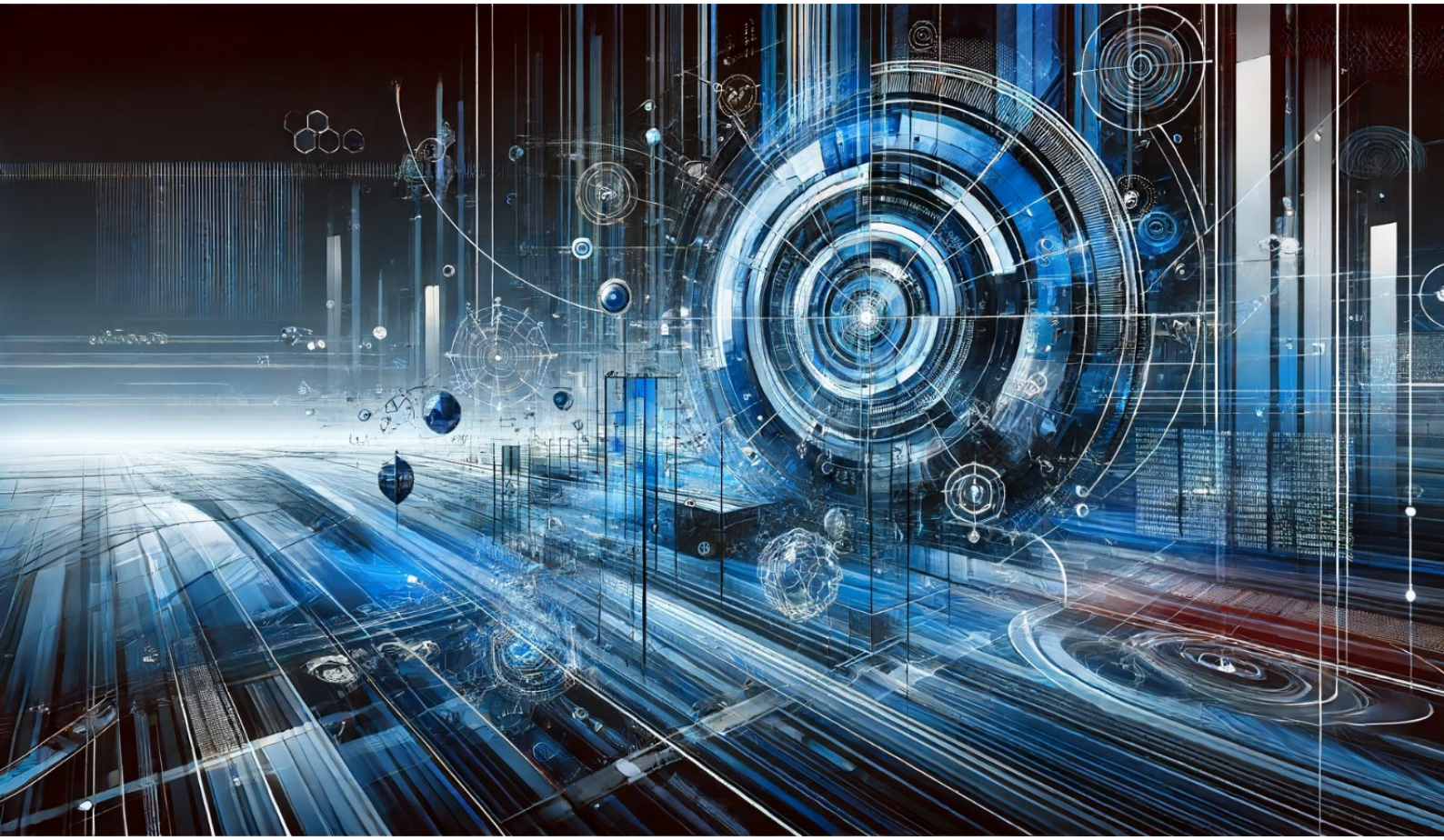
AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES



White Paper Cibersegurança & Regulação:
perspectivas para o Setor de Telecomunicações

ANATEL
Agência Nacional de Telecomunicações

Agência Nacional de Telecomunicações

SAUS Quadra 06, Blocos C, E, F e H

CEP 70.070-940 - Brasília/DF

Tel.: (61) 2312-2000 – www.gov.br/anatel

AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES

***White Paper* Cibersegurança & Regulação:** perspectivas para o Setor de Telecomunicações

Coordenador: Alexandre Reis Siqueira Freire

Brasília – DF

2024

Equipe de pesquisa

Coordenação
Alexandre Reis Siqueira Freire

Autores

Gabinete do Conselheiro Diretor Alexandre Freire
Alexandre Reis Siqueira Freire
Leonardo Albuquerque Marques
Ailfran Moraes Martins
Michelle Adriane de Assis Silva de Andrade

Superintendência de Controle de Obrigações
Grupo Técnico de Segurança Cibernética e Gestão de Riscos de Infraestrutura Crítica (GT-Ciber)
Gustavo Santana Borges
Vanessa Copetti Cravo

Assessoria Internacional
Ronaldo Neves de Moura Filho
Victor Muniz Estevam Dias

Catalogação na fonte – Biblioteca da Anatel

W582 White paper cibersegurança & regulação: perspectivas para o setor de telecomunicações [recurso eletrônico] / coordenação: Alexandre Reis Siqueira Freire – Brasília : Anatel, 2024.

1 recurso online [113 p.] : il.

Modo de acesso : World Wide Web.

Publicação digital (e-book) no formato PDF.

Vários autores.

1. Segurança cibernética. 2. Regulação governamental. 3. Setor de Telecomunicações. 4. Benchmarking. I. Agência Nacional de Telecomunicações (Brasil). II. Freire, Alexandre Reis Siqueira (coord.).

Ficha catalográfica elaborada por Carolina Pereira Marinho - CRB1/2275

Como citar este livro:
FREIRE, Alexandre Reis Siqueira (coord.). **White paper cibersegurança & regulação**: perspectivas para o setor de telecomunicações. Brasília: Anatel, 2024. e-Book. (1 recurso online (113 p.)), il

Agência Nacional de Telecomunicações
SAUS, Quadra 06, Bloco C, E, F e H
CEP: 70.070-940 – Brasília/DF
Tel.: (61) 2312-2000
Site: www.gov.br/anatel

Sumário

Página deixada intencionalmente em branco

Apresentação

No seu segundo quarto de século de existência, a Anatel se encontra em meio a novos desafios que vão muito além da missão de universalização da telefonia fixa que norteou os primórdios de sua existência.

Um desses desafios é a promoção da cibersegurança no ambiente de telecomunicações, o que compreende diversos aspectos de integridade do ambiente digital, incluindo a regularidade da cadeia de suprimentos de produtos e serviços que integrarão a camada de transmissão, o fornecimento de equipamentos ao consumidor final, a higidez do funcionamento da própria camada de transmissão, com a prevenção e mitigação de riscos e vulnerabilidades, e, atualmente, a aplicação de inteligência artificial nesse segmento, dentre outros pontos.

Com efeito, testemunhamos o crescimento de redes baseadas em nuvens e em *softwares* com emprego de aplicações de inteligência artificial e em arquiteturas abertas, além do uso cada vez mais intenso de *data centers* como elemento inerente à prestação de serviços de telecomunicações, em que os serviços de computação de borda (*edge computing*) se tornarão mais presentes para as diversas aplicações de Internet das Coisas (IoT).

Como marcador desses fenômenos disruptivos, cita-se a recente divulgação de resultados da gigante de chips Nvidia, expoente do fenômeno de aplicações de inteligência artificial, cujas receitas associadas a *data centers* já representam 85% (oitenta e cinco por cento) do seu faturamento total (cerca de vinte e seis bilhões de dólares) no primeiro trimestre de 2024, segundo o periódico *online* Infomoney (DINIZ, 2024). Há cerca de dezoito meses, essa receita trimestral de *data centers* não chegava a quatro bilhões de dólares trimestrais e, há cinco anos, não alcançava um bilhão de dólares (STATISTA.COM, 2024).

