seus consumidores. A gestão razoável da rede inclui práticas para a garantia da segurança e integridade da rede, incluindo o tratamento de

[17] Disponível em: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-R1-PDF-E.pdf. Acesso em: 25/04/2018.
[18] Disponível em: https://www.itu.int/dms_pub/itu-d/opb/stg/D-STG-SG01.22-2010-PDF-E.pdf. Acesso em 01/06/2010.
[19] Disponível em: https://apps.fcc.gov/edocs_public/attachmatch/DOC-343096A1.pdf. Acesso em 14/06/2018.

tráfego nocivo à rede, como ataques DoS. A Comissão possui uma divisão específica no âmbito do *Public Safety and Homeland Security Bureau*, chamada de *Cybersecurity and Communications Reliability Division* (CCR).

A FCC também possui o *Communications Security, Reliability and Interoperability Council* (CSRIC), que é um Comitê Assessor composto por entidades do setor privado, associações e organizações não governamentais constituída para oferecer recomendações ao Conselho de Diretores da FCC quanto a melhores práticas e ações que a FCC pode implementar para garantir a segurança e a interoperabilidade dos sistemas de comunicações.

Conforme relatado no *FCC White Paper: Cybersecurity Risk Reduction*[20].As principais ações da FCC incluem: promoção de melhores práticas; consideração antecipada das questões de segurança cibernética e não tardia, como o conceito de *security by design* e a obrigação das licenças para redes sem fio 5G submeterem um plano de segurança cibernética antes do início das operações; aumento da conscientização; aprimoramento da troca de informações; e estabelecimento de uma visão integral de segurança cibernética para o interesse público.

Em fevereiro de 2013 o Governo dos Estados Unidos emitiu a Ordem Executiva 13636, "Melhorando a Segurança Cibernética das Infraestruturas Críticas", que determinou o desenvolvimento de uma "abordagem priorizada, flexível, reprodutível, baseada em desempenho e de custo razoável" para gerenciar os riscos de segurança cibernética para processos, informações e sistemas diretamente envolvidos na prestação de serviços de infraestruturas críticas. Daí, um arcabouço para segurança cibernética foi desenvolvido pelo Instituto Nacional de Padrões e Tecnologia (2014 NIST *Framework*) em colaboração com a indústria. Este arcabouço fornece orientação para uma organização na gestão de riscos de segurança cibernética. É uma abordagem baseada em risco para o gerenciamento da segurança cibernética.

O CSRIC recomendou uma abordagem compreensiva para o gerenciamento dos riscos cibernéticos do setor baseada na 2014 NIST *Framework*.

Desde 2014 a FCC trabalha com um novo paradigma de que, apesar de considerar a liderança do setor privado, atua quando os incentivos de mercado não são suficientes para enfrentar adequadamente aos riscos cibernéticos.

A FCC exige que os prestadores de serviço notifiquem interrupção de serviço, incluindo a causa suspeita e as ações para remediar e restabelecer o serviço. Essas informações abastecem o *Network Outage Reporting System* (NORS), sendo esses dados utilizados pelo Centro de Integração Nacional de Segurança Cibernética e Comunicações (NCCIC), a fim de suportar consciência situacional, e para guiar a atuação da FCC. Em 2016 o rol de notificações foi ampliado e continua em consulta nova ampliação, a fim de abranger a notificação de outros incidentes de segurança.

[20] Disponível em: https://apps.fcc.gov/edocs_public/attachmatch/DOC-343096A1.pdf. Acesso em 14/06/2018

Quanto ao princípio de *security by design*, a FCC tem se aproveitado da fase de desenvolvimento das redes 5G para incentivar que o princípio seja incorporado no processo de desenvolvimento, a fim de mitigar os riscos associados com IoT.

Portugal - Autoridade Nacional de Comunicações de Portugal – ANACOM

A Anacom sucede nas atribuições e competências a Comissão de Planeamento de Emergência das Comunicações (CPEC) e integra funções em matéria de planeamento civil de emergência. Além disso, detém competências específicas no que se refere ao funcionamento das redes e dos serviços de telecomunicações em situações de emergência ou de força maior, bem como no acesso aos serviços de emergência pelos serviços telefônicos, nomeadamente através do número único de emergência europeu 112.

Com a entrada em vigor da Lei nº 51/2011, de 13 de setembro de 2011, a Anacom adquiriu novas competências ao nível da segurança das redes e serviços de comunicações e às empresas reguladas foram cometidas obrigações em matéria de segurança e integridade destas redes e serviços (artigos 54.º-A a 54º-G).

De acordo com os estatutos da Anacom, é atribuição dessa Autoridade promover a normalização técnica no setor das comunicações eletrônicas e áreas relacionadas, em colaboração com outras organizações. Neste contexto, a Anacom promove o debate sobre trabalhos normativos na área da segurança em sistemas de informação, em especial no que diz respeito às comunicações eletrônicas.

A Anacom também promove a sensibilização e a promoção de boas práticas de defesa da confidencialidade das comunicações e dinamiza as discussões sobre normalização organizando seminários e divulgando os trabalhos de normalização provenientes da ISO/IEC JTC1/SC27 com potencial impacto nas comunicações eletrônicas.

A Anacom possui na sua estrutura uma Direção de Segurança das Comunicações (DSC), ligada diretamente ao Conselho de Administração do órgão, com a missão de assegurar a supervisão e a regulação do setor e atuar como coadjuvante do Governo no âmbito da segurança das comunicações, como, por exemplo, integridade das redes e serviços de comunicações eletrônicas; e proteção dos dados pessoais e da privacidade no setor. Além disso, também assegura e promove a normalização técnica e a gestão e disponibilização do sistema de informação sobre infraestruturas de rede.

No nível regulatório, a Anacom baseia suas ações nos aspectos das notificações de violações de segurança e de perdas de integridade. Para atingir esse objetivo a Anacom estipula várias obrigações para as empresas que oferecem redes de comunicações públicas ou serviços de comunicações electrônicas acessíveis ao público e concretizam competências, poderes e deveres de informação para a Autoridade. A Anacom define as circunstâncias, o formato e os procedimentos aplicáveis às exigências de comunicação de violações de segurança ou perdas de integridade das redes.

Reino Unido - Ofcom

Segurança cibernética é uma das mais altas prioridades para o governo do Reino Unido e a Estratégia Nacional de Segurança Cibernética ressaltou que a regulação tem um importante papel garantindo que a segurança cibernética seja adequadamente endereçada, especialmente por empresas operando infraestruturas críticas nacionais.

O Ofcom e os fornecedores de redes e serviços de comunicações estão sujeitos a requisitos estabelecidos no artigo 13-A do "*Framework Directive*" e nas seções 105A-D da Lei de Comunicações do Reino Unido[21], o que inclui exigir que os operadores gerenciem adequadamente os riscos de segurança, minimizem os impactos nos consumidores e relatem quaisquer falhas de segurança ou falhas de rede à Ofcom. Em maio de 2011, o Ofcom publicou as primeiras diretrizes sobre toda a gama de requisitos de segurança. Essas orientações foram atualizadas em agosto de 2014 concedendo maior qualidade às informações recebidas e de forma a refletir a mudança relativa à importância dos diferentes serviços nos últimos anos. A orientação também estabelece expectativas para uma abordagem baseada em risco para a gestão da segurança. O documento destaca fontes apropriadas de melhores práticas da indústria e detalha os requisitos de relatórios de incidentes.

O regulamento que se intitula "Diretrizes sobre requisitos de segurança nas seções 105-A a 105-D da lei de Comunicações de 2003" é direcionado aos provedores relevantes, define as condições em que se devem reportar os incidentes de segurança e o que o Ofcom considera ser de impacto significativo.

Os elementos mais relevantes da regulamentação britânica ajudam a mitigar os riscos levando em consideração os seguintes requisitos:

a) A rede e os prestadores de serviços devem tomar medidas adequadas para gerir os riscos para a segurança, nomeadamente para minimizar o impacto nos usuários finais e nas redes interligadas;

b) Os provedores de rede devem tomar todas as medidas apropriadas para proteger, na medida do possível, a disponibilidade da rede;

c) Os fornecedores de redes e de serviços devem comunicar à Ofcom os incidentes de segurança ou reduções de disponibilidade que tenham um impacto significativo na rede ou no serviço;

d) O Ofcom deve, quando julgar conveniente, notificar os reguladores de outros Estados-Membros, a Agência Europeia para a Segurança das Redes e da Informação (ENISA), o público, sobre quaisquer relatórios recebidos;

e) O Ofcom deve enviar um resumo anual dos relatórios à Comissão Europeia e à ENISA;

[21] https://www.ofcom.org.uk/consultations-and-statements/category-1/cfi-security-resilience e https://www.ofcom.org.uk/__data/assets/pdf_file/0021/51474/ofcom-guidance.pdf

f) O Ofcom pode exigir que uma rede ou prestador de serviços submeta e pague uma auditoria das medidas que está tomando para cumprir os novos requisitos; e

g) O Ofcom pode utilizar as disposições de recebimento de informações e aplicação da lei para investigar, retificar e sancionar qualquer infração a estes requisitos.

Ressalta-se que o Ofcom requer que os provedores designem um ponto de contato para demandas urgentes. Com relação ao prazo para notificação, o Ofcom exige que incidentes urgentes sejam informados preferencialmente dentro do prazo de 3 horas de sua detecção, sendo que os demais eventos seguem uma tabela de prazos diferenciada.

Terminologia

No escopo do presente projeto, mostra-se importante a definição do termo "Segurança Cibernética". O Setor de Normalização da UIT define segurança cibernética de forma bastante ampla[22]:

> É o conjunto de ferramentas, políticas, conceitos de segurança, salvaguardas de segurança, diretrizes, abordagens de gestão de riscos, ações de treinamento, melhores práticas, garantias e tecnologias que podem ser usados para proteger o ambiente cibernético e ativos de usuários e de organizações. Ativos de usuários e organizações incluem dispositivos de computação conectados, pessoal, infraestrutura, aplicações, serviços, sistemas de telecomunicações, e a totalidade das informações transmitidas e/ou armazenadas no ambiente virtual. A Segurança Cibernética se esforça para assegurar a obtenção e a manutenção das propriedades de segurança de ativos dos usuários e das organizações contra relevantes riscos de segurança no ambiente cibernético. Os objetivos gerais de segurança incluem: disponibilidade, integridade e confidencialidade (tradução nossa).

Ressalta-se que a terminologia "segurança cibernética" é reconhecida nacional, regional e internacionalmente, sendo a nomenclatura adotada pela UIT e expressamente mencionada em resoluções da AGNU[23]. Além disso, também é utilizada por órgãos de normalização como a *International Organization for Standardization – ISO*[24].

No Brasil, a Portaria nº 45, de 8 de setembro de 2009, do Gabinete de Segurança Institucional da Presidência da República[25] define, em seu art. 2º, segurança cibernética como "*a arte de assegurar a existência e continuidade da Sociedade da Informação de uma Nação, garantindo e protegendo, no Espaço Cibernético, seus Ativos de Informação e suas Infraestruturas Críticas*".

---

[22] Recomendação nº X.1205 – *Overview of cybersecurity*, disponível em: <http://www.itu.int/rec/T-REC-X.1205-200804-I>. Acesso em: 23/04/2018.

[23] Resolução 57/239 – Criação de uma Cultura Global de Segurança Cibernética Disponível em: .http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/57/239. Acesso em: 14/05/2018.

[24] ISO/IEC 27032. Disponível em: - https://www.iso.org/obp/ui/#iso:std:iso-iec:27032:ed-1:v1:en. Acesso em 16/05/2018.

[25] Disponível em http://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?jornal=1&pagina=2&data=09/09/2009.

A terminologia também é utilizada nas publicações do GSI[26]: Livro Verde – Segurança Cibernética no Brasil e Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética da Administração Pública Federal 2015-2018.

Também se verifica a utilização dessa nomenclatura na E-Digital recentemente publicada. Nesse mesmo documento, é citada a finalização da Política Nacional de Segurança da Informação, desde já se notando a preferência pela terminologia "Segurança da Informação".

Salienta-se que "Segurança da Informação", internacionalmente, é uma terminologia mais restrita e é identificada com a preservação dos atributos da informação: confidencialidade, integridade e disponibilidade[27].

Tendo em vista o exposto, opta-se pela terminologia "Segurança Cibernética". No entanto, independentemente da nomenclatura utilizada, é preciso ter clareza que a atuação da Agência nessa seara restringe-se ao setor de telecomunicações, nos termos de suas competências legalmente estabelecidas.

Vencidas as questões acima expostas na introdução, passa-se às temáticas que serão tratadas no presente relatório de Análise de Impacto Regulatório. Ao longo das discussões no âmbito da equipe do presente projeto, foram identificados os seguintes temas:

- *Tema 01 – Governança da Segurança Cibernética;*
- *Tema 02 – Processos referentes à Segurança Cibernética;*

  Subtema 1 – Compartilhamento de informações sobre incidentes;

  Subtema 2 - Estrutura organizacional, gestão da Segurança Cibernética e Infraestruturas críticas;

  Subtema 3 – Cultura de segurança por parte dos consumidores.
- *Tema 03 – Produtos para telecomunicações;*
- *Tema 04 – Requisitos técnicos para operação das redes;*
- *Tema 05 – Armazenamento seguro de dados pessoais.*

[26] Disponível em http://dsic.planalto.gov.br/assuntos/publicacoes

[27] ISSO/IEC 27000. Disponível em: https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-5:v1:en:term:3.10. Acesso em 16/05/2018.

TEMA 01: Governança da Segurança Cibernética

SEÇÃO 1
RESUMO DA ANÁLISE DE IMPACTO REGULATÓRIO

Descrição introdutória do Tema

Em consonância com o crescente número de incidentes cibernéticos no ambiente digital, a segurança cibernética se torna cada vez mais uma preocupação de Governos visto que a infraestrutura nacional é fortemente dependente de redes privadas e pode ser sensivelmente afetada por eventuais ataques cibernéticos.

Nesta esteira, encontra-se na Subchefia para Assuntos Jurídicos da Casa Civil Projeto de Lei que dispões sobre a Política Nacional de Segurança da Informação (PNSI) que prevê ações específicas a serem implementadas pelas Agências Reguladoras de seus respectivos setores, entres as quais se pode citar a definição de regras de implementação da gestão de segurança da informação, implementação de práticas de gestão de riscos e a coordenação de ações referentes à segurança da informação.

Por mais que não haja, ainda, previsibilidade de aprovação do projeto, mostra-se extremamente oportuno avaliar a atuação da Agência como promotora das ações elencadas, tendo em vista a total sinergia com o projeto da Anatel.

Neste sentido, o presente tema contempla a avaliação da pertinência da criação de um fórum específico para endereçamento de questões relativas à segurança cibernética.

Qual é o contexto do problema?

Hoje, na Anatel, há diversos grupos técnicos sendo conduzidos juntamente com as prestadoras de serviços de telecomunicações para a condução de ações específicas. Entre eles, podemos citar os GT-SITTEL (Sistema de Investigações Telefônicas e Telemáticas), GT-CEMI (Cadastro de Estações Móveis Impedidas), GT-SIGA (Sistema Integrado de Gestão de Aparelhos), GT-LOC (Localização em chamadas de emergência), GT-RISCOS (Grupo Técnico de Segurança das Infraestruturas Críticas e Desastres) e GT-REDES(Grupo Técnico de Desempenho e Disponibilidade das Redes), entre outros. Em especial, o GT-RISCOS e o GT-REDES possuem alguma sinergia com o tema. No entanto, não há um fórum específico para tratar de questões específicas de segurança cibernética.

Historicamente, a Anatel realizou algumas ações neste sentido utilizando-se, como instrumento, o envio de Ofícios às prestadoras para adoção de medidas. A solicitação de bloqueio da porta 25/TCP com o intuito de mitigar ações de *spam* e a solicitação de guarda do registro de portas lógicas quando do compartilhamento do endereço público IPv4, com o objetivo de auxiliar nas ações investigativas de crimes cibernéticos são exemplos destas ações.

Ademais, nos dois ciclos de gestão de riscos (2014 e 2016), a Anatel incluiu questões sobre segurança da informação no questionário respondido pelas prestadoras para identificação de possíveis vulnerabilidades tanto em relação à segurança física quanto em relação à segurança cibernética a que estavam submetidas as redes das operadoras dos serviços de SMP ("telefonia celular e banda larga móvel"), STFC ("telefonia fixa") e SCM ("banda larga fixa").

Em 2015, a Agência editou o Regulamento sobre Gestão de Risco das Redes de Telecomunicações e Uso de Serviços de Telecomunicações em Desastres, Situações de Emergência e Estado de Calamidade Pública, aprovado pela Resolução nº 656 de 17 de agosto de 2015.

Cumpre ressaltar que a Anatel fez parte do grupo voltado à segurança cibernética quando da preparação para os Jogos Olímpicos Rio 2016, coordenado pelo CDCiber do Exército, quanto a possíveis ataques que estariam sujeitas as redes de telecomunicações, tanto no tocante ao usuário dos serviços de telecomunicações como a rede de dados usada para a comunicações de informações relevantes ao evento (rede *games*).

Adicionalmente, destaca-se o processo nº 53500.006013/2014, que tratou das denúncias sobre o monitoramento internacional de comunicações eletrônicas e telefônicas no Brasil (caso *Edward Snowden*), em que foi solicitado pelo Ministério das Comunicações a adoção de medidas cabíveis, na esfera administrativa, para esclarecimento das denúncias. Na ocasião, o processo foi conduzido pela Superintendência de Fiscalização da Anatel (SFI).

Por fim, deve-se analisar a necessidade de um nivelamento de comprometimento do setor de telecomunicações, como um todo, em questões de segurança cibernética.

Qual o problema a ser solucionado?

Existe um baixo grau de institucionalização da segurança cibernética no setor de telecomunicações, inexistindo mecanismos efetivos que promovam a necessária e ampla participação de todas as prestadoras de serviços de telecomunicações, envolvendo desde as grandes prestadoras até as de menor porte, assim como a articulação da Anatel com demais órgãos de governo.

A Agência tem competência para atuar sobre o problema?

A competência da Anatel para atuar no problema se origina na Lei Geral de Telecomunicações (Lei nº 9.472 de 1997), particularmente, em seu art. 19:

> Art. 19. À Agência compete adotar as medidas necessárias para o atendimento do interesse público e para o desenvolvimento das telecomunicações brasileiras, atuando com independência, imparcialidade, legalidade, impessoalidade e publicidade, e especialmente:
>
> (...)

IV - expedir normas quanto à outorga, prestação e fruição dos serviços de telecomunicações no regime público;

(...)

X - expedir normas sobre prestação de serviços de telecomunicações no regime privado;

Qual(is) o(s) objetivo(s) da ação?

Analisar a oportunidade e pertinência de oferecer uma abordagem institucional da segurança cibernética nas redes de telecomunicações e buscar um maior nivelamento de comprometimento em relação a este tema, tanto da Agência, quanto das prestadoras de serviços de telecomunicações em seus diferentes portes empresariais.

Como o tema é tratado no cenário internacional?

Como citado na parte introdutória da presente AIR, a FCC possui um Comitê Assessor: o *Communications Security, Reliability and Interoperability Council* (CSRIC), multissetorial, constituído para oferecer recomendações ao Conselho de Diretores da FCC quanto a melhores práticas e ações que a FCC pode implementar para garantir a segurança e a interoperabilidade dos sistemas de comunicações.

Na Anacom a importância do tema é refletida e institucionalizada em seu organograma, visto que a autoridade possui a Direção de Segurança das Comunicações (DSC) diretamente subordinada ao Conselho de Administração, ao lado das demais diretorias (regulação de mercado, gestão do espectro, fiscalização, informação e consumidores, entre outras).

A Estratégia Nacional de Segurança Cibernética do Reino Unido ressaltou o importante papel da regulação. Assim o Ofcom busca garantir que a segurança cibernética seja adequadamente endereçada, especialmente por empresas operando infraestruturas críticas nacionais.

Relatório final da Questão de Estudos 22 da Comissão de Estudos 1 da UIT-D do ciclo de 2006-2010[28], que oferece aos administradores nacionais um arcabouço gerencial para o tratamento e para a organização da abordagem da questão da segurança cibernética no âmbito interno, identifica como um dos itens principais dessa abordagem a necessidade de colaboração nacional entre governo e indústria, destacando que a proteção da infraestrutura crítica é uma responsabilidade compartilhada e conquistada somente através da colaboração entre governo e setor privado, que detém e opera grande parte da infraestrutura. Como metas, tem-se o desenvolvimento de relações de colaboração entre governo e indústria que trabalhem efetivamente para gerenciar o risco cibernético e proteger esse ambiente; e o fornecimento de um mecanismo para congregar a variedade de perspectivas, de ações e de conhecimento e alcançar um consenso, e, assim, possibilitar o aumento de segurança em nível nacional.

[28] Disponível em: https://www.itu.int/dms_pub/itu-d/opb/stg/D-STG-SG01.22-2010-PDF-E.pdf. Acesso em 01/06/2018.

Já como objetivos específicos, identifica: inclusão das perspectivas da indústria já nos estágios iniciais de desenvolvimento e implementação da política de segurança e esforços relacionados; encorajamento do desenvolvimento de grupos de diferentes indústrias de infraestrutura crítica no setor privado para tratar interesses de segurança em comum, colaborando com o governo; agrupamento de grupos do setor privado com o governo em fóruns confiáveis para o tratamento de dificuldades comuns de segurança cibernética; encorajamento da cooperação entre grupos de indústrias interdependentes; e estabelecimento de acordos de cooperação entre governo e setor privado para o gerenciamento de incidentes.

Quais os grupos afetados?

- Prestadoras de serviços de telecomunicações;
- Anatel;
- Consumidores.

Quais são as opções regulatórias consideradas para o tema?

- *Alternativa A – Manutenção do status quo;*
- *Alternativa B –Comitê específico na Anatel sobre o tema;*
- *Alternativa C – Aproveitamento da estrutura do GGRR;*
- *Alternativa D – Indicação de área específica da Anatel responsável pelo acompanhamento do tema;*

SEÇÃO 2
ANÁLISE DAS ALTERNATIVAS

Alternativa A

Manutenção do status quo

Neste cenário, opta-se pela manutenção da regulamentação atual e pela ausência de um fórum específico para tratamento de questões relativas à segurança cibernética. Desta forma, as demandas e ações referentes a este tema seriam tratadas pontualmente, caso a caso.

Este cenário não apresenta custos para a Agência e aos demais envolvidos. No entanto a temática "Segurança Cibernética" não usufruiria de um fórum institucional dentro da Anatel. Por possuir pouca aderência à resolução do problema identificado, tal alternativa somente se justifica se os custos das demais alternativas superarem seus benefícios.

Alternativa B

Comitê específico na Anatel sobre o tema

A existência de um Comitê específico, nos termos previstos no Regimento Interno da Anatel, para discussões e deliberações acerca da segurança cibernética nas redes de telecomunicações confere uma abordagem institucional do tema dentro da Agência e sinaliza para o setor a importância e a necessidade de acompanhamento desta temática.

O acompanhamento de eventuais requisitos ou ações demandadas pela Agência seria realizado neste fórum, assim como a avaliação sobre a necessidade de adoção pela Agência de novas ações. Nesse sentido, este Comitê específico seria a interface da Anatel na cooperação multissetorial e responsável pelo acompanhamento de relatórios de segurança enviados pelas prestadoras de serviços de telecomunicações. Esse acompanhamento pode ter um uso interessante na definição de campanhas educacionais e nas atividades de cooperação internacional.

Especificamente sobre este último ponto, observa-se que esse fórum poderia auxiliar na internalização de decisões, padrões e recomendações de organismos internacionais de telecomunicações, nos quais a Anatel representa o Brasil, sob coordenação do Poder Executivo (art. 19, II, da LGT), bem como na construção de posicionamentos a serem levados a esses órgãos, nos quais a temática de segurança cibernética tem tido constante destaque. Na qualidade de custos desta alternativa, estão aqueles decorrentes dos procedimentos normativos e administrativos para instituição de um novo Comitê no âmbito da Agência.

Por se tratar de Comitê, este dever ser presidido por um Conselheiro da Agência, nos termos das competências estabelecidas no inciso XVI do artigo 134 do Regimento Interno da Agência.

Alternativa C

Aproveitamento da estrutura do GGRR

O Regulamento sobre Gestão de Risco das Redes de Telecomunicações e Uso de Serviços de Telecomunicações em Desastres, Situações de Emergência e Estado de Calamidade Pública, aprovado pela Resolução nº 656, de 17 de agosto de 2015, prevê, em seu art. 8º, a existência do Grupo de Gestão de Riscos e Acompanhamento do Desempenho das Redes de Telecomunicações (GGRR) o qual define os prazos e formatos das informações que as prestadoras (excluem-se as prestadoras de pequeno porte) devem enviar sobre sua infraestrutura de telecomunicações, capacidades, desempenho e ocorrências, abrangendo no mínimo: as respostas a questionários, formulados pela Anatel, referentes à infraestrutura da prestadora, as informações referentes aos inventários de elementos de redes e rotas e as informações que permitam compor indicadores de disponibilidade e desempenho. O regulamento também traz uma série de atribuições ao Grupo que visam o acompanhamento da gestão de riscos e do desempenho das redes de telecomunicações.

