Boletim de Serviço Eletrônico em 17/12/2020

ANATEL
Agência Nacional de Telecomunicações

VOTO Nº 87/2020/PR

Processo nº 53500.078752/2017-68

Interessado: Prestadoras de Serviços de Telecomunicações

CONSELHEIRO

LEONARDO EULER DE MORAIS

1. **ASSUNTO**

1.1. Proposta de reavaliação da regulamentação relacionada a serviços públicos de emergência e à segurança de redes de telecomunicações - Item nº 7 da Agenda Regulatória para biênio o 2019-2020.

2. **EMENTA**

REAVALIAÇÃO DA REGULAMENTAÇÃO RELACIONADA A SERVIÇOS PÚBLICOS DE EMERGÊNCIA E À SEGURANÇA DE REDES DE TELECOMUNICAÇÕES. ITEM 7 DA AGENDA REGULATÓRIA DO BIÊNIO 2019-2020. ACOMPANHA O RELATOR, COM ACRÉSCIMOS. DETERMINA OUTRAS PROVIDÊNCIAS.

2.1. Proposta de Reavaliação da regulamentação relacionada a serviços públicos de emergência e à segurança de redes de telecomunicações prevista no item nº 7 da Agenda Regulatória para biênio o 2019-2020.

2.2. Pela aprovação de Resoluções que: (i) alteram o Regulamento dos Serviços de Telecomunicações, para incluir disposições sobre sigilo, prevenção à fraude e ações de apoio à segurança pública; (ii) aprovam o Regulamento sobre o Uso de Serviços de Telecomunicações em Desastres, Situações de Emergência e Estado de Calamidade Pública; e (iii) aprovam o Regulamento de Segurança Cibernética Aplicada ao Setor de Telecomunicações, nos termos da Análise do Relator, com os acréscimos do Voto do Presidente Leonardo Euler de Morais.

2.3. Determina outras providências a serem tomadas pelo Grupo Técnico de Segurança Cibernética e Gestão de Riscos de Infraestrutura Crítica (GT-Ciber) e pela Superintendência de Planejamento e Regulamentação (SPR).

3. **REFERÊNCIAS**

3.1. Lei Geral de Telecomunicações (LGT), Lei nº 9.472, de 16 de julho de 1997;

3.2. Marco Civil da Internet, Lei nº 12.965, de 23 de abril de 2014;

3.3. Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709, de 14 de agosto de 2018;

3.4. Política Nacional de Segurança da Informação, Decreto nº 9.637, de 26 de dezembro de 2018;

3.5. Glossário de Segurança da Informação, Portaria nº 93, de 26 de setembro de 2019;

3.6. Estratégia Nacional de Segurança Cibernética, Decreto nº 10.222, de 05 de fevereiro de 2020;

3.7. Requisitos Mínimos de Segurança Cibernética para as redes 5G, Instrução Normativa – GSI nº 4, de 26 de março de 2020;

3.8. Estrutura de Gestão da Segurança da Informação nos Órgãos e nas Entidades da Administração Pública Federal, Instrução Normativa GSI nº 1, de 27 de maio de 2020;

3.9. Consulta Pública nº 52/2019 (SEI nº 3726050);

3.10. Informe nº 40/2019/PRRE/SPR (SEI nº 4013678);

3.11. Análise nº 31/2020/MM (SEI nº 5233452);

3.12. Voto nº 113/2020/PR (SEI nº 6133338);

3.13. Informe nº 161/2020/PRRE/SPR (SEI nº 6236795); e

3.14. Regimento Interno da Anatel, aprovado pela Resolução nº 612, de 29 de abril de 2013.

4. **RELATÓRIO**

4.1. A presente proposta esteve disponível para comentários e contribuições da sociedade em geral por meio da Consulta Pública nº 52/2019 (SEI nº 3726050). Foram recebidas ao todo 336 (trezentas e trinta e seis) manifestações, que se encontram consolidadas, devidamente analisadas e motivadamente respondidas no Informe nº 40/2019/PRRE/SPR (SEI nº 4013678) e seus anexos.

4.2. Em 30 de abril de 2020, na 883ª Reunião do Conselho Diretor, o Conselheiro Moisés Queiroz Moreira apresentou relatoria da matéria em epígrafe, consubstanciada em sua Análise nº 31/2020/MM (SEI nº 5233452).

4.3. Naquela ocasião, com o fito de analisar mais detidamente o mérito da proposta, foi solicitada vista dos autos, com fundamento no art. 15 do Regimento Interno da Anatel (RIA), aprovado mediante a Resolução nº 612/2013.

4.4. Em razão da complexidade do tema e da necessidade de colher subsídios complementares para formação do convencimento, solicitou-se a prorrogação do prazo de vistas, por 120 (cento e vinte) dias, conforme previsão constante do art. 16, § 1º do RIA.

4.5. Posteriormente, na 892ª Reunião, realizada em 29 de outubro de 2020, o Conselho Diretor aprovou, por unanimidade, a conversão da deliberação em diligência à Superintendência de Planejamento e Regulamentação (SPR), pelo prazo de 30 (trinta) dias, nos termos do Voto nº 113/2020/PR (SEI nº 6133338).

4.6. Mediante o Informe nº 161/2020/PRRE/SPR (SEI nº 6236795) a SPR prestou os esclarecimentos solicitados.

4.7. É o breve relato.

DAS CONSIDERAÇÕES POR PARTE DESTE CONSELHEIRO

4.8. A presente matéria objetiva a atualização e o aprimoramento do arcabouço normativo relacionado a três áreas de atuação regulatória, condensadas nos seguintes grupos temáticos inter-relacionados:

1. o acesso aos serviços públicos de emergência, a guarda de informações e registros dos usuários e as regras operacionais aplicáveis para cumprimento de decisões de violação de sigilo, previstas na legislação, além de condutas a serem adotadas pelas prestadoras para o combate das diversas formas de fraude em suas redes e serviços;
2. a preparação e a resposta das redes e serviços de telecomunicações face a desastres, emergências e calamidades públicas, a divulgação de alertas aos usuários dos diferentes serviços, a coordenação de esforços com autoridades nacionais e locais e os respectivos planejamentos de contingência e de restabelecimento dos serviços; e
3. as medidas de proteção e segurança cibernética para as redes e serviços de telecomunicações, associadas à gestão de riscos em infraestruturas críticas, consoantes às diretrizes estabelecidas na respectiva política nacional.

4.9. Para tratar do primeiro tema, a proposta de revisão regulamentar prevê a inclusão de uma seção específica ao “Regulamento dos Serviços de Telecomunicações” (Resolução nº 73/1998), com capítulos distintos para cada um dos tópicos desse grupo. Adicionalmente, a proposta dispõe sobre o estabelecimento do Grupo Técnico de Suporte à Segurança Pública (GT-Seg), com competências para orientar e acompanhar a implementação das medidas.

4.10. Para o segundo tema acima relacionado está prevista a bipartição e substituição do "Regulamento sobre Gestão de Risco das Redes de Telecomunicações e Uso de Serviços de Telecomunicações em Desastres, Situações de Emergência e Calamidade Pública" (Resolução nº 656/2015). Como primeiro produto dessa secção, o novo "Regulamento Sobre o Uso de Serviços de Telecomunicações em Desastres, Situações de Emergência e Estado de Calamidade Pública" terá por foco o preparo e a atuação em emergências e desastres, e contará com o suporte operacional da Rede Nacional de Emergência de Prestadoras de Telecomunicações (RENET), coordenada pela Anatel e já implantada no bojo do regulamento hoje vigente.