Outro ponto que merece ênfase é a peculiaridade do ecossistema brasileiro de prestadores de serviços de telecomunicações, especialmente no Serviço de Comunicação Multimídia (SCM), notadamente associado à expansão da banda larga fixa no país. O SCM é responsável pela conectividade, motor da transformação digital e da qual dependem todas as outras infraestruturas críticas do país, além de ser o meio pelo qual grande parte das ameaças são disseminadas e as vulnerabilidades, exploradas.

Como se pode ver, projeta-se um novo panorama para as telecomunicações em que os modelos de negócios tendem a migrar cada vez mais da granularidade do foco nas infraestruturas físicas para convergências no gerenciamento de rede por *software*. Nessa transição, identificam-se reconfigurações de processos de produção, que se tornam cada vez mais sofisticados e singulares, demandando, por sua vez, a devida adaptação dos reguladores para que tomem as providências necessárias para o fornecimento de um serviço adequado e seguro para o usuário.

Igualmente evidentes são a preocupação e os movimentos iniciais para endereçar os novos e emergentes desafios relacionados à segurança cibernética (inteligência artificial, cabos submarinos, *data centers*, computação em nuvem *etc.*), objeto de atenção pela Agência e já com resultado concreto de inclusão de um novo item na Agenda Regulatória para desenvolvimento ainda no ano de 2024.

Acrescenta-se que, durante a relatoria do processo de revisão do R-Ciber, a cargo do Conselheiro Alexandre Freire, aprovada pelo Conselho Diretor da Anatel em sessão realizada em 04 de julho de 2024, realizaram-se missões internacionais das quais se extraíram importantes subsídios para a análise da matéria em questão. Essas missões ocorreram no ano de 2023, em Israel, Finlândia e Suécia, e, no ano de 2024, no Reino Unido, Bélgica, Estônia, Suíça, Grécia e Portugal.

Dentre os temas que demandaram mais atenção, destacam-se: a compreensão da abrangência das obrigações dos regulados; o acompanhamento e controle dessas obrigações; e, no caso da União Europeia, a proposta de esquema de certificação em computação na nuvem, a Recomendação da Comissão Europeia sobre segurança e

resiliência das infraestruturas de cabo submarinos e o planejamento da implementação do NIS2, especialmente no que diz respeito à assimetria regulatória das pequenas prestadoras.

Traz-se, ainda, como exemplo, o Reino Unido, cujo regulador (OFCOM) possui aproximadamente 30 (trinta) pessoas dedicadas para a segurança cibernética no setor de telecomunicações, sem contar outras dezenas de profissionais de áreas relacionadas, como fraude, *legal* e *enforcement*.

Ainda na esteira das ações do OFCOM, tal agência contratou 350 (trezentas e cinquenta) pessoas para se dedicarem ao seu novo mandato decorrente do *Online Safety Act,* com o objetivo de chegar a uma equipe de 500 (quinhentos) profissionais dedicados a garantir a implementação do ato para proteger a segurança no ambiente digital.

Embora o tema se relacione com o R-Ciber de forma tangencial – tão somente na perspectiva de conscientização e de disseminação de uma cultura de segurança cibernética e na diretriz de respeito e proteção dos direitos e garantias fundamentais, todos expressamente contemplados no R-Ciber vigente – é forçoso reconhecer que o *Online Safety Act* abarca diversas perspectivas que são alvo de intensos debates no Congresso Nacional.

Cita-se, como exemplo, a regulação de plataformas e desinformação, cuja adequada normatização é essencial para a Soberania Digital do país e para a proteção da população nesse ambiente. A alocação desses recursos na OFCOM para o tema releva a complexidade da missão e a sua fundamental importância.

Sobretudo, como resultado das missões, interações e debates desenvolvidos durante a relatoria da revisão do R-Ciber, firmou-se a convicção de que a segurança cibernética deve ser pensada cada vez mais holisticamente, o que já vem sendo adotado por diversos reguladores mundo afora.

Além disso, evidenciou-se que a atuação do regulador de telecomunicações em segurança cibernética transborda esse segmento, na medida em que os serviços de

telecomunicações servem de instrumento para o funcionamento de várias outras infraestruturas críticas e para a circulação de bens e serviços, cada vez mais dependente do ambiente digital para o seu funcionamento.

Os casos de sucesso desses países revelam que a abordagem de riscos, gestão e respostas deve ser coerente e integrada, o que faz sobressaltar a importância de se internalizar um panorama que vai muito além do setor de telecomunicações.

Além dessa transversalidade, a eficiência da regulação aplicada deve considerar incentivos que impulsionem todos os atores do ecossistema digital a atingirem o propósito de maior segurança por meio da adoção de práticas que se encontrem no estado da arte. Isso é particularmente importante no setor de telecomunicações, essencial para a vivência da sociedade brasileira nas suas diversas dimensões.

É nesse contexto que não se pode pensar no setor sem enfrentar os desafios de segurança cibernética, que são cada vez maiores e mais complexos.

Por esse motivo, a missão da Agência é de extrema relevância para o Brasil como um todo, o qual possui singularidades não encontradas nas diversas jurisdições visitadas, como um ecossistema com quase 21 (vinte e uma) mil empresas que conectam o país, levando banda larga fixa a diversas localidades e municípios mais remotos.

Tais desenvolvimentos reafirmam a relevância desses assuntos e a acertada decisão da Agência de desenvolver os estudos necessários para subsidiar suas ações nos próximos anos.

Diante desse cenário, a Anatel tomou a iniciativa de produzir este *white paper* para, no contexto da revisão do seu Regulamento de Cibersegurança Aplicado ao Setor de Telecomunicações (R-Ciber), aprovado pela Resolução nº 740/2020, concluída em 04 de julho de 2024, proceder a um *overview* dos obstáculos que se avizinham para os próximos anos sobre o tema no Brasil, numa reflexão que leva em conta os cenários regulatórios para cibersegurança de alguns dos principais *players* em nível mundial, resultando na Resolução nº 767/2024.

Como o leitor perceberá, há muito a ser feito tanto no Brasil quanto nas jurisdições mencionadas.

Temas que, até pouco tempo, eram estudados apenas tangencialmente na regulamentação dos serviços de telecomunicações, são, neste momento, merecedores de um novo olhar regulatório. Citam-se, exemplificativamente, os *data centers*, inclusive quando empregados em atividades não diretamente relacionadas aos serviços de telecomunicações, e os cabos submarinos, que se revelam como um ativo cada vez mais estratégico nesse contexto. Certamente, essa discussão não parará por aqui.

Dito isso, espera-se que as reflexões aqui trazidas sirvam para inspirar os *stakeholders* dos setores público e privado a construir, de maneira dialogada e compartilhada, soluções para esses desafios que se aproximam.

É certo que o presente trabalho deixou de estudar como o tema é desenvolvido em outros locais igualmente relevantes, notadamente os países em desenvolvimento e os que se encontram no Oriente, a exemplo de China, Índia, Japão e Coreia do Sul. Dito isso, já se estuda a elaboração de um segundo volume do *white paper* para melhor compreensão da cibersegurança no setor de telecomunicações desses e de outros *players* a nível global.

Certos de que estamos dando um passo importante em uma caminhada incessante e contínua, apresentamos essas reflexões à sociedade brasileira, esperando que sirvam para inspirar e fomentar o desenvolvimento de soluções para um tema tão instigante quanto fundamental na atual transição para a economia e cidadania digitais.