Trata-se de um grupo composto por integrantes de cada uma das Superintendências finalísticas da Agência e por representantes das prestadoras de serviços de telecomunicações abrangidas pelo regulamento, cujo regimento interno, aprovado pela Portaria nº 36, de 14 de janeiro de 2016, atribuiu a coordenação do grupo à Superintendência de Controle de Obrigações da Anatel (SCO) e instituiu dois grupos técnicos com a finalidade de assessorar o GGRR: o Grupo Técnico de Segurança das Infraestruturas Críticas e Desastres (GT-RISCOS) e o Grupo Técnico de Desempenho e Disponibilidade das Redes (GT-REDES).

Vale ressaltar que o regimento interno do GGRR prevê a criação de outros grupos técnicos, por decisão do GGRR, para a realização de atividades complementares ou atendimento de novas demandas.

Portanto, há a possibilidade de se aproveitar a estrutura do GGRR com a criação ou alteração de um grupo técnico que se destine a tratar de questões de segurança cibernética.

Entre as fragilidades deste modelo está a ausência de um Conselheiro presidindo o grupo, como acontece nos Comitês instituídos pela Anatel. Além disso, segurança cibernética, na concepção da definição da UIT parece extrapolar o escopo do GGRR e do próprio Regulamento sobre Gestão de Risco das Redes de Telecomunicações e Uso de Serviços de Telecomunicações em Desastres, Situações de Emergência e Estado de Calamidade Público, uma vez que tais foros preocupam-se essencialmente com a segurança física de tais infraestruturas de redes, e não com a segurança em um nível lógico, como propõe o conceito de segurança da informação ou segurança cibernética.

Ressalva-se, no entanto, que a opção por esta alternativa poderia ser operacionalizada com a proposição de alterações na estrutura de governança do grupo para conferir um maior nível de institucionalização ao tema.

Alternativa D

Indicação de área específica da Anatel responsável pelo acompanhamento do tema

Neste cenário, opta-se pela designação de uma área técnica específica da Agência para acompanhamento de questões referentes à segurança cibernética. Como benefício desta alternativa está a desnecessidade de criação de uma estrutura na Agência, específica para tratar do tema. Por outro lado, a atribuição de um tema tão amplo e complexo a uma única área da Anatel pode não refletir, para os agentes envolvidos, a real importância do tema e comprometer o atingimento de um nível de institucionalização compatível com a sua necessidade, além de ter o condão de poder prejudicar a execução das demais atividades da área que seja apontada responsável.

Resumo da Análise das Alternativas

Alternativa	Vantagens			Desvantagens		
	Prestadoras	Consumidores	Anatel	Prestadoras	Consumidores	Anatel
A	- Não é necessária adequação em relação ao que é feito hoje.	- Não foram identificadas vantagens.	- Não há custos administrativos referente s à criação de um fórum específico.	- Dificuldade de participação de prestadoras de pequeno porte.	- Possível sinalização de baixa priorização do tema pela Anatel.	- Ausência de um tratamento institucional do tema pela Anatel.
B	- Participação ampla das prestadoras em discussões sobre o tema.	- Sinalização de priorização do tema pela Anatel, pois a existência de um Comitê, coordenado por Conselheiro Diretor da Agência, confere um caráter mais institucional.	- Tratamento institucional do tema.	- Custos relativos à participação e acompanhamento do fórum específico.	- Não foram identificadas desvantagens.	- Custos administrativos referentes à criação e condução deste fórum.
C	- Participação ampla das prestadoras em discussões sobre o tema.	- Sinalização de priorização do tema pela Anatel, embora menor do que a alternativa anterior.	- Estabelecimento de um posicionamento da Agência quanto ao tema	- Custos relativos à participação e acompanhamento das novas diretrizes no âmbito do GGRR.	- Não foram identificadas desvantagens.	- Custos administrativos referentes à alteração normativa que define a estrutura do GGRR.
D	- Centralização do ponto de contato para discussão do tema.	- Tratamento do tema pela Anatel, mesmo que de forma menos institucional.	- Tratamento do tema pela Anatel, mesmo que de forma menos institucional.	- Custos relativos à participação e acompanhamento das novas diretrizes estabelecidas por área específica.	- Não foram identificadas desvantagens.	- Baixo tratamento institucional do tema. - Risco de prejuízo às demais atividades da área indicada caso esta não seja dotada dos recursos necessários para esta nova atividade.

SEÇÃO 3
CONCLUSÃO E ALTERNATIVA SUGERIDA

Qual a conclusão da análise realizada?

Em decorrência das vantagens e desvantagens elencadas para cada alternativa, conclui-se que a alternativa que melhor endereça o problema elencado é a alternativa B, que propõe a utilização de um fórum específico para discussão e deliberação em temas referentes à segurança cibernética, qual seja, um Comitê, nos termos do Regimento Interno da Agência. Desta forma, seria conferido alto grau de institucionalização ao tema, compatível com a priorização que é dada internacionalmente a este assunto, sem custos significativos (basicamente administrativos).

Como será operacionalizada a alternativa sugerida?

No sentido de operacionalizar a alternativa sugerida, faz-se necessário mencionar o projeto constante do item nº 41 da Agenda Regulatória para o biênio 2017-2018, que trata da reavaliação da regulamentação relacionada a serviços públicos de emergência. O projeto em questão possui meta de elaboração de Relatório de Análise de Impacto Regulatório coincidente com a do projeto objeto da presente análise e também aponta como produto a utilização de um fórum específico (também um Comitê) para discussão e deliberação de temas relacionados à segurança pública.

Diante da sinergia temática entre os dois projetos, parece oportuna a utilização de um Comitê presidido por um Conselheiro da Anatel, no qual estariam inseridos, a priori, três grupos técnicos: um referente à segurança pública, outro referente à segurança cibernética e o terceiro referente ao Grupo de Gestão de Riscos e Acompanhamento do Desempenho das Redes de Telecomunicações (GGRR) estabelecido no Regulamento sobre Gestão de Risco das Redes de Telecomunicações e Uso de Serviços de Telecomunicações em Desastres, Situações de Emergência e Estado de Calamidade Pública, aprovado pela Resolução nº 656, de 17 de agosto de 2015. Estes grupos cumpririam a função de assessorar o Comitê no âmbito das referidas temáticas. Ressalta-se que a inclusão do GGRR no rol destes grupos vinculados ao Comitê justifica-se devido de este se preocupar com uma parcela importante da segurança das redes de telecomunicações, qual seja, a segurança física. Complementarmente, o grupo referente à segurança cibernética daria foco principalmente à segurança lógica, da informação. Assim, há sinergia também entre os aspectos discutidos no presente relatório de AIR e aqueles debatidos no âmbito do GGRR, o que justifica a vinculação deste também ao Comitê.

Ainda, considerando os Comitês já existentes e suas atribuições, entendeu-se adequada uma adequação do C-INI (Comitê sobre Infra-estrutura Nacional de Informações), criado por meio da Resolução nº 53, de 14 de novembro de 1998, com o objetivo de contemplar as temáticas aqui propostas. Assim, a implementação da alteração sugerida se dará por meio da atualização do Regimento Interno do C-INI, ajustando também seu nome para explicitar sua competência sobre aspectos de segurança.

Como a alternativa sugerida será monitorada?

O monitoramento da alternativa poderá realizado por meio da avaliação da efetividade das atividades conduzidas no âmbito do Comitê.

TEMA 02: Processos referentes à Segurança Cibernética

RESUMO DO TEMA

Descrição introdutória do Tema

Tendo em vista a amplitude e complexidade das vulnerabilidades inerentes do ambiente cibernético, mostra-se indispensável uma reflexão acerca de processos ou procedimentos necessários nas instituições e empresas para que se obtenha o nível de resiliência necessário que garanta níveis mínimos de segurança cibernética.

Neste sentido, observa-se um movimento de governos e de órgãos reguladores de se exigir procedimentos mínimos para que as entidades reguladas garantam padrões adequados de medidas em prol de maior segurança cibernética.

Qual é o contexto do problema?

Com a crescente proliferação de incidentes relacionados à segurança cibernética, Governos ao redor do mundo se debruçam sobre o tema, com fins de buscar maneiras de mitigar tais riscos que afetam diretamente a sociedade e o estabelecimento de um ecossistema sustentável e favorável à realização de transações e negócios.

No Brasil, o problema vem ganhando cada vez mais atenção e isso vem sendo refletido nas políticas públicas. Conforme mencionado anteriormente, a E-Digital estabeleceu como um de seus eixos temáticos a "Confiança no Ambiente Digital" e também existe um projeto de lei na Casa Civil dispondo sobre uma Política Nacional de Segurança da Informação (PNSI).

Além disso, no âmbito da Administração Pública Federal, o Brasil conta, desde o ano 2000, com um Comitê Gestor da Segurança da Informação, que presta assessoramento à Secretaria Executiva do Conselho de Defesa Nacional na consecução das diretrizes da Política de Segurança da Informação nos órgãos e nas entidades da administração pública federal.

Em face do desafio proposto pela temática, em 2006 foi criado o Departamento de Segurança da Informação e Comunicações (DSIC), no âmbito do Gabinete de Segurança Institucional (GSI) da Presidência da República, com atribuições de coordenar a execução de ações de segurança da informação e comunicações na administração pública federal, definir requisitos metodológicos para implementação de ações de segurança da informação e comunicações pelos órgãos e entidades da administração pública federal, operacionalizar e manter centro de tratamento e resposta a incidentes ocorridos nas redes de computadores da administração pública federal, e avaliar tratados, acordos ou atos internacionais relacionados à segurança da informação e comunicações.

Em 2015, foi publicada a Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética da Administração Pública Federal 2015-2018 versão 1.0[29], documento que fornece instrumento de apoio ao planejamento estratégico governamental e complementa a Instrução Normativa GSI/PR 01/2008, reúne um conjunto de objetivos estratégicos e metas para os próximos quatro anos, e visa a busca da excelência da Segurança da Informação e Comunicações (SIC) e da Segurança Cibernética (SegCiber) no âmbito da administração pública federal do país, contemplando relevantes aspectos, dada a complexidade e a dinâmica de tais temas no cenário atual, nacional e mundial.

Em cumprimento da Meta III de 2015 prevista na referida Estratégia de Segurança Informação e Comunicações e de Segurança Cibernética da Administração Pública, o DSIC, assessorado pelo Comitê Gestor de Segurança da Informação (CGSI/SE-CDN), articulou com outros Ministérios a inserção das áreas de Segurança da Informação e Comunicações (SIC) e de Segurança Cibernética (SegCiber) no Plano Plurianual do Governo Federal - PPA 2016-2019. O fato foi concretizado na Lei nº 13.249/2016, publicada no Diário Oficial da União de 14 de janeiro, que dispõe sobre o Plano Plurianual do Governo Federal - PPA 2016-2019. Este é sem dúvida um importante e histórico marco para a SIC e SegCiber do país. Porém existem ainda diversos desafios e metas a serem alcançados, conforme prevê a citada Estratégia.

Ademais, cumpre destacar que foi publicada, recentemente, Resolução específica pelo Banco Central do Brasil[30] (Resolução nº 4.658, de 26 de abril de 2018) dispondo sobre a política de segurança cibernética e sobre requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem a serem observados pelas instituições financeiras e demais instituições autorizadas a funcionar no Brasil pela Autarquia, que se apresentam como um dos principais alvos de ataques no ambiente cibernético, dado o potencial retorno financeiro envolvido.

Nesta esteira, cumpre à Anatel a análise sobre a adoção de processos pela própria Agência e sobre a regulamentação de requisitos ou procedimentos mínimos a serem estabelecidos aos seus regulados, ou seja, as prestadoras de serviços de telecomunicações, detentoras de grande parte da infraestrutura nacional de telecomunicações.

Qual o problema a ser solucionado?

No âmbito deste tema, foram identificados mais de um problema verificando-se a necessidade de dividir a temática em subtemas para a condução adequada da análise. Os problemas identificados são elencados a seguir:

- Constatação, por meio de tomada de subsídios, da ausência de um ambiente ou plataforma destinada ao compartilhamento de informações de incidentes referentes à

[29] O Diário Oficial da União, nº 88, Seção I, de 12 de maio de 2015, publicou a Portaria CDN Nº 14, de 11 de maio de 2015, que homologa a "Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética da Administração Pública Federal - 2015/2018, versão 1.0".

[30] Disponível em http://www.bcb.gov.br/pre/normativos/busca/downloadNormativo.asp?arquivo=/Lists/Normativos/Attachments/50581/Res_4658_v1_O.pdf

segurança cibernética, de forma segura e sigilosa. Atualmente, este compartilhamento ocorre de maneira não uniforme, informal e restrita aos agentes com afinidade entre si. Algumas prestadoras sequer compartilham informação. Tal dinâmica compromete a existência de diagnósticos dos incidentes no setor, a gestão de risco e a reatividade e eficiência na mitigação de ataques cibernéticos, ressaltando a inexistência de colaboração e cooperação entre o setor privado.

- Há um desnivelamento em relação à priorização e importância dada à estrutura organizacional e aos processos relativos à melhoria da segurança cibernética nas diversas prestadoras de serviços de telecomunicações. Assim como se verifica uma grande disparidade do tratamento institucional do assunto nas diversas prestadoras.
- A cultura e costumes na utilização de tecnologias conectadas às redes, de forma geral, não acompanharam a velocidade do crescimento de vulnerabilidades e riscos em relação às ameaças cibernéticas.

A Agência tem competência para atuar sobre o problema?

A competência da Anatel para atuar no problema se origina na Lei Geral de Telecomunicações (Lei nº 9.472 de 1997), particularmente, em seu art. 19:

> Art. 19. À Agência compete adotar as medidas necessárias para o atendimento do interesse público e para o desenvolvimento das telecomunicações brasileiras, atuando com independência, imparcialidade, legalidade, impessoalidade e publicidade, e especialmente:
>
> (...)
>
> IV - expedir normas quanto à outorga, prestação e fruição dos serviços de telecomunicações no regime público;
>
> (...)
>
> X - expedir normas sobre prestação de serviços de telecomunicações no regime privado;

Qual(is) o(s) objetivo(s) da ação?

Aprimorar os níveis de segurança do ambiente cibernético, avaliando a necessidade de estabelecer procedimentos mínimos relativos à gestão da segurança cibernética a serem adotados pelas prestadoras de serviços de telecomunicações e promover a conscientização da população em relação aos riscos do ambiente digital.

Como o tema é tratado no cenário internacional?

O compartilhamento de informações e a conscientização de todos os atores são fundamentais para a adequada gestão dos incidentes de segurança cibernética.

As Diretrizes da Organização para a Cooperação e Desenvolvimento Econômico (OCDE) para a Segurança das Redes e Sistemas de Informação: em Direção à Cultura de Segurança de 2002[31] já elencava como conteúdo do Princípio da Resposta, a necessidade de todos interessados agirem de forma cooperativa e oportuna para prever, detectar, responder e tratar os incidentes de segurança, destacando-se o compartilhamento de informações sobre ameaças e vulnerabilidade. Além disso, no mesmo documento, o Princípio da Conscientização aborda a necessidade de que todos os participantes da cadeia estejam conscientes dos riscos, da necessidade de segurança e das medidas que eles podem adotar para aumentar a segurança, enquanto que o Princípio da Responsabilidade atesta que todos os participantes da cadeia (governos, setor privado e usuários) são responsáveis pela segurança, dentro dos seus respectivos papéis, devendo compreender sua responsabilidade.

No mesmo ano, a Assembleia Geral das Nações Unidas, na 57° Sessão, aprovou a Resolução n° 239, intitulada "Criação de uma Cultura Global de Segurança Cibernética"[32], que aborda o aspecto cultural do problema que afronta a segurança da informação e consagrando essas diretrizes.

As diretrizes foram revistas em 2015, pelo documento Gestão do Risco Digital para a Prosperidade Econômica e Social[33], que continua a contemplar essas ideias. Além disso, na Seção destinada às estratégias nacionais, ressalta que elas devem incluir o engajamento do governo com outros atores, a fim de encorajar a divulgação, notificação e correção responsável de vulnerabilidades e de aumentar o nível de conscientização em toda sociedade. Ainda destaca a necessidade de criação das condições para que todos interessados colaborem no gerenciamento do risco de segurança cibernética, promovendo participação ativa de importantes interessados em iniciativas e parcerias mutuamente confiáveis para compartilhamento de informações.

Nos termos relatados anteriormente, a FCC, além de trabalhar para o compartilhamento de informações, exige a notificação de interrupção de serviço, que permite diagnóstico dos incidentes e guia sua atuação, além de prover essa informação ao Centro de Integração Nacional de Segurança Cibernética e Comunicações (NCCIC).

Interessante notar que, no FCC *White Paper: Cybersecurity Risk Reduction*[34], é relatado que pequenas e médias empresas sofrem barreiras desproporcionais para o compartilhamento de informação, especialmente em relação ao custo, ainda que estejam tão vulneráveis quanto grandes empresas, sendo recomendado pelo *Public Safety and Homeland Security Bureau* a criação de um projeto piloto financiado para compartilhamento de informação e análise organizacional.

---

[31] http://www.oecd.org/sti/ieconomy/15582260.pdf

[32] Resolução n.° 57/239, "Criação de uma Cultura Global de Segurança Cibernética", texto disponível em: http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/57/239.

[33] OECD (2015), *Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document*, OECD Publishing, Paris. http://dx.doi.org/10.1787/9789264245471-en.

[34] Disponível em: https://apps.fcc.gov/edocs_public/attachmatch/DOC-343096A1.pdf. Acesso em 14/06/2018

Já a Anacom também promove a sensibilização e a promoção de boas práticas de defesa da confidencialidade das comunicações e promove a normalização técnica do setor de telecomunicações, assim como também exige a notificação do órgão regulador para casos de violações de segurança ou perdas de integridade das redes.

O Ofcom também exige a comunicação dos incidentes ou reduções de disponibilidade com impacto significativo na rede ou no serviço, assim como pode exigir que seus regulados se submetam e arquem com os custos de auditoria para a verificação dos requisitos relacionados à segurança da informação.

Menciona-se ainda que relatório final da Questão de Estudos 22 da Comissão de Estudos 1 da UIT-D do ciclo de 2006-2010[35], além de elencar o compartilhamento de informações como meta, salienta a necessidade de promoção de uma cultura de segurança cibernética, liderada pelos governos, devendo ser implementados programas e iniciativas de conscientização para usuários e encorajamento dessa cultura no âmbito das empresas.

Quais os grupos afetados?

- Prestadoras de serviços de telecomunicações;
- Anatel;
- Consumidores.

[35] Disponível em: https://www.itu.int/dms_pub/itu-d/opb/stg/D-STG-SG01.22-2010-PDF-E.pdf. Acesso em 01/06/2018.

SUBTEMA 01: COMPARTILHAMENTO DE INFORMAÇÕES SOBRE INCIDENTES

SEÇÃO 1
RESUMO DA ANÁLISE DE IMPACTO REGULATÓRIO

No âmbito das discussões sobre Segurança Cibernética, nos diferentes fóruns onde ocorrem, parece ser um consenso que a coordenação e o compartilhamento de informações sobre incidentes, entre os agentes que atuam no ambiente cibernético, são elementos essenciais para a prevenção e mitigação dos efeitos de ataques cibernéticos. O Setor de Normalização da UIT apresenta um conceito básico[36] acerca do compartilhamento de informações relativas à segurança cibernética, no qual podemos destacar alguns pontos:

> "...técnicas pelas quais entidades afetas à segurança cibernética podem trocar informações utilizando métodos que provêm um nível adequado de garantia. Tais entidades, tipicamente, consistem em organizações, pessoas, dispositivos ou processos que possuem ou demandam informações relativas à segurança cibernética. Na maior parte dos casos, estas entidades são CIRTs (Computer Incident Response Teams) e operadores ou fornecedores de equipamento, software ou sistemas baseados em rede.
>
> O Compartilhamento de informações relativas à segurança cibernética é valioso para alcançar um ambiente cibernético seguro e uma maior proteção das infraestruturas, assim como contribuir para as principais atividades realizadas pelos CIRTs. A troca de informações de segurança cibernética pode ocorrer dentro de comunidades de confiança altamente compartimentadas e que aderem a princípios de necessidade de conhecimento destas informações, baseado em políticas previamente acordadas, bem como dentro do domínio público. O conhecimento de ameaças, vulnerabilidades, incidentes, riscos, mitigações e seus remédios associados são típicos exemplos de informações relativas à segurança cibernética compartilhadas entre entidades."(Tradução nossa)

No Brasil, o CERT.br é o Grupo de Resposta a Incidentes de Segurança para a internet no Brasil, mantido pelo Núcleo de Informação e Coordenação do Ponto BR (NIC.br), entidade civil, de direito privado, sem fins lucrativos, que foi criado para implementar as decisões e os projetos do Comitê Gestor da Internet no Brasil (CGI.br)[37] e há diversos CSIRTs[38] (Grupos de Segurança e Resposta a Incidentes) espalhados pelo território nacional, inclusive, constituídos por prestadoras de serviços de telecomunicações. No entanto, verificou-se, por meio de tomada de subsídios com as prestadoras, que o compartilhamento de informações, relacionadas à segurança cibernética, é realizado de maneira informal entre os agentes que

[36] Recomendação ITU-T X.1500 – *Overview of cybersecurity information exchange*, disponível em: <https://www.itu.int/rec/T-REC-X.1500/en>. Acesso em: 11/05/2018.
[37] https://www.cert.br/sobre/
[38] https://www.cert.br/csirts/

possuem confiança mútua e não envolve todo o rol de prestadoras do setor. Questionados se reportavam os incidentes em tempo real ao CERT.br, todas prestadoras se manifestaram negativamente e ainda que possuíam mecanismos próprios de compartilhamento de informações para mitigação de incidentes, a despeito do trabalho que o CERT.br faz de elaboração de relatórios, recomendações e cartilhas sobre segurança cibernética.

Destaca-se ainda a existência do CTIR Gov[39] que é o Centro de Tratamento de Incidentes de Redes do Governo. Está subordinado ao DSIC/GSI e sua finalidade é o atendimento aos incidentes em redes de computadores da administração pública federal.

No evento de segurança cibernética "*Brazil Cyber Defence CSTM 2018*"[40], foi exposta pelo representante do Comando de Defesa Cibernética (ComDCiber) a ideia de implantação de uma plataforma de compartilhamento de ameaças cibernéticas entre diversas instituições e órgãos governamentais, que traria como premissas uma rede confiável, padronização da troca de informações, compartilhamento rápido e eficiente, possibilidade de contribuições anônimas.

No setor bancário, a Febraban (Federação Brasileira de Bancos) estabeleceu, no âmbito da Subcomissão de *Cybersecurity*, parceria entre 12 instituições financeiras para a contratação de uma plataforma virtual de compartilhamento de informações. As instituições podem fornecer informações sobre data, horário, tipo de ameaça detectada, assim como sistemas afetados e soluções para resolver o problema identificado, alertando automaticamente os demais parceiros cadastrados[41].

Por todo o exposto, o presente subtema propõe-se a elencar alternativas para que o compartilhamento de informações relativas à segurança cibernética seja realizado na maneira mais eficiente e inclusiva possível no setor de telecomunicações.

Quais são as opções regulatórias consideradas para o subtema?

- *Alternativa A – Manutenção do status quo;*
- *Alternativa B – Utilização de plataforma disponibilizada pelo CERT.br;*
- *Alternativa C – Criação de plataforma de compartilhamento de informações na Anatel;*
- *Alternativa D – Incumbência às prestadoras da criação de plataforma de compartilhamento de informações.*

[39] http://www.ctir.gov.br/sobre-CTIR-gov.html
[40] http://brazilcyberdefence.com/
[41] http://www.ciab.org.br/publicacoes/edicao/73/bancos-em-alerta

SEÇÃO 2
ANÁLISE DAS ALTERNATIVAS

Alternativa A

Manutenção do status quo

Neste cenário, o compartilhamento das informações seria realizado da forma como é feito atualmente. Ou seja, as prestadoras de serviços de telecomunicações buscariam suas próprias soluções e parceiros para realizar este compartilhamento. Esta alternativa apresenta algumas fragilidades, pois não integra o ecossistema como um todo. Por meio da tomada de subsídios foi possível verificar uma falta de padronização na dinâmica de compartilhamento e também que a atividade era restrita a alguns agentes de forma colaborativa. Por outro lado, esta alternativa não apresenta custos incrementais de implementação e se baseia na livre pactuação de acordos e confiança entre as partes. Por possuir pouca aderência à resolução do problema identificado, tal alternativa somente se justifica se os custos das demais alternativas superarem seus benefícios.