4.11. Para o terceiro e último tema, em um novo normativo, o "Regulamento de Segurança Cibernética Aplicada ao Setor de Telecomunicações", soma-se a temática de segurança cibernética às regras que tratam de infraestruturas críticas, reformuladas e ampliadas. Para coordenar a implementação das ações, de modo semelhante aos dois casos anteriores, a proposta em tela prevê o estabelecimento do Grupo Técnico de Segurança Cibernética e Gestão de Riscos de Infraestrutura Crítica (GT-Ciber).

4.12. Como visto, nesta revisão normativa há três grandes frentes temáticas sendo reavaliadas. Duas delas, todavia, já se encontram consideravelmente abrangidas pela regulamentação vigente (muito embora com alguma dispersão, em alguns casos) e para elas são discutidos aprimoramentos e atualizações às regras e procedimentos atualmente utilizados.

4.13. Diferentemente, para a segurança cibernética há um trabalho mais elementar a ser realizado nesta primeira interação do tema no arcabouço normativo da Agência. Ela começa, porém, a tomar forma a partir de uma sólida base regulatória já estabelecida e rastreada na experiência acumulada das reavaliações de institutos, normas e instrumentos promovidas pela Agência nos últimos anos.

4.14. E nisto justamente repousa a essência das considerações que serão apresentadas ao longo do presente Voto, qual seja: a formulação e consolidação, pela Anatel, das ferramentas, capacidades e informações necessárias para o adequado cumprimento do seu papel na regulação dos aspectos técnico-regulatórios relacionados à segurança do espaço cibernético.

4.15. Antecipa-se que o teor deste Voto é bastante próximo ao daquele constante da proposta relatada na 883ª Reunião do Conselho Diretor pelo Conselheiro Moisés Queiroz Moreira, mediante sua Análise nº 31/2020/MM (SEI nº 5233452).

4.16. Os dois primeiros temas são acompanhados quase que na íntegra, ressalvados pequenos ajustes textuais, enquanto que para o último deles se propõe a modulação de algumas das obrigações previstas e um refinamento e aprofundamento nas atribuições e diretivas de trabalho a serem perseguidas pelo grupo técnico que será estabelecido, o GT-Ciber, pelos motivos que serão explicados nas seções seguintes.

4.17. Além disso, considerando as mudanças de redação e inovações incorporadas à minuta da proposta em decorrência das contribuições recebidas na Consulta Pública e da instrução processual subsequente, propõe-se uma reorganização das seções e capítulos da minuta, para fins de clareza e facilidade de compreensão.

4.18. Por fim, em vista da recente publicação de novas referências nacionais e internacionais sobre o tema, para conferir maior objetividade e uniformidade aos dispositivos normativos, são apresentadas algumas propostas de aprimoramento conceitual e terminológico.

Do Órgão Regulador das Telecomunicações no contexto da segurança cibernética

4.19. O termo 'segurança cibernética' é bastante profícuo em significados e interpretações. No âmbito das telecomunicações, utiliza-se normalmente como referência o conceito definido na Recomendação ITU-T X.1205[1], do Setor de Normatização da União Internacional de Telecomunicações (UIT).

4.20. Essa Recomendação estabelece a taxonomia elementar associada ao tema e define termos e conceitos tais como ameaça e vulnerabilidade cibernética, elenca princípios de segurança e resiliência

de redes e sistematiza diferentes técnicas, abordagens, ferramentas tecnológicas e remédios utilizados na gestão de riscos de cibersegurança. Ressalta-se aqui a grande amplitude e generalidade reservada ao conceito de cibersegurança, definido como "*o conjunto de instrumentos, políticas, acepções de segurança, salvaguardas de segurança, diretrizes, abordagens de gestão de risco, ações, treinamentos, melhores práticas, garantias e tecnologias que podem ser empregados para proteger o ambiente cibernético e os ativos de usuários e organizações (...)*"[2].

4.21. Não bastasse o desafio de regular, no âmbito das telecomunicações, algo conceitualmente tão abrangente e de contornos tão nebulosos, a segurança cibernética, em sua implementação, é intrinsecamente multidisciplinar, transversal e intersetorial. Disso resulta uma pulverização de atribuições e competências entre as mais variadas instituições e jurisdições da Administração Pública, bem como uma constante presença do tema, ainda que por vezes tangencial, em diversas políticas públicas e nas relações intergovernamentais.

4.22. A cibersegurança atrai para si discussões associadas à política econômica e industrial, por exemplo. Ela contempla questões afetas à privacidade dos usuários e à proteção da propriedade intelectual. É elemento essencial na gestão dos riscos relacionados às infraestruturas críticas deste setor regulado pela Anatel, bem como todas as demais infraestruturas (energia, saneamento, transportes, finanças etc.), pois são justamente as telecomunicações que fornecem o elo fundamental que a todos une.

4.23. As telecomunicações não apenas viabilizam e potencializam a produtividade econômica e a geração de riqueza, como são essenciais para a realização da plena cidadania na sociedade da informação em que vivemos. Por conseguinte, a salvaguarda da integralidade do sistema brasileiro de telecomunicações e, individualmente, de suas funcionalidades e componentes essenciais, são da mais alta importância para o Estado brasileiro. Em outros termos, a segurança do espaço cibernético deve compor a agenda de prioridade máxima de um Estado Soberano.

4.24. Nesse sentido, o Decreto nº 10.222/2020 instituiu a Estratégia Nacional de Segurança Cibernética (E-Ciber) para o quadriênio 2020-2023, em complementação da Política Nacional de Segurança da Informação (PNSI), estabelecida no âmbito da administração pública federal pelo Decreto nº 9.637/2018.

4.25. A E-Ciber é o primeiro "módulo" de objetivos e ações estratégicas a ser publicado, dos cinco previstos no art. 6º da PNSI. Ela foi concebida com o propósito de alinhar e nortear ações públicas para tornar mais resiliente e seguro o uso do espaço cibernético. Para isso, a E-Ciber especifica um conjunto de dez ações estratégicas, a saber:

- Fortalecer as ações de governança cibernética;
- Estabelecer um modelo centralizado de governança no âmbito nacional;
- Promover ambiente participativo, colaborativo, confiável e seguro, entre setor público, setor privado e sociedade;
- Elevar o nível de proteção do Governo;
- Elevar o nível de proteção das Infraestruturas Críticas Nacionais;
- Aprimorar o arcabouço legal sobre segurança cibernética;
- Incentivar a concepção de soluções inovadoras em segurança cibernética;
- Ampliar a cooperação internacional do Brasil em Segurança cibernética;
- Ampliar a parceria, em segurança cibernética, entre setor público, setor privado, academia e sociedade; e
- Elevar o nível de maturidade da sociedade em segurança cibernética.

4.26. A E-Ciber, ao mesmo tempo em que estabelece diretrizes e prioridades para a temática de cibersegurança, também fornece o contexto institucional de atuação para o Órgão Regulador de

Telecomunicações, integrado a um amalgamado mais amplo de ações e esforços coordenados em diferentes esferas governamentais.

4.27. Dito de outro modo, a atuação da Anatel não é, de forma alguma, dissociada dessa plataforma unificada concebida pela Política e pela Estratégia Nacional. Muito pelo contrário: ao exporem, por exemplo, suas preocupações com o verificado crescimento das ameaças no espaço virtual e dos índices de criminalidade cibernética, bem como indicarem como rumos a serem perseguidos, ainda a título exemplificativo, uma maior segurança no uso de serviços de governo eletrônico, uma maior resiliência para as infraestruturas críticas nacionais e um aprimoramento geral da cultura em segurança cibernética, esses instrumentos de política pública tecem o próprio substrato de atuação da Anatel sobre a temática de cibersegurança, no âmbito de atribuições e competências institucionais da Agência.

4.28. Em vista disso e considerando as disposições legais e sua missão institucional, o vetor de atuação reservado para a Agência nesse contexto só pode-deve ser eminentemente técnico-regulatório e exercido exclusivamente dentro desse mesmo *framework*.