Atenciosamente,

Carlos Baigorri
Presidente da Anatel

Alexandre Freire
Conselheiro Diretor da Anatel

Introdução

Cibersegurança (ou Segurança Cibernética, aqui utilizadas como sinônimos) é definida pelo Glossário de Segurança da Informação do Gabinete de Segurança Institucional da Presidência da República (GSI/PR), como as "*ações voltadas para a segurança de operações, visando garantir que os sistemas de informação sejam capazes de resistir a eventos no espaço cibernético, capazes de comprometer a disponibilidade, a integridade, a confidencialidade e a autenticidade dos dados armazenados, processados ou transmitidos e dos serviços que esses sistemas ofereçam ou tornem acessíveis*" (BRASIL, 2021). É considerada um subconjunto da Segurança da Informação, a qual é definida no mesmo Glossário como "ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações".

Desde logo, cabe uma nota terminológica para reconhecer que, historicamente, os marcos brasileiros na matéria utilizaram a nomenclatura "segurança cibernética". No entanto, a recente edição da Política Nacional de Cibersegurança (PNCiber), instituída pelo Decreto nº 11.856, de 26 de dezembro de 2023 (BRASIL, 2023), demonstra a opção pela alteração terminológica no título. Ainda assim, a expressão "segurança cibernética" é utilizada como sinônimo ao longo do texto do Decreto, permitindo, portanto, sua utilização intercambiável no presente documento.

A importância do tema para o setor, para o país e para a comunidade internacional dispensa maiores ilações. Não obstante, evidencia-se a centralidade do ambiente digital na dinâmica securitária dos Estados e o ataque às infraestruturas críticas como uma nova forma de violência, com danos significativos às sociedades e aos países (PINTO; GRASSI, 2020), como se pode observar em conflitos recentes, incluindo

ataques dedicados às infraestruturas do setor de telecomunicações. Em âmbito nacional, o tema é disciplinado pela recente PNCiber, cuja finalidade é orientar a atividade de cibersegurança no país.

Elencam-se, como princípios da Política Nacional, nos termos do art. 2º do aludido Decreto, os seguintes: a soberania e interesse nacional; a garantia dos direitos fundamentais; a prevenção aos incidentes cibernéticos; a resiliência cibernética; a educação e o desenvolvimento tecnológico; a cooperação multissetorial; e a cooperação internacional.

Como objetivos, conforme o art. 3º do Decreto nº 11.856/2023, destacam-se: o desenvolvimento de mercado de segurança cibernética nacional; o fortalecimento da atuação diligente no ciberespaço; o combate aos crimes cibernéticos; o estímulo a ações de prevenção e gestão de riscos; o incremento da resiliência cibernética; o desenvolvimento da educação e capacitação profissional; o fomento às atividades de pesquisa, desenvolvimento tecnológico e inovação; a atuação coordenada dos entes da federação, Poderes e demais atores; o desenvolvimento de instrumentos de regulação, a fiscalização e controle; e a implementação de estratégias de colaboração para o desenvolvimento da cooperação internacional na matéria.

A PNCiber estabelece (art. 4º), como ferramentas, a Estratégia Nacional de Cibersegurança e o Plano Nacional de Cibersegurança, sendo a Política o documento de mais alto nível que estabelece os princípios e objetivos, os quais serão materializados pelas ações previstas na Estratégia e pelo planejamento detalhado no Plano.

Para além da PNCiber, o Decreto mencionado constituiu o Comitê Nacional de Cibersegurança (CNCiber), cujo papel central é orientar a atuação estratégica do país e promover a necessária coordenação nesse tema.

Compete ao CNCiber (art. 6º): a proposição de atualizações para a PNCiber, Estratégia e Plano Nacionais; a avaliação e proposição de medidas de incremento de cibersegurança; a formulação de propostas para prevenção e respostas a incidentes;

a proposição de medidas para desenvolvimento da educação em cibersegurança; a promoção de interlocução com entes federativos e a sociedade; a proposição de estratégias de colaboração para desenvolvimento de cooperação técnica internacional; e a manifestação em temas relacionados por solicitação do Presidente da Câmara de Relações Exteriores e Defesa Nacional do Conselho de Governo (CREDEN).

O CNCiber possui composição multissetorial com 15 (quinze) assentos destinados a órgãos e entidades que compõem a Administração Pública Federal, além de representação do Comitê Gestor da Internet (CGI.br) e da sociedade civil, academia e setor privado relacionados à cibersegurança.

Cada um desses setores é representado por 3 (três) membros, os quais são designados pelo Ministro de Estado Chefe do GSI/PR, órgão responsável pela Secretaria-Executiva do Comitê. A primeira composição do comitê foi designada em 9 de fevereiro de 2024, pela Portaria nº 6, do Gabinete de Segurança Institucional (BRASIL, 2024), tendo o CNCiber já iniciado seus trabalhos.

Além do Regimento Interno do CNCiber, os trabalhos iniciais resultaram na aprovação da criação de três Grupos de Trabalho Temáticos (GTT). O primeiro trata do processo de revisão e atualização da Estratégia Nacional de Segurança Cibernética; o segundo, da proposta de criação de órgão regulador para a governança de segurança cibernética nacional; e, finalmente, o terceiro, da coordenação do engajamento internacional do país no tema.

A Anatel integra os 3 GTTs e coordena, em conjunto com o Ministério da Gestão e da Inovação em Serviços Públicos, o GTT dedicado à discussão sobre uma autoridade nacional de cibersegurança, cuja atuação é mais bem detalhada neste link (BRASIL, 2024b).

Ressalva-se que a Anatel foi a única Agência Reguladora com vínculo ministerial a receber um assento no CNCiber. Isso se deve à centralidade do papel das telecomunicações no ecossistema digital, uma vez que o setor possui peculiaridades

que o diferenciam das demais infraestruturas críticas (IEC) no contexto de transformação digital e de cibersegurança.

Dadas suas características, o setor de telecomunicações é transversal a todos, tornando-se essencial para o funcionamento de cada um deles, constituindo-se em pedra angular do ecossistema digital.

O setor de telecomunicações apresenta uma enorme superfície de ataque, envolvendo não apenas as redes que formam a internet, mas, igualmente, o próprio ciberespaço. Além disso, é o principal meio para a disseminação de ameaças. Como consequência, as ações para promover a cibersegurança no setor têm um enorme impacto no ecossistema digital.

A Anatel, por sua vez, está encarregada de representar o Brasil nos organismos internacionais de telecomunicações, nos quais os debates de cibersegurança são predominantes em suas agendas. Isso implica que ela igualmente deve acompanhar e participar ativamente no desenvolvimento do estado da arte das discussões sobre o tema, encontrando-se em condições propícias para contribuir relevantemente com os trabalhos do CNCiber.

Dessa maneira, a Agência desempenha um papel peculiar e privilegiado na promoção da segurança cibernética do ecossistema digital brasileiro.

No que se refere à política pública em estudo, e salientando a inexistência de um marco legal específico (isto é, de uma lei em sentido formal dedicada à cibersegurança), menciona-se a Estratégia Nacional de Segurança Cibernética (E-Ciber), instituída pelo Decreto nº 10.222, de 5 de fevereiro de 2020.

A E-Ciber foi concebida como um módulo da Estratégia Nacional de Segurança da Informação (ENSI), a qual, por sua vez, busca implementar a Política Nacional de Segurança da Informação (PNSI), instituída pelo Decreto nº 9.637, de 26 de dezembro de 2018.

A E-Ciber apresentou a visão do Governo Federal para o quadriênio de 2020-2023 e está atualmente em processo de revisão, tendo o CNCiber designado grupo de

trabalho temático para essa finalidade em deliberação tomada em reunião realizada em 20 de março de 2024.

A E-Ciber parte de uma metodologia de identificação de eixos temáticos e transformadores para estabelecer três objetivos estratégicos: tornar o país mais próspero e confiável no ambiente digital; aumentar a resiliência do país às ameaças cibernéticas; e fortalecer a atuação brasileira em segurança cibernética no cenário internacional.