Alternativa B

Utilização de plataforma disponibilizada pelo CERT.br

Conforme exposto na própria página do Núcleo de Informação e Coordenação do Ponto BR (NIC.br), o CERT.br é o responsável por tratar de aspectos de segurança na internet.

> "Atua como um ponto central para notificações de incidentes de segurança no Brasil, provendo a coordenação e o apoio no processo de resposta a incidentes e, quando necessário, colocando as partes envolvidas em contato.
>
> Além do processo de tratamento a incidentes em si, o CERT.br também atua através do trabalho de conscientização sobre os problemas de segurança, da análise de tendências e correlação entre eventos na Internet brasileira e do auxílio ao estabelecimento de novos CSIRTs no Brasil."42

Diante desse fato, mostra-se evidente a sinergia do tema com o escopo de atuação do CERT.br, podendo ser buscada uma parceria entre a Anatel e o Comitê Gestor da Internet (CGI.br) para viabilizar a implementação de uma plataforma de compartilhamento de informações, relativas à segurança cibernética no âmbito do CERT.br. De fato, a entidade trata do assunto há algum tempo e possui o conhecimento adequado para endereçamento da questão. Em contribuição apresentada ao tema, a entidade afirma que os processos mais frutíferos de cooperação e compartilhamento de informações dos quais o CERT.br participa internacionalmente foram estabelecidos de maneira informal, após o estabelecimento de uma relação de confiança, que foi construída após anos de relacionamento com as

[42] https://www.cert.br/sobre/

organizações e não por meio de um acordo, memorando de entendimento ou regulamento. Citam, ainda, o grupo de troca de informações sobre incidentes de segurança no setor financeiro, criado com auxílio do CERT.br, e que não é ligado ao órgão regulador (Banco Central) e sim à Febraban. Ressaltam que o sucesso deste grupo foi o processo de construção de confiança entre os profissionais que participam do grupo e se colocam a disposição das prestadoras para compartilhar o caso de sucesso.

Alternativa C

Criação de plataforma de compartilhamento de informações na Anatel

Neste cenário, a Anatel seria a responsável pela criação de uma plataforma de compartilhamento de informações relativas à segurança cibernética. Para tanto, seria necessário o emprego de recursos financeiros para o desenvolvimento da solução e também recursos humanos para sua administração.

Ainda, tal plataforma deve garantir conectividade com todas as prestadoras ininterruptamente, operar sob regime de sigilo e garantir contribuições anônimas, uma vez que, para se obter a eficácia almejada, o compartilhamento de informações depende da proteção de informações sensíveis às empresas de forma a incentivar a participação de todos os agentes.

Cumpre destacar que a administração de uma plataforma dessa natureza pode exigir alterações na aplicação que devem ser implementadas de maneira rápida e eficiente, características estas não compatíveis com os procedimentos de contratação da administração pública.

Por meio desta alternativa, a administração da plataforma seria realizada pela Anatel e seria possível apurar, com maior precisão, diagnósticos da segurança das redes de telecomunicações. Por outro lado, sua eficaz utilização poderia ser comprometida pela desconfiança dos agentes em operar uma plataforma administrada pelo órgão regulador.

Alternativa D

Incumbir as prestadoras da criação de plataforma de compartilhamento de informações

Trata-se de alternativa de destinar às prestadoras de serviços de telecomunicações a incumbência de criação ou aquisição de uma plataforma ou fórum de compartilhamento de informações que seja inclusiva a todas as prestadoras. Neste cenário, haveria um maior alinhamento de interesses e eficiência no desenvolvimento da plataforma, conferindo uma maior confiança no uso da plataforma por parte de seus usuários.

No entanto, neste caso, o custo de desenvolvimento desta plataforma seria imposto ao setor, cabendo a ele elaborar mecanismos de rateio dos custos entre os participantes.

Cumpre notar que esta foi a opção regulatória escolhida pelo Banco Central do Brasil quando da edição da Resolução nº 4.658, de 26 de abril de 2018, por meio da qual estabeleceu que as instituições financeiras devem desenvolver iniciativas para o compartilhamento de informações sobre os incidentes relevantes.

Resumo da Análise das Alternativas

Alternativa	Vantagens			Desvantagens		
	Prestadoras	Consumidores	Anatel	Prestadoras	Consumidores	Anatel
A	- Não há necessidades de adaptações.	- Não foram identificadas vantagens	- Não há custos a serem imputados à Agência	- O compartilhamento de informações é restrito a grupos de confiança, e de maneira geralmente pessoal, pouco institucionalizada.	- Possível mitigação menos efetiva de ataques cibernéticos	- Não há um compartilhamento de informações do setor como um todo.
B	- Existência de uma plataforma unificada de compartilhamento de informações	- Mitigação mais efetiva de ataques cibernéticos nas redes de telecomunicações	- Não há custos a serem imputados à Agência	- Adaptação em seus processos para reportar os incidentes e compartilhar informações, em tempo real, utilizando plataforma disponibilizada pelo CERT.br	- Não foram identificadas desvantagens	- Não há um acompanhamento próximo, nem uma gestão do compartilhamento das informações.
C	- Existência de uma plataforma unificada de compartilhamento de informações	- Mitigação mais efetiva de ataques cibernéticos nas redes de telecomunicações	- Gestão e acompanhamento do compartilhamento de informações de ameaças cibernéticas no setor de telecomunicações	- Adaptação em seus processos para reportar os incidentes e compartilhar informações, em tempo real, utilizando plataforma disponibilizada pela Anatel	- Não foram identificadas desvantagens	- Necessidade de desenvolver e administrar plataforma de compartilhamento de informações. - Falta de agilidade em eventuais adaptações que se fizerem necessárias.
D	- Existência de uma plataforma unificada de compartilhamento de informações. Desenvolvimento e gestão da plataforma de acordo com suas necessidades.	- Mitigação mais efetiva de ataques cibernéticos nas redes de telecomunicações	- Não há custos a serem imputados à Agência.	- Custos referentes ao desenvolvimento de uma plataforma de compartilhamento de informações	- Não foram identificadas desvantagens	- A gestão do compartilhamento de informações pelas prestadoras pode trazer riscos associadas à assimetria de informação

SEÇÃO 3
CONCLUSÃO E ALTERNATIVA SUGERIDA

Qual a conclusão da análise realizada?

Tendo em vista as alternativas analisadas, a alternativa considerada mais adequada é a alternativa D. Partindo da premissa que o compartilhamento de informações somente ocorre de maneira eficaz em um ambiente de confiança, o que, de acordo com a análise das alternativas acima, melhor ocorrerá por meio de uma plataforma que seja desenvolvida ou adquirida pelas próprias prestadoras. Desta forma, o desenvolvimento ou especificação da solução estariam mais alinhados com as características e necessidades do setor, além de que eventuais atualizações e gestões a serem implementadas de forma mais célere. Cabe destacar que a plataforma, se implementada de forma adequada e eficiente, pode significar relevante economia de custos relativos a incidentes cibernéticos. Por fim, ainda que se trate de plataforma a ser desenvolvida pelas prestadoras, faz-se essencial o alinhamento de esforços entre prestadoras, Anatel e CERT.br para permitir um compartilhamento mais eficaz de incidentes.

Como será operacionalizada a alternativa sugerida?

Para operacionalizar a alternativa sugerida, propõe-se a inclusão de normativo prevendo a promoção de iniciativas de compartilhamento de informações entre as prestadoras. Tais iniciativas estariam inclusas no âmbito de uma política de segurança cibernética a ser implementada pelas prestadoras.

Como a alternativa sugerida será monitorada?

O acompanhamento da Agência seria realizado por meio de relatórios de acompanhamento da política a serem enviados anualmente ou quando solicitado à Anatel (por meio do Comitê de que trata o tema 1). Nestes relatórios, devem estar inseridas estatísticas acerca dos incidentes cibernéticos, como principais ataques realizados, sua natureza e ações corretivas. Também é possível que seja feita a análise de quais ações corretivas tiveram sucesso ou maior celeridade devido ao compartilhamento das informações.

SUBTEMA 02: ESTRUTURA ORGANIZACIONAL, GESTÃO DA SEGURANÇA CIBERNÉTICA E INFRAESTRUTURAS CRÍTICAS

SEÇÃO 1
RESUMO DA ANÁLISE DE IMPACTO REGULATÓRIO

Este subtema trata da estrutura organizacional das prestadoras de serviços de telecomunicações, dos processos e medidas adotadas quanto à segurança cibernética pela governança dessas empresas e das infraestruturas de telecomunicações de extrema relevância ao funcionamento do sistema de telecomunicações brasileiro como um todo, as quais pertençam aos entes regulados por esta Agência.

Primeiramente, por meio da tomada de subsídios, identificou-se um desnivelamento em relação à priorização e importância dada à estrutura organizacional e aos processos relativos à melhoria da segurança cibernética entre as diversas prestadoras de serviços de telecomunicações.

As grandes prestadoras de serviços de telecomunicações de interesse coletivo possuem, de forma geral, profissionais dedicados à identificação de riscos que possam ameaçar a continuidade de seus negócios, incluídos nestes os riscos associados à segurança cibernética, tanto sob o aspecto de garantir a fruição do serviço prestado quanto sob a perspectiva de sua imagem perante a população, por exemplo, em casos de quebra de confidencialidade. Neste sentido, parece ser verdadeira a hipótese de que os interesses das grandes empresas de telecomunicações estariam alinhados com a preocupação crescente dos órgãos governamentais no que tange à segurança cibernética, uma vez que a própria fruição da prestação desses serviços está inserida no contexto de ameaças cibernéticas.

Destaca-se, ainda, que existem prestadoras de serviços de telecomunicações de pequeno e médio portes, que, primariamente, visam se estabelecer no mercado. Desta forma, estas possuem incentivos em adiar os investimentos, tanto de gestão de processos internos quanto de medidas técnicas relacionadas à segurança cibernética, principalmente, nos riscos associados à quebra da confidencialidade e autenticidade, que não afetam diretamente a fruição dos serviços prestados. Entretanto, tal questão é crítica, pois, se tratando de segurança, falhas em quaisquer uma das redes podem servir de porta de entrada para ataques em todas as redes de interesse coletivo, interconectadas entre si.

No cenário atual, os temas estrutura organizacional das prestadoras e gestão de infraestruturas críticas estão inseridos no escopo do Regulamento sobre Gestão de Risco das Redes de Telecomunicações e Uso de Serviços de Telecomunicações em Desastres, Situações de Emergência e Estado de Calamidade Pública, aprovado pela Resolução nº 656/2015.

O artigo 1º do referido Regulamento estabelece:

> Art. 1º O presente Regulamento <u>tem por objetivo</u> estabelecer definições, procedimentos e condutas para a <u>promoção da disponibilidade, da segurança e do desempenho das</u>

> redes e serviços de telecomunicações de interesse coletivo, em especial quando da ocorrência de desastres e emergências, ou sua iminência, mediante:
>
> I – adoção de medidas para acompanhamento do desempenho das redes;
>
> II - adoção de processo de gestão de riscos das infraestruturas críticas de telecomunicações; e,
>
> III - estabelecimento de medidas de preparação e de resposta para desastre, situação de emergência ou estado de calamidade pública. (grifo nosso)

No âmbito do mesmo Regulamento, optou-se, de imediato, por instruir a aplicação de técnicas de gestão de riscos somente às infraestruturas de telecomunicações consideradas de extrema relevância, determinadas de acordo com seu potencial impacto à sociedade brasileira na eventualidade de sua destruição ou interrupção, conforme a definição do termo "Infraestruturas Críticas de Telecomunicações" no artigo 4º, inciso V, do mesmo Regulamento.

É razoável indicar que a gestão de riscos das infraestruturas de telecomunicações pressupõe a identificação de riscos relacionados à gestão de segurança da informação com vistas a mitigar as vulnerabilidades passíveis de afetar a disponibilidade, ou seja, a fruição do serviço de telecomunicações, tal qual, por exemplo, a ameaça de um ataque de negação de serviço a um provedor deste serviço de telecomunicações.

Ademais, destaca-se também o artigo 5º do referido Regulamento:

> Art. 5º As prestadoras abrangidas por este Regulamento devem implantar o Plano de Gestão de Riscos – PGRiscos para gerir os riscos que possam afetar a segurança das Infraestruturas Críticas de Telecomunicações.
>
> § 1º Os riscos citados no caput são aqueles relacionados à segurança física e à segurança da informação das Infraestruturas Críticas de Telecomunicações que possam prejudicar a prestação de um serviço de telecomunicações. (grifo nosso)

A figura do Plano de Gestão de Riscos, supracitada, introduzida no âmbito do setor de telecomunicações pelo Regulamento em questão, fomentou a necessidade de adaptação da estrutura organizacional da empresa de telecomunicações para melhorias na temática analisada. De forma análoga, a Resolução nº 4.658, de 26 de abril de 2018, do Banco Central do Brasil, que dispõe sobre a política de segurança cibernética a ser observada pelas instituições financeiras, orienta os seus entes regulados a focar em política de segurança cibernética e, se necessário, adequar a suas estruturas organizacionais, conforme redação de seu artigo 6º, transcrito abaixo.

> Art. 6º As instituições referidas no art. 1º devem estabelecer plano de ação e de resposta a incidentes visando à implementação da política de segurança cibernética.
>
> Parágrafo único. O plano mencionado no caput deve abranger, no mínimo:

> I - as ações a serem desenvolvidas pela instituição para adequar suas estruturas organizacional e operacional aos princípios e às diretrizes da política de segurança cibernética; (grifo nosso)

A primeira questão para descrição de alternativas é, naturalmente, a avaliação sobre o órgão regulador se abster de regulamentar medidas relacionadas à temática de segurança cibernética. No caso específico da Agência, devido à existência do Regulamento supracitado, existe a possibilidade de demandar a adoção de práticas por intermédio do Grupo de Gestão de Riscos e Acompanhamento do Desempenho das Redes de Telecomunicações (GGRR).

O segundo questionamento trata especificamente entre a definição de requisitos (diretrizes) ou de normas exaustivas sobre esta temática. Considera-se que a Resolução nº 4.658, de 26 de abril de 2018, do Banco Central do Brasil, bem como a figura do PGRiscos, presente na Resolução nº 656/2015, são exemplos da definição de requisitos (diretrizes). Ainda, como requisitos se poderiam citar, como exemplo, a indicação para constituição de uma estrutura dedicada de governança de segurança cibernética nas empresas, estabelecimento de manuais para disseminação de boas práticas, diretrizes, classificações e procedimentos e, possivelmente, a determinação de investimento em planos anuais de auditoria externa.

Por último, há de se considerar proceder com instrução normativa, se for o caso, aplicável somente a certo grupo de prestadoras ou de forma equânime a todas as prestadoras independentemente do escopo do serviço (interesse coletivo ou restrito). Tal consideração se justifica, pois os diferentes escopos dos serviços implicam em diversos portes e características das empresas de telecomunicações.

Quais são as opções regulatórias consideradas para o tema?

- *Alternativa A – Manutenção do status quo;*
- *Alternativa B – Estabelecimento de requisitos de gestão da segurança cibernética a todas as prestadoras, de forma equânime;*
- *Alternativa C – Estabelecimento de requisitos de gestão da segurança cibernética às prestadoras de forma assimétrica e não exaustiva;*
- *Alternativa D – Previsão exaustiva de processos.*

SEÇÃO 2
ANÁLISE DAS ALTERNATIVAS

Alternativa A

Manutenção do status quo

Neste cenário, tem-se a possibilidade da manutenção do *status quo*, que, inclusive, possui arcabouço regulamentar já estabelecido. Neste ínterim, ter-se-ia, por meio da identificação de riscos relacionados à fruição do serviço de telecomunicações e à segurança de informação, a determinação, por intermédio do Grupo de Gestão de Riscos e Acompanhamento do Desempenho das Redes de Telecomunicações (GGRR), da adoção de boas práticas relacionadas à gestão da segurança da informação e estrutura organizacional das prestadoras.

Por outro lado, desde a vigência do Regulamento aprovado pela Resolução nº 656/2015, os ciclos de gestão de riscos das infraestruturas críticas mostraram-se focados na identificação de vulnerabilidades apenas indiretamente relacionadas a processos relevantes da temática de segurança da informação. Em outras palavras, tem-se focado mais em aspectos relacionados à "segurança física" das redes e menos naqueles referentes à sua "segurança lógica".

Nos grandes eventos internacionais, Copa do Mundo FIFA 2014 e Jogos Olímpicos/Paralímpicos 2016, optou-se, inclusive, pela separação, em grupos de trabalhos distintos, dos riscos associados a ameaças cibernéticas, a vulnerabilidades inerentes à segurança física e aos requisitos técnicos tradicionais de rede de telecomunicações (redundância lógica, plano de contingência, capacidade do sistema, entre outros), ainda que, em certa medida, as vulnerabilidades de processos de segurança física (acessos lógicos e/ou acessos físicos) contribuam para um aumento de risco de ameaça cibernética.

Por todo exposto, os custos de implantação da alternativa aqui exposta estariam associados ao acompanhamento das futuras deliberações do Grupo de Gestão de Riscos e Acompanhamento do Desempenho das Redes de Telecomunicações (GGRR) sobre a temática, sendo, portanto, similares aos custos de acompanhamento decorrentes de uma alternativa em que se venha a publicar novos normativos dispondo especificamente sobre requisitos de segurança cibernética.

No cenário aqui elencado, tem-se a vantagem de menores custos administrativos e temporais, na medida que este grupo executivo encontra-se, atualmente, em pleno funcionamento.

Alternativa B

Estabelecimento de requisitos de gestão da Segurança Cibernética a todas as prestadoras, de forma equânime

O ecossistema digital vem respondendo por parcelas cada vez mais significativas da produção e da renda nacional e, assim, espera-se que os elementos garantidores de sua segurança evoluam no mesmo

sentido, sem os quais se corre o risco de fragilizar todo o sistema nacional de produção de bens e serviços que estão cada vez mais dependentes do pleno funcionamento das redes de telecomunicações.

Portanto, é razoável a análise do estabelecimento de requisitos de gestão de segurança cibernética de forma equânime a todas prestadoras de serviços de telecomunicações.

Todavia, o estabelecimento de requisitos de forma equânime amplifica, colateralmente, a carga fiscalizatória imputada à Agência ao abarcar todas as empresas do setor, não obstante o escopo do serviço prestado (interesse restrito ou coletivo). Nesse sentido, a opção em tela pode significar a imposição de uma carga regulatória talvez desproporcional com a estruturação e tamanho de algumas empresas.

Alternativa C

Estabelecimento de requisitos de gestão da segurança cibernética às prestadoras de forma assimétrica e não exaustiva

A Agência tem adotado, ao longo dos anos, uma postura de determinação de normativos regulamentares assimétricos no tocante ao porte das empresas de telecomunicações.

Ainda, tendo como base a definição clássica de risco (dano potencial multiplicado por probabilidade de ocorrência) aplicado ao sistema de telecomunicações como um todo, poder-se-ia inferir que é mais eficiente concentrar recursos na determinação e fiscalização regulatória da adoção de tais requisitos num escopo de prestadoras de maior porte, tendo em vista que grande parte dos usuários de serviços de telecomunicações é atendida por grandes prestadoras, e que, para se diminuir a probabilidade de um incidente cibernético, é necessária a efetiva adoção de tais requisitos, o que demanda processos de fiscalização regulatória por parte da Agência.

Poder-se-ia aqui questionar se tal diferenciação deveria ter como base o porte da empresa ou o escopo do serviço prestado. Cabe análise, porém, da definição de porte neste contexto. Por um lado, existe a definição vigente de prestadora de pequeno porte, a qual se aplica, somente, a empresas de telecomunicações de interesse coletivo. Ainda, no contexto brasileiro, existem algumas empresas de telecomunicações de interesse coletivo e restrito que prestam serviços de telecomunicações, com alto tráfego agregado e/ou relevância, e não se enquadram na definição de prestadora de pequeno porte vigente, esta criada, de fato, para obrigações regulamentares no âmbito de venda de serviços telecomunicações no varejo.

Neste ínterim, o processo de gestão de riscos amparado no Regulamento sobre Gestão de Risco das Redes de Telecomunicações e Uso de Serviços de Telecomunicações em Desastres, Situações de Emergência e Estado de Calamidade Pública, aprovado pela Resolução nº 656/2015, é destinado, a priori, aos detentores das infraestruturas de telecomunicações que suportam os serviços de telecomunicações de interesse coletivo. No entanto, o Regulamento prevê a possibilidade de inclusão, no rol das empresas afetadas por ele, de prestadoras de serviços de telecomunicações de interesse restrito.

Em linha com tais aspectos, a presente alternativa exclui das obrigações a serem criadas aquelas empresas que prestam serviços de interesse restrito. Entre as que prestam serviços de interesse coletivo, às de pequeno porte o rol de princípios e requisitos deve ser substancialmente menor do que aquele aplicado às empresas de maior porte. Tal proposição está alinhada a outras regulamentações temáticas da Agência (qualidade e direitos dos consumidores, por exemplo), sem contudo prejudicar os aspectos relacionados à segurança cibernética, visto que mesmo para as empresas de pequeno porte um rol mínimo de requisitos seria exigido.

Alternativa D

Previsão exaustiva de processos

Trata-se de hipótese de se regulamentar exaustivamente a gestão interna e os processos relativos à segurança cibernética.

Neste caso, haveria um natural engessamento dos regramentos aplicáveis, impondo maiores dificuldades para a manutenção da atualidade dos requisitos, processos e procedimentos vis-à-vis as sempre mutáveis necessidades inerentes ao dinâmico cenário em que se insere o setor de telecomunicações, principalmente quando se associa a temática de segurança cibernética, extremamente inovadora em termos de identificação de novas vulnerabilidades e definição de novas recomendações de boas práticas aos prestadores de serviços e aos usuários.

Portanto, não é razoável presumir que seria eficiente conduzir as empresas de telecomunicações a seguirem instruções exaustivas do órgão regulador para mitigar os riscos associados à segurança cibernética, mesmo que, eventualmente, uma ou outra recomendação nacional ou internacional possa ser determinada aos entes regulados, desde que esta tenha se tornado referência indiscutível nesta temática.

Resumo da Análise das Alternativas

Alternativa	Vantagens			Desvantagens		
	Prestadoras	Consumidores	Anatel	Prestadoras	Consumidores	Anatel
A	- As principais prestadoras estão presentes no GGRR e haveria um custo relativamente inferior de adaptação.	- Não foram identificadas vantagens.	- Estrutura administrativa já criada. - Maior celeridade para adaptar os procedimentos vigentes.	- Não foram identificadas desvantagens.	- Não foram identificadas desvantagens.	- Necessidade de adaptar a estrutura atual do GGRR para aprimorar o acompanhamento de procedimentos relativos à segurança cibernética
B	- O estabelecimento de requisitos formais a todas as prestadoras eleva a proteção das redes de telecomunicações a ataques cibernéticos, inclusive oriundos	- Mitigação dos riscos no ambiente cibernético	- Desnecessidade de estabelecer critério para selecionar quais agentes estarão submetidos a procedimentos mais rigorosos.	- Carga regulatória desproporcional a empresas que prestam serviço de menor escopo (interesse coletivo).	- Custos advindos da regulamentação podem ser refletidos nos preços de serviços ofertados.	- Carga Fiscalizatória alta (alto quantitativo de empresas)

	de outras redes, sem contudo enrijecer, de forma exaustiva, a maneira com tais requisitos devem ser atendidos.					
C	- O estabelecimento de requisitos formais a todas as prestadoras de serviços de interesse coletivo eleva a proteção das redes de telecomunicações a ataques cibernéticos, inclusive oriundos de outras redes, sem contudo enrijecer, de forma exaustiva, a maneira com tais requisitos devem ser atendidos. - As empresas excluídas da aplicabilidade do normativo seriam beneficiadas (serviços de telecomunicações de interesse restrito ou de pequeno porte, para os serviços de interesse coletivo).	- Mitigação dos riscos no ambiente cibernético	- Carga fiscalizatória relativamente menor.	- Custos advindos das adaptações às determinações regulamentares	- Clientes de empresas não obrigadas a seguir procedimentos mais rigorosos, poderiam estar mais sujeitos a riscos.	- - Clientes de empresas não obrigadas a seguir procedimentos mais rigorosos, poderiam estar mais sujeitos a riscos.
D	- Não foram identificadas vantagens	- Mitigação dos riscos no ambiente cibernético.	- Maior facilidade no acompanhamento, tendo em vista a maior objetividade dos critérios a serem cumpridos	- Regulação muito prescritiva tende a não englobar os diversos modelos de negócio e estruturas organizacionais do mercado	- Custos advindos da regulamentação podem ser refletidos nos preços de serviços ofertados..	Risco de - Anacronismo das normas regulamentares tendo em vista a dinâmica do tema.