Da transição à quinta geração das redes móveis terrestres (5G)

4.29. Muito embora a temática segurança cibernética preceda o IMT-2020, as redes móveis de quinta geração têm, de certa forma, simbolizado essa discussão, uma vez que com a virtualização de funções de rede e o nível de conectividade decorrente da internet das coisas, dentre outros aspectos inerentes ao mencionado padrão, a criticidade da segurança das redes, dos dispositivos e das aplicações adquire contornos mais complexos e desafiadores.

4.30. Dito isso, está evidente que a transição à tecnologia 5G ganhou grande relevo nos últimos meses no espaço geopolítico das relações internacionais e nas discussões sobre a estratégia econômico-industrial a ser adotada pelo País para o desenvolvimento de sua economia digital.

4.31. Ambas vertentes, geopolítica e macroeconômica, estão alheias à jurisdição desta Agência, que deve, por seu turno, concentrar seus esforços nos aspectos tecnológicos e mercadológicos concernentes à expansão e massificação das redes e serviços de telecomunicações. Nesse tocante, cabe uma reflexão inicial acerca da competição na indústria que alimenta o setor de telecomunicações.

4.32. No contexto em que se discute o planejamento de redes e investimentos na prestação de serviços na tecnologia 5G, o tema da competição entre os fabricantes e fornecedores de infraestrutura, os chamados *vendors*, ganha particular proeminência. Tal questão também se manifesta no debate sobre segurança cibernética, objeto da proposta ora em comento.

4.33. O tema abrange aspectos técnicos e concorrenciais, abarcados pela atuação da Anatel, e outros, de natureza geopolítica e macroeconômica, cuja condução é realizada por outras esferas governamentais.

4.34. De antemão, cabe destacar que atualmente o mercado de *vendors* se caracteriza por sua natureza eminentemente oligopolista, cuja configuração se fundamenta em peculiaridades a ele intrínsecas, à exemplo da intensidade tecnológica e a escala-dependência necessária para a viabilidade dessa indústria.

4.35. Um passo essencial para compreender a origem dessa dinâmica consiste no exame da evolução desse mercado. O ano de 2006 pode ser tomado como referência histórica pelo fato de concentrar uma das mais significativas transformações em direção à sua concentração.

4.36. Aquele ano se encerrou com o anúncio da fusão dos fornecedores globais de equipamentos de telecomunicações das empresas Nokia e Siemens. Foi o terceiro grande negócio nessa indústria em menos de um ano.

4.37. Sem surpresa, a tendência se manteve para os anos seguintes quando outros *players* relevantes se uniriam, com destaque para a absorção da Marconi pela Ericsson, da fusão entre Alcatel e Lucent Technologies, da aquisição de partes da Nortel Networks pela Ericsson, Ciena e Avaya.

4.38. Examinado à luz da evolução tecnologia dos padrões de tecnologia móvel, fica evidente como o setor tem se concentrado ao longo dos anos.

TABELA: Mercado de *Vendors* com mais de 1% do *marketshare* global

Ano 2005 Tecnologia GSMA/CDMA Vendors: 14	**Ano 2010** Tecnologia 3G Vendors: 11	**Ano 2015** Tecnologia 4G Vendors: 8	**Ano 2020** Tecnologia 5G Vendors: 7
Alcatel	Alcatel-Lucent	Alcatel-Lucent	Ericsson
Ericsson	Ericsson	Ericsson	Fujitsu
Fujitsu	Fujitsu	Fujitsu	Huawei
Huawai	Huawei	Huawei	NEC
NEC	NEC	NEC	Nokia
Lucent	Matsushita	Nokia	Samsung
Matsushita	Motorola	Samsung	ZTE
Motorola	Nokia-Siemens	ZTE	
Nokia	Panasonic		
Nortel	Samsung		
Panasonic	ZTE		
Samsung			
Siemens			
ZTE			

Fonte: Conforme dados do Mobile Vendor Market Share Worldwide [4]

4.39. À despeito da dinâmica usualmente associada às tecnologias móveis, não foi esse um movimento esporádico, mas uma tendência que se manifestava há décadas, mesmo no contexto de transformação de tecnologias legadas de comutação. A própria Nortel, para utilizar como exemplo, já havia adquirido a Bay Networks que, por sua vez, foi resultado da fusão entre SynOptics (fabricante de *hubs* e *switches*) e da WellFleet (roteadores).

4.40. Além disso, atualmente três dos sete fornecedores relacionados respondem por parcela superior a 3/4 (três quartos) do total de equipamentos disponibilizados, de acordo com dados do Sistema Mosaico, da Anatel, para o segundo semestre de 2020.

4.41. Esse quadro geral é revelador da inequívoca concentração no setor e, por conseguinte, dos riscos dela decorrentes.

4.42. Não se trata de apontar qual seria uma "quantidade ótima" de competidores nesse mercado, mas é certo que a condição oligopolista impõe pressão adicional sobre sua estabilidade, com efeitos sobre a capacidade e a velocidade de disponibilização de novas tecnologias e, por fim, sobre o preço final do serviço ao consumidor.

4.43. Tal hipótese se justifica pelas circunstâncias técnicas, financeiras e de sustentabilidade típicas desse mercado. Abrange, por exemplo, a política de financiamento de longo prazo, os custos adicionais de comutação entre redes legadas e as novas redes e a manutenção de contratos de fornecimento, garantias e manutenção que, uma vez desequilibrados ou rompidos, impõem riscos à continuidade e qualidade dos serviços e aos preços de varejo dos serviços de telecomunicações.

4.44. Dadas as consequências desses aspectos sobre o preço e a qualidade do serviço, variáveis relevantes para o consumo em país de média renda per capita, as dinâmicas de disponibilidade tecnológica e de viabilidade de competição na cadeia de infraestrutura passam a ser elementos de atenção por parte do Regulador.

4.45. Não por acaso, iniciativas baseadas em ecossistemas abertos e virtualizados, com maior diversidade de fornecedores e padrões de interoperabilidade, estão sendo discutidas e impulsionadas pela indústria e pela academia.

4.46. Nessa linha, cabe mencionar a título exemplificativo as arquiteturas de rede de acesso via rádio aberta, que utilizam padrões de interconexão unificado para hardware de computação genérico e elementos de software de código aberto de diferentes fornecedores. Com a decomposição em elementos e interfaces bem definidas, tem-se menor dependência e maior competição e variedade na cadeia de fornecimento de insumos para as redes de acesso.

Da precaução e da prevenção em riscos de segurança cibernética

4.47. A pluralidade e a efetiva competição entre fornecedores de infraestruturas e soluções tecnológicas é, a princípio, saudável para o setor de telecomunicações, tal qual ocorre com diversos outros setores de alta dinamicidade e intensivos em investimentos, capital e/ou pesquisa e desenvolvimento (P&D).

4.48. No que concerne à segurança do espaço cibernético, deve ser exigida de fabricantes e prestadores a adesão a padrões, protocolos e boas práticas de segurança cibernética que busquem mitigar vulnerabilidades, fortalecer a resiliência das infraestruturas de telecomunicações e tornar o ambiente cibernético menos suscetível a ataques e fraudes.

4.49. Caso essas ações não se mostrem suficientes para a consecução dos objetivos pretendidos e se evidenciem situações de risco ou de insegurança, medidas mais severas e imediatas podem vir a ser tomadas no caso concreto pelo Regulador, conforme as respectivas responsabilidades e os contornos fáticos presentes.

4.50. Assim, a vigilância panóptica e permanente do mercado e das infraestruturas, moderada pelo **princípio da precaução,** e a atuação corretiva factu-proporcional, sob os auspícios os **princípio da prevenção**, são, em apertada síntese, as principais ferramentas que o Órgão Regulador de Telecomunicações dispõe para tratar da temática de segurança cibernética dentro da alçada a ele reservada no contexto da política setorial.