Para o alcance desses objetivos, estabeleceram-se 10 (dez) ações estratégicas, a saber: fortalecimento das ações de governança cibernética; estabelecimento de um modelo centralizado de governança no âmbito nacional; promoção de um ambiente participativo, colaborativo, confiável e seguro, entre setor público, setor privado e sociedade; elevação do nível de proteção do Governo; aumento do nível de proteção das Infraestruturas Críticas Nacionais; aprimoramento do arcabouço legal sobre segurança cibernética; incentivo à concepção de soluções inovadoras em segurança cibernética; ampliação da cooperação internacional do Brasil em segurança cibernética; fortalecimento da parceria, em segurança cibernética, entre setor público, setor privado, academia e sociedade; e elevação do nível de maturidade da sociedade em segurança cibernética.

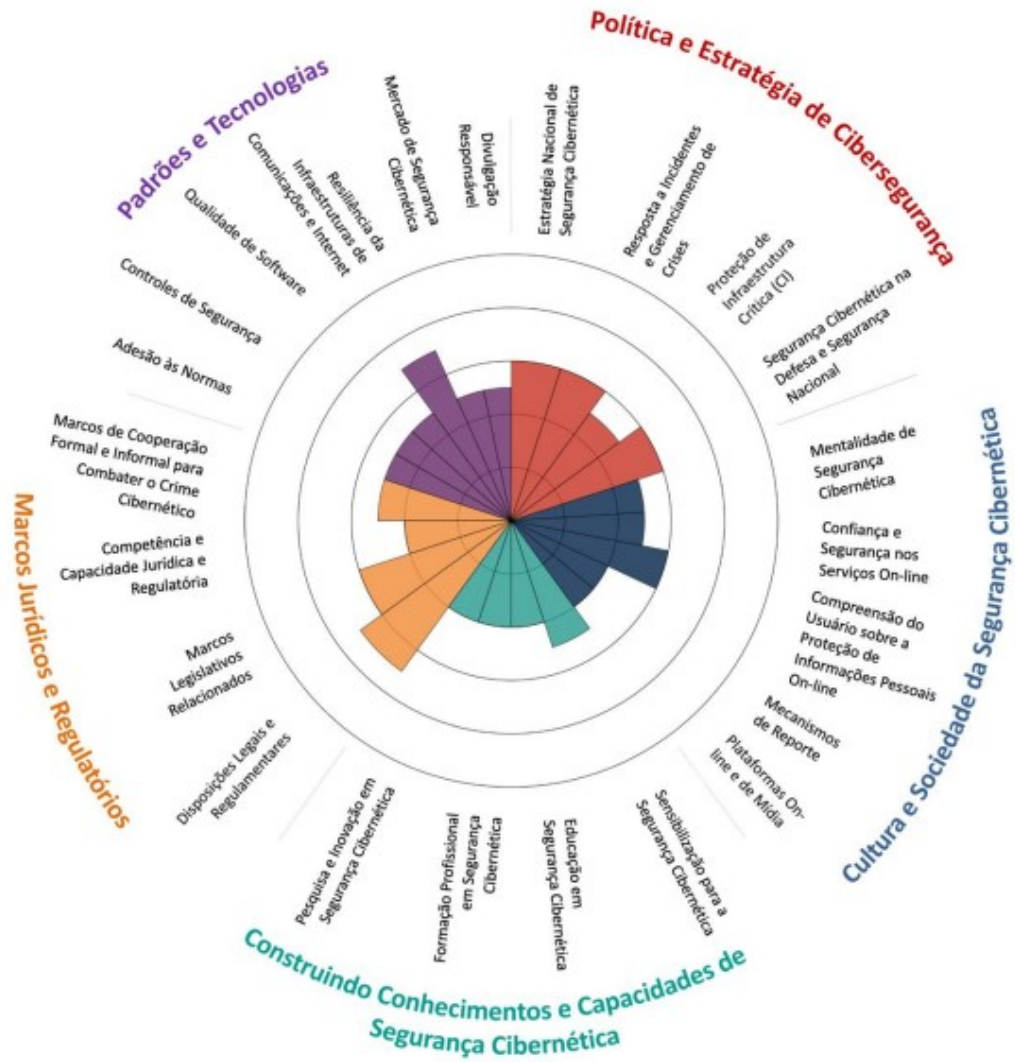
Um aspecto particularmente interessante da Estratégia aborda o papel dos órgãos reguladores, conforme descrito na sua Parte II, ao tratar do Eixo Temático de Proteção e Segurança, no estímulo à adoção de procedimentos de segurança cibernética pelos regulados.

Cita, como exemplos, a criação de estrutura de governança de segurança cibernética nas empresas de infraestruturas críticas; a realização de auditorias externas; a adoção de práticas e de requisitos de segurança cibernética; a criação de centros de tratamento e resposta a incidentes por empresa e por setor; a capacitação contínua de seus colaboradores em todos os níveis; a notificação ao Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo (CTIR Gov); a notificação dos incidentes aos consumidores; promoção de campanhas de

conscientização; a exigência de segurança cibernética para fornecedores; e a elaboração de planos de resposta a incidentes cibernéticos.

O desenvolvimento da E-Ciber recebeu subsídios do processo de revisão das capacidades brasileiras de segurança cibernética realizada pelo *Global Cyber Security Capacity Centre* (GCSCC), da Universidade de Oxford, em conjunto com a Organização dos Estados Americanos e com o Gabinete de Segurança Institucional (OEA, 2020).

Esse processo foi novamente conduzido durante o ano de 2023, com o objetivo de subsidiar o processo de revisão da E-Ciber. A maturidade das capacidades de segurança cibernética no Brasil em 2023 é ilustrada no seguinte gráfico (OEA, 2020, p. 8):



A figura acima apresenta as cinco dimensões do modelo e os fatores que compõem cada uma delas. O centro colorido representa o estágio de maturidade em cada fator. Quanto mais próximo do centro, mais incipiente será o estágio de maturidade.

Os círculos mais afastados do centro representam os estágios mais avançados de maturidade, quais sejam, os estágios estratégico e dinâmico, respectivamente, para os quais não há evidência de maturidade no contexto das capacidades brasileiras.

Percebe-se que, de uma forma geral, as capacidades brasileiras estão avaliadas nos estágios de maturidade formativo (segundo estágio) e estabelecido (terceiro estágio), destacando-se que o relatório em estudo (OEA, 2020, p. 8) disponibiliza informações sobre a metodologia do modelo.

Nota-se que uma das competências do recém-criado CNCiber será justamente propor a atualização da E-Ciber e a revisão realizada pelo GCSCC será um valioso insumo ao processo.

Após o panorama nacional, importa olhar para o setor de telecomunicações.

O tema da cibersegurança sempre recebeu atenção dedicada pela Anatel e tem sido progressivamente priorizado com a aceleração da transformação digital.

Essa transformação faz com que a vida cotidiana em nossa sociedade seja, em maior ou menor grau, mediada pela utilização das Tecnologias de Informação e Comunicação (TICs).

Tais tecnologias são utilizadas para tratamento, organização e disseminação de informações e hoje estão presentes nas atividades educacionais, financeiras, de compra de produtos e serviços, de prestação de serviços públicos, de lazer *etc*. Todas as esferas da vida em sociedade foram e continuam a ser experimentadas e transformadas por essas tecnologias.

Para ilustrar a relevância das TICs para a prestação de serviços públicos para a população brasileira, destaca-se que mais de 4.200 (quatro mil e duzentos) serviços digitais (BRASIL, 2024a) são oferecidos à população pela Plataforma Gov.br, a qual é utilizada por mais de 150 (cento e cinquenta) milhões de pessoas.

É justamente nesse contexto que a cibersegurança tornou-se um dos pilares fundamentais da nossa vida em sociedade. A utilização massiva das TICs depende da confiança dos seus usuários. E a confiança baseia-se no nível de segurança que se espera dessas tecnologias.

Um exemplo recente e revolucionário é a utilização do PIX, o meio de pagamento mais utilizado no Brasil, o qual facilitou a vida da população brasileira. Sua adoção em larga escala decorre da confiança depositada pelos seus usuários, de modo que as transações ocorram conforme o esperado. Para garantir essa confiança, é necessário contar com uma robusta estrutura para a cibersegurança e resiliência cibernética do sistema de pagamentos.