SEÇÃO 3
CONCLUSÃO E ALTERNATIVA SUGERIDA

Qual a conclusão da análise realizada?

Em face ao desafio proposto pela temática, justificada pelos fenômenos da sociedade da informação, tais quais aumento crescente e bastante substantivo de acesso à internet e às redes sociais, aumento das ameaças e das vulnerabilidades de segurança cibernética, ambientes complexos, múltiplos atores e, principalmente, mudanças constantes e rápidas, tem-se que não seria factível estabelecer de forma exaustiva, em regulamento, obrigações aos entes regulados, considerando as limitações práticas para sua atualização em horizonte de tempo adequado.

Por outro lado, devido à relevância da temática, mesmo se considerada a hipótese de que os interesses das empresas de telecomunicações estarem alinhados com os da Agência em mitigar as ameaças e vulnerabilidades no ambiente cibernético, é sugerido para a Agência acompanhar a evolução das medidas adotadas neste ambiente pelos diversos agentes, dado o dano potencial associada a tais ameaças à sociedade brasileira como um todo.

A previsão exaustiva de processos, através de especificações e normas, deveria ser evitada, principalmente, devido à dinâmica inerente do ambiente cibernético. À medida que sejam identificadas as boas práticas, passíveis de serem convertidas em detalhamento de processos e medidas a serem adotadas, estas deveriam ser propostas pelo Comitê específico ao tema (apontado como alternativa preferencial nos temas anteriores) e submetidas ao Conselho Diretor para deliberação. Desta forma, se adquire flexibilidade no escopo das medidas necessárias a serem adotadas.

Ainda, é importante se ponderar os custos a serem impostos às diferentes redes conforme o escopo dos serviços de telecomunicações (interesse coletivo ou restrito) frente aos benefícios e proteções contra ataques cibernéticos que se obteria. É fato que os ataques às redes de interesse coletivo têm potencial de trazer maiores prejuízos não somente pelo total de usuários como também pelas suas características de interconexão às demais redes de interesse coletivo. Os ataques contra redes de interesse restrito têm, por outro lado, menor prejuízo potencial, justificando o estabelecimento de maiores requisitos para as redes dos serviços de telecomunicações de interesse coletivo. E, com relação àquelas que prestam serviços de interesse coletivo, justifica-se o estabelecimento de requisitos substancialmente menores para aquelas de pequeno porte, nos termos da regulamentação, também em razão do menor potencial de influência dos ataques originados em suas redes. Desta forma, a alternativa sugerida é a alternativa C, com a expedição de normativo, específico sobre a temática, considerando as diferentes características das empresas atuantes no mercado e sem adentrar de forma exaustiva em regras de procedimentos.

Como será operacionalizada a alternativa sugerida?

Por intermédio de regulamento específico sobre a temática de segurança cibernética, que determinará às empresas de telecomunicações instituírem Política de Segurança Cibernética em suas

empresas, de acordo com a sua base de clientes, a natureza e a complexidade dos produtos, serviços, atividades, processos e sistemas das empresas. Desta forma, aspectos de segurança da informação seriam excluídos do escopo do GGRR e seriam transferidos para o referido regulamento.

Este regulamento deve propor, de imediato, os princípios e diretrizes norteadores de tal Política de Segurança Cibernética, bem como instruções mínimas que deveriam estar no escopo desta política.

Sugere-se a restrição da aplicabilidade deste regulamento recair sobre as prestadoras de interesse coletivo, excluídas as de pequeno porte, nos termos definidos na regulamentação da Agência. Por outro lado, é necessário estabelecer, no próprio normativo, mecanismo para inclusão e exclusão de empresas de telecomunicações, de forma que, se necessário, por meio de ato, devidamente motivado, seja possível estender a vigência de tais normativos a qualquer prestadora de serviços de telecomunicações, sob a tutela da Agência, individualmente.

Como a alternativa sugerida será monitorada?

A Agência, a qualquer tempo, poderá requisitar os documentos relacionados à Política de Segurança Cibernética, bem como os documentos que comprovem a sua aprovação pela diretoria da empresa. Porém, este é um controle que visa garantir uma estrutura organizacional e equipe responsável focada na temática de segurança cibernética por parte das empresas. A apresentação, por parte das empresas, de sua Política de Segurança Cibernética à Agência, permite ao órgão regulador comparar as práticas adotadas em cada empresa, e agir como disseminador das melhores práticas identificadas entre as empresas.

Sugere-se, porém, que seja instituído, de imediato no próprio regulamento a ser confeccionado, a figura de um relatório anual sobre esta temática. Os responsáveis pela temática nas empresas, deveriam então, anualmente, apresentar à Agência um relatório identificando os pontos que foram atualizados nos seus processos internos, a quantidade de incidentes relevantes registrados, a análise de suas causas e soluções, a identificação de novas vulnerabilidades, bem como uma análise de riscos atualizada.

Desta forma, o monitoramento da aplicação da Política de Segurança Cibernética ocorre de fato em dois pontos:

a) a própria instituição da Política, identificação de equipe responsável e estrutura organizacional da empresa e aprovação obrigatória da diretoria. Neste ponto é necessário garantir a comprovação da aprovação de tal política pela diretoria da empresa.

b) anualmente ou sempre que solicitado, a empresa deve apresentar relatório à Anatel (por meio do Comitê de que trata o tema 1) sobre a implementação e eficiência da política instaurada, contendo informações importantes como os incidentes relevantes ocorridos naquele ano, identificação dos pontos atualizados na política (alteração de processos internos) e, principalmente, a análise dos riscos identificados relacionados à temática de Segurança Cibernética.

SUBTEMA 03: CULTURA DE SEGURANÇA POR PARTE DOS CONSUMIDORES

SEÇÃO 1
RESUMO DA ANÁLISE DE IMPACTO REGULATÓRIO

A massificação dos dispositivos conectados já é uma realidade e provocou importantes mudanças na economia e no dia a dia das pessoas. Cada vez mais serviços que eram realizados ou solicitados em ambientes físicos agora são feitos no ambiente virtual, com maior facilidade e comodidade. Com a popularização dos *smartphones*, o número de aplicações cresceu vertiginosamente, o que representou uma alta contestabilidade dos mercados tradicionais.

No entanto, a velocidade do aparecimento de inovações trouxe consigo uma série de riscos e vulnerabilidades aos usuários das tecnologias. A convergência dos serviços e dados em um ambiente virtual resultou num atrativo chamariz para criminosos, tendo em vista a forte dependência que se criou das tecnologias e alta atratividade econômica nestes ilícitos. Neste cenário, foi possível observar nos últimos anos a ocorrência de diversos ataques mundiais massivos que tiveram destaque na mídia, em sua maioria, do tipo *ramsonware*, que consiste no sequestro de dados de empresas e indivíduos, exigindo-se uma contrapartida financeira para que estes sejam devolvidos aos seus proprietários.

Além disso, tem-se notícia da crescente utilização de engenharia social na aplicação de golpes e extorsões no ambiente virtual, que se utilizam de técnicas de *phishing*[43] e manipulações nas redes sociais para induzir o usuário de internet a expor vulnerabilidades ou disponibilizar dados valiosos. A mitigação destas ações passa por uma mudança comportamental e adaptação aos dinâmicos riscos virtuais.

Tendo em vista o exposto, cabe a análise de um possível maior protagonismo da Agência e das prestadoras nestas ações de educação e orientação ao consumidor, visto que os referidos riscos, por mais que estejam relacionados ao uso dos serviços de valor adicionado, sujeitam o consumidor desde o momento em que lhe é prestado o serviço de telecomunicação que dá suporte a estes serviços de valor adicionado.

Quais são as opções regulatórias consideradas para o tema?

- *Alternativa A – Manutenção do status quo;*
- *Alternativa B – Promoção, pela Anatel, de ações de conscientização e educação dos consumidores sobre segurança cibernética;*
- *Alternativa C - Promoção, pelas prestadoras, de ações de conscientização e educação dos consumidores sobre segurança cibernética;*

[43] Termo que designa as tentativas de obtenção de informações pessoais por meio de uma suplantação de identidade por parte de criminosos no contexto da internet.

- *Alternativa D – Promoção, pela Anatel e prestadoras, de ações de conscientização e educação dos consumidores sobre segurança cibernética.*

SEÇÃO 2
ANÁLISE DAS ALTERNATIVAS

Alternativa A

Manutenção do status quo

Trata-se manutenção da situação atual, em que há ações desenvolvidas na educação dos consumidores dos serviços de telecomunicações em relação a aspectos de segurança promovidas pela Anatel.

Adicionalmente questões deste tipo também tem sido atualmente feitas pelo CGI.br, muito atuante em questões de segurança na internet e na conscientização dos usuários, por meio do NIC.br, que dispõe de diversas matérias e iniciativas, como o Internet Segura.br (com material destinado à educação de pais e filhos)[44], Antispam.br[45], a Cartilha de Segurança para Internet do CERT.br[46], dentre outras ações.

Caso opte-se por esta alternativa, não haveria custos adicionais dispendidos em campanhas de conscientização, por parte da Anatel, nem por prestadoras que ainda não o fazem. Cumpre mencionar que, por meio da tomada de subsídios, foi possível verificar que a maioria das prestadoras já realiza ações de conscientização de seus clientes, destinando seção específica em seus portais na internet.

Como aspecto negativo desta ação estaria a falta de um engajamento maior da Agência em termos de conscientização do consumidor acerca dos riscos no ambiente cibernético.

Alternativa B

Promoção, pela Anatel, de campanhas de conscientização e educação dos consumidores sobre segurança cibernética.

Neste cenário, a Anatel assumiria um papel mais representativo na conscientização e educação dos consumidores sobre este tema, por meio de campanhas específicas sobre segurança cibernética. Importante destacar, inclusive, que a temática já é tratada pela área da Agência com competência para educação para o consumo. Adicionalmente ao que já é feito, podem ser realizadas divulgações periódicas de boas práticas em segurança e também orientações no caso de incidentes específicos com potenciais impactos na população, como os ocorridos recentemente. Ainda, podem ser divulgadas as cartilhas elaboradas pelo NIC.br que congregam um extenso material abordando diferentes aspectos da segurança cibernética para diferentes públicos (crianças, adolescentes, pais, adultos e empresas).

A desvantagem desta alternativa estaria relacionada aos custos inerentes à elaboração de materiais e realização de atividades de divulgação. Deve-se mencionar, porém, que esse protagonismo da Anatel não

[44] https://internetsegura.br
[45] http://antispam.br/
[46] https://cartilha.cert.br/

implicaria necessariamente em impacto orçamentário de grande vulto, uma vez que a Agência pode utilizar materiais já existentes, assim como colaborar com iniciativas de outras entidades e órgãos dos setores público e privado, academia e sociedade civil. Além disso, pode fazer uso das suas ferramentas de comunicação institucional como página da internet e perfis nas redes sociais para promover essa conscientização.

Alternativa C

Promoção, pelas prestadoras, de ações de conscientização e educação dos consumidores sobre segurança cibernética.

Neste cenário a Anatel continuaria a não se engajar na promoção da conscientização e educação dos consumidores, porém atribuiria essa obrigação às prestadoras de serviços de telecomunicações, as quais já realizam algum tipo de ação, conforme verificado na tomada de subsídios.

De toda sorte, esta alternativa tem como desvantagem a possibilidade de gerar custos adicionais, inerentes à elaboração de materiais e realização de atividades de divulgação, para as prestadoras.

Alternativa D

Promoção, pela Anatel e prestadoras, de campanhas de conscientização e educação dos consumidores sobre segurança cibernética.

Nesta alternativa, além do protagonismo proposto na alternativa B, ficaria estabelecida também a responsabilidade das prestadoras de serviços de telecomunicações da realização de ações de conscientização e educação de seus clientes no que tange aspectos de segurança cibernética. Cumpre destacar mais uma vez a temática já é tratada pela área da Agência com competência para educação para o consumo. Entretanto, devido à relevância do tema, é importante a coordenação entre os diversos agentes envolvidos para permitir a realização de campanhas e ações mais estruturadas.

Cumpre mencionar que, por meio da tomada de subsídios, verificou-se que a maioria das empresas já realiza algum tipo orientação ou educação de seus clientes e algumas oferecem, inclusive, serviços específicos de aprimoramento da segurança. De toda sorte, a Agência poderia facilitar a colaboração e cooperação das prestadoras nessa seara e incentivar a busca da cultura de segurança cibernética no setor de forma mais consistente e efetiva.

Quanto aos custos, valem as mesmas considerações apresentadas para as alternativas B e C.

Resumo da Análise das Alternativas

Alternativa	Vantagens			Desvantagens		
	Prestadoras	Consumidores	Anatel	Prestadoras	Consumidores	Anatel
A	- Prestadoras que não promovem ações de conscientização do	- Não foram identificadas vantagens	- Não há custos envolvidos na promoção de ações de conscientização	- Não foram identificadas desvantagens	- Menor conscientização acerca de aspectos de segurança na	- Não atua no problema apontado.

	consumidor não estariam obrigadas a fazê-lo				utilização dos serviços de telecomunicações	
B	- A campanha feita pela Anatel pode agregar e ter impacto positivo nos ataques cibernéticos contra suas redes em razão da maior conscientização dos usuários.	- Maior conscientização dos consumidores acerca de aspectos de segurança, advindos de ações promovidas pela Anatel.	- Posicionamento institucional de conscientização dos consumidores de serviços de telecomunicações	- Não foram identificadas desvantagens	- Não foram identificadas desvantagens	- Custos advindos da realização de ações de conscientização, mas que podem ser mitigados utilizando se materiais já elaborados por outros órgãos e por meio dos canais já utilizados (página na internet e perfis em redes sociais).
C	- A campanha feita pelas prestadoras que ainda não a fazem pode agregar e ter impacto positivo nos ataques cibernéticos contra suas redes em razão da maior conscientização dos usuários.	- Maior conscientização dos consumidores acerca de aspectos de segurança, advindos de ações promovidas pelas prestadoras.	- Não há custos envolvidos na promoção de ações de conscientização.	- Custos advindos de ações de conscientização dos clientes, no caso de empresas que não realizam tais ações atualmente.	- Menor conscientização acerca de aspectos de segurança na utilização dos serviços de telecomunicações, em relação à alternativa D	- Não participa da atuação no problema apontado (apenas determina atuação dos regulados).
D	- A campanha feita pela Anatel e pelas prestadoras que ainda não a fazem pode agregar e ter impacto positivo nos ataques cibernéticos contra suas redes em razão da maior conscientização dos usuários.	- Maior conscientização dos consumidores acerca de aspectos de segurança, advindos de ações promovidas pelas prestadoras e Anatel	- Ações conjuntas entre Anatel e prestadoras tendem a dar mais efetividade para o problema apontado	- Custos provenientes de ações de conscientização de seus clientes, no caso de empresas que não realizam tais ações atualmente.	- Não foram identificadas desvantagens	- Custos advindos da realização de ações de conscientização, mas que podem ser mitigados utilizando se materiais já elaborados por outros órgãos e por meio dos canais já utilizados (página na internet e perfis em redes sociais)..

SEÇÃO 3
CONCLUSÃO E ALTERNATIVA SUGERIDA

Qual a conclusão da análise realizada?

Tendo em vista as vantagens e desvantagens de cada alternativa, propõe-se a adoção da alternativa D, com a promoção de ações de conscientização da sociedade acerca de aspectos relativos à segurança cibernética, tanto por parte das prestadoras quanto por parte da Anatel. De tal forma, busca-se a disseminação de uma cultura de prevenção a ameaças cibernéticas em um contexto em que estas se tornam cada vez mais frequentes. Assim, adicionalmente às ações de educação para o consumo que já são conduzidas pela área responsável na Anatel, a coordenação entre os diversos agentes afetados poderá implicar em ações e campanhas mais estruturadas. Ainda, é importante ressaltar que os problemas que assim se busca resolver tem causas também em problemas educacionais mais estruturais da sociedade brasileira, de maneira que as ações a serem promovidas pela Anatel e demais agente envolvidos certamente tem uma eficácia limitada.

Como será operacionalizada a alternativa sugerida?

Propõe-se como um dos itens constantes da política cibernética, a ser implementada pelas prestadoras, a disseminação da cultura de segurança cibernética na sociedade. Além disso, ficaria a cargo da Anatel a iniciativa de realizar ações de conscientizações. Tais ações não necessariamente implicariam na produção de um conteúdo próprio por parte da Agência, sendo possível a divulgação de material produzido por outras entidades como o CGI.br. Ainda, poderiam ser utilizados os canais já disponíveis tais como a página da Agência na internet e seus perfis em redes sociais.

Ainda, a Anatel, por intermédio do Comitê específico, pode propor temas e promover o alinhamento das diversas ações de conscientização e educação dos consumidores.

Como a alternativa sugerida será monitorada?

Com a adoção da medida sugerida, espera-se um maior nível de conscientização da sociedade acerca de aspectos relativos à segurança cibernética. No entanto, o monitoramento dos efeitos decorrentes desta ação é de difícil implementação, tendo em vista a complexidade de se determinar o nível de conscientização da população. Assim, o monitoramento dos resultados deve estar alinhado aos processos que a área da Agência com competência para promoção da educação para consumo já possua para aferir os resultados das diversas ações e campanhas que já realiza.

TEMA 03: Produtos para telecomunicações

SEÇÃO 1
RESUMO DA ANÁLISE DE IMPACTO REGULATÓRIO

Descrição introdutória do Tema

A Lei Geral de Telecomunicações (LGT, Lei 9.472/1997) e os instrumentos aprovados pelas Resoluções nº 242/2000 (Regulamento para Certificação e Homologação de Produtos para Telecomunicações) e nº 323/2002 (Norma para Certificação de Produtos para Telecomunicações) estabelecem que cabe à Agência Nacional de Telecomunicações a expedição de normas e padrões a serem cumpridos pelas prestadoras de serviços de telecomunicações quanto aos equipamentos que utilizarem, bem como define todo o sistema de avaliação da conformidade, certificação e homologação dos produtos para telecomunicações no país. Ressalta-se que, consequentemente, tais produtos somente podem ser utilizados ou comercializados no Brasil se forem certificados e homologados pela Agência.

No processo brasileiro, o fabricante submete seu produto de telecomunicação comercial a um laboratório de ensaio, credenciado pelo Inmetro ou avaliado por um Organismo de Certificação Designado pela Anatel (OCD), para a avaliação da conformidade segundo os requisitos técnicos estabelecidos pela Agência e divulgadas em sua página na internet. O fluxograma está delineado na figura a seguir.

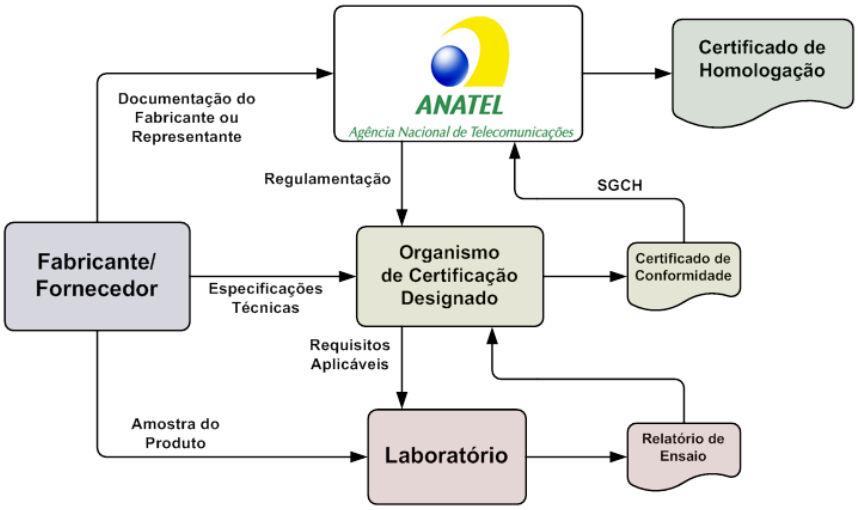

Figura 1. Fluxograma do Processo de Certificação (Fonte: Anatel)

No tocante ao desenvolvimento de normas técnicas, o Regulamento aprovado pela Resolução nº 242/2000 estabelece os princípios gerais dos processos de certificação e homologação de produtos para telecomunicações, entre os quais: assegurar que os fornecedores dos produtos atendam a requisitos mínimos de qualidade para seus produtos; assegurar o atendimento aos requisitos de segurança e de não agressão ao ambiente; e assegurar que os produtos para telecomunicações comercializados no país, em particular aqueles ofertados pelo comércio diretamente ao público, possuam um padrão mínimo de qualidade e adequação aos serviços a que se destinam.

Tema 03: Produtos para telecomunicações

Quando se fala em telecomunicações, encontramos uma diversidade enorme de produtos com características distintas. Dentro dessa categoria de produtos, podemos destacar aqueles que se enquadram no ecossistema da Internet das Coisas (IoT – *Internet of Things*). O conceito de Internet das Coisas significa que "coisas" sejam capazes de usar os protocolos da internet. Esse conceito denota a interligação de várias entidades heterogêneas e de redes que seguem diferentes padrões de comunicações, tais como: Pessoa-para-Pessoa, Pessoa-para-Coisa, Coisa-para-Coisa ou Coisa-para-Coisas.

Nesse conceito, vários dispositivos estão sendo desenvolvidos para utilizar a internet de alta velocidade (redes de quinta geração – 5G) e também aproveitar a estrutura de redes existentes para comunicações com pouco volume de informação e pequenas velocidades de conexão.

O contexto atual sugere uma proliferação de dispositivos utilizando-se das redes de telecomunicações e isso pode se tornar um potencial risco de segurança.

Na prática, o que se observa é que a maior parte dos produtos para telecomunicações que se conectam à internet podem ser enxergados como dispositivos computacionais que entendem e reagem ao ambiente que eles residem. Por exemplo, um drone pode identificar a composição do solo e interagir com a sua central de controle para facilitar o tratamento que será dado àquele terreno antes do seu plantio.

Como dispositivos computacionais, várias questões de segurança merecem atenção. Abaixo, vamos destacar três questões que estão sendo consideradas nos fóruns de discussão internacionais:

***Software* embarcado**: Esses dispositivos embarcam *softwares* que podem conter vulnerabilidades. Tais vulnerabilidades podem ser exploradas para diversos tipos de ataques, como por exemplo, o *Denial-of-Service* (DoS).

Privacidade: Esses dispositivos podem conter câmeras e sistemas de localização por GPS. Um acesso não autorizado poderá indicar a localização de uma pessoa ou poderá revelar informações sensíveis de empresas ou de pessoas por meio do acesso às câmeras ou microfones instalados nos produtos.

Firmware: Semelhante ao caso dos *softwares* embarcados, o *firmware* dos dispositivos pode ser susceptível a ataques quando possui vulnerabilidades. Um grande tema da discussão, na área de segurança dos dispositivos é o processo de atualização do *firmware*. A falta de atualização do *firmware* é um problema recorrente. Outro problema neste contexto é a forma de atualização, que pode ser realizada sem autenticação ou garantia da veracidade do *firmware* que será instalado. Um ataque possível é a substituição do *firmware* do dispositivo por outro "preparado" de tal forma que pode, por exemplo, conceder o controle total do equipamento a uma pessoa não autorizada.

Dado esse pequeno conjunto de exemplos de questões relacionadas à segurança, observa-se que, para tratar tais questões, é necessário desenvolver todo um ecossistema capaz de mitigar esses incidentes. No entanto, é importante lembrar que a cada dia produtos são desenvolvidos em diferentes ambientes para diferentes aplicações e, também, novos ataques surgem a cada nova descoberta de uma vulnerabilidade. Cada produto possui sua particularidade, como poder de processamento e capacidade de memória, entre outras, tornando a solução dependente de uma avaliação quase que caso-a-caso. Assim, propiciar um adequado nível de segurança na área de produtos é um grande desafio.

Qual é o contexto do problema?

A maioria dos produtos para telecomunicações está conectado à internet para troca de informações ou mesmo para sua própria gerência. A conexão com a internet permite o seu gerenciamento remoto, o que é uma facilidade para o suporte da rede. No entanto, esses equipamentos podem possuir vulnerabilidades que permitirão a exploração do produto, de forma não autorizada, com diversos fins, tais como: a realização de ataques e fraudes, especialmente ataques de negação de serviços, propagação de *malwares*, envio de *spam*, furto de credenciais, entre outros.