4.51. Ademais, independentemente de serem ou não estabelecidas restrições em matéria de cibersegurança por outras esferas governamentais – qualquer que seja sua origem, natureza e fundamento –, a atuação do Regulador de Telecomunicações e os seus instrumentos regulatórios são expressão de suas competências técnicas. Explica-se.

Dos instrumentos de atuação regulatória (em Cibersegurança)

4.52. Para além de zelar pela qualidade dos serviços e livre concorrência do mercado, cabe ao Órgão Regulador o poder-dever de eliminar elementos nocivos às redes e aos serviços de telecomunicações.

4.53. Quanto à precaução – isto é, evitarem-se os riscos em abstrato, por se agir com cautela –, os principais mecanismos de atuação regulatória encontram-se consubstanciados, primeiro, na sistemática de certificação de produtos e equipamentos para telecomunicações e, segundo, no procedimento de licenciamento de estações, ambos objeto de recentes atualizações normativas.

4.54. Quanto à certificação, cumpre memorar que em outubro passado, por meio da Resolução nº 715/2019, a Agência editou o novo Regulamento de Avaliação da Conformidade e de Homologação de Produtos para Telecomunicações.

4.55. A atividade de conferência da conformidade das diversas categorias de produtos e equipamentos utilizados para telecomunicações, organizada pela Anatel, é de fundamental importância para assegurar aos consumidores e às prestadoras de serviço que os equipamentos por eles adquiridos e empregados são condizentes com os padrões de qualidade e segurança, bem como operam de acordo com as especificações, funcionalidades e condições estabelecidas.

4.56. Atualmente são mais de 70 (setenta) mil produtos certificados pela Anatel, sendo que apenas no ano passado foram emitidos 3.886 (três mil, oitocentos e oitenta e seis) certificados, para mais de 5,5 mil produtos, isso sem considerar todas as declarações de conformidade expedidas para os produtos e equipamentos para uso próprio.

4.57. A revisão das regras e do processo de avaliação da conformidade procurou tornar o procedimento mais simples e versátil, além de diminuir o fardo regulatório incidente sobre a produção e comercialização de produtos e equipamentos para telecomunicações. A atualização normativa também tratou das regras para reconhecimento recíproco das certificações expedidas em outros países, com

vistas a aumentar as opções disponíveis no mercado doméstico, reduzir os custos dos equipamentos e facilitar a exportação dos produtos e sistemas aqui produzidos.

4.58. Uma premissa extremamente importante que norteou essa simplificação e flexibilização, todavia, foi a de manter o rigor necessário para garantir a segurança e confiabilidade dos produtos (*i*) diretamente utilizados/manuseados pelos usuários/consumidores e (*ii*) dos transmissores e transceptores que fazem uso do espectro eletromagnético destinado aos serviços de interesse coletivo e de radiodifusão.

4.59. Isso se justifica para mitigar o risco, por exemplo, de expor os usuários a descargas elétricas e sobreaquecimento dos equipamentos, falhas mecânicas e operacionais, vazamentos de baterias e à radiação não ionizante (RNI) acima dos limites tolerados.

4.60. De igual modo, os serviços de interesse coletivo e de radiodifusão, particularmente, têm grande relevância social e econômica, razão pela qual se exige maior rigor na aferição da adequação dos equipamentos às características técnico-operacionais prescritas, como forma de privilegiar um uso do espectro radioelétrico mais eficiente e menos propenso a eventuais interferências prejudiciais. Além disso, sua cobertura prioritária consiste em áreas urbanas e suburbanas, o que justifica maior apuro quanto à verificação da exposição humana à RNI.

4.61. Sobre a exposição humana aos campos elétricos, magnéticos e eletromagnéticos, aliás, cabe rapidamente ressaltar que a Anatel segue rigorosamente as orientações e práticas recomendadas pela Comissão Internacional de Proteção Contra Radiação Não Ionizante (ICNIRP), instituição científica de referência pela qualidade e seriedade de seus estudos, reconhecida pelas Organizações Mundial da Saúde (OMS) e Internacional do Trabalho (OIT) e adotada por mais de cinquenta países.

4.62. Ao estabelecer as condições de operação e procedimentos de avaliação da conformidade para os diferentes grupos e famílias de produtos e equipamentos para telecomunicações, a Anatel sempre busca aplicar as melhores práticas e referências da indústria e do mercado, justificadas em estudos e experiências de uso, e sob as diretrizes e valores intrínsecos que regem o processo de análise – quais sejam: segurança, confiabilidade, compatibilidade, eficiência e não agressão ao meio ambiente.

4.63. Assim, dentro da sistemática de certificação promovida pela Agência, antes de chegarem ao mercado e serem oferecidos aos consumidores, os equipamentos e terminais de usuário têm sua conformidade avaliada em exaustivos ensaios laboratoriais e testes de operação.

4.64. Já para os equipamentos profissionais, em particular aqueles de elevada carga e potência, ou mesmo os utilizados em aplicações críticas e/ou de alto desempenho, além do processo prévio de certificação, pode haver uma série de exigências associadas tanto à *manutenção* da validade da certificação, quanto ao licenciamento dos sítios e estações de telecomunicações – o que varia, novamente, conforme o risco percebido decorrente de sua regular operação.

4.65. Dessa forma, para algumas famílias de equipamentos profissionais, os respectivos procedimentos de certificação podem exigir reavaliações de conformidade, tanto periódicas quanto incidentais, de modo a atestar a manutenção da aderência às condições especificadas na regulamentação, mesmo após múltiplos ciclos de operação e significativas atualizações de *software*, por exemplo.

4.66. Adicionalmente, para as estações desse tipo é preciso apresentar, no momento do licenciamento, os relatórios de avaliação dos níveis de RNI e as certificações exigidas para os equipamentos que se pretende utilizar, sem os quais o pedido de licenciamento sequer é processado. Por fim, em determinados casos de elevada potência, para *manter* a licença para funcionamento da estação é preciso inclusive realizar e apresentar reavaliações periódicas do sítio instalado, de modo assemelhado ao procedimento que ocorre para a manutenção de determinadas certificações de equipamentos.

4.67. **Essa mesma abordagem regulatória operará como primeira barreira de proteção para os riscos em cibersegurança**. Isto é, uma vigilância prévia, geral e universal que, baseada em cautela, procura afastar das redes e infraestruturas de suporte os elementos que, por não terem demonstrado estar em acordo com as normas e especificações ou aderentes às práticas e protocolos de operação exigidos, representam potenciais riscos à segurança e integridade delas.

4.68. **Em ocorrendo incidentes que extrapolem essa primeira abordagem de proteção, ou ao menos em havendo fundados indícios que levantem a possibilidade de vulnerabilidade, dano ou prejuízo ao sistema brasileiro de telecomunicações e seus componentes, por outro lado, passa-se à utilização de outro conjunto de ferramentas regulatórias com vistas à prevenção, em concreto, do risco aventado**.

4.69. Nessa segunda abordagem, motivadamente o Regulador pode exigir, no âmbito da certificação e licenciamento já processados, por exemplo, novas avaliações de conformidade, suspender as certificações expedidas, determinar incidentalmente a adoção de providências complementares para a operação de determinados grupos ou famílias de produtos, ou mesmo proibir sua utilização em determinados acessos, sítios, redes e serviços.

4.70. **Justamente por ter um potencial tão amplo e invasivo, esse poder-dever de tutelar a integralidade do sistema brasileiro de telecomunicações, quando efetivamente agindo para prevenir e mitigar o risco vislumbrado, precisa estar devidamente motivado e fundamentado para ser exercido**.