O cenário é desafiador. O mais recente relatório de riscos globais do Fórum Econômico Mundial destaca que a insegurança cibernética é o quarto risco global de curto prazo (2 anos), figurando no oitavo lugar na visão de longo prazo (10 anos), momento em que os resultados adversos das tecnologias de inteligência artificial passam a figurar no sexto lugar da lista. No mesmo relatório, o panorama de riscos revela que 39% dos entrevistados na pesquisa de percepção de riscos apontam ataques cibernéticos como um dos cinco riscos mais prováveis de gerar uma crise material de escala global no ano de 2024 (WEF, 2024).

A promoção de cibersegurança não é um fim em si mesmo. A Estratégia Brasileira para a Transformação Digital (E-Digital) reconhece a confiança no ambiente digital como eixo habilitador da Transformação Digital, com o objetivo de aproveitar a potencialidade das TICs para fomentar o desenvolvimento econômico e social do nosso país e, assim, o bem-estar de toda a população brasileira (BRASIL, 2022).

Toda a nossa vida contemporânea baseia-se, portanto, na utilização das TICs. Dessa forma, apesar de a cibersegurança carregar um forte viés técnico que lhe é associado, ela não se limita a essa perspectiva e nem se encontra alheia ao cotidiano das pessoas.

Ao contrário, abrange uma série de condutas rotineiras - conhecidas como medidas de higiene cibernética (em uma analogia às condutas de higiene sanitária que diminuem os riscos à saúde humana) - que contemplam a utilização, armazenamento e alteração de senhas; cuidado ao clicar em *links* e abrir anexos; usar segundo fator de habilitação em aplicativos *etc*. Essas condutas preventivas são essenciais para a confiança individual no uso das tecnologias e, além disso, têm um impacto positivo em todo o ecossistema. A adoção de tais medidas mitiga riscos associados ao ecossistema digital.

Um exemplo da externalidade positiva das ações de higiene cibernética é a proteção com o uso de senha forte na rede doméstica. Ao proteger a rede doméstica, protegem-se os dispositivos que nela estão conectados e os dados que nela trafegam.

Se a rede ficar desprotegida, além de um ataque aos dispositivos nela conectados e aos dados trafegados, esses mesmos dispositivos podem ser utilizados como "poder de fogo" para a realização de um ataque de negação de serviço distribuído (DDoS) em outra rede ou serviço, no território brasileiro ou no exterior.

Todos os atores do ecossistema (órgãos e entidades públicas, setor privado, academia e sociedade civil) têm um relevante papel a cumprir para a promoção de um ambiente digital mais seguro, que não pode ser negligenciado nem subestimado, sendo responsáveis pela manutenção, construção e aprimoramento de uma sociedade resiliente, que tenha condições de responder aos crescentes desafios em matéria de segurança cibernética. Assegurar uma abordagem de cibersegurança para todo o país demanda essa congregação multissetorial (HUREL, 2021).

Por isso, fala-se na responsabilidade compartilhada de todos os atores. Nesse sentido, a Recomendação do Conselho da Organização para a Cooperação e Desenvolvimento Econômico (OCDE, 2022a) sobre Gestão de Risco de Segurança Digital, aderida pelo Brasil em 26 de setembro de 2022, destaca que a responsabilidade dos atores é baseada no seu papel, contexto e habilidade de agir.

É justamente nesse contexto que o papel da Agência em cibersegurança é ressaltado.

A Anatel reconhece a prioridade, multidisciplinaridade, transversalidade e multissetorialidade do tema, o qual vem sendo amadurecido internamente ao longo da última década. Isso resultou na aprovação do Regulamento de Segurança Cibernética Aplicada ao Setor de Telecomunicações (R-Ciber), aprovado pela Resolução nº 740, de 21 de dezembro de 2020 (BRASIL, 2020a).

O R-Ciber começou a ser gestado a partir da inclusão do tema como item 58 da Agenda Regulatória da Agência para o biênio 2017 – 2018. Após um processo regulamentar, que compreendeu tomada de subsídios com atores relevantes e consulta pública, o R-Ciber foi aprovado em 2020 com uma redação alinhada à E-Ciber, implementando as ações estratégicas nela contidas.

Assim, o R-Ciber estabelece os princípios e diretrizes que devem ser observados por todas as prestadoras de serviços de telecomunicações. Esses princípios são: autenticidade, confidencialidade, disponibilidade, diversidade, integridade, interoperabilidade, prioridade, responsabilidade e transparência.

Já as diretrizes abrangem a adoção de boas práticas e normas internacionais referentes à segurança cibernética, a disseminação da cultura de segurança cibernética, a utilização segura e sustentável das redes e serviços de telecomunicações, a identificação, proteção, diagnóstico, resposta e recuperação de incidentes de segurança cibernética, a cooperação entre os diversos agentes envolvidos com fins de mitigação dos riscos cibernéticos, o respeito e a promoção dos direitos humanos e das garantias fundamentais - em especial a liberdade de expressão, a proteção de dados pessoais, a proteção da privacidade e o acesso à informação do usuário dos serviços de telecomunicações - e o incentivo à adoção de conceitos de *security by design* e *privacy by design* no desenvolvimento e aquisição de produtos e serviços no setor de telecomunicações.

Além desse conjunto mandatório para todas as prestadoras, o R-Ciber adicionou um conjunto de medidas de controle *ex ante* para as prestadoras dos serviços de telecomunicações de interesse coletivo que não sejam enquadradas como Prestadoras de Serviços de Telecomunicações de Pequeno Porte (PPP).

Veja-se que o R-Ciber estabeleceu um regime assimétrico de controle, desenhado para conformar o fomento da adoção de medidas que promovam a segurança e a resiliência cibernéticas pelas prestadoras de serviço de telecomunicações com a inibição da criação de ônus regulatórios que possam configurar barreiras à entrada, prejudicando a competição no setor (FREITAS *et al.*, 2021). Relembra-se, nesse ponto, que foi justamente o regime de regulação assimétrica praticado pela Agência que permitiu o florescimento do ecossistema de prestadores do serviço de banda larga fixa, possibilitando a expansão da conectividade.

O conjunto de obrigações *ex ante* abrangem: elaboração, manutenção e implementação de uma Política de Segurança Cibernética (PSC); publicação, pela prestadora, na sua página na Internet, de extrato da sua PSC; apresentação à Anatel de relatório sobre implementação da PSC; utilização de fornecedores de produtos e equipamentos de telecomunicações que possuam PSC compatíveis com os princípios e diretrizes dispostos no R-Ciber e que realizem processos de auditoria independentes e periódicos; alteração da configuração padrão de autenticação dos equipamentos fornecidos em regime de comodato aos seus usuários; notificação da Agência e comunicação às demais prestadoras e aos usuários dos incidentes relevantes; adoção, pelas prestadoras, de procedimento de compartilhamento de informações sobre incidentes relevantes; realização de ciclos de avaliação de vulnerabilidades; e envio de informações sobre suas Infraestruturas Críticas de Telecomunicações à Anatel.