Nos últimos anos, como apontado na introdução deste documento, teve-se conhecimento de alguns incidentes em que foram exploradas as vulnerabilidades destes equipamentos para a realização de ataques, por exemplo, de negação de serviço distribuído (DDoS), ataque este indicado como sendo o mais recorrente pelas prestadoras de serviços de telecomunicações.

Em outubro de 2016, a Dyn, empresa provedora de serviços de desempenho na internet, sofreu um ataque, onde o *malware* "Mirai" foi responsável pela "captura" de dispositivos de rede para formação de uma *botnet* (ataque por um exército de zumbis) que, por sua vez, foi responsável por um massivo ataque distribuído de negação de serviço nos servidores DNS da empresa, um volume de tráfego aproximado de 1,2 Tbps. Estima-se que, deste volume total de tráfego, cerca de 12% foi proveniente de endereços IPs brasileiros.

Desta forma, tais vulnerabilidades não comprometem apenas a segurança do consumidor proprietário, como também a segurança das demais pessoas conectadas à rede mundial.

Uma atuação da Anatel no tocante aos problemas citados ainda não foi explorada nem desenvolvida nos últimos anos. Assim, faz-se necessário o estudo dos cenários vigente e futuros de modo a identificar ações eficazes capazes de serem concretizadas pela Agência.

Qual o problema a ser solucionado?

Em linha com o contexto exposto, identifica-se como problema a presença de vulnerabilidades de segurança em produtos para telecomunicações conectados à rede mundial (internet), que propicia, entre outros, a proliferação de ataques cibernéticos.

A Agência tem competência para atuar sobre o problema?

As competências da Anatel relacionadas à certificação de produtos estão especificadas na Lei Geral das Telecomunicações – LGT (Lei nº 9.472, de julho de 1997), Título II, artigo 19, incisos XIII e XIV.

O Regimento Interno da Anatel também dispõe, no seu art. 156, inciso VI, que a Superintendência de Outorga e Recursos à Prestação – SOR é a responsável por certificar e homologar produtos de comunicação e sistemas de telecomunicações, habilitar laboratórios e designar organismos certificadores.

No âmbito da SOR, a Gerência de Certificação e Numeração tem, dentre suas competências, as de: (i) elaborar atos normativos de certificação de produtos, em conjunto com a Superintendência de Planejamento e Regulamentação; (ii) elaborar requisitos técnicos, especificações mínimas e procedimentos de ensaio para certificação de produtos e sistemas; além de (iii) realizar a homologação de produtos de comunicação e sistemas de telecomunicações, conforme artigo 185, incisos I, XIX e XX, do Regimento Interno.

Qual(is) o(s) objetivo(s) da ação?

O objetivo geral das ações em estudo é identificar e proporcionar ao consumidor um ambiente com maior segurança cibernética. Aí se incluem a estabilidade e a confiabilidade.

O objetivo imediato é mitigar a probabilidade de ocorrência de ataques cibernéticos que explorem vulnerabilidades existentes em produtos para telecomunicações.

Como o tema é tratado no cenário internacional?

Há diretrizes da OCDE para a Segurança das Redes e Sistemas de Informação: em Direção à Cultura de Segurança, de 2002[47], destacavam como princípio a "Implementação e Desenho de Segurança", alertando que a segurança deveria ser incorporada como elemento essencial das redes e sistemas de informação, os quais deveriam ser desenhados, implementados e coordenados para otimizar a segurança, a fim de evitar ou limitar os potenciais danos das ameaças e vulnerabilidades identificadas sendo que, para o usuário final, o princípio consistiria na seleção e configuração de produtos e serviços para seus sistemas.

Não foram identificadas, até o presente momento, ações em outros países que se relacionem à avaliação da conformidade e homologação de produtos para telecomunicações específicos decorrente de requisitos técnicos específicos compulsórios de segurança digital.

No entanto, verifica-se a tentativa dos reguladores de incentivar a adoção do conceito de "*security by design*", que busca definições mínimas de segurança a serem observadas desde os estágios inicias da concepção dos produtos.

Nesse sentido, a FCC lançou, no final de 2016, consulta pública buscando comentários relacionados à promoção do conceito de "*security by design*" como princípio fundamental do início do desenvolvimento do 5G[48]. A consulta encerrou-se no final de maio de 2017 e aguarda-se o resultado desse processo.

Quais os grupos afetados?

- Fabricantes de equipamentos de telecomunicações;

[47] http://www.oecd.org/sti/ieconomy/15582260.pdf
[48] Disponível em: https://apps.fcc.gov/edocs_public/attachmatch/DOC-343096A1.pdf. Acesso em 14/06/2018. p. 17.

- Prestadoras de serviços de telecomunicações;
- Anatel;
- Consumidores;
- Laboratórios de certificação;
- Organismos de Cerificação Designados (OCDs).

Quais são as opções regulatórias consideradas para o tema?

- *Alternativa A – Manutenção do status quo;*
- *Alternativa B – Estabelecimento de compromisso de correção de vulnerabilidades por parte do fabricante do produto;*
- *Alternativa C – Certificação e homologação de equipamentos de rede, levando em conta requisitos de segurança;*
- *Alternativa D – Avaliações de segurança em produtos já homologados seguindo-se um processo de procura de falhas – Pós-venda específico;*
- *Alternativa E – Criação de especificações para o projeto e a construção de produtos observando-se critérios específicos de segurança;*
- *Alternativa F – Previsão de instrumentos autodeclaratórios em relação à segurança cibernética, para a certificação e homologação de equipamentos.*

SEÇÃO 2
ANÁLISE DAS ALTERNATIVAS

Alternativa A

Manutenção do status quo.

Esta alternativa implica em manter a não atuação desta Agência em relação à avaliação da conformidade e homologação de produtos para telecomunicações no tocante aos requisitos de segurança cibernética.

Assim, não se exige qualquer ação por parte da Agência, evitando assim os percalços da adoção de novas medidas, a exemplo, uma alteração de requisitos técnicos, que poderia gerar custos derivados na cadeia de atores do sistema de avaliação da conformidade brasileiro.

Por outro lado, a manutenção do *status quo* indica que a Agência não atuará sobre o tema, o que é prejudicial para todo o ecossistema de segurança. Assim, esta alternativa somente se justifica na hipótese de os custos das demais alternativas superarem seus respectivos benefícios.

Adicionalmente, tal linha de conduta de não se estabelecer qualquer ação sobre os aspectos de segurança nos produtos poderá induzir os solicitantes da homologação (fabricantes ou representantes comerciais) a não corrigir as falhas de segurança encontrada nos seus produtos, deixando os usuários e as redes de telecomunicações susceptíveis a ataques.

Alternativa B

Estabelecimento de compromisso de correção de vulnerabilidades por parte do fabricante do produto.

Uma outra alternativa que pode ser vislumbrada é a Agência estabelecer uma sistemática de identificação e obrigação de correção de vulnerabilidades encontradas nos dispositivos por parte do fabricante do produto. A partir da identificação de vulnerabilidades pela Agência, o fabricante do produto será notificado a corrigir a vulnerabilidade em um prazo adequado ou, em casos extremos, suspender a comercialização do produto e o retirar do mercado. No caso da correção, o fabricante deverá distribuir a correção da falha de segurança aos seus usuários. Caso o fabricante não faça a correção da vulnerabilidade, a Agência poderá suspender a sua homologação até que a correção seja realizada, considerando-se a legislação vigente. Em último caso, poderá cancelar a homologação do produto.

A grande vantagem dessa alternativa é que a solução poderá ser alcançada nos vários cenários possíveis de vulnerabilidades. Isso permite a flexibilidade de solução necessária para o tratamento das questões de segurança. Assim, a cada vulnerabilidade, o fabricante deverá lançar uma solução para o problema, demonstrando para a Agência a correção da falha.

Essa alternativa possui como desvantagem os custos do processo de comprovação e notificação dos incidentes. Após a identificação da vulnerabilidade, a correção também deverá ser avaliada, para que seja considerada sanada. Para essas atividades, há a necessidade de profissionais específicos e laboratórios de ensaios competentes nesta área, o que, hoje, não fazem parte do escopo dos profissionais da Agência nem do processo de avaliação da conformidade.

Alternativa C

Certificação e homologação de equipamentos de rede, levando em conta requisitos de segurança.

Nesta alternativa, os requisitos técnicos de homologação de produtos para telecomunicações deverão estabelecer parâmetros com propósito de identificar um conjunto mínimo de requisitos de segurança que serão aplicados aos equipamentos quando do seu processo de avaliação da conformidade. Esses requisitos se traduzem em critérios específicos e testes para sua comprovação da conformidade.

A criação de requisitos de segurança verificará se o produto satisfaz aos critérios de segurança fixados no processo de avaliação da conformidade na época dos testes do produto. Essa aproximação tem a vantagem de que os problemas de segurança descritos nos requisitos poderão ser evitados por meio do processo de avaliação da conformidade.

No entanto, em face das características do processo de avaliação da conformidade, observa-se que tende a ser ineficaz a criação de requisitos técnicos de segurança cibernética. Novas vulnerabilidades e formas de ataques são descobertas dinamicamente, o que tornam os requisitos e os ensaios laboratoriais obsoletos rapidamente. Assim, produto que foi ensaiado de acordo com alguns critérios de segurança poderá ser susceptível a novas formas de ataque, o que invalidará a sua “certificação de segurança”. Também, devido à complexidade e a diversidade de tipos de produtos e suas aplicações, serão necessários vários conjuntos de requisitos específicos para cada tipo de aplicação específica. Outra desvantagem a ser considerada é a falsa impressão de que a homologação da Anatel poderia passar com relação à segurança do produto, uma vez que o consumidor acreditará que o seu produto é invulnerável.

Outro custo deste processo é a necessidade de atualização constante dos requisitos técnicos, considerando-se a rapidez da evolução do tema. Essa alteração constante representará em um aumento de custos para o fabricante do produto no processo de certificação, uma vez que tais alterações regulamentares implicarão em novos ensaios aos produtos já homologados.

Ainda, tal alternativa, por si só, não resolve o problema apontado, pois os equipamentos de telecomunicações podem estar sujeitos a problemas de segurança surgidos após sua certificação conforme requisitos que não avaliaram tal falha. Além disso, esta alternativa não vislumbra alinhamento internacional, conforme práticas apontadas na seção anterior.

Alternativa D

Avaliações de segurança em produtos já homologados seguindo-se um processo de procura de falhas – Pós-venda específico.

Uma outra abordagem possível dentro do cenário de avaliação da conformidade de produtos para telecomunicações é o estabelecimento de um programa de testes em produtos já homologados para verificar sua robustez com relação a possíveis ataques ou existência de vulnerabilidades. Esse tipo de processo é muito usado no desenvolvimento de *softwares*, onde várias empresas "certificam" os *softwares* realizando diversos tipos de testes que simulam ataques e outros vários tipos de testes que buscam identificar a robustez dos produtos com relação aos critérios de segurança. A Agência poderia, dentro de um programa de auditoria de pós-venda, coletar vários produtos no mercado e encaminhar para laboratórios específicos de análises de segurança para verificar o seu nível de segurança.

Nesse processo, a cada vez que os produtos são testados, será verificada a existência das vulnerabilidades conhecidas, bem como serão realizados diversos tipos de testes para verificar a robustez do produto com os critérios existentes à época. Essa aproximação tem a grande vantagem da flexibilidade dos ensaios, já que eles serão sempre os mais atualizados, bem como, será um meio de comprovar a possível falha de segurança, permitindo à Agência tomar as ações necessárias.

No entanto, este processo possui a desvantagem da oneração do fabricante com relação aos custos dos novos ensaios que serão realizados na amostra.

Alternativa E

Criação de recomendações técnicas para o projeto e construção de produtos observando-se critérios específicos de segurança.

Nessa alternativa, a Agência desenvolverá e publicará recomendações com o propósito de subsidiar a construção de produtos menos susceptíveis a ataques cibernéticos. Essas recomendações serão publicadas na página da Agência na internet e poderão ser uma base para possíveis ações da Agência com relação aos critérios de segurança. Diferentemente dos requisitos técnicos, que são compulsórios de avaliação da conformidade, as recomendações técnicas serão referências para os projetos de produtos. Assim, não é necessária a sua verificação no processo de avaliação da conformidade.

Essa é a alternativa que vem sendo adotada por diversos países, pois não estabelece soluções engessadas. Isto continua a permitir o desenvolvimento de soluções específicas pelos fabricantes, ao passo que oferece uma referência técnica para a melhoria da segurança dos produtos de telecomunicações.

A grande vantagem dessa alternativa é que serão envolvidos vários atores na construção dessas especificações, sendo que a Agência poderá adotar especificações já desenvolvidas em outros fóruns internacionais, como o IETF (*Internet Engineering Task Force*).

Uma desvantagem para essa alternativa é a necessidade constante de atualização das especificações contidas nas recomendações, exigindo considerável empenho dos envolvidos na atualização dos textos.

Alternativa F

Previsão de instrumentos autodeclaratórios relacionados à segurança cibernética para a certificação e homologação de produtos para telecomunicações.

Neste cenário, os fabricantes interessados na homologação de produtos declaram o atendimento de critérios de segurança vigentes à época da sua expedição. Essa declaração será inserida no processo de avaliação da conformidade.

Em um primeiro momento, foi identificada uma vantagem onde esta declaração estabeleceria um compromisso pelo fabricante de fornecer um produto atendendo aos critérios de segurança vigentes à época.

No entanto, considerando o processo de avaliação da conformidade de certificação vigente, foram identificadas desvantagens com a implementação de tal medida.

A primeira é que, num processo de certificação, as características normalmente devem ser ensaiadas e comprovadas para a expedição de sua conformidade. Uma declaração pode significar a quebra do conceito do processo de avaliação da conformidade por certificação, significando que a avaliação por terceira parte não será realizada, fazendo-se que o processo de certificação da Agência perca credibilidade com relação aos modelos padronizados internacionalmente.

Outra desvantagem é que o fabricante, a partir do momento em que declara atender aos critérios de segurança, isto valeria para a data da expedição de sua declaração. Assim, posteriormente à data de expedição desta declaração, quando for identificada uma vulnerabilidade de segurança no produto decorrente de novos tipos de ataques, por exemplo, o fabricante não poderia ser responsabilizado, já que teria sido certificado para os requisitos de segurança cibernética existentes à época de sua avaliação. Neste contexto, o objetivo não seria alcançado.

Por fim, observou-se que a declaração em si não produz efeitos práticos, além de representar um custo regulatório adicional para o fabricante, materializando-se em mero documento formal.

Resumo da Análise das Alternativas

Alternativa	Vantagens						Desvantagens					
	A	B	C	D	E	F	A	B	C	D	E	F
Fabricantes	- Evita novos custos regulatórios decorrentes da adoção de novas medidas pela Agência.	- Aumento da confiabilidade na empresa ao se comprometer a corrigir as vulnerabilidades identificadas.	- Não foram identificadas vantagens.	- Propicia um cenário competitivo mais justo ao se submeter produtos congêneres de fabricantes diversos aos mesmos testes. - Eliminação de produtos com especificações inferiores.	- Possibilita com que os fabricantes se atentem às diretrizes de segurança cibernética já na fase de projeto do produto. - Mantém a flexibilidade para criação de tecnologias específicas, sem engessamentos produzidos por requisitos técnicos.	- Desnecessidade de avaliação, a priori, por terceiros.	- Falta de transparência perante a sociedade sobre suas ações relacionadas a segurança cibernética.	- Custos decorrentes das correções das vulnerabilidades identificadas.	- Custos muito altos para avaliação e reavaliação da conformidade dos produtos, devido à dinâmica atualização dos requisitos de segurança cibernética.	- Custos decorrentes dos ensaios definidos nas auditorias de pós-venda.	- Não foram identificadas desvantagens.	- Aumento do custo regulatório em face de documentação formal sem efeitos práticos. - Responsabilização em casos conflitantes com a autodeclaração
Prestadoras	- Evita novos custos regulatórios decorrentes da adoção de novas medidas pela Agência.	- Propicia maior segurança cibernética para as redes de telecomunicações.	- Propicia maior segurança cibernética para as redes de telecomunicações.	- Propicia maior segurança cibernética para as redes de telecomunicações.	- Propicia maior segurança cibernética para as redes de telecomunicações.	- Não foram identificadas vantagens.	- Falta de transparência perante a sociedade sobre suas ações relacionadas a segurança cibernética.	- Não foram identificadas desvantagens.	- Não foram identificadas desvantagens.	- Não foram identificadas desvantagens.	- Não foram identificadas desvantagens.	- Não foram identificadas desvantagens.

Tema 03: Produtos para telecomunicações

Anatel	- Evita custos operacionais decorrentes da adoção de novas medidas.	- Fortalece a imagem da Agência em face do seu papel regulador. - Mitiga a ocorrência de incidentes relacionados à segurança cibernética.	- Estabelece de forma direta a conformidade de produtos para telecomunicações com relação à segurança cibernética	- Fortalece a imagem da Agência em face do seu papel regulador. - Mitiga a ocorrência de incidentes relacionados à segurança cibernética.	- Fortalece a imagem da Agência em face do seu papel regulador. - Mitiga a ocorrência de incidentes relacionados à segurança cibernética. - Atua preventivamente.	- Compromisso pelo fabricante de fornecer um produto atendendo aos critérios de segurança vigentes à época	- Depreciação da imagem da Agência em face da não atuação. - Falta de transparência perante a sociedade sobre suas ações relacionadas a segurança cibernética.	- Complexidade na identificação e notificação das vulnerabilidades. - Necessidade de entidade especializada reconhecida pela Anatel para subsidiar a decisão. - Custos operacionais para acompanhamento da atuação do fabricante.	- Alta demanda de recursos operacionais para acompanhar e implementar requisitos de segurança cibernética. - O excesso dessa regulação impede o surgimento de novas tecnologias e soluções para cenários específicos.	- Demanda de recursos operacionais para implementação do programa de auditoria de pós-venda.	- Demanda de recursos operacionais para atualização das recomendações técnicas.	- Deturpa o conceito de avaliação da conformidade centrado em entidades de terceira parte.
Consumidores	- Não foram identificadas vantagens	- Aumento da segurança cibernética experimentada pelos consumidores.	- Aumenta o sentimento de que a segurança cibernética está sendo observada por toda a cadeia.	- Aumento da segurança cibernética experimentada pelos consumidores.	- Aumento da segurança cibernética experimentada pelos consumidores.	- Não foram identificadas vantagens.	- Consumidores ficam mais sujeitos a riscos provenientes de produtos inseguros.	- O compromisso de correção de vulnerabilidades a posteriori poderia deixar o consumidor temporariamente suscetível a falhas e vulnerabilidades. Entretanto, dada à dinâmica da questão, tal problema dificilmente	- Falsa impressão de que os produtos certificados seriam invioláveis.	- Não foram identificadas desvantagens.	- Não foram identificadas desvantagens.	- Não foram identificadas desvantagens.

								não ocorreria mesmo com a definição de requisitos a serem avaliado nos momento da certificação.				
Laboratórios e OCDs	- Não foram identificadas vantagens.	- Agrega valor às suas atividades, tanto em termos financeiros quanto de conhecimentos técnicos. - Desenvolve o corpo técnico brasileiro.	- Agrega valor às suas atividades, tanto em termos financeiros quanto de conhecimentos técnicos. - Desenvolve o corpo técnico brasileiro.	- Agrega valor às suas atividades, tanto em termos financeiros quanto de conhecimentos técnicos. - Desenvolve o corpo técnico brasileiro.	- Agrega valor às suas atividades, tanto em termos financeiros quanto de conhecimentos técnicos. - Desenvolve o corpo técnico brasileiro.	- Não foram identificadas vantagens.	- Não foram identificadas desvantagens.	- Custos para preparação e adequação para a realização dos trabalhos decorrentes das medidas corretivas impostas pela Agência.	- Altos custos para preparação e adequação para a realização dos trabalhos decorrentes dos novos requisitos técnicos.	- Custos para preparação e adequação para a realização dos trabalhos decorrentes do programa de auditoria de pós-venda.	- Não foram identificadas desvantagens.	- Não foram identificadas desvantagens.

SEÇÃO 3
CONCLUSÃO E ALTERNATIVA SUGERIDA

Qual a conclusão da análise realizada?

No caso dos produtos para telecomunicações, de acordo com a análise realizada, verificou-se que as alternativas não são excludentes e, portanto, não existe apenas uma alternativa a ser escolhida. Para se mitigar os problemas de segurança cibernética, identificou-se que será adequado aplicar as alternativas B, D e E para cada caso específico, considerando-se a análise de custos e benefícios apresentados na seção anterior.

Como será operacionalizada a alternativa sugerida?

A implementação das alternativas será realizada conforme descrito abaixo:

- A **alternativa B** será implementada pela monitoração e atuação da Agência quando forem reportados os incidentes, devendo o fabricante ser intimado a corrigir a(s) falha(s) de segurança;
- A **alternativa D** será implementada pela criação de eventos específicos de pós-venda para avaliação dos critérios de segurança em produtos determinados pela Anatel. Essas avaliações compreenderão ensaios que verificarão a robustez dos produtos quanto a ataques cibernéticos;
- Por fim, a **alternativa E** será implementada pela criação de um grupo permanente de estudos e elaboração de especificações técnicas de produtos para telecomunicações, servindo como referência à indústria para o projeto de seus produtos no tocante às questões de segurança.

Ainda, salienta-se que, para a implementação das alternativas escolhidas não se fazem necessários ajustes regulamentares adicionais no presente projeto, uma vez que a regulamentação de certificação (a atual ou mesmo a que se encontra em revisão, já tendo sido realizada Consulta Pública, conforme processo nº 53500.010924/2016-15) são aderentes a tais ações. Em outras palavras, as alternativas aqui escolhidas já encontram respaldo na regulamentação atual sobre certificação ou estão sendo trabalhadas no âmbito do item 16.1 da Agenda Regulatória da Anatel para o biênio 2017-2018, que versa sobre a reavaliação deste regulamentação sobre certificação de produtos de telecomunicações.

Como as alternativas sugeridas serão monitoradas?

As alternativas escolhidas serão monitoradas pela Agência, por meio do processo de avaliação da conformidade, nas atividades específicas da área. Ainda, é possível que a Agência acompanhe e avalie, no âmbito do Comitê específico, proposto no tema 01 deste relatório, a influência dos produtos de telecomunicações em casos concretos (incidentes cibernéticos ocorridos).

TEMA 04: Requisitos técnicos para operação das redes

SEÇÃO 1
RESUMO DA ANÁLISE DE IMPACTO REGULATÓRIO

Descrição introdutória do Tema

Um dos pilares do combate às ameaças cibernéticas é a utilização de tecnologias e soluções desenvolvidas especificamente para proteger o funcionamento das redes destas ameaças. Atualmente, no mercado, há diversas ferramentas dessa natureza: anti-virus, *firewall*, soluções anti-DDoS, anti-*spam*, soluções DNS, entre outros.

Naturalmente, as prestadoras de serviços de telecomunicações investem nestes recursos para garantir um bom funcionamento de suas redes e o volume destes investimentos depende de uma série de variáveis como a base de clientes, valor dos ativos a serem protegidos, capacidade de investimento, riscos relativos a processos judiciais, desempenho da rede, diferencial competitivo, dentre outras.

Neste cenário, cumpre analisar a pertinência de se estabelecer requisitos técnicos mínimos de operação das redes a serem observados pelas prestadoras de serviços de telecomunicações, visto que, diante do fato das diferentes redes serem interconectadas, uma eventual baixa priorização em investimentos em segurança cibernética poderia comprometer o funcionamento e o nível de segurança das demais redes.

Qual é o contexto do problema?

Diante da crescente virtualização dos serviços e a globalização promovida pela evolução tecnológica, aspectos de segurança cibernética tem sido tratados com elevada prioridade no âmbito de discussões envolvendo a indústria, academia e governo. O aumento no número, na robustez e complexidade dos ataques cibernéticos tem gerado preocupações para a sociedade como um todo.

Ainda, em frente ao florescimento e amadurecimento da Internet das Coisas (IoT), a tendência é que aspectos de segurança se tornem cada vez mais relevantes diante de um mundo extremamente interconectado e de forte dependência tecnológica. Relatórios de consultorias no tema têm reportado um forte crescimento do mercado de segurança cibernética, tendo em vista a relevância estratégica que o tema assumiu[49].

Neste contexto, conforme já exposto, a Anatel tem atuado de forma pontual em questões de segurança cibernética (bloqueio da porta 25/TCP e guarda do registro de portas no compartilhamento de

[49] http://www.valor.com.br/empresas/5464667/seguranca-cibernetica-movimenta-us-58-bi-no-brasil

IPv4, por exemplo), sem contar com uma regulamentação específica para o estabelecimento de requisitos mínimos de operação das redes.

Qual o problema a ser solucionado?

Risco de baixo engajamento por parte das prestadoras quanto à utilização de tecnologias e recursos adequados em prol do fortalecimento da segurança de suas redes, comprometendo a segurança das demais redes interconectadas e de seus clientes.