4.71. Isto é, como premissa do exercício de cada uma das competências, A Anatel deve ser guiada por **razoabilidade e motivação** na hipótese em que vier a exigir de uma prestadora, por exemplo, que substitua equipamentos identificados como potenciais vulnerabilidades e/ou ameaças, ou não os utilize em determinadas redes ou interligações, ou até mesmo que cesse imediatamente a operação dos elementos considerados prejudicados, enquanto não assegurada a sua segurança e conformidade, ainda que isso repercuta negativamente sobre a operação dos demais elementos e os serviços prestados.

4.72. **Na via regulatória tem prevalecido atuação pautada por melhores práticas e fundados indícios**, o que, por certo, não impede que na esfera governamental se teçam entendimentos e se adotem medidas lastreados em outras premissas, igualmente legítimas, motivados pelas razões e preocupações que lhes cabem.

4.73. Para além do respaldo de parecer técnico-fático, tal sistemática, adotada pela Agência, que a todos vigia e de todos desconfia, de forma imparcial e transparente, traz adicionalmente como um de seus corolários a exposição pública e, por conseguinte, uma "estigmatização" dos produtos e equipamento comprovadamente perigosos e/ou inadequados.

4.74. Nesse sentido, está a se reforçar que os efeitos das eventuais medidas concretas adotadas pelo Regulador transcendem o caráter de simples barreira técnica imediata e colocam baliza ao mercado como um todo.

4.75. Em um cenário onde a busca por confiabilidade e segurança está na pauta não só da indústria, mas inclusive dos usuários, a detecção técnica de riscos e inconsistências de determinados produtos de um fabricante pode afetá-lo em diversos aspectos mercadológicos.

Das atribuições e diretivas de trabalho para o GT-Ciber

4.76. Como mencionado, as principais inovações sugeridas pelo presente Voto consistem em ajustes e faseamento de algumas obrigações, do que resulta o necessário redesenho de algumas das atribuições e diretivas de trabalho para o GT-Ciber.

4.77. Este Grupo, muito mais do que os outros dois, precisará se debruçar para, antes de qualquer realização, soerguer os alicerces sobre os quais desempenhará suas atividades. Isso porque, como é cediço, a temática de cibersegurança é novidadeira para a Agência, para o setor e para a sociedade em geral.

4.78. Muito embora a aferição da conformidade e certificação de produtos e equipamentos para telecomunicações acumule décadas de conhecimento e *expertise*, somente nos últimos anos a temática de cibersegurança efetivamente começou a despontar como parte intrínseca desse processo.

4.79. A Anatel, aliás, há poucos meses realizou sua primeira incursão na certificação do 5G e segurança cibernética, com a realização de quatro Consultas Públicas (CP). As CP nº 6/2020, 11/2020 e 12/2020 submeteram para comentários e contribuições da sociedade em geral propostas de requisitos

técnicos tanto para os equipamentos das prestadoras quanto para as estações terminais de acesso que serão utilizados nas redes da próxima geração da telefonia móvel.

4.80. Como é de praxe, as propostas foram baseadas nos padrões e referências internacionais e abrangem requisitos de segurança, funcionalidade, gerenciamento, *software* e afins, com o intuito de estabelecer um patamar mínimo de interoperabilidade, qualidade e segurança dos equipamentos, além de assegurar sua compatibilidade com as regras brasileiras de ocupação do espectro radioelétrico.

4.81. Já a Consulta Pública nº 13/2020 especificamente tratou do estabelecimento de requisitos mínimos de segurança cibernética a serem seguidos pelos fabricantes e fornecedores de equipamentos de infraestrutura de rede e terminais que se conectam à Internet.

4.82. A proposta foi concebida já alinhada às diretrizes e orientações da E-Ciber e da **Instrução Normativa nº 4/2020**, do Gabinete de Segurança Institucional da Presidência da República (GSI).

4.83. Além das exigências usuais do processo, os fabricantes desses equipamentos deverão ainda, dentre outras coisas: (i) estabelecer uma política de suporte ao produto, especialmente em relação à disponibilização de atualizações para correção de vulnerabilidades de segurança; (ii) promover atualizações de segurança por, no mínimo, dois anos após o lançamento do produto ou enquanto o equipamento estiver sendo distribuído ao mercado consumidor; e (iii) disponibilizar canal de comunicação para interação com seus usuários.

4.84. Como se pode facilmente verificar nessa primeira incursão a fundo sobre a temática de verificação de conformidade dos produtos e equipamentos quanto à segurança cibernética, está sendo desenvolvido um grande esforço por parte da Agência para compreender o fenômeno, construir capacidades e se posicionar estrategicamente.

4.85. **É justamente nesse trabalho de preparo e transformação que repousa a contribuição maior do GT-Ciber**. A ele cabe subsidiar esse processo de conceber e adaptar conceitos, práticas e procedimentos, para que então possam ser reproduzidos no nosso contexto.

4.86. O GT-Ciber terá, por conseguinte, duas frentes de trabalho. Primeiro, ele irá internamente colaborar para a preparação e adaptação da própria Anatel, construindo conhecimentos e capacidades em segurança cibernética. Nessa linha, por exemplo, encontram-se o estudo e reprodução de padrões técnicos e referências internacionais em cibersegurança, o aprimoramento das normas e procedimentos de avaliação da conformidade e licenciamento de estações e a proposição de arranjos e iniciativas de inteligência fiscalizatória, dentre outros.

4.87. Por outro lado, o GT-Ciber será também uma interface institucional e uma instância operacional sobre o tema. A ele caberá interagir, em nível técnico-operacional, com prestadores de serviço, fabricantes de equipamentos, laboratórios de certificação e órgãos governamentais afetos ao tema de segurança cibernética.

4.88. Em particular, essas interações serão essenciais para auxiliar a Agência na **dosagem do ônus regulatório a ser aplicado aos diferentes elos da cadeia, conforme suas respectivas responsabilidades e capacidades, bem como estabelecer e aprimorar as práticas de atuação de preparação e resposta a incidentes de segurança cibernética, no âmbito de atuação da Anatel**.

4.89. Como é sabido, a adoção de medidas em prol da segurança cibernética implica uma variedade de custos, dentre os quais se destacam mão-de-obra, capital e serviços destinados a remediar ataques, de forma preventiva e proativa, e a reduzir os eventuais danos causados por tais eventos. Inclui, ainda, a adoção de procedimentos de minimização do impacto, inclusive aqueles em tempo real e de coordenação.

4.90. Dado o contexto, o porte e a região onde essas empresas operam, cabe ao Regulador ponderar sobre o ônus a elas atribuído no processo de criação de um ecossistema integrado de segurança cibernética.

4.91. No Brasil, milhares de empresas usualmente atuam nas franjas de polos econômicos ou em regiões com notória ausência de provedores de grande porte. Nessas circunstâncias, os prestadores de pequeno porte devem, para serem competitivos, operar em condições de baixo custo operacional.

4.92. Desse modo, as expectativas mais racionais em relação aos Prestadores de Pequeno Porte (PPP) muito possivelmente recaem sobre a adesão a canais seguros de comunicação e a disponibilidade e efetividade para lidar com incidentes de segurança. Esses canais se prestam a integrar esses prestadores ao sistema de segurança cibernética e permitir, dentre outras finalidades a coordenação, o compartilhamento de informações, a participação ativa na notificação de vulnerabilidades e nas ações de resposta a incidentes e a contribuição para documentação dos incidentes.

4.93. O compartilhamento de informações tem um papel essencial nesse escopo. Em outros termos, são de particular importância os procedimentos de compartilhamento de informações sobre incidentes de segurança com clientes, com outros provedores de serviços, com equipes de resposta a incidentes, com as autoridades policiais e regulatórias, imprensa e o público em geral.

4.94. Uma notificação qualitativa abrange, a título de exemplo, a identificação de um responsável pela resposta ao incidente, o ponto de vulnerabilidade, como o serviço foi afetado, o que está sendo feito para responder ao incidente, o *status* da integridade dos dados do cliente, o que está sendo feito para eliminar a vulnerabilidade e o cronograma esperado para resposta.