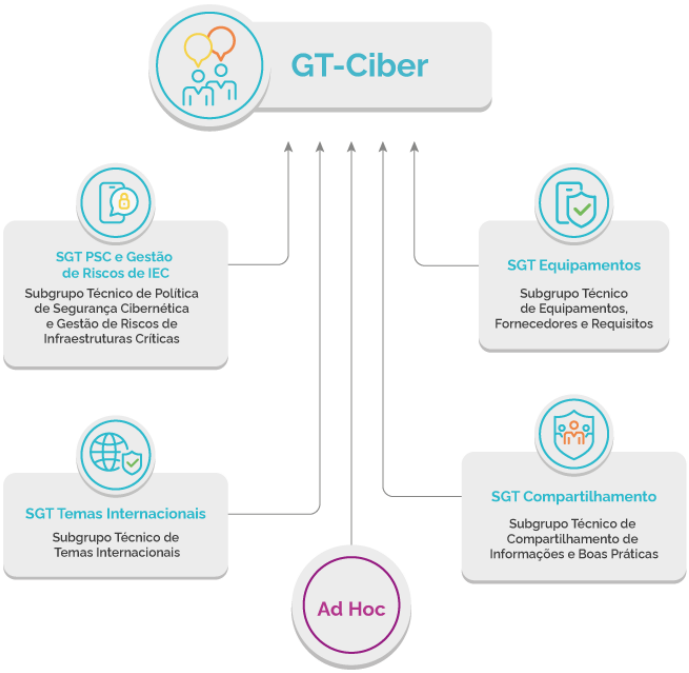
O R-Ciber, igualmente, regulamenta a governança de cibersegurança no setor de telecomunicações, criando o Grupo Técnico de Segurança Cibernética e Gestão de Riscos de Infraestruturas Críticas (GT-Ciber).

O Grupo técnico tem um rol bastante amplo de atribuições, as quais abarcam o auxílio à Agência para acompanhamento da implementação da PSC; acompanhamento de novas tecnologias e seu impacto na utilização segura e sustentável das redes e serviços de telecomunicações; elaboração das definições necessárias para a implementação do R-Ciber; internalização de boas práticas e padrões; elaboração de estudos; promoção de ações de capacitação; promoção de ações de conscientização; e interação com órgãos e entidades, dentre outras.

O GT-Ciber é coordenado pelo Superintendente de Controle de Obrigações, conforme designação do Conselho Diretor da Agência, contando com a participação de servidores da Anatel e de prestadoras detentoras de Poder de Mercado Significativo (PMS), assim como uma entidade representando as PPPs. Pode, ainda, contar com a participação de outros convidados, de acordo com a pertinência temática.

Mais recentemente, com a aprovação da revisão do R-Ciber em 04 de julho de 2024, resultando na Resolução nº 767, de 07 de agosto de 2024, o GT-Ciber passa a contar com a participação das operadoras de cabo submarino com destino internacional, das prestadoras do Serviço Móvel Pessoal detentoras de rede própria e das operadoras de rede que ofertam tráfego em mercado de atacado, as quais passam a ter assento no GT-Ciber.

O GT-Ciber possui subestruturas que espelham as atribuições e temas tradados no Grupo. O organograma abaixo reflete a estrutura atualmente vigente:



No R-Ciber, a Anatel, a exemplo do que já consta em outras regulamentações, procedeu a uma abordagem assimétrica de obrigações regulatórias, impondo esse conjunto de controles às prestadoras que não podem ser qualificadas como PPPs.

Considera-se PPP o grupo detentor de participação de mercado nacional inferior a 5% (cinco por cento) em cada mercado de varejo em que atua.

Dessa forma, com base no Ato nº 6539, de 18 de outubro de 2019 (BRASIL, 2019), as prestadoras **pertencentes** aos Grupos Econômicos da Telefônica; Telecom Americas; Telecom Itália; e Oi devem implementar as obrigações estabelecidas pelo Regulamento.

Todavia, é esperado que o Grupo Oi, no que diz respeito ao STFC, com a recente aprovação da adaptação do seu regime de concessão para autorização no Tribunal de Contas da União, e as prestadoras integrantes do Grupo Sky/AT&T, ante deliberação cautelar recente do Conselho Diretor da Anatel em decorrência do hibridismo de mercado do SeAC com o de serviços de *streaming over the top*, não mais estejam sujeitos às obrigações *ex ante* exigíveis das detentoras de Poder de Mercado Significativo, segundo o conceito estabelecido no inciso XV do artigo 4º do

Plano Geral de Metas de Competição, aprovado pela Resolução nº 600, de 8 de novembro de 2012, e alterado pela Resolução nº 694, de 17 de julho de 2018.

Esclarece-se que a decisão do Conselho Diretor que inicialmente aprovou o R-Ciber iniciou, em paralelo, um processo de revisão da abrangência desses controles *ex ante.*

O Acórdão nº 692, de 21 de dezembro de 2020, determinou ao GT-Ciber que enviasse à Superintendência de Planejamento e Regulamentação (SPR) contribuições 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*".

Esse processo motivou a criação de um grupo *ad hoc* no âmbito do GT-Ciber para discussão. O resultado dos seus trabalhos foi apreciado na revisão do R-Ciber (Processo nº 53500.057799/2021-74), o qual foi conduzido sob a relatoria do Conselheiro Alexandre Freire. Salienta-se que os seus documentos preparatórios foram tornados públicos para a consulta da sociedade, antes da deliberação do Conselho Diretor da Anatel (BRASIL, 2023a), denotando a transparência que se buscou imprimir a esse processo normativo.

Por sua vez, no início de 2024, o Conselho Diretor da Agência decidiu, por unanimidade, no Acórdão nº 65, de 28 de fevereiro de 2024, que acolheu a Análise nº 4/2024/AF (BRASIL, 2024c), de autoria do Conselheiro Diretor Alexandre Freire, alterar a Agenda Regulatória da Anatel para o biênio 2023-2024, a fim de contemplar a reavaliação do R-Ciber frente aos novos e emergentes desafios, motivando a inclusão do seguinte item nos seguintes termos:

> Nome: Proposta de alteração do Regulamento de Segurança Cibernética Aplicada ao Setor de Telecomunicações, aprovado pela Resolução nº 740, de 21 de dezembro de 2020.
>
> Descrição: Revisão do Regulamento de Segurança Cibernética Aplicada ao Setor de Telecomunicações, aprovado pela Resolução nº 740, de 21 de dezembro de 2020, de modo a atualizá-lo para contemplar novos elementos, novas tecnologias e novos

> pontos de criticidade, tais como aplicação maliciosa de soluções de inteligência artificial, novas vulnerabilidades nas diversas camadas de transmissão da rede, aspectos normativos relativos à prestação dos serviços de cloud computing e de data centers quando associadas ao setor de telecomunicações, incluindo estudos para avaliação da competência da Anatel para regulamentação direta desses serviços, sem prejuízo de eventual disciplinamento do tema, que deve compreender aspectos associados à sustentabilidade ambiental dos modelos de negócios adotados, inclusive no que diz respeito ao consumo de energia, em alinhamento com o Objetivo de Desenvolvimento Sustentável nº 9 da Agenda 2030 da Organização das Nações Unidas (ONU), que trata da indústria, inovação e infraestrutura e busca construir infraestruturas resilientes, promover a industrialização inclusiva e sustentável e fomentar a inovação.
>
> Prioridade: prioritário.
>
> Meta (para a vigência da Agenda Regulatória 2023-2024): conclusão do Relatório de AIR e da respectiva proposta até o 2º semestre 2024.

No contexto da relatoria e da importante deliberação tomada pelo Conselho Diretor em reunião realizada em 04 de julho de 2024, de aprovação final da revisão do R-Ciber (Resolução nº 767/2024), este trabalho emerge como uma importante documentação dos subsídios ao processo regulamentar em menção.

Ele apresenta a contextualização do tema, incluindo uma análise descritiva das políticas públicas brasileiras, do papel da Anatel e da sua regulamentação, da relevância do tema e da centralidade do setor de telecomunicações. Além disso, aborda vários *benchmarks* estrangeiros numa perspectiva comparativa, com o propósito de trazer alguns dos *insights* que nortearam a recente revisão do R-Ciber e que guiarão a as pautas regulatórias futuras para a cibersegurança no setor de telecomunicações.

Igualmente, reflete-se sobre temas importantes de fronteira que possuem relevante intersecção com a cibersegurança e com o setor telecomunicações.