A Agência tem competência para atuar sobre o problema?

A competência da Anatel para atuar no problema se origina na Lei Geral de Telecomunicações (Lei nº 9.472 de 1997), particularmente, em seu art. 19:

> Art. 19. À Agência compete adotar as medidas necessárias para o atendimento do interesse público e para o desenvolvimento das telecomunicações brasileiras, atuando com independência, imparcialidade, legalidade, impessoalidade e publicidade, e especialmente:
>
> (...)
>
> IV - expedir normas quanto à outorga, prestação e fruição dos serviços de telecomunicações no regime público;
>
> (...)
>
> X - expedir normas sobre prestação de serviços de telecomunicações no regime privado;

Qual(is) o(s) objetivo(s) da ação?

Buscar o nível adequado de engajamento por parte das prestadoras de serviços de telecomunicações no que se refere à adoção de tecnologias e recursos necessários para a manutenção de níveis mínimos de segurança nas redes.

Como o tema é tratado no cenário internacional?

Não foram identificadas regulamentações prescritivas, no que se refere a requisitos técnicos de operação das redes. Em geral, tendo em vista a dinâmica da evolução das tecnologias, as normas tendem a recomendar boas práticas e a adoção de processos e estruturas organizacionais como forma de promover a segurança cibernética, conforme apresentado na seção “Tratamento Internacional” disposto na introdução geral deste Relatório.

Quais os grupos afetados?

- Prestadoras de serviços de telecomunicações;
- Anatel;
- Consumidores.

Quais são as opções regulatórias consideradas para o tema?

- *Alternativa A – Manutenção do status quo;*
- *Alternativa B – Definição em regulamentação específica;*
- *Alternativa C – Estabelecimento de diretrizes e comandos no âmbito de um fórum específico, com o apoio do Conselho Diretor;*

SEÇÃO 2
ANÁLISE DAS ALTERNATIVAS

Alternativa A

Manutenção do status quo.

Trata-se de hipótese de não regulamentar mecanismos para estabelecer requisitos técnicos de operação de rede, seja de forma exaustiva em regulamentação ou de forma pontual, no âmbito de um fórum específico. Desta maneira, a Agência continuaria a endereçar este tipo de questão de maneira pontual, caso a caso, sem que esteja definido, a priori, uma área técnica ou grupo responsável por tais medidas.

Esta alternativa não traria custos administrativos advindos de alteração regulamentar. Todavia perde-se a oportunidade de definição de um arcabouço regulatório estruturado para tratamento de questões técnicas de operação das redes. Por possuir pouca aderência à resolução do problema identificado, tal alternativa somente se justifica se os custos das demais alternativas superarem seus benefícios.

Alternativa B

Definição em regulamentação específica.

Neste cenário, propõe-se a edição de um regulamento exaustivo de requisitos técnicos de operação de rede. Este normativo poderia exigir a utilização de protocolos ou soluções tecnológicas (implementação do DNSSEC, obrigatoriedade de utilização de soluções anti-DDoS, entre outros) com o intuito de definir contornos mínimos de segurança das redes.

No entanto, tecnologias empreendidas em segurança de redes são extremamente dinâmicas, em virtude da constante atualização tecnológica e evolução das técnicas envolvidas nas ameaças cibernéticas. Nesta esteira, a edição de um regulamento exaustivo corre o risco de se tornar obsoleto em pouco tempo, requerendo sua constante atualização, que enfrenta como obstáculo para sua viabilidade o tradicional rito processual regulamentar que possui diversas fases, com o envolvimento de diversas áreas da Anatel e, por isso, possui tempo médio de duração não compatível com a dinâmica que o tema de segurança cibernética demanda.

Alternativa C

Estabelecimento de diretrizes e comandos no âmbito de um fórum específico, com o apoio do Conselho Diretor.

Nesta alternativa, eventuais necessidades de se estabelecer requisitos técnicos para a operação das redes de telecomunicações seriam discutidas e deliberadas no âmbito de um fórum específico (no caso, o Comitê apontado como alternativa preferencial no tema 01). Neste caso, decisões acerca de medidas a serem adotadas poderiam ser tomadas dinamicamente caso a caso, como foi feito, por exemplo, na orientação de bloqueio da porta 25/TCP.

Tal cenário é mais compatível com a dinâmica e evolução das tecnologias, protocolos e técnicas de mitigação das ameaças cibernéticas. Por outro lado, em tal cenário, poderia haver maior insegurança jurídica por parte dos regulados, tendo em vista um maior grau de imprevisibilidade das decisões a serem tomadas com base nas discussões deste fórum (seja pelo Conselho Diretor, seja pela área técnica no que se referir a aspectos técnicos ou operacionais), o que certamente pode ser mitigado com a ampla participação no processo de discussão neste fórum.

Resumo da Análise das Alternativas

Alternativa	Vantagens			Desvantagens		
	Prestadoras	Consumidores	Anatel	Prestadoras	Consumidores	Anatel
A	- Não há custos adicionais envolvidos	- Não foram identificadas vantagens	- Não há custos administrativos decorrentes da atuação da Agência no problema	- Não foram identificadas desvantagens	- Risco de utilização de redes menos seguras	- Ausência de atuação da Agência pode gerar insegurança jurídica para o setor, em decorrência de eventuais atuações de outras entidades.
B	- Não foram identificadas vantagens	- Utilização de redes potencialmente mais seguras	- Atuação da Agência no sentido de promover a utilização de redes mais seguras	- Custos decorrentes da possível adaptação de suas redes frente à regulação - Riscos usualmente relacionados à regulamentação excessivamente prescritiva, que pode se tornar obsoleta rapidamente e não endereçar adequadamente a resolução do problema	- Não foram identificadas desvantagens	- Risco de obsolescência do normativo em frente às constantes atualizações tecnológicas
C	- Ações mais alinhadas com a realidade tecnológica, em um ambiente de co-regulação.	- Utilização de redes potencialmente mais seguras	- Atuação da Agência no sentido de promover a utilização de redes mais seguras baseadas em diretrizes mais alinhadas com a realidade tecnológica	- Maior insegurança jurídica em relação à alternativa B, o que pode ser mitigado com ampla participação no processo de discussão no fórum específico.	- Não foram identificadas desvantagens	- Custos relativos ao acompanhamento e às deliberações a serem realizadas acerca de requisitos técnicos para as prestadoras

SEÇÃO 3
CONCLUSÃO E ALTERNATIVA SUGERIDA

Qual a conclusão da análise realizada?

Tendo em vista as vantagens e desvantagens de cada alternativa, sugere-se a adoção da alternativa C, uma vez que uma regulamentação muito prescritiva (alternativa B) tende a se tornar anacrônica, dada a dinâmica e velocidade de evolução das tecnologias. Portanto, propõe-se que eventual decisão por requisitos técnicos deveria ser estudada em fórum específico dentro da Agência, encaminhando-se a proposta para acolhimento ou não pelo Conselho Diretor. Ainda, a alternativa A não endereça adequadamente o problema, somente se justificando caso os custos das demais alternativas superassem seus respectivos custos.

Como será operacionalizada a alternativa sugerida?

A alternativa escolhida pode ser operacionalizada com a criação de um fórum específico (tema 01, que indicou como alternativa preferencial a existência de um Comitê específico para tratar de questões de segurança) para assuntos de segurança cibernética com a previsão regulamentar para que seja possível a adoção de eventuais requisitos técnicos no âmbito deste fórum.

Como a alternativa sugerida será monitorada?

O monitoramento da alternativa pode ser realizado por meio do acompanhamento dos trabalhos a serem desempenhados no âmbito do fórum específico.

TEMA 05: Armazenamento seguro de dados pessoais

SEÇÃO 1
RESUMO DA ANÁLISE DE IMPACTO REGULATÓRIO

Descrição introdutória do Tema

Dentro da temática de segurança cibernética, vários dos ataques cibernéticos que se tem notícia têm como alvo a obtenção de informações sobre dados pessoais armazenados pelo prestador de serviços. Assim, a discussão sobre os níveis de segurança a serem aplicados quando do armazenamento de informações dos usuários dos serviços de telecomunicações naturalmente torna-se elemento relevante no debate amplo sobre segurança cibernética.

Nesse aspecto é que se insere o presente tema que aborda aspectos relacionados ao armazenamento de dados pessoais por prestadoras de telecomunicações no contexto da busca pela segurança da informação.

A proposta, neste tópico, é aprofundar diagnóstico sobre o tratamento normativo da questão no âmbito da regulamentação dos serviços de telecomunicações, com o objetivo de propor, caso necessário, aprimoramentos ao arcabouço regulamentar.

Destaca-se, desde já, que a presente discussão não tem o escopo de antecipar juízo ou mesmo debater sobre a regularidade de novos modelos de negócio relativos ao uso de dados pessoais para o desenvolvimento de produtos e serviços, tendência que vem sendo detectada pelos reguladores de telecomunicações de todo o mundo e também por esta Agência.

Qual é o contexto do problema?

A possibilidade de ações regulatórias da Anatel sobre o presente tema recomenda análise prévia a respeito do arcabouço normativo aplicável à segurança do armazenamento de dados pessoais de consumidores de serviços de telecomunicações.

Quanto a este tema, observa-se que este aspecto específico é objeto, como já mencionado, de disciplina constitucional, a que se alinham diversos dispositivos normativos de ordem legal e regulamentar.

No quadro abaixo, listam-se os dispositivos identificados à temática.

Diplomas normativos	Texto dos dispositivos afetos ao tema
Constituição	Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes: (...) X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o

	direito a indenização pelo dano material ou moral decorrente de sua violação; (...) XII - é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal; (...)
Código de Defesa dos Consumidores – CDC (Lei nº 8.078/1990)	Art. 43. O consumidor, sem prejuízo do disposto no art. 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes. § 1° Os cadastros e dados de consumidores devem ser objetivos, claros, verdadeiros e em linguagem de fácil compreensão, não podendo conter informações negativas referentes a período superior a cinco anos. § 2° A abertura de cadastro, ficha, registro e dados pessoais e de consumo deverá ser comunicada por escrito ao consumidor, quando não solicitada por ele. § 3° O consumidor, sempre que encontrar inexatidão nos seus dados e cadastros, poderá exigir sua imediata correção, devendo o arquivista, no prazo de cinco dias úteis, comunicar a alteração aos eventuais destinatários das informações incorretas. § 4° Os bancos de dados e cadastros relativos a consumidores, os serviços de proteção ao crédito e congêneres são considerados entidades de caráter público. § 5° Consumada a prescrição relativa à cobrança de débitos do consumidor, não serão fornecidas, pelos respectivos Sistemas de Proteção ao Crédito, quaisquer informações que possam impedir ou dificultar novo acesso ao crédito junto aos fornecedores. § 6o Todas as informações de que trata o caput deste artigo devem ser disponibilizadas em formatos acessíveis, inclusive para a pessoa com deficiência, mediante solicitação do consumidor.(Incluído pela Lei nº 13.146, de 2015)
Lei Geral de Telecomunicações – LGT (Lei nº 9.472/1997)	Art. 3º O usuário de serviços de telecomunicações tem direito:(...) IX - ao respeito de sua privacidade nos documentos de cobrança e na utilização de seus dados pessoais pela prestadora do serviço;
Cadastramento de pré-pagos (Lei nº 10.703/2003)	Art. 1º Incumbe aos prestadores de serviços de telecomunicações na modalidade pré-paga, em operação no território nacional, manter cadastro atualizado de usuários. § 1 º O cadastro referido no caput, além do nome e do endereço completos, deverá conter: I - no caso de pessoa física, o número do documento de identidade ou o número de registro no cadastro do Ministério da Fazenda;
Marco Civil da Internet – MCI (Lei nº 12.965/2014)	Art. 3º A disciplina do uso da internet no Brasil tem os seguintes princípios: III - proteção dos dados pessoais, na forma da lei; (...) Art. 7 º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos: (...) VII - não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei;(...) VIII - informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que: a) justifiquem sua coleta;

	b) não sejam vedadas pela legislação; e c) estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet; (...) IX - consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais; X - exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei; (...) Art. 10. A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet de que trata esta Lei, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas. § 1º O provedor responsável pela guarda somente será obrigado a disponibilizar os registros mencionados no caput, de forma autônoma ou associados a dados pessoais ou a outras informações que possam contribuir para a identificação do usuário ou do terminal, mediante ordem judicial, na forma do disposto na Seção IV deste Capítulo, respeitado o disposto no art. 7 º. § 2º O conteúdo das comunicações privadas somente poderá ser disponibilizado mediante ordem judicial, nas hipóteses e na forma que a lei estabelecer, respeitado o disposto nos incisos II e III do art. 7 º. § 3 º O disposto no caput não impede o acesso aos dados cadastrais que informem qualificação pessoal, filiação e endereço, na forma da lei, pelas autoridades administrativas que detenham competência legal para a sua requisição. § 4º As medidas e os procedimentos de segurança e de sigilo devem ser informados pelo responsável pela provisão de serviços de forma clara e atender a padrões definidos em regulamento, respeitado seu direito de confidencialidade quanto a segredos empresariais. Art. 11. Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros. § 1º O disposto no caput aplica-se aos dados coletados em território nacional e ao conteúdo das comunicações, desde que pelo menos um dos terminais esteja localizado no Brasil. § 2 º O disposto no caput aplica-se mesmo que as atividades sejam realizadas por pessoa jurídica sediada no exterior, desde que oferte serviço ao público brasileiro ou pelo menos uma integrante do mesmo grupo econômico possua estabelecimento no Brasil. § 3º Os provedores de conexão e de aplicações de internet deverão prestar, na forma da regulamentação, informações que permitam a verificação quanto ao cumprimento da legislação brasileira referente à coleta, à guarda, ao armazenamento ou ao tratamento de dados, bem como quanto ao respeito à privacidade e ao sigilo de comunicações. § 4º Decreto regulamentará o procedimento para apuração de infrações ao disposto neste artigo. (...) Art. 13. Na provisão de conexão à internet, cabe ao administrador de sistema autônomo respectivo o dever de manter os registros de conexão, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 1 (um) ano, nos termos do regulamento. § 1º A responsabilidade pela manutenção dos registros de conexão não poderá ser transferida a

	terceiros. § 2º A autoridade policial ou administrativa ou o Ministério Público poderá requerer cautelarmente que os registros de conexão sejam guardados por prazo superior ao previsto no caput. § 3º Na hipótese do § 2o, a autoridade requerente terá o prazo de 60 (sessenta) dias, contados a partir do requerimento, para ingressar com o pedido de autorização judicial de acesso aos registros previstos no caput. § 4º O provedor responsável pela guarda dos registros deverá manter sigilo em relação ao requerimento previsto no § 2o, que perderá sua eficácia caso o pedido de autorização judicial seja indeferido ou não tenha sido protocolado no prazo previsto no § 3º. § 5º Em qualquer hipótese, a disponibilização ao requerente dos registros de que trata este artigo deverá ser precedida de autorização judicial, conforme disposto na Seção IV deste Capítulo. § 6º Na aplicação de sanções pelo descumprimento ao disposto neste artigo, serão considerados a natureza e a gravidade da infração, os danos dela resultantes, eventual vantagem auferida pelo infrator, as circunstâncias agravantes, os antecedentes do infrator e a reincidência. Art. 14. Na provisão de conexão, onerosa ou gratuita, é vedado guardar os registros de acesso a aplicações de internet. Art. 15. O provedor de aplicações de internet constituído na forma de pessoa jurídica e que exerça essa atividade de forma organizada, profissionalmente e com fins econômicos deverá manter os respectivos registros de acesso a aplicações de internet, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 6 (seis) meses, nos termos do regulamento. § 1 º Ordem judicial poderá obrigar, por tempo certo, os provedores de aplicações de internet que não estão sujeitos ao disposto no caput a guardarem registros de acesso a aplicações de internet, desde que se trate de registros relativos a fatos específicos em período determinado. § 2º A autoridade policial ou administrativa ou o Ministério Público poderão requerer cautelarmente a qualquer provedor de aplicações de internet que os registros de acesso a aplicações de internet sejam guardados, inclusive por prazo superior ao previsto no caput, observado o disposto nos §§ 3o e 4o do art. 13. § 3º Em qualquer hipótese, a disponibilização ao requerente dos registros de que trata este artigo deverá ser precedida de autorização judicial, conforme disposto na Seção IV deste Capítulo. § 4o Na aplicação de sanções pelo descumprimento ao disposto neste artigo, serão considerados a natureza e a gravidade da infração, os danos dela resultantes, eventual vantagem auferida pelo infrator, as circunstâncias agravantes, os antecedentes do infrator e a reincidência. Art. 16. Na provisão de aplicações de internet, onerosa ou gratuita, é vedada a guarda: I - dos registros de acesso a outras aplicações de internet sem que o titular dos dados tenha consentido previamente, respeitado o disposto no art. 7o; ou II - de dados pessoais que sejam excessivos em relação à finalidade para a qual foi dado consentimento pelo seu titular. Art. 17. Ressalvadas as hipóteses previstas nesta Lei, a opção por não guardar os registros de acesso a aplicações de internet não implica responsabilidade sobre danos decorrentes do uso desses serviços por terceiros.
Regulamentação do Serviço de Atendimento ao Consumidor – SAC	Art. 11. Os dados pessoais do consumidor serão preservados, mantidos em sigilo e utilizados exclusivamente para os fins do atendimento.

(Decreto nº 6.523/2008)	
Contratação de comércio eletrônico (Decreto nº 7.962/2013)	Art. 4º Para garantir o atendimento facilitado ao consumidor no comércio eletrônico, o fornecedor deverá: (...) VII - utilizar mecanismos de segurança eficazes para pagamento e para tratamento de dados do consumidor.
Regulamentação do Marco Civil da Internet (Decreto nº 8.771/2016)	Art. 11. As autoridades administrativas a que se refere o art. 10, § 3º da Lei nº 12.965, de 2014, indicarão o fundamento legal de competência expressa para o acesso e a motivação para o pedido de acesso aos dados cadastrais. § 1º O provedor que não coletar dados cadastrais deverá informar tal fato à autoridade solicitante, ficando desobrigado de fornecer tais dados. § 2º São considerados dados cadastrais: I - a filiação; II - o endereço; e III - a qualificação pessoal, entendida como nome, prenome, estado civil e profissão do usuário. § 3º Os pedidos de que trata o caput devem especificar os indivíduos cujos dados estão sendo requeridos e as informações desejadas, sendo vedados pedidos coletivos que sejam genéricos ou inespecíficos. Art. 12. A autoridade máxima de cada órgão da administração pública federal publicará anualmente em seu sítio na internet relatórios estatísticos de requisição de dados cadastrais, contendo: I - o número de pedidos realizados; II - a listagem dos provedores de conexão ou de acesso a aplicações aos quais os dados foram requeridos; III - o número de pedidos deferidos e indeferidos pelos provedores de conexão e de acesso a aplicações; e IV - o número de usuários afetados por tais solicitações. Art. 13. Os provedores de conexão e de aplicações devem, na guarda, armazenamento e tratamento de dados pessoais e comunicações privadas, observar as seguintes diretrizes sobre padrões de segurança: I - o estabelecimento de controle estrito sobre o acesso aos dados mediante a definição de responsabilidades das pessoas que terão possibilidade de acesso e de privilégios de acesso exclusivo para determinados usuários; II - a previsão de mecanismos de autenticação de acesso aos registros, usando, por exemplo, sistemas de autenticação dupla para assegurar a individualização do responsável pelo tratamento dos registros; III - a criação de inventário detalhado dos acessos aos registros de conexão e de acesso a aplicações, contendo o momento, a duração, a identidade do funcionário ou do responsável pelo acesso designado pela empresa e o arquivo acessado, inclusive para cumprimento do disposto no art. 11, § 3º, da Lei nº 12.965, de 2014; e IV - o uso de soluções de gestão dos registros por meio de técnicas que garantam a inviolabilidade dos dados, como encriptação ou medidas de proteção equivalentes. § 1º Cabe ao CGIbr promover estudos e recomendar procedimentos, normas e padrões técnicos e operacionais para o disposto nesse artigo, de acordo com as especificidades e o porte dos provedores de conexão e de aplicação. § 2º Tendo em vista o disposto nos incisos VII a X do caput do art. 7º da Lei nº 12.965, de 2014,

	os provedores de conexão e aplicações devem reter a menor quantidade possível de dados pessoais, comunicações privadas e registros de conexão e acesso a aplicações, os quais deverão ser excluídos: I - tão logo atingida a finalidade de seu uso; ou II - se encerrado o prazo determinado por obrigação legal. Art. 14. Para os fins do disposto neste Decreto, considera-se: I - dado pessoal - dado relacionado à pessoa natural identificada ou identificável, inclusive números identificativos, dados locacionais ou identificadores eletrônicos, quando estes estiverem relacionados a uma pessoa; e II - tratamento de dados pessoais - toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração. Art. 15. Os dados de que trata o art. 11 da Lei nº 12.965, de 2014, deverão ser mantidos em formato interoperável e estruturado, para facilitar o acesso decorrente de decisão judicial ou determinação legal, respeitadas as diretrizes elencadas no art. 13 deste Decreto. Art. 16. As informações sobre os padrões de segurança adotados pelos provedores de aplicação e provedores de conexão devem ser divulgadas de forma clara e acessível a qualquer interessado, preferencialmente por meio de seus sítios na internet, respeitado o direito de confidencialidade quanto aos segredos empresariais.
Regulamento Geral de Direitos do Consumidor de Serviços de Telecomunicações – RGC (Resolução Anatel nº 632/2014)	Art. 3º O Consumidor dos serviços abrangidos por este Regulamento tem direito, sem prejuízo do disposto na legislação aplicável e nos regulamentos específicos de cada serviço: (...) VII - à privacidade nos documentos de cobrança e na utilização de seus dados pessoais pela Prestadora;
Regulamento do Serviço Móvel Pessoal (Resolução Anatel nº 477/2007)	Art. 42. O documento de adesão do Usuário a Plano Pós-Pago de Serviço deve conter, no mínimo, as seguintes informações: I - a descrição do seu objeto; II - o Código de Acesso do Usuário; III - o Plano de Serviço de opção do Usuário; IV - os dados pessoais do Usuário incluindo, no mínimo: a) nome completo; b) número do documento de identidade; c) número do registro no cadastro do Ministério da Fazenda, se o Usuário estiver incluído neste cadastro; d) endereço.

Tabela 1: Normatização aplicável ao armazenamento de dados de usuários

Acrescente ao quadro acima a discussão corrente, no Poder Legislativo, a respeito de lei ampla que venha a se aplicar à proteção de dados pessoais nos processos de tratamento realizados pelos setores público e privado. A Câmara dos Deputados, aprovou em 29 de maio de 2018, o Projeto de Lei 4.060/2012 que regulamenta o tratamento de dados pessoais no Brasil, o qual tramitará no Senado Federal como

Projeto de Lei da Câmara (PLC) nº 53/2018, juntamente com o Projeto de Lei do Senado (PLS) nº 330/2013, que trata da mesma matéria.

A tabela abaixo consolida alguns conceitos relacionados às discussões legislativas, em contraponto aos dispositivos normativos que já se encontram em vigor.

Tema	Lei nº 12.965/2014	Decreto nº 8.771/2016	PLC nº 4.060/2012	PLS nº 330/2013	PL nº 5.276/2016
Conceituação de dados pessoais	Não há	Art. 14. Para os fins do disposto neste Decreto, considera-se: I - dado pessoal - dado relacionado à pessoa natural identificada ou identificável, inclusive números identificativos, dados locacionais ou identificadores eletrônicos, quando estes estiverem relacionados a uma pessoa;	Art. 7º. Para os fins da presente lei, entende-se como: I – dado pessoal: qualquer informação que permita a identificação exata e precisa de uma pessoa determinada.	Art. 3º Para os efeitos desta lei, considera-se: (...) VIII - dado pessoal: qualquer informação relacionada a pessoa natural identificada ou identificável	Art. 5º Para os efeitos desta Lei, considera-se: I- dado pessoal: dado relacionado à pessoa natural identificada ou identificável, inclusive números identificativos, dados locacionais ou identificadores eletrônicos quando estes estiverem relacionados a uma pessoa;
Definição de tratamento de dados pessoais	Não há	Art. 14. Para os fins do disposto neste Decreto, considera-se: (...) II - tratamento de dados pessoais - toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.	Art. 7º. Para os fins da presente lei, entende-se como: (...) II – tratamento de dados: toda operação ou conjunto de operações, realizadas com ou sem o auxílio de meios automatizados, que permita o armazenamento, ordenamento, conservação, atualização, comparação, avaliação, organização, seleção, extração de dados pessoais.	Art. 3º Para os efeitos desta lei, considera-se: (...) XV -tratamento: qualquer operação ou conjunto de operações realizadas sobre dados pessoais ou banco de dados, com ou sem o auxílio de meios automatizados, tais como coleta, armazenamento, ordenamento, conservação, modificação, comparação, avaliação, organização, seleção, extração, utilização, bloqueio, cancelamento, anonimização, pseudonimização e fornecimento a terceiros, por meio de transferência, comunicação, interconexão ou difusão;	Art. 5º Para os efeitos desta Lei, considera-se: (...) II – tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;
Conceituação de bancos de dados	Não há	Não há	Art. 7º. Para os fins da presente lei, entende-se como: (...) III - banco de dados: todo conjunto estruturado e organizado de dados pessoais, coletados e armazenado em um ou vários locais, em meio eletrônico ou não.	Art. 3º Para os efeitos desta lei, considera-se: (...) II - banco de dados: conjunto estruturado e organizado de dados pessoais, armazenado em um ou vários locais, em meio eletrônico ou não;	Art. 5º Para os efeitos desta Lei, considera-se: (...) V - banco de dados: conjunto estruturado de dados pessoais, localizado em um ou em vários locais, em suporte eletrônico ou físico.