4.95. Iniciativas nesse plano de comunicação seriam, todavia, suficientes para permitir uma integração necessária e adequada dos PPP – em tese, os elos com menor preparação para a cibersegurança de toda a cadeia – para ao sistema de segurança cibernética objeto desta regulamentação?

4.96. Ou ainda, por outro lado, seria razoável exigir desses pequenos prestadores, que muitas vezes operam próximos dos limites de suas capacidades financeiras, que despendam recursos significativos para a contratação de profissionais especializados em segurança cibernética, aquisição de *softwares* e equipamentos específicos e instalação de elaborados sistemas de redundância?

4.97. Muito embora a minuta de Regulamento ora discutida proponha dispensar os PPP das obrigações, é certo que essas prestadoras não podem ficar completamente alheias ao sistema coordenado de monitoração e resposta a incidentes cibernéticos. A proposta de texto normativo, aliás, não prevê sua isenção em relação aos princípios e diretrizes de atuação em segurança cibernética, que devem se aplicar universalmente aos agentes do setor de telecomunicações.

4.98. Assim, caberá ao GT-Ciber, como instância tecnicamente capacitada, interagir e discutir com os atores do setor a eventual adoção de assimetrias regulatórias e, consoante previsão constante da própria minuta de Regulamento, propor e subsidiar a decisão de sua adoção pelo Colegiado.

4.99. Nessa mesma linha, para as empresas não dispensadas das obrigações regulamentares principais, o GT-Ciber operará como principal fórum de interlocução e participação para as discussões relacionadas à implantação e acompanhamento das medidas em cibersegurança.

4.100. Desse modo, além de oportunizar que participem da construção e aperfeiçoamento do arcabouço regulatório relacionado ao tema, possibilitará aos regulados contribuir para a definição de condições e parâmetros de avaliação de vulnerabilidades, tais como, por exemplo, a definição da periodicidade dos ciclos de avaliação, os aspectos que serão avaliados e a forma como os relatórios deverão ser estruturados e apresentados pelas empresas especializadas.

4.101. Além dos ciclos de avaliação por **auditoria independente**, ao GT-Ciber também cabe auxiliar a Anatel na formatação e avaliação das informações sobre as Infraestruturas Críticas de Telecomunicações das prestadoras, com a identificação das redes, seu perfil de utilização, mapeamento geográfico das estruturas físicas e as rotas interligadas, entre outras informações. Nesse tocante, será importante avaliar e implementar mecanismos de confidencialidade, de modo a proteger a segurança das informações sensíveis.

4.102. Caberá ainda ao Grupo Técnico dispor sobre aspectos de forma e procedimento para a operacionalização das obrigações de realizar os registros de notificação dos incidentes relevantes e de compartilhamento de informações, bem como apresentação de relatórios de acompanhamento da implantação da política e protocolos de tratamento dos dados sigilosos colhidos no trabalho do GT-Ciber.

4.103. Como se observa, nos primeiros meses após sua ativação, caberá ao Grupo, no âmbito da jurisdição regulatória da Agência, discutir uma série de condições, parâmetros e procedimentos

relacionados à implantação, pelos agentes abrangidos, das condutas e medidas de atuação em segurança cibernética e mitigação de riscos em infraestruturas críticas de telecomunicações.

4.104. Assim, **o presente Voto adiciona à proposta do Relator determinação de que o GT-Ciber avalie, em colaboração com as prestadoras e a sociedade em geral, a possibilidade de participação e colaboração dos diferentes agentes do ecossistema para o *framework* estabelecido pelo próprio Regulamento.**

4.105. Em outras palavras, se por um lado é conhecida a importância de se organizar e mobilizar as grandes prestadoras para que atuem em conformidade com determinadas condutas e procedimentos em segurança cibernética, para, desta forma, ampliar e robustecer os patamares de segurança e resiliência das redes e serviços; por outro é igualmente salutar discutir, de modo aberto e transparente, como agentes outros desse mesmo ecossistema podem contribuir para a consecução desse mesmo objetivo comum.

4.106. Nessa esteira, propõe-se determinar ao GT-Ciber que nos seus primeiros meses de trabalho priorize alguns tópicos específicos, de modo a possibilitar que, em 150 (cento e cinquenta) dias, contatos da instauração do Grupo, remeta à Superintendência de Planejamento e Regulamentação (SPR) suas contribuições para uma minuta de Resolução contendo proposta de incluir ou dispensar, total ou parcialmente, das obrigações regulamentares, as prestadoras ainda não abrangidas pelo Regulamento, independentemente do porte, operadoras de capacidade satelital e demais empresas do ecossistema de telecomunicações envolvidos direta ou indiretamente na gestão ou no desenvolvimento das redes e serviços de telecomunicações.

4.107. Dessa forma, após eventualmente serem incluídos pelo Conselho Diretor no escopo das obrigações regulamentares, esses novos atores passariam a ser objeto da atuação da Anatel e do GT-Ciber nos termos previstos no Capítulo IV, especialmente de sua Seção II.

4.108. Nesse sentido, observadas as atribuições e competências do GT-Ciber, antes de integrarem o *framework* regulatório, tais disposições serão discutidas no âmbito do GT-Ciber, com a participação dos agentes setoriais e das Superintendências afetas, e realizada uma Consulta Pública para tomada de subsídios junto à sociedade em geral.

4.109. Dentro desse mesmo período, propõe-se que o GT-Ciber avalie a viabilidade de uma modelagem complementar à estrutura prevista no Regulamento, e que possa amparar a atuação setorial via a constituição de entidade, ou designação ente já existente, que credite boas práticas de segurança.

4.110. Essa creditação por terceiro, o qual demonstre garantias de impessoalidade, isonomia e integridade na execução da atividade, pode se constituir em variável chave de *compliance* e de transparência ao mercado e aos usuários sobre a matéria.

4.111. Assim, caso o GT-Ciber julgue viável tal tipo de complementação da sistemática do Regulamento proposto, deverá apresentar as características de sua estruturação, financiamento e relacionamento com a Anatel.

4.112. A Superintendência de Planejamento e Regulamentação (SPR), por seu turno, terá 90 (noventa) dias para instruções complementares e submeter a proposta ao Colegiado, após oitiva da Procuradoria Federal Especializada junto à Anatel.

4.113. Considerando os prazos usuais para a realização dessas etapas, mencionados pela área técnica no Informe nº 161/2020/PRRE/SPR (SEI nº 6236795), em resposta à diligência consubstanciada no Voto nº 113/2020/PR (SEI nº 6133338), os prazos aqui previstos parecem ser suficientes para a realização dessas atividades. Ressalta-se, contudo, que dilações poderão ser consideradas pelo Colegiado, caso instado pelo GT-Ciber ou pelas áreas envolvidas.

4.114. Outrossim, considerando as competências regimentais da SPR, caso se verifique a necessidade de promover ajustes em outros instrumentos normativos ou no planejamento estratégico da Anatel, por exemplo, a Superintendência poderá providenciar os eventuais encaminhamentos na agenda regulatória e no planejamento estratégico-operacional.

Dos ajustes estruturais e redacionais

4.115. Para conferir maior clareza e objetividade, a proposta foi segregada em três minutas de Resolução, a saber:

- **Minuta de Resolução SEI nº 5963805**: altera o Regulamento dos Serviços de Telecomunicações para incluir disposições sobre sigilo, prevenção à fraude e ações de apoio à segurança pública, e dá outras providências;

- **Minuta de Resolução SEI nº 5963838:** aprova o Regulamento sobre o Uso de Serviços de Telecomunicações em Desastres, Situações de Emergência e Estado de Calamidade Pública, e dá outras providências; e

- **Minuta de Resolução SEI nº 5963841:** aprova o Regulamento de Segurança Cibernética Aplicada ao Setor de Telecomunicações.