Em 4 de julho de 2024, o Conselho Diretor aprovou a proposta de revisão do Regulamento de Segurança Cibernética aplicável ao Setor de Telecomunicações, por meio da Resolução nº 767, de 07 de agosto de 2024. Destacam-se as seguintes alterações, resultantes em grande parte da atuação que culminou na elaboração deste trabalho:

1. Independente do porte, todas as Prestadoras dos Serviços de Telecomunicações de Interesse Coletivo, ficam sujeitas ao cumprimento do art. 8º do R-Ciber, cujo escopo consiste em mitigar vulnerabilidades relacionadas aos equipamentos cedidos aos consumidores dos serviços de telecomunicações;

2. Ampliação do rol de entidades sujeitas ao controle *ex ante* da Anatel, que passam a incluir as operadoras de cabo submarino com destino internacional, as prestadoras do Serviço Móvel Pessoal detentoras de rede própria e as operadoras de rede que ofertam tráfego em mercado de atacado, as quais passam a ter assento no GT-Ciber;

3. Para reforçar a transparência e a coordenação entre as entidades reguladoras, todas as prestadoras devem notificar a Anatel sobre incidentes de segurança quando tal medida for obrigatória perante a Autoridade Nacional de Proteção de Dados (ANPD);

4. Para fomentar a inovação no setor, as prestadoras terão a possibilidade de contratar *startups*, isentando-as de certos requisitos de segurança cibernética, desde que a prestadora contratante garanta a conformidade com as disposições do Regulamento;

5. Atualização do regramento aplicável às políticas de segurança cibernética, para tornar mais claras as rotinas a serem empregadas nas contratações de *data centers* e de serviços de computação em nuvem, em que se procede à regulação indireta destes últimos, quando essa contratação estiver relacionada à prestação de serviços de telecomunicações.

Dessa maneira, o presente *white paper* visita a temática no contexto do arcabouço nacional e setorial, incluindo a revisão regulamentar recentemente encerrada.

Além disso, apresenta a experiência internacional trazida como subsídio regulatório e, por fim, enfrenta os temas emergentes, apresentando diversas reflexões, com o objetivo de fomentar o debate público para o futuro e contribuir para o amadurecimento das discussões sobre cibersegurança no setor de telecomunicações e fora dele.

1

Visão Geral do Setor de Telecomunicações no Brasil

Atualmente, conforme já visto acima, o setor de telecomunicações brasileiro é responsável pela comunicação, educação, lazer e entretenimento, prestação de serviços públicos, além de uma parcela relevante da experiência de consumo dos brasileiros e de diversos modelos de negócios, que passaram a florescer com a ampliação das tecnologias de informação e comunicação, especialmente a partir da implementação das redes 4G na década passada.

A essencialidade dos serviços de telecomunicações decorre de sua transversalidade, visto que diversos segmentos da economia, em maior ou menor grau, tornaram-se dependentes do seu funcionamento regular, a ponto de não ser mais possível conceber a manutenção de seus modelos de negócio sem essa dependência, ainda que para simples processamentos de pagamentos via PIX.

Na E-Digital ciclo 2022-2026, identificou-se uma tendência crescente dessa dependência, com uma economia progressivamente baseada em dados. Contudo, foi pontuado que "a *governança dos riscos associados ao compartilhamento de dados é, no geral, prematura em todo o mundo, mas especialmente nos países de baixa renda*" (BRASIL, 2022, p. 58).

Ainda, destacou-se a importância de se endereçar os seguintes temas:

01) transferências internacionais: devendo ser mantida a adoção de um modelo de transferências abertas de dados (isto é, sem a imposição de condições), "*como forma de estimular novos negócios e soluções para a sociedade, mas, ao mesmo tempo, garantir que o Estado controle e reduza os riscos associados ao uso indevido de dados, a exemplo da vigilância política, de práticas monopolistas e anticompetitivas, espionagem e vazamento de dados pessoais ou sensíveis*" (BRASIL, 2022, p. 60);

02) *data centers*: que podem atrair investimentos e empresas inovadoras, embora tenham sido destacados uma série de entraves, tais como custos elevados para a construção e operação de *data centers* relacionados à alta carga tributária e ao custo elevado de energia e de importação de equipamentos; incerteza jurídica e regulatória, derivada de uma instabilidade nas regras e nos marcos legais; e falta de mão de obra qualificada nas diferentes *expertises* necessárias ao setor de TI (BRASIL, 2022, p. 61); e

03) o advento da internet das coisas (IoT), em que sociedades (mercados e governos) que se adiantam no desenvolvimento de novas aplicações associadas ao consumo e à produção de bens e serviços (*frontrunners*) tendem a se beneficiar mais que aqueles que se atrasam nesse processo. Estima-se, aliás, que metade dos 29,3 bilhões de dispositivos conectados já se referiam a conexões máquina-a-máquina - M2M (BRASIL, 2022, p. 65).

No cenário brasileiro, o CNCiber representa um relevante e recente fórum institucional para a concepção de novas medidas e regulamentos voltados à promoção da Cibersegurança, bem como à promoção de sua cultura.

No entanto, o Brasil conta notadamente com iniciativas esparsas de regulamentação setorial, a exemplo do R-Ciber.

Citam-se, ainda, a Resolução CMN Nº 4.893, de 26 de fevereiro de 2021, que dispõe sobre a política de segurança cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem a serem observados pelas instituições autorizadas a funcionar pelo Banco Central do Brasil; e a Resolução BCB n º 85, de 8 de abril de 2021, que dispõe sobre a política de segurança cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem a serem observados pelas instituições de pagamento autorizadas a funcionar pelo Banco Central do Brasil, as quais foram atualizadas em 2024. Igualmente, cita-se a Resolução Normativa ANEEL nº 964, de 14 de dezembro de 2021, que dispõe sobre a política de segurança cibernética a ser adotada pelos agentes do setor de energia elétrica.

Desde a aprovação do R-Ciber em meados do ano de 2020, o Brasil passou por diversas mudanças, especialmente no que diz respeito às transformações econômicas e sociais provocadas pela pandemia de Covid-19. Destaca-se, aqui, a aceleração do processo de transição para a economia digital, que é um subproduto das políticas de confinamento adotadas na ocasião, levando a novas configurações dos modelos de negócios até então predominantes.

Nesse novo contexto, deflagraram-se diversas discussões no GT-Ciber, em que se reconheceu a criticidade de alguns atores para a conectividade e se identificaram novos temas, refletidos na alteração da Agenda Regulatória anteriormente referida, tais como cabos submarinos, *data centers* e computação em nuvem, os quais, aliás, já eram considerados na Estratégia Brasileira de Inteligência Artificial.

Esses pontos foram objeto de deliberação na revisão do R-Ciber em 04 de julho de 2024, conforme visto acima.

2

Benchmark: União Europeia (UE)

Perante a Comissão Europeia, encontra-se bem sedimentada a ideia de que a competividade da sua economia como um todo depende do aprimoramento da infraestrutura das redes e serviços digitais (EC, 2024, p. 3).

Esse processo compreende, dentre outros pontos, a construção de uma infraestrutura de cabos submarinos resiliente, os quais já possuíam relevância no passado e, com o surgimento e avanço da Internet, tornaram-se elementos centrais para as dimensões econômica, política e securitária dos países (AYRES PINTO; MEDEIROS, 2022). A resiliência desses cabos está diretamente relacionada ao crescimento do PIB.

Menciona-se, ainda, estudo desenvolvido a pedido da Google a respeito de cabo submarino em recente operação em Portugal, que destaca os ganhos de instalação desse cabo ligando Portugal à África, na ordem de 500 (quinhentos) milhões de euros por ano (COPENHAGEN ECONOMICS, 2021, p. 16 *et seq.*).

A partir dos desenvolvimentos geopolíticos posteriores ao conflito Rússia-Ucrânia, há uma percepção razoável no sentido de que a resiliência e a segurança da

infraestrutura são importantes para se preservar a segurança do desenvolvimento econômico na própria União Europeia (EC, 2024, p. 4-5).