Tema 05: Armazenamento seguro de dados pessoais

Tema	Lei nº 12.965/2014	Decreto nº 8.771/2016	PLC nº 4.060/2012	PLS nº 330/2013	PL nº 5.276/2016
Requisitos de segurança de bancos de dados	Art. 13. Na provisão de conexão à internet, cabe ao administrador de sistema autônomo respectivo o dever de manter os registros de conexão, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 1 (um) ano, nos termos do regulamento. Art. 14. Na provisão de conexão, onerosa ou gratuita, é vedado guardar os registros de acesso a aplicações de internet. Art. 15. O provedor de aplicações de internet constituído na forma de pessoa jurídica e que exerça essa atividade de forma organizada, profissionalmente e com fins econômicos deverá manter os respectivos registros de acesso a aplicações de internet, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 6 (seis) meses, nos termos do regulamento. Art. 16. Na provisão de aplicações de internet, onerosa ou gratuita, é vedada a guarda: I - dos registros de acesso a outras aplicações de internet sem que o titular dos dados tenha consentido previamente, respeitado o disposto no art. 7º; ou II - de dados pessoais que sejam excessivos em relação à finalidade para a	Art. 13. Os provedores de conexão e de aplicações devem, na guarda, armazenamento e tratamento de dados pessoais e comunicações privadas, observar as seguintes diretrizes sobre padrões de segurança: I - o estabelecimento de controle estrito sobre o acesso aos dados mediante a definição de responsabilidades das pessoas que terão possibilidade de acesso e de privilégios de acesso exclusivo para determinados usuários; II - a previsão de mecanismos de autenticação de acesso aos registros, usando, por exemplo, sistemas de autenticação dupla para assegurar a individualização do responsável pelo tratamento dos registros; III - a criação de inventário detalhado dos acessos aos registros de conexão e de acesso a aplicações, contendo o momento, a duração, a identidade do funcionário ou do responsável pelo acesso designado pela empresa e o arquivo acessado, inclusive para cumprimento do disposto no art. 11, § 3º, da Lei nº 12.965, de 2014; e IV - o uso de soluções de gestão dos registros por meio de técnicas que garantam a inviolabilidade dos dados, como encriptação ou medidas de proteção equivalentes. (Art. 13, I, II, III e IV)	Art. 11. O responsável pelo tratamento de dados, bem como eventuais subcontratados, deverão adotar medidas tecnológicas aptas a reduzir ao máximo o risco da destruição, perda, acesso não autorizado ou de tratamento não permitido pelo titular. Parágrafo Único. As medidas a serem adotadas devem ser proporcionais ao atual estado da tecnologia, à natureza dos dados e às características específicas do tratamento, em particular no caso do tratamento de dados sensíveis.	Art. 27. O responsável, o contratado e todos aqueles que tiverem acesso aos dados pessoais por comunicação, interconexão ou qualquer outra forma deverão: I – adotar medidas técnicas de segurança e proteção dos dados atualizadas e compatíveis com os padrões internacionais, com a natureza dos dados tratados e com a finalidade do tratamento; II - limitar seu uso à finalidade que gerou sua coleta; e III - guardar sigilo em relação aos dados, observadas as hipóteses legais. § 1º O dever de sigilo permanece após o encerramento do tratamento. § 2º O responsável e o operador devem manter, por pelo menos cinco anos, registro das operações de tratamento de dados pessoais que realizarem, observada a regulamentação da autoridade competente. Art. 28 . O responsável deverá comunicar imediatamente à autoridade competente a ocorrência de qualquer incidente de segurança que exponha os dados armazenados e tratados ou que possa acarretar prejuízo aos titulares. § 1º O regulamento estabelecerá o conteúdo mínimo da comunicação. § 2º A pronta	Art. 45. O operador deve adotar medidas de segurança técnicas e administrativas aptas a proteger os dados pessoais de acesso não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito. § 1º O órgão competente poderá dispor sore padrões técnicos e organizacionais para tornar aplicável o disposto no caput, levando-se em consideração a natureza das informações tratadas, características específicas do tratamento e o estado atual da tecnologia, em particular no caso de dados sensíveis. § 2º As medidas de segurança deverão ser observadas desde a fase de concepção do produto ou serviço até a sua execução. Art. 46. Os agentes de tratamento ou qualquer outra pessoa que intervenha em uma das fases do tratamento obriga-se ao dever de sigilo em relação aos dados pessoais, mesmo após o seu término. Art. 47. O responsável deverá comunicar ao órgão competente a ocorrência de qualquer incidente de segurança que possa acarretar risco ou prejuízo relevante aos titulares. Parágrafo único. A comunicação será feita em prazo razoável, conforme definido pelo órgão competente, e

Tema	Lei nº 12.965/2014	Decreto nº 8.771/2016	PLC nº 4.060/2012	PLS nº 330/2013	PL nº 5.276/2016
	qual foi dado consentimento pelo seu titular. Art. 17. Ressalvadas as hipóteses previstas nesta Lei, a opção por não guardar os registros de acesso a aplicações de internet não implica responsabilidade sobre danos decorrentes do uso desses serviços por terceiros.			comunicação aos titulares afetados pelo incidente de segurança a que se refere o caput será obrigatória, independente de determinação da autoridade competente, nos casos em que coloque em risco a segurança pessoal do titular. Art. 29. Os responsáveis pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e outros aspectos relacionados ao tratamento de dados pessoais. § 1º Ao estabelecer regras de boas práticas, o responsável pelo tratamento e o operador levarão em consideração a natureza, o escopo e a finalidade do tratamento e dos dados e a probabilidade e a gravidade dos riscos de danos aos indivíduos. § 2º As regras de boas práticas serão disponibilizadas publicamente e atualizadas e poderão ser reconhecidas e divulgadas pela autoridade competente [	deverá mencionar, no mínimo: I – a descrição da natureza dos dados pessoais afetados; II- as informações sobre os titulares envolvidos; III – a indicação das medidas de segurança utilizadas para a proteção dos dados, inclusive procedimentos de encriptação; IV- os riscos relacionados ao incidente; V – os motivos da demora, no caso da comunicação não ter sido imediata; e VI – as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo. Art. 48. O órgão competente verificará a gravidade do incidente e poderá, caso necessário para a salvaguarda dos direitos dos titulares, determinar ao responsável a adoção de outras providências, como: I – pronta comunicação aos titulares; II – ampla divulgação do fato em meios de comunicação; e III- medidas para reverter ou mitigar o efeitos do incidente. § 1º No juízo de gravidade do incidente, será avaliada eventual comprovação de que forma adotadas medidas técnicas adequadas que tornem os dados pessoais afetados ininteligíveis para terceiros não autorizadas a acessá-los. § 2º A pronta comunicação aos titulares afetados pelo

Tema	Lei nº 12.965/2014	Decreto nº 8.771/2016	PLC nº 4.060/2012	PLS nº 330/2013	PL nº 5.276/2016
					incidente de segurança será obrigatória, independente de determinação do órgão competente, nos casos em que for possível identificar que o incidente coloque em risco a segurança pessoal dos titulares ou lhes possa causar danos. Art. 49. Os sistemas utilizados para o tratamento de dados pessoais devem ser estruturados de forma a atender os requisitos de segurança, aos princípios gerais previstos nesta Lei e às demais normas regulamentares. Art. 50. Os responsáveis pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e outros aspectos relacionados ao tratamento de dados pessoais. § 1º Ao estabelecer regras de boas práticas, o responsável pelo tratamento e o operador levarão em consideração a natureza, o escopo e a finalidade do tratamento e dos dados e a probabilidade e a gravidade dos riscos de danos aos indivíduos. § 2º As regras de boas

Tema	Lei nº 12.965/2014	Decreto nº 8.771/2016	PLC nº 4.060/2012	PLS nº 330/2013	PL nº 5.276/2016
					práticas serão disponibilizadas publicamente e atualizadas e poderão ser reconhecidas e divulgadas pelo órgão competente. Art. 51. O órgão competente estimulará a adoção de padrões técnicos que facilitem o controle dos titulares sobre seus dados pessoais.

Tabela 2: Normatização aplicável a dados de usuários x propostas legislativas em andamento

Neste contexto, o foco do presente trabalho de análise consiste em identificar pontos de melhoria ou ajuste da normatização aplicável às tarefas relacionadas <u>especificamente ao armazenamento de dados pessoais por prestadores de serviços de telecomunicações</u>.

Na linha do que dispõe o artigo 13, caput, e incisos I, II, III e IV do Decreto nº 8.771/2016, que regulamentou o Marco Civil da Internet, questões importantes a serem abordadas são, por exemplo, a responsabilidades e perfis de acesso e privilégio, mecanismos de autenticação de acesso aos registros, inventário de acessos aos registros de conexão e de acesso a aplicações, soluções de gestão e técnicas que garantam a inviolabilidade dos dados, como encriptação ou medidas de proteção equivalentes, entre outras.

Qual o problema a ser solucionado?

Riscos de segurança associados ao armazenamento de dados pessoais dos consumidores dos serviços de telecomunicações por parte das prestadoras destes serviços.

A Agência tem competência para atuar sobre o problema?

Com fundamento no que prevê a Lei nº 9.472/1997, Lei Geral de Telecomunicações, especialmente em seu artigo 1º, parágrafo único, e artigo 19, inciso X, a Agência possui competência para tratar de aspectos de segurança cibernética relacionadas aos serviços de telecomunicações, sem prejuízo das competências estabelecidas para o CGI.br, nos termos do art. 13 do Decreto nº 8.771/2016, que regulamentou o Marco Civil da Internet, abaixo copiado.

> Art. 13. Os provedores de conexão e de aplicações devem, na guarda, armazenamento e tratamento de dados pessoais e comunicações privadas, observar as seguintes diretrizes sobre padrões de segurança:

I - o estabelecimento de controle estrito sobre o acesso aos dados mediante a definição de responsabilidades das pessoas que terão possibilidade de acesso e de privilégios de acesso exclusivo para determinados usuários;

II - a previsão de mecanismos de autenticação de acesso aos registros, usando, por exemplo, sistemas de autenticação dupla para assegurar a individualização do responsável pelo tratamento dos registros;

III - a criação de inventário detalhado dos acessos aos registros de conexão e de acesso a aplicações, contendo o momento, a duração, a identidade do funcionário ou do responsável pelo acesso designado pela empresa e o arquivo acessado, inclusive para cumprimento do disposto no art. 11, § 3º, da Lei nº 12.965, de 2014; e

IV - o uso de soluções de gestão dos registros por meio de técnicas que garantam a inviolabilidade dos dados, como encriptação ou medidas de proteção equivalentes.

§ 1º Cabe ao CGIbr promover estudos e **recomendar** procedimentos, normas e padrões técnicos e operacionais para o disposto nesse artigo, de acordo com as especificidades e o porte dos provedores de conexão e de aplicação.

§ 2º Tendo em vista o disposto nos incisos VII a X do caput do art. 7º da Lei nº 12.965, de 2014, os provedores de conexão e aplicações devem reter a menor quantidade possível de dados pessoais, comunicações privadas e registros de conexão e acesso a aplicações, os quais deverão ser excluídos:

I - tão logo atingida a finalidade de seu uso; ou

II - se encerrado o prazo determinado por obrigação legal.

Isto porque o Decreto nº 8.771, de 11 de maio de 2016, que regulamentou o Marco Civil da Internet estabelece claramente, em seu artigo 17, que a Anatel atuará "na regulação, na fiscalização e na apuração de infrações, nos termos da Lei no 9.472, de 16 de julho de 1997". Assim, o dispositivo acima grifado, sobre as competências do CGI.br deve ser interpretado conjuntamente às competências legais da Anatel estabelecidas na LGT e no referido Decreto, especialmente os artigos destacados acima. Ainda, há que se lembrar que o Comitê Gestor da Internet no Brasil (CGI.br), criado por meio do Decreto nº 4.829, de 3 de setembro de 2003, tem como principais competências o estabelecimento de diretrizes e programas relacionados ao uso e desenvolvimento da internet no Brasil, sem contudo retirar as competências legalmente estabelecidas à Anatel como órgão regulador das redes de telecomunicações sobre as quais a internet funciona. Exemplo disso foi o recente trabalho conduzido pela Anatel para a implementação da versão 6 do protocolo de internet (IPv6) nas redes das prestadoras de serviços de telecomunicações brasileiras, situação que somente foi possível frente à competência legal da Agência para regular e fiscalizar estes agentes. Ressalta-se que, durante o referido trabalho em nenhum momento foi questionada a competência da Agência para o trabalho ali conduzido.

Qual(is) o(s) objetivo(s) da ação?

O objetivo imediato da presente ação regulatória é mapear os principais pontos do arcabouço normativo relacionado à segurança cibernética dos serviços de telecomunicações, sob o ângulo da proteção da privacidade e dos dados pessoais de consumidores especificamente no que diz respeito ao armazenamento seguro destes dados.

Em momento posterior da análise, é possível que o presente diagnóstico venha a servir de insumo para a proposição de aprimoramentos ao mencionado arcabouço normativo.

Como o tema é tratado no cenário internacional?

No cenário internacional, o tema da proteção de dados pessoais sob custódia de prestadoras de serviços de telecomunicações também é objeto de iniciativas de segurança cibernética.

Ressalte-se, neste ponto, o marco histórico representado pela entrada em vigor, em 25 de maio de 2018, do Regulamento nº 2016/679 da União Europeia, conhecido como Regulamento Geral de Proteção de Dados (RGPD) – ou, na sigla em língua inglesa, "GDPR" –, o qual contém dispositivos relacionados à segurança dos dados armazenados, transcritos a seguir.

Dispositivo e tema	Texto
Art. 32. Segurança do tratamento	1. Tendo em conta as técnicas mais avançadas, os custos de aplicação e a natureza, o âmbito, o contexto e as finalidades do tratamento, bem como os riscos, de probabilidade e gravidade variável, para os direitos e liberdades das pessoas singulares, o responsável pelo tratamento e o subcontratante aplicam as medidas técnicas e organizativas adequadas para assegurar um nível de segurança adequado ao risco, incluindo, consoante o que for adequado: a) A pseudonimização e a cifragem dos dados pessoais; b) A capacidade de assegurar a confidencialidade, integridade, disponibilidade e resiliência permanentes dos sistemas e dos serviços de tratamento; c) A capacidade de restabelecer a disponibilidade e o acesso aos dados pessoais de forma atempada no caso de um incidente físico ou técnico; d) Um processo para testar, apreciar e avaliar regularmente a eficácia das medidas técnicas e organizativas para garantir a segurança do tratamento. 2. Ao avaliar o nível de segurança adequado, devem ser tidos em conta, designadamente, os riscos apresentados pelo tratamento, em particular devido à destruição, perda e alteração acidentais ou ilícitas, e à divulgação ou ao acesso não autorizados, de dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento. 3. O cumprimento de um código de conduta aprovado conforme referido no artigo 40. ou de um procedimento de certificação aprovado conforme referido no artigo 42. pode ser utilizado como elemento para demonstrar o cumprimento das obrigações estabelecidas no n.o 1 do presente artigo. 4. O responsável pelo tratamento e o subcontratante tomam medidas para assegurar que qualquer pessoa singular que, agindo sob a autoridade do responsável pelo tratamento ou do subcontratante, tenha acesso a dados pessoais, só procede ao seu tratamento mediante instruções do responsável pelo tratamento, exceto se tal lhe for exigido pelo direito da União ou de um Estado-Membro.

Art. 33. Notificação de uma violação de dados pessoais à autoridade de controlo	1. Em caso de violação de dados pessoais, o responsável pelo tratamento notifica desse facto a autoridade de controlo competente nos termos do artigo 55, sem demora injustificada e, sempre que possível, até 72 horas após ter tido conhecimento da mesma, a menos que a violação dos dados pessoais não seja suscetível de resultar num risco para os direitos e liberdades das pessoas singulares. Se a notificação à autoridade de controlo não for transmitida no prazo de 72 horas, é acompanhada dos motivos do atraso. 2. O subcontratante notifica o responsável pelo tratamento sem demora injustificada após ter conhecimento de uma violação de dados pessoais. 3. A notificação referida no n.o 1 deve, pelo menos: a) Descrever a natureza da violação dos dados pessoais incluindo, se possível, as categorias e o número aproximado de titulares de dados afetados, bem como as categorias e o número aproximado de registos de dados pessoais em causa; b) Comunicar o nome e os contactos do encarregado da proteção de dados ou de outro ponto de contacto onde possam ser obtidas mais informações; c) Descrever as consequências prováveis da violação de dados pessoais; d) Descrever as medidas adotadas ou propostas pelo responsável pelo tratamento para reparar a violação de dados pessoais, inclusive, se for caso disso, medidas para atenuar os seus eventuais efeitos negativos; 4. Caso, e na medida em que não seja possível fornecer todas as informações ao mesmo tempo, estas podem ser fornecidas por fases, sem demora injustificada. 5. O responsável pelo tratamento documenta quaisquer violações de dados pessoais, compreendendo os factos relacionados com as mesmas, os respetivos efeitos e a medida de reparação adotada. Essa documentação deve permitir à autoridade de controlo verificar o cumprimento do disposto no presente artigo.
Art. 34. Comunicação de uma violação de dados pessoais ao titular dos dados	1. Quando a violação dos dados pessoais for suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares, o responsável pelo tratamento comunica a violação de dados pessoais ao titular dos dados sem demora injustificada. 2. A comunicação ao titular dos dados a que se refere o n.o 1 do presente artigo descreve em linguagem clara e simples a natureza da violação dos dados pessoais e fornece, pelo menos, as informações e medidas previstas no artigo 33.o, n.o 3, alíneas b), c) e d). 3. A comunicação ao titular dos dados a que se refere o n.o 1 não é exigida se for preenchida uma das seguintes condições: a) O responsável pelo tratamento tiver aplicado medidas de proteção adequadas, tanto técnicas como organizativas, e essas medidas tiverem sido aplicadas aos dados pessoais afetados pela violação de dados pessoais, especialmente medidas que tornem os dados pessoais incompreensíveis para qualquer pessoa não autorizada a aceder a esses dados, tais como a cifragem; b) O responsável pelo tratamento tiver tomado medidas subsequentes que assegurem que o elevado risco para os direitos e liberdades dos titulares dos dados a que se refere o n.o 1 já não é suscetível de se concretizar; ou c) Implicar um esforço desproporcionado. Nesse caso, é feita uma comunicação pública ou tomada uma medida semelhante através da qual os titulares dos dados são informados de forma igualmente eficaz. 4. Se o responsável pelo tratamento não tiver já comunicado a violação de dados pessoais ao titular dos dados, a autoridade de controlo, tendo considerado a probabilidade de a violação de dados pessoais resultar num elevado risco, pode exigir-lhe que proceda a essa notificação ou pode constatar que se encontram preenchidas as condições referidas no n.o 3.
Artigo 40. Códigos de conduta	1. Os Estados-Membros, as autoridades de controlo, o Comité e a Comissão promovem a elaboração de códigos de conduta destinados a contribuir para a correta aplicação do presente regulamento, tendo em conta as características dos diferentes setores de tratamento e as necessidades específicas das micro, pequenas e médias empresas. 2. As associações e outros organismos representantes de categorias de responsáveis pelo tratamento ou de subcontratantes podem elaborar códigos de conduta, alterar ou aditar a esses códigos, a fim de especificar a aplicação do presente regulamento, como por exemplo: a) O tratamento equitativo e transparente; b) Os legítimos interesses dos responsáveis pelo tratamento em contextos específicos; c) A recolha de dados pessoais; d) A pseudonimização dos dados pessoais; e) A informação prestada ao público e aos titulares dos dados; f) O exercício dos direitos dos titulares dos dados; g) As informações prestadas às crianças e a sua proteção, e o modo pelo qual o consentimento do titular das responsabilidades parentais da criança deve ser obtido; h) As medidas e procedimentos a que se referem os artigos 24.o e 25.o e as medidas destinadas a garantir a segurança do tratamento referidas no artigo 30.o; i) A notificação de violações de dados pessoais às autoridades de controlo e a comunicação dessas violações de dados pessoais aos titulares dos dados; j) A transferência de dados pessoais para países terceiros ou organizações internacionais; ou k) As ações extrajudiciais e outros procedimentos de resolução de litígios entre os responsáveis pelo tratamento e os titulares dos dados em relação ao tratamento, sem prejuízo dos direitos dos titulares dos dados nos termos dos artigos 77.o e 79.o. 3. Além dos responsáveis pelo tratamento ou dos subcontratantes sujeitos ao presente regulamento, também os responsáveis pelo tratamento ou subcontratantes que não estão sujeitos ao presente regulamento por força do artigo 3.o podem cumprir códigos de conduta aprovados em conformidade com o n.o 5 do presente artigo e de aplicabilidade geral por força do n.o 9 do presente artigo, de modo a fornecer garantias apropriadas no quadro das transferências dos dados pessoais para países terceiros ou organizações internacionais nos termos referidos no artigo 46.o, n.o 2, alínea e). Os responsáveis pelo tratamento ou os subcontratantes assumem compromissos vinculativos e com força executiva, por meio de instrumentos contratuais ou de outros instrumentos juridicamente vinculativos, no sentido de aplicar as garantias apropriadas, inclusivamente em relação aos direitos dos titulares dos dados. 4. Os códigos de conduta referidos no n.o 2 do presente artigo devem prever procedimentos que permitam ao organismo referido no artigo 41.o, n.o 1, efetuar a supervisão obrigatória do cumprimento das suas disposições por parte dos responsáveis pelo tratamento ou subcontratantes que se comprometam a aplicá-lo, sem prejuízo das funções e competências das autoridades de controlo competentes por força do artigo 55.o ou 56.o. 5. As associações e outros organismos a que se refere o n.o 2 do presente artigo que tencionem elaborar um código de conduta, ou alterar ou aditar a um código existente, apresentam o projeto de código, a alteração ou o aditamento à autoridade de controlo que é competente por força do artigo 55.o. A autoridade de controlo emite um parecer sobre a conformidade do projeto de código de conduta ou da alteração ou do aditamento com o presente regulamento e aprova este projeto, esta alteração ou este aditamento se determinar que são previstas garantias apropriadas suficientes.