4.116. Como mencionado, as duas primeiras minutas receberam principalmente ajustes redacionais, enquanto o texto da terceira, que trata da temática de segurança cibernética, recebeu ajustes notadamente de estruturação da normativa e alterações para possibilitar a implementação do faseamento mencionado na seção anterior. Cabe mencionar ainda que, na primeira minuta, ao GT-Seg foram aplicadas as mesmas alterações que serão apresentadas mais adiante para o GT-Ciber, respeitadas as suas particularidades.

4.117. No tocante à estrutura, optou-se por uma modificação no arranjo organizacional dos capítulos e artigos da minuta de Regulamento da seguinte forma:

Antes	Depois
CAPÍTULO I DAS DISPOSIÇÕES GERAIS Seção I Do Objeto Seção II Das Definições Seção III Dos Princípios	CAPÍTULO I DAS DISPOSIÇÕES GERAIS Seção I Do Objeto Seção II Da Abrangência Seção III Das Definições
	CAPÍTULO II DOS PRINCÍPIOS E DIRETRIZES EM SEGURANÇA CIBERNÉTICA Seção I Dos Princípios Seção II Das Diretrizes
CAPÍTULO III DA POLÍTICA DE SEGURANÇA CIBERNÉTICA	CAPÍTULO III DA SEGURANÇA CIBERNÉTICA NO ÂMBITO DAS REDES E SERVIÇOS DE TELECOMUNICAÇÕES E DA MITIGAÇÃO DE RISCOS EM INFRAESTRUTURAS CRÍTICAS Seção I Das Obrigações da Prestadora Seção II Da Política de Segurança Cibernética Seção III Da Notificação e da Comunicação dos Incidentes Relevantes Seção IV Dos Ciclos de Avaliação de Vulnerabilidades Relacionadas à Segurança Cibernética Seção V Do Envio de Informações sobre Infraestruturas Críticas de Telecomunicações

CAPÍTULO II DO GRUPO TÉCNICO DE SEGURANÇA CIBERNÉTICA E GESTÃO DE RISCOS DE INFRAESTRUTURA CRÍTICA CAPÍTULO IV DA ATUAÇÃO DA ANATEL	CAPÍTULO IV DA ATUAÇÃO DA ANATEL E DO GRUPO TÉCNICO EM SEGURANÇA CIBERNÉTICA Seção I Da Atuação da Anatel em Segurança Cibernética Seção II Do Grupo Técnico de Segurança Cibernética e Gestão De Riscos De Infraestruturas Críticas
CAPÍTULO V DAS SANÇÕES	CAPÍTULO III DAS SANÇÕES
CAPÍTULO VI DAS DISPOSIÇÕES FINAIS	CAPÍTULO IV DAS DISPOSIÇÕES FINAIS

4.118. No Capítulo I, como pode ser observado, além das disposições iniciais sobre objeto e definições adotadas no Regulamento, optou-se por criar uma seção específica sobre a abrangência de suas disposições, que na proposta original da área técnica após a Consulta Pública estava localizado no Capítulo III, mas já havia sido pinçado para o começo do Regulamento pelo Conselheiro Relator.

4.119. Quanto às definições, o termo 'risco', herdado da Resolução nº 656/2019 e de caráter mais genérico, foi substituído pelo termo 'risco cibernético', mais preciso para o contexto dos espaços cibernéticos, enquanto a definição de 'vulnerabilidade', também resquício do Regulamento que está sendo substituído, foi atualizada para uma definição mais corrente. Além disso, foram incluídas definições para outros termos utilizados no Regulamento ora discutido, a saber: autenticidade, confidencialidade, disponibilidade, espaço cibernético, incidente e integridade.

4.120. Um ponto a ser ressaltado sobre o rol de definições é a sua conciliação com o Glossário de Segurança da Informação, aprovado por intermédio da Portaria nº 93, de 26 de setembro de 2019, do Gabinete de Segurança Institucional da Presidência da República (GSI) . A utilização do referido Glossário é conveniente e oportuna para a harmonização do sustentáculo jurídico-normativo adotado pelos diferentes entes.

4.121. O Capítulo II, por seu turno, reúne os Princípios e Diretrizes orientadores das condutas e procedimentos para a promoção da segurança cibernética, com redação bastante semelhante àquela da proposta do Relator. Tendo em vista, todavia, as modificações introduzidas pela proposta constante deste Voto, optou-se por reuni-los em um capítulo específico, pois são universais e vigentes desde a publicação da norma.

4.122. O Capítulo III, na sua primeira Seção, elenca as principais obrigações das empresas abrangidas pelas disposições do Regulamento, em particular, as prestadora de serviços de telecomunicações, enquanto as demais Seções desse Capítulo III explicitam e abordam aspectos específicos de algumas delas.

4.123. A saber, são seis as obrigações em relação à temática de segurança cibernética. Primeiro, a empresa deve elaborar, implementar e manter a sua política de Segurança Cibernética. Segundo, deve utilizar, em suas redes, produtos e equipamentos provenientes de fornecedores que adotem políticas de segurança cibernética compatíveis com os princípios e diretrizes dispostos no Regulamento e que realizem processos de auditoria independente periódicos.

4.124. A terceira obrigação é a de alterar a configuração padrão de autenticação dos equipamentos fornecidos em regime de comodato aos seus usuários, tais como *modems* e pontos de acesso. O GT-Ciber ficará encarregado de especificar quais equipamentos estão abrangidos por essa obrigação, bem como demais aspectos de forma e procedimento.

4.125. A quarta obrigação diz respeito ao dever de informar sobre os incidentes relevantes e possui dois aspectos. O primeiro deles concerne ao dever de realizar o registro de notificação do incidente, junto à Anatel. Já o segundo diz respeito às obrigações legais e regulamentares de comunicar os usuários e a de compartilhar informações com as demais prestadoras.

4.126. A quinta obrigação é a de realizar ciclos de avaliação de vulnerabilidades relacionadas à Segurança Cibernética.

4.127. A sexta e última obrigação diz respeito ao dever da prestadora de enviar à Anatel informações sobre suas Infraestruturas Críticas de Telecomunicações, hoje vigente no bojo do Regulamento aprovado pela Resolução nº 656/2015, que será substituído pela proposta de Regulamento ora discutida.

4.128. A Seção II, *Da Política de Segurança Cibernética*, trata dos aspectos pertinentes à implantação e operacionalização dessa obrigação. De certo modo, ela resulta de uma evolução e ampliação do Plano de Gestão de Riscos (PGRiscos), previsto no art. 5º do Regulamento aprovado pela Resolução nº 656/2015, no bojo da gestão dos riscos em Infraestruturas Críticas de Telecomunicações. De modo semelhante, prevê-se o mapeamento e mitigação de vulnerabilidades, os procedimentos e controles de resposta e a estrutura responsável na prestadora ou seu Grupo Econômico. À temática de riscos somam-se elementos de segurança do espaço cibernético e proteção dos dados dos usuários.

4.129. A Seção prevê ainda a publicação de extrato da Política de Segurança Cibernética na página da empresa, contendo apenas as informações não sensíveis, conforme orientações que serão expedidas pelo GT-Ciber, e ainda a apresentação anual, ou sempre que requisitado, de relatório sobre o acompanhamento da execução da Política estabelecida pela prestadora.

4.130. A Seção seguinte, *Da Notificação e da Comunicação dos Incidentes Relevantes*, dispõe sobre a realização, junto à Anatel, do registro de notificação dos incidentes relevantes que afetem de maneira substancial a segurança das redes de telecomunicações e dos dados dos usuários.