	6. Se o código de conduta, ou a alteração ou o aditamento for aprovado nos termos do n.o 5, e se o código de conduta em causa não estiver relacionado com atividades de tratamento realizadas em vários Estados-Membros, a autoridade de controlo regista e publica o código. 7. Se o projeto do código de conduta estiver relacionado com atividades de tratamento realizadas em vários Estados-Membros, a autoridade de controlo competente nos termos do artigo 55.o, antes da aprovação, apresenta o projeto do código, a alteração ou o aditamento, pelo procedimento referido no artigo 63.o, ao Comité, que emite um parecer sobre a conformidade do projeto de código de conduta, ou da alteração ou do aditamento, com o presente regulamento, ou, na situação referida no n.o 3 do presente artigo, sobre a previsão de garantias adequadas. 8. Se o parecer a que se refere o n.o 7 confirmar que o projeto do código de conduta, ou a alteração ou o aditamento, está conforme com o presente regulamento ou, na situação referida no n.o 3, prevê garantias adequadas, o Comité apresenta o seu parecer à Comissão. 9. A Comissão pode, através de atos de execução, decidir que os códigos de conduta aprovados, bem como as alterações ou os aditamentos, que lhe sejam apresentados nos termos do n.o 8 do presente artigo, são de aplicabilidade geral na União. Os referidos atos de execução são adotados pelo procedimento de exame a que se refere o artigo 93.o, n.o 2. 10. A Comissão assegura a publicidade adequada dos códigos aprovados que declarou, mediante decisão, serem de aplicabilidade geral em conformidade com o n.o 9. 11. O Comité recolhe todos os códigos de conduta aprovados, respetivas alterações e respetivos aditamentos num registo e disponibiliza-os ao público pelos meios adequados.
Artigo 42. Certificação	1. Os Estados-Membros, as autoridades de controlo, o Comité e a Comissão promovem, em especial ao nível da União, a criação de procedimentos de certificação em matéria de proteção de dados, bem como selos e marcas de proteção de dados, para efeitos de comprovação da conformidade das operações de tratamento de responsáveis pelo tratamento e subcontratantes com o presente regulamento. Serão tidas em conta as necessidades específicas das micro, pequenas e médias empresas. 2. Além do cumprimento pelos responsáveis pelo tratamento ou pelos subcontratantes sujeitos ao presente regulamento, os procedimentos de certificação em matéria de proteção de dados, bem como selos ou marcas aprovados de acordo com o n.o 5 do presente artigo também podem ser estabelecidos para efeitos de comprovação da existência de garantias adequadas fornecidas por responsáveis pelo tratamento ou por subcontratantes que não estão sujeitos ao presente regulamento por força do artigo 3.o no quadro das transferências de dados pessoais para países terceiros ou organizações internacionais nos termos referidos no artigo 46.o, n.o 2, alínea f). Os responsáveis pelo tratamento ou os subcontratantes assumem compromissos vinculativos e com força executiva, por meio de instrumentos contratuais ou de outros instrumentos juridicamente vinculativos, no sentido de aplicar as garantias adequadas, inclusivamente em relação aos direitos dos titulares dos dados. 3. A certificação é voluntária e está disponível através de um processo transparente. 4. A certificação prevista no presente artigo não diminui a responsabilidade dos responsáveis pelo tratamento e subcontratantes pelo cumprimento do presente regulamento nem prejudica as funções e competências das autoridades de controlo competentes por força do artigo 55.o ou 56.o. 5. A certificação prevista no presente artigo é emitida pelos organismos de certificação referidos no artigo 43.o ou pela autoridade de controlo competente, com base nos critérios por esta aprovados por força do artigo 58.o, n.o 3, ou pelo Comité por força do artigo 63.o. Caso os critérios sejam aprovados pelo Comité, podem ter como resultado uma certificação comum, o Selo Europeu de Proteção de Dados. 6. Os responsáveis pelo tratamento ou subcontratantes que submetem o seu tratamento ao procedimento de certificação fornecem ao organismo de certificação a que se refere o artigo 43.o, ou, consoante o caso, à autoridade de controlo competente, todo o acesso às suas atividades de tratamento e toda a informação de que haja necessidade para efetuar o procedimento de certificação. 7. A certificação é emitida aos responsáveis pelo tratamento e subcontratantes por um período máximo de três anos e pode ser renovada nas mesmas condições, desde que os requisitos aplicáveis continuem a estar reunidos. A certificação é retirada, consoante o caso, pelos organismos de certificação referidos no artigo 43.o ou pela autoridade de controlo competente, se os requisitos para a certificação não estiverem ou tiverem deixados de estar reunidos. 8. O Comité recolhe todos os procedimentos de certificação e todos os selos e marcas de proteção de dados aprovados num registo e disponibiliza-os ao público por todos os meios adequados.

Tabela 3: Resumo dos principais aspectos trazidos pela regulamentação recente da União Europeia sobre proteção de dados (RGPD)

Importante mencionar, ainda, que se encontra em discussão, na Europa, proposta de nova regulamentação aplicável à proteção de dados pessoais no contexto da prestação dos serviços de comunicação eletrônica[50] – conceito que tem sentido definido pela União Europeia. A iniciativa de atualização regulatória trata, em síntese, de rever o conteúdo da diretiva 2002/58, atualmente aplicável à proteção de dados nos serviços de telecomunicações regulados, e harmonizar o teor daquela norma ao previsto no RGPD – este documento, aplicável de forma direta pelos países membros, difere da diretiva existente no que se refere aos seus efeitos imediatos, uma vez que as diretivas exigem esforços dos países membros no sentido da internalização das regras.

50 A proposta de revisão da diretiva 2002/58 encontra-se disponível em https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-privacy-and-electronic-communications.

Tema 05: Armazenamento seguro de dados pessoais

Os seguintes pontos da diretiva 2002/58 que se relacionam à presente AIR são destacados a seguir. Como afirmado acima, tais comandos estão sujeitos à revisão proposta no contexto do esforço regulatório da União Europeia conhecido como *e-Privacy Regulation*, lançado em janeiro de 2017:

Dispositivo e tema	Texto
Artigo 4.o Segurança	1. O prestador de um serviço de comunicações electrónicas publicamente disponível adoptará as medidas técnicas e organizativas adequadas para garantir a segurança dos seus serviços, se necessário conjuntamente com o fornecedor da rede pública de comunicações no que respeita à segurança da rede. Tendo em conta o estado da técnica e os custos da sua aplicação, essas medidas asseguram um nível de segurança adequado aos riscos existentes. 2. Em caso de risco especial de violação da segurança da rede, o prestador de um serviço de comunicações electrónicas publicamente disponível informará os assinantes desse risco e, sempre que o risco se situe fora do âmbito das medidas a tomar pelo prestador do serviço, das soluções possíveis, incluindo uma indicação dos custos prováveis daí decorrentes.
Artigo 5.o Confidencialidade das comunicações	1. Os Estados-Membros garantirão, através da sua legislação nacional, a confidencialidade das comunicações e respectivos dados de tráfego realizadas através de redes públicas de comunicações e de serviços de comunicações electrónicas publicamente disponíveis. Proibirão, nomeadamente, a escuta, a instalação de dispositivos de escuta, o armazenamento ou outras formas de intercepção ou vigilância de comunicações e dos respectivos dados de tráfego por pessoas que não os utilizadores, sem o consentimento dos utilizadores em causa, excepto quando legalmente autorizados a fazê-lo, de acordo com o disposto no n.o 1 do artigo 15.o O presente número não impede o armazenamento técnico que é necessário para o envio de uma comunicação, sem prejuízo do princípio da confidencialidade. 2. O n.o 1 não se aplica às gravações legalmente autorizadas de comunicações e dos respectivos dados de tráfego, quando realizadas no âmbito de práticas comerciais lícitas para o efeito de constituir prova de uma transacção comercial ou de outra comunicação de negócios. 3. Os Estados-Membros velarão por que a utilização de redes de comunicações electrónicas para a armazenagem de informações ou para obter acesso à informação armazenada no equipamento terminal de um assinante ou utilizador só seja permitida na condição de serem fornecidas ao assinante ou ao utilizador em causa informações claras e completas, nomeadamente sobre os objectivos do processamento, em conformidade com a Directiva 95/46/CE, e de lhe ter sido dado, pelo controlador dos dados, o direito de recusar esse processamento. Tal não impedirá qualquer armazenamento técnico ou acesso que tenham como finalidade exclusiva efectuar ou facilitar a transmissão de uma comunicação através de uma rede de comunicações electrónicas, ou que sejam estritamente necessários para fornecer um serviço no âmbito da sociedade de informação que tenha sido explicitamente solicitado pelo assinante ou pelo utilizador.
Artigo 6.o Dados de tráfego	1. Sem prejuízo do disposto nos n.os 2, 3 e 5 do presente artigo e no n.o 1 do artigo 15.o, os dados de tráfego relativos a assinantes e utilizadores tratados e armazenados pelo fornecedor de uma rede pública de comunicações ou de um serviço de comunicações electrónicas publicamente disponíveis devem ser eliminados ou tornados anónimos quando deixem de ser necessários para efeitos da transmissão da comunicação. 2. Podem ser tratados dados de tráfego necessários para efeitos de facturação dos assinantes e de pagamento de interligações. O referido tratamento é lícito apenas até final do período durante o qual a factura pode ser legalmente contestada ou o pagamento reclamado. 3. Para efeitos de comercialização dos serviços de comunicações electrónicas ou para o fornecimento de serviços de valor acrescentado, o prestador de um serviço de comunicações electrónicas publicamente disponível pode tratar os dados referidos no n.o 1 na medida do necessário e pelo tempo necessário para a prestação desses serviços ou dessa comercialização, se o assinante ou utilizador a quem os dados dizem respeito tiver dado o seu consentimento. Será dada a possibilidade aos utilizadores ou assinantes de retirarem a qualquer momento o seu consentimento para o tratamento dos dados de tráfego. 4. O prestador de serviços informará o assinante ou utilizador dos tipos de dados de tráfego que são tratados e da duração desse tratamento para os fins mencionados no n.o 2 e, antes de obtido o consentimento, para os fins mencionados no n.o 3. 5. O tratamento de dados de tráfego, em conformidade com o disposto nos n.os 1 a 4, será limitado ao pessoal que trabalha para os fornecedores de redes públicas de comunicações ou de serviços de comunicações electrónicas publicamente disponíveis encarregado da facturação ou da gestão do tráfego, das informações a clientes, da detecção de fraudes, da comercialização dos serviços de comunicações electrónicas publicamente disponíveis, ou da prestação de um serviço de valor acrescentado, devendo ser limitado ao necessário para efeitos das referidas actividades. 6. Os n.os 1, 2, 3 e 5 são aplicáveis sem prejuízo da possibilidade de os organismos competentes serem informados dos dados de tráfego, nos termos da legislação aplicável, com vista à resolução de litígios, em especial os litígios relativos a interligações ou à facturação.
Artigo 9.o Dados de localização para além dos dados de tráfego	1. Nos casos em que são processados dados de localização, para além dos dados de tráfego, relativos a utilizadores ou assinantes de redes públicas de comunicações ou de serviços de comunicações electrónicas publicamente disponíveis, esses dados só podem ser tratados se forem tornados anónimos ou com o consentimento dos utilizadores ou assinantes, na medida do necessário e pelo tempo necessário para a prestação de um serviço de valor acrescentado. O prestador de serviços deve informar os utilizadores ou assinantes, antes de obter o seu consentimento, do tipo de dados de localização, para além dos dados de tráfego, que serão tratados, dos fins e duração do tratamento e da eventual transmissão dos dados a terceiros para efeitos de fornecimento de serviços de valor acrescentado. Os utilizadores ou assinantes devem dispor da possibilidade de retirar em qualquer momento o seu consentimento para o tratamento dos dados de localização, para além dos dados de tráfego. 2. Nos casos em que tenha sido obtido o consentimento dos utilizadores ou assinantes para o tratamento de dados de localização para além dos dados de tráfego, o utilizador ou assinante deve continuar a ter a possibilidade de, por meios simples e gratuitos, recusar temporariamente o tratamento desses dados para cada ligação à rede ou para cada transmissão de uma comunicação. 3. O tratamento de dados de localização para além dos dados de tráfego, em conformidade com os n.os 1 e 2, deve ficar reservado ao pessoal que trabalha para o fornecedor de redes públicas de comunicações ou de serviços de comunicações electrónicas publicamente disponíveis ou para terceiros que forneçam o serviço de valor acrescentado, devendo restringir-se ao necessário para efeitos de

	prestação do serviço de valor acrescentado.
Artigo 15.o Aplicação de determinadas disposições da Directiva 95/46/CE	1. Os Estados-Membros podem adoptar medidas legislativas para restringir o âmbito dos direitos e obrigações previstos nos artigos 5.o e 6.o, nos n.os 1 a 4 do artigo 8.o e no artigo 9.o da presente directiva sempre que essas restrições constituam uma medida necessária, adequada e proporcionada numa sociedade democrática para salvaguardar a segurança nacional (ou seja, a segurança do Estado), a defesa, a segurança pública, e a prevenção, a investigação, a detecção e a repressão de infracções penais ou a utilização não autorizada do sistema de comunicações electrónicas, tal como referido no n.o 1 do artigo 13.o da Directiva 95/46/CE. Para o efeito, os Estados-Membros podem designadamente adoptar medidas legislativas prevendo que os dados sejam conservados durante um período limitado, pelas razões enunciadas no presente número. Todas as medidas referidas no presente número deverão ser conformes com os princípios gerais do direito comunitário, incluindo os mencionados nos n.os 1 e 2 do artigo 6.o do Tratado da União Europeia. 2. O disposto no capítulo III da Directiva 95/46/CE relativo a recursos judiciais, responsabilidade e sanções é aplicável no que respeita às disposições nacionais adoptadas nos termos da presente directiva e aos direitos individuais decorrentes da presente directiva. 3. O Grupo de Protecção das Pessoas no que respeita ao Tratamento de Dados Pessoais, instituído nos termos do artigo 29.o da Directiva 95/46/CE, realizará também as tarefas previstas no artigo 30.o da mesma directiva no que respeita às matérias abrangidas pela presente directiva, nomeadamente a protecção dos direitos e liberdades fundamentais e dos interesses legítimos no sector das comunicações electrónicas.

Tabela 4: Resumo dos principais aspectos trazidos pela regulamentação da União Europeia sobre proteção de dados e serviços de telecomunicações regulados (Diretiva 2002/58)

Ainda em relação a abordagens internacionais, o Setor de Normalização da UIT (UIT-T) possui recomendação que versa sobre um código de conduta acerca da proteção de informações pessoais. A recomendação ITU-T X.1058 – *Code of practice for personally identifiable information protection*[51] traz uma série de orientações a serem observadas no armazenamento e proteção de dados pessoais. Entre os tópicos, são abordados a estrutura organizacional da empresa, a gestão de recursos humanos, gestão de ativos, controle de acesso, criptografia, segurança física, segurança das operações segurança das comunicações, relações contratuais com fornecedores, entre outros.

Quais os grupos afetados?

- Prestadoras de serviços de telecomunicações;
- Anatel;
- Consumidores.

Quais são as opções regulatórias consideradas para o tema?

- *Alternativa A – Manutenção das regras e requisitos de segurança cibernética atualmente aplicáveis ao armazenamento de dados pessoais por prestadoras de serviços de telecomunicações;*
- *Alternativa B – Estabelecimento, além das regras já existentes nos normativos vigentes, de princípios de segurança cibernética aplicáveis ao armazenamento dos dados pessoais de consumidores por prestadoras de serviços de telecomunicações;*
- *Alternativa C – Estabelecimento, além das regras já existentes nos normativos vigentes, de princípios e regras com detalhamento razoável sobre segurança cibernética, aplicáveis ao*

[51] https://www.itu.int/rec/T-REC-X.1058/

armazenamento dos dados pessoais de consumidores por prestadoras de serviços de telecomunicações;

SEÇÃO 2
ANÁLISE DAS ALTERNATIVAS

Alternativa A

Manutenção das regras e requisitos de segurança cibernética atualmente aplicáveis ao armazenamento de dados pessoais por prestadoras de serviços de telecomunicações

A presente alternativa pressupõe a manutenção integral das regras atualmente existentes quanto à segurança cibernética, como já apontados na introdução desta temática, quando aplicáveis ao armazenamento de dados pessoais por prestadoras de serviços de telecomunicações. Cumpre salientar que atualmente já existem regramentos relacionados à guarda destes dados, tanto na regulamentação da Anatel (por exemplo, sobre guarda de dados cadastrais) quanto em outros normativos (por exemplo, no Marco Civil da Internet e no Decreto nº 8.771/2016, que o regulamentou).

A principal vantagem desta alternativa é a estabilidade gerada pela interlocução já existente entre os atores do setor regulado, a qual pode ser percebida pelos comentários recebidos na tomada de subsídios e pela experiência da Agência com grupos técnicos que abordam determinados aspectos do tema da segurança pública e cibernética.

As principais desvantagens consistem na baixa institucionalização da abordagem atual do tema e na possível lentidão da resposta do regulador a episódios de violação de segurança em situação de acesso indevido aos dados pessoais dos consumidores.

Ainda, por possuir pouca aderência à resolução do problema identificado, tal alternativa somente se justifica se os custos das demais alternativas superarem seus benefícios.

Alternativa B

Estabelecimento, além das regras já existentes nos normativos vigentes, de princípios de segurança cibernética aplicáveis ao armazenamento dos dados pessoais de consumidores por prestadoras de serviços de telecomunicações

A presente alternativa pressupõe a elaboração de princípios aplicáveis ao armazenamento de dados pessoais de consumidores por prestadoras de serviços de telecomunicações, sob o prisma da segurança de redes e sistemas.

O proveito de tal abordagem pode ser exemplificada pelos eixos trazidos pelo RGPD quanto à segurança dos dados pessoais: princípios gerais de segurança de dados pessoais, obrigações relacionadas às notificações ao regulador e ao consumidor do serviço e a adoção de códigos de conduta.

Em juízo preliminar, tal alternativa apresenta, contudo, riscos de persistência do quadro de baixa institucionalização da abordagem atual do tema ante ao baixo esforço dos atores na implantação de procedimentos de segurança não mandatórios.

Alternativa C

Estabelecimento, além das regras já existentes nos normativos vigentes, de princípios e regras com detalhamento razoável sobre segurança cibernética, aplicáveis ao armazenamento dos dados pessoais de consumidores por prestadoras de serviços de telecomunicações

A alternativa C corresponde à abordagem regulatória de construção de regulamentação razoavelmente detalhada (mais exaustiva do que a alternativa anterior, sobre o estabelecimento de princípios e diretrizes) acerca dos requisitos de segurança cibernética aplicáveis aos dados pessoais armazenados por prestadoras de serviços de telecomunicações.

Em juízo superficial, a presente alternativa apresenta vantagem de distribuição adequada do risco negocial envolvido no armazenamento de dados pessoais e, também, do desenvolvimento da confiança necessária à realização das atividades econômicas do setor.

As desvantagens detectadas nesta análise prévia relacionam-se aos custos de transação relacionados ao controle efetivo de tais obrigações pelo órgão regulador, bem como a necessidade de constante atualização de regulamentação mais exaustiva, o que, conforme já disposto nas temáticas anteriores, não atende à dinâmica que as questões de segurança cibernética exigem.

Ainda, ao se optar por um normativo com regras detalhadas, incorre-se no risco de restringir modelos de gestão relativos ao armazenamento de dados, que podem se utilizar de diferentes mecanismos ou procedimentos para resguardar a devida segurança ao consumidor.

Resumo da Análise das Alternativas

Alternativa	Vantagens			Desvantagens		
	Prestadoras	Consumidores	Anatel	Prestadoras	Consumidores	Anatel
A	- Estabilidade que pode ser atribuída à interlocução existente entre os atores do setor regulado.	- Não foram identificadas vantagens	- Estabilidade que pode ser atribuída à interlocução existente entre os atores do setor regulado, a qual pode ser percebida na experiência da Agência com grupos técnicos que abordam determinados aspectos do tema da segurança pública e cibernética.	- Não foram identificadas desvantagens	- Baixa institucionalização da abordagem atual do tema. - Sentimento coletivo no sentido da desproteção de dados pessoais repassados às prestadoras, normalmente associado a episódios publicamente divulgados de vazamentos ou outras modalidades de ataques cibernéticos.	- Baixa institucionalização da abordagem atual do tema. - Baixa capacidade relativa de resposta a eventos de segurança, bem como dificuldade de obtenção dos exatos detalhes de incidentes envolvendo dados pessoais de consumidores armazenados por prestadoras de

			Manutenção do nível atual de familiaridade com a disciplina regulatória atual e contorno de custos indiretos/administrativos relacionados à criação de novas regras, monitoramento e controle da sua aplicação.			serviços de telecomunicações.
B	- Maior liberdade na adoção de procedimentos específicos para o aprimoramento do armazenamento dos dados.	- Possível alinhamento aos eixos trazidos pelo RGPD quanto à segurança dos dados pessoais: princípios gerais de segurança de dados pessoais, obrigações relacionadas às notificações ao regulador e ao consumidor do serviço e adoção de códigos de conduta	- Institucionalização moderada da interlocução existente entre os atores do setor regulado, a qual pode ser percebida na experiência da Agência com grupos técnicos que abordam determinados aspectos do tema da segurança pública e cibernética. - Manutenção ou aumento moderado do nível atual de familiaridade com a disciplina regulatória atual e contorno de custos indiretos/administrativos relacionados à criação de novas regras, monitoramento e controle da sua aplicação.	- Eventuais custos relativos à obrigatoriedade de implantar procedimentos acerca do armazenamento de dados.	- Não foram identificadas desvantagens	- A maior flexibilidade na adoção de procedimentos relativos ao armazenamento dos dados pode dificultar o acompanhamento da Agência.
C	- Aprovação de normas setoriais específicas pode levar a possível aumento da sensação de segurança jurídica no que se refere ao armazenamento de dados pessoais por operadoras de serviços de telecomunicações.	- Possível aumento de confiança do consumidor, essencial para o desenvolvimento das atividades econômicas do setor.	- Maior facilidade de acompanhamento pela Agência, dada a menor flexibilidade concedida às empresas.	- Extensão do trabalho – custos indiretos --de mapeamento das obrigações regulatórias a serem propostas, bem como custos de transação relacionados ao controle efetivo de tais obrigações pelo órgão regulador. - Risco de restrição a diferentes modelos de gestão de segurança do armazenamento dos dados. - Regulamentação mais detalhada pode impor alta carga regulatória.	- Não foram identificadas desvantagens.	- Riscos relacionados ao estabelecimento de uma regulamentação detalhada que pode restringir modelos de negócio e inibir a competição. - Altos custos administrativos relacionados à constante necessidade de atualização do arcabouço regulamentar mais detalhado, que corre o risco de se tornar rapidamente obsoleto frente à dinâmica que as questões de segurança cibernética exigem.

SEÇÃO 3
CONCLUSÃO E ALTERNATIVA SUGERIDA

Qual a conclusão da análise realizada?

Propõe-se a adoção da alternativa B, que consiste no estabelecimento de princípios gerais de segurança cibernética aplicáveis ao armazenamento de dados pessoais de consumidores por prestadoras de serviços de telecomunicações.

Como exposto na seção anterior, a principal vantagem da alternativa B consiste na oportunidade de aproveitar o esforço multissetorial decorrente da entrada em vigor do RGPD (regulamentação da União Europeia sobre o tema) para construir consensos nacionais a respeito do caráter essencial da proteção de dados pessoais para a inovação tecnológica e o desenvolvimento de novos negócios.

Espera-se que as desvantagens apontadas sejam superadas como os esforços propostos pela Agência no sentido da construção de mecanismos institucionais aplicáveis ao tema da segurança cibernética, os quais também poderão ser ativados em contextos e/ou episódios de violação de dados pessoais. Neste sentido, o fórum (Comitê de Segurança) apontado como solução preferencial para o tema 1 certamente ocupará espaço importante na discussão desta temática.

Ainda, a alternativa B foi escolhida em detrimento da alternativa C por endereçar tais questões de maneira mais dinâmica. Em outras palavras, considerando a velocidade em que evoluem as práticas que atentem contra estes aspectos de segurança, é mais efetivo que a regulamentação estabeleça princípios gerais ao invés de ser por demais exaustiva, sob pena de se tornar rapidamente obsoleta. Com base nestes princípios gerais, os foros criados a partir da proposta deste relatório de AIR poderão debater e recomendar medidas e aspectos operacionais de maneira mais dinâmica e célere como o tema demanda.

Como será operacionalizada a alternativa sugerida?

A alternativa proposta será operacionalizada por meio da inclusão, em regulamento sobre segurança cibernética, da exigência de procedimentos relativos ao armazenamento seguro dos dados pessoais, no âmbito da política de segurança cibernética a ser implementada pela prestadora de serviços de telecomunicações. Ainda, sugere-se a inclusão de princípios visando à adoção de boas práticas e ao direito à privacidade do usuário em relação aos seus dados pessoais.

Como já observado, a abordagem regulamentar baseia-se, em linhas gerais, na construção de diretrizes aplicáveis ao tema e no desenvolvimento de mecanismos institucionais de diálogo e cooperação entre os atores direta ou indiretamente envolvidos no processo regulatório e os agentes econômicos do setor de telecomunicações.

Vale destacar que, a despeito da regulamentação a ser adotada pela Agência, o Decreto nº 8.771/2016, que regulamenta o Marco Civil da Internet, já estabeleceu obrigações e procedimentos relativos ao armazenamento de dados pessoais a serem observados pelos provedores de conexão. Quanto

a isso, cumpre à Anatel realizar a verificação se tais procedimentos estão sendo adotados, por meio do acompanhamento da política de segurança cibernética, a ser implementada pelas prestadoras.

Como a alternativa sugerida será monitorada?

A luz do seu caráter específico, a alternativa escolhida não permite, no presente momento, o desenvolvimento de indicadores quantitativos.

Sob a perspectiva qualitativa, contudo, espera-se que a abordagem proposta contribua para aumentar a agilidade da resposta do regulador de telecomunicações no cenário descrito e, também, para a elevação dos níveis de percepção da segurança cibernética pelos atores envolvidos com a temática. A temática também será acompanhada dentro do Comitê de Segurança, apontado como alternativa preferencial no tema 1.