4.131. Tal registro de notificação deve incluir análise da causa e do impacto, bem como ações de mitigação adotadas, conforme o caso, e não exime do atendimento de outras obrigações de comunicação previstas em leis, normas e regulamentos. Ademais, os incidentes considerados relevantes e o prazo de registro serão estabelecidos pelo GT-Ciber, bem como os demais aspectos de forma e procedimento de registro.

4.132. Os aspectos de forma e procedimento relacionado ao compartilhamento de informações sobre incidentes relevantes, e outras informações relativas à Segurança Cibernética, de forma sigilosa e não discriminatória, entre as prestadoras serão estabelecidos pelo GT-Ciber, que igualmente acompanhará o desenvolvimento dessa iniciativa.

4.133. A Seção IV trata do ciclos de avaliação de vulnerabilidades, que deverão ser realizados por entidade aferidora ou empresa capacitada e independente e cujos resultados deverão ser compartilhados com a Anatel.

4.134. Ao GT-Ciber, cabe dispor sobre as diretrizes do procedimento de avaliação, a periodicidade dos ciclos e as situações que demandarão reavaliação, além dos demais aspectos de forma e procedimento de avaliação e apresentação dos resultados, observadas suas competências e prerrogativas.

4.135. Por fim, a última Seção desse Capítulo trata da obrigação de envio de informações sobre as Infraestruturas Críticas de Telecomunicações, abrangendo, no mínimo, dados de rede e mapeamento geográfico das estruturas físicas e rotas. Considerando que se trata essencialmente da continuidade de um trabalho já em curso e que há diretrizes governamentais estabelecidas sobre a temática, cabe inteiramente ao GT-Ciber dispor sobre os aspectos complementares, como formatos e procedimentos.

4.136. O Capítulo IV versa em sua primeira Seção sobre a atuação institucional do Órgão Regulador, que acompanhará a implantação das disposições regulamentares e observará aspectos de segurança cibernética nos procedimentos de avaliação da conformidade dos produtos e equipamentos para telecomunicações.

4.137. Além disso, um artigo prevê que, sem prejuízo da adoção de outras medidas necessárias para o cumprimento do disposto neste Regulamento, a Anatel pode, motivadamente, determinar a observação de requisitos técnicos e a adoção de medidas específicas na implementação, operação e manutenção das redes de telecomunicações quanto à Segurança Cibernética.

4.138. A importância dessa previsão repousa na mencionada multisetorialidade e multiplicidade de agentes e competências envolvidos nas temáticas e políticas afetas, dentre outras, à segurança dos dados dos usuários, do espaço cibernético e das infraestruturas críticas brasileiras.

4.139. Nessa linha, considerando as competências constitucionais e legais da Anatel e de outros órgãos e autarquias, e ainda os objetivos gerais traçados pelas Leis nº 12.965/2014 (Marco Civil da Internet) e nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais), eventualmente poderão ser estabelecidas agendas e firmados acordos para a colaboração e o compartilhamento de informações setoriais com outros elos do amalgamado de ações e esforços coordenados em proteção de dados pessoais e segurança cibernética.

4.140. Outrossim, como resultado do envolvimento desses atores, respeitadas as competências dos órgãos e instituições envolvidas, condutas e procedimentos outros que aqueles já estabelecidos no Regulamento ora discutido poderão vir a ser requisitadas dos agentes abrangidos pela atuação regulatória da Anatel.

4.141. Sobre a estrutura, atribuições e sistemática de atuação do GT-Ciber, cabe destacar que o Grupo será coordenado por um Superintendente da Anatel contará com a participação das grandes prestadoras. Para além disso, sugere-se conferir maior flexibilidade e espaço de atuação para o Superintendente Coordenador, que terá maior liberdade para organizar os trabalhos e convocar/franquear a participação dos representantes das prestadoras ou de suas associações e dos órgãos e entidades afetos, nos temas de interesse dessas empresas, órgãos e entidades.

4.142. A maior flexibilidade é desejável considerando que diferentes discussões poderão envolver diferentes atores, como, por exemplo, aspectos de reconhecimento de conformidade, tratados com organismos e laboratórios de certificação de um lado, e protocolos de segurança a serem adotados nos núcleos de rede, com prestadores de serviço, de outro. Outrossim, é preciso ainda considerar que algumas das atividades realizadas pelo GT-Ciber serão internas ou mero expediente (como a realização de workshops e capacitações, avaliação de recursos e sistemas internos, elaboração de respostas, participação em eventos etc.).

4.143. De toda sorte, as discussões e deliberações no âmbito do GT-Ciber serão pautadas pelo diálogo e consenso, ficando a decisão final sempre com o Superintendente Coordenador. Cabe memorar que dessa decisão é cabível Recurso Administrativo, conforme disposto no Regimento Interno da Anatel.

4.144. O Capítulo V, que dispõe sobre a possibilidade de imposição de sanções administrativas ao infratores das disposições regulamentares, não sofre alterações.

4.145. Finalmente, o Capítulo VI, Das Disposições Finais, prevê, primeiro, que as prestadoras são integralmente responsáveis pelos ônus decorrentes da adoção e execução das regras previstas no Regulamento. Depois, quanto à vacância, ele estabelece que as prestadoras terão 180 (cento e oitenta dias) para se adequar às novas disposições regulamentares.

5. **CONCLUSÃO**

5.1. Em vista do exposto, voto por acompanhar a proposta do Conselheiro Moisés Queiroz Moreira, com os acréscimos e ajustes descritos neste Voto, conforme minutas de Resolução SEI nº 5963805, nº 5963838 e nº 5963841.

5.2. Adicionalmente, proponho determinar que:

a) o Grupo Técnico de Segurança Cibernética e Gestão de Riscos de Infraestrutura Crítica (GT-Ciber), no prazo de 150 (cento e cinquenta) dias contados da sua instauração;

a.1) remeta à Superintendência de Planejamento e Regulamentação (SPR) contribuições à minuta de Resolução com proposta de incluir ou dispensar, total ou parcialmente, da incidência das obrigações em segurança cibernética outros agentes do setor de telecomunicações ainda não abrangidos pelo Regulamento; e

a.2) paralelamente, avalie a viabilidade de modelagem complementar à estrutura prevista no Regulamento com vistas à constituição de entidade, ou designação de ente já existente, para creditação de conformidade em boas práticas de segurança

cibernética, e, se entender pertinente, proponha as características de sua estruturação, financiamento e relacionamento com a Anatel; e

b) a Superintendência de Planejamento e Regulamentação (SPR), no prazo de 90 (noventa) dias contados do recebimento dos subsídios mencionados na alínea 'a', promova as instruções complementares que julgar pertinentes e submeta uma proposta ao Colegiado, após oitiva da Procuradoria Federal Especializada junto à Anatel.

5.3. É como considero.

6. **NOTAS**

[1] UIT, Recomendação ITU-T X.1205. Disponível em: <http://www.itu.int/rec/T-REC-X.1205-200804-I>.
[2] No original, em inglês – **Cybersecurity**: *Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets* (...)
[3] BRASIL (2020). Estratégia Nacional de Segurança Cibernética. Decreto n° 10.222, de 5 de fevereiro de 2020. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/D10222.htm>.
[4] *Mobile Vendor Market Share Worldwide*. Disponível em: <https://gs.statcounter.com/vendor-market-share/mobile>.

Documento assinado eletronicamente por **Leonardo Euler de Morais**, **Presidente do Conselho**, em 17/12/2020, às 18:17, conforme horário oficial de Brasília, com fundamento no art. 23, inciso II, da Portaria nº 912/2017 da Anatel.

A autenticidade deste documento pode ser conferida em http://www.anatel.gov.br/autenticidade, informando o código verificador **5963564** e o código CRC **85C00C0D**.

Referência: Processo nº 53500.078752/2017-68 SEI nº 5963564