Adicionalmente, tem-se percebido uma migração cada vez mais intensa do setor de equipamentos de redes baseadas em nuvens e em *softwares* e em arquiteturas abertas. Por sua vez, identifica-se a possiblidade de gargalos nos mercados de serviços de infraestrutura, de *cloud computing* e de fornecimento de plataformas de *chips* (EC, 2024, p. 4).

O principal instrumento regulatório em vigência para a União Europeia é a Diretiva NIS 1 - Diretiva (UE) 2016/1148. O termo "NIS" constitui-se em acrônimo para "*Network and Information Security*". A referida diretiva, adotada em 2016, foi a primeira medida legislativa para a União editada com a finalidade de promover a cooperação entre os seus membros no tema, e de criar a primeira camada de harmonização no domínio da cibersegurança. Destaca-se que 67% dos europeus se encontram insatisfeitos com o seu nível de proteção *online* e pedem por mais ações de educação e cooperação entre estados membros (EC, 2023a, p. 22).

São destinatários da Diretiva NIS 1: a) operadores das chamadas "infraestruturas críticas" (energia, transportes, bancos, mercados financeiros, saúde, abastecimento e distribuição de água potável e infraestrutura digital) e b) prestadores de serviços digitais relevantes (motores de pesquisa *on-line*, plataformas *on-line* de *marketplace* e provedores de serviço de computação em nuvem), com exceção das pequenas e médias empresas (SMEs, assim compreendidas como aquelas que tenham menos de cinquenta empregados e um faturamento anual inferior a dez milhões de euros) que não façam parte da estrutura de grandes organizações.

Embora a NIS 1 tenha por finalidade a promoção da cibersegurança, seu escopo não se limita a isso. Ele está relacionado a quaisquer incidentes que possam produzir algum efeito disruptivo significativo, incluindo eventos que, a princípio, não estão relacionados à cibersegurança propriamente dita, tais como desastres naturais (inundações, ondas de calor *etc.*) e interrupções na cadeia de suprimentos (*v.g.*, interrupção no fornecimento de eletricidade).

Acrescenta-se que, atualmente, o arcabouço regulatório da União Europeia para redes e serviços de comunicações não impõe obrigações a provedores de infraestrutura de serviços em computação em nuvem e não regulamenta a relação entre vários novos atores nesse complexo ecossistema da infraestrutura digital, em que mais de 60% do tráfego internacional se dá por cabos fora do escopo regulatório da União e em que muitos dos provedores de computação em nuvem operam seu tráfego em redes privadas, que são menos sujeitas à regulamentação, transferindo os dados quando já estão dentro das redes públicas que farão a sua distribuição (EC, 2024, p. 15).

Ainda nesse cenário, um risco de cibersegurança já percebido pela Comissão Europeia está relacionado ao aumento esperado do poder computacional bruto nos próximos dez anos, o qual pode ser potencializado pela implementação da computação quântica.

Nesse cenário, não se descarta o comprometimento de criptografias legadas, com o risco de exposição de serviços e redes de comunicações e de dados sensíveis, que vão desde dados de saúde até informações estratégicas de defesa (EC, 2024, p. 9).

Com base nisso, a Comissão Europeia entende que é necessário preparar seus diversos ativos digitais para enfrentar esse risco. Para a referida Comissão, ou os provedores europeus se adaptam a esse risco, ou ficarão à mercê de novos *players* que se encontrem fora de sua jurisdição, especialmente no que diz respeito aos serviços de *cloud computing,* ao passo que os modelos de negócios devem se tornar cada vez mais dependentes do uso desses serviços (EC, 2023a, p. 13).

Outro risco identificado foi a crescente dependência das empresas operantes na UE em relação a fornecedoras localizadas em países alheios ao bloco, seja no ecossistema de serviços de comunicações eletrônicas, seja na cadeia de suprimentos. Segundo a Comissão Europeia, a dependência de um pequeno número de fornecedores de infraestruturas e de serviços críticos, como ferramentas de *cloud*, aplicações de IA e infraestruturas de cabos submarinos, acarreta o risco de novos gargalos ou bloqueios (EC, 2024, p. 38).

No que diz respeito a cabos submarinos, buscam-se a criação de linhas de financiamento para novas infraestruturas estratégicas e o aumento da segurança e resiliência daquelas atualmente existentes, acompanhado de um sistema de governança destinado a essa finalidade, o qual deve compreender (EC, 2024, p. 39): (i) elementos adicionais para mitigar e abordar riscos, vulnerabilidades e dependências no âmbito de uma avaliação consolidada a nível da UE, e prioridades para aumentar a resiliência; (ii) revisão de requisitos para atualizar cabos existentes ou para financiar novos cabos; (iii) uma atualização da lista de prioridades co-criada de *Cable Projects of European Interest* (CPEI), tanto intra-UE como internacionais, com base na importância estratégica e no respeito pelos critérios acima; (iv) financiamento conjunto de várias fontes para esses projetos, incluindo fundos de capital nos quais a União participe com os Estados-Membros, para reduzir o risco do investimento privado; e (v) outras ações para proteger as cadeias de abastecimento e evitar a dependência de fornecedores estrangeiros de alto risco.

Por sua vez, o Parlamento Europeu (2023, p. 22) se manifestou no sentido de que a vulnerabilidade do ambiente digital como um todo ainda não é monitorada de forma completa, nos moldes dos testes de esforço macroprudenciais aplicados no setor financeiro, sendo necessário evoluir para um monitoramento mais abrangente, com uma nova infraestrutura analítica e com conjuntos de dados expansivos para simular potenciais perturbações.

Elencou-se, ainda, a necessidade de se harmonizarem os requisitos de segurança, incluindo discussões em fóruns internacionais. Isso envolveria a identificação das melhores normas e práticas que aproveitem os mais recentes desenvolvimentos em segurança e capacidades de automonitoramento para cabos – abrangendo roteamento e retransmissão a eles associados – e equipamentos, o que poderia ser reconhecido por meio de um sistema de certificação específico da própria UE.

A ENISA (*European Union Agency for Cybersecurity*, ou Agência Europeia para a Segurança das Redes e da Informação), por exemplo, vem envidando esforços focados na implementação de uma criptografia pós-quântica padronizada, tendo a

Comissão Europeia entendido que isso deve ser feito por todos os seus membros de forma harmoniosa e coordenada, com o emprego sinérgico de computação quântica com chaves distribuídas (EC, 2024, p. 37-38).

No entanto, tal cenário revela uma situação sensível, pois, segundo a Comissão Europeia, as empresas de telecomunicações não têm interesse nos massivos investimentos requeridos para atravessar o caminho necessário para a transformação digital, incluindo a manutenção e retomada do funcionamento dos serviços em casos de crises ou desastres (EC, 2024, p. 10). Destaca-se que a performance das ações de companhias europeias com capital aberto, em geral, tem sido inferior à dos índices de referência dos mercados de ações europeus como um todo, sendo essas empresas de telecomunicações marcadas por um aumento constante da dívida líquida sobre o EBITDA ao longo do tempo (EC, 2024, p. 11).

A União Europeia entende, ainda, como medida necessária à segurança e resiliência de sua rede, que os elementos de cibersegurança devem compreender as diversas camadas de tráfego, desde os diversos itens de *hardware* que compõem a rede até as diversas camadas de serviços. Isso inclui a definição de padrões de segurança para mensagens e videoconferências (EC, 2024, p. 17).

Mais recentemente, em 14 de dezembro de 2022, aprovou-se a Diretiva 2022/2555, conhecida como NIS 2, que exige que os Estados-Membros da União Europeia adotem as medidas necessárias para a sua internalização até 17 de outubro 2024. A partir de 18 de outubro de 2024, a NIS 1 não será mais aplicável.

A aprovação da NIS 2 decorreu de uma percepção de um aumento significativo dos ataques cibernéticos entre 2016 e 2021, inclusive em infraestruturas críticas. Estima-se que o mercado global de segurança deve crescer de USD 150 bilhões para USD 400 bilhões até o ano de 2026 (EP, 2023, p. 2). Isso levou o Parlamento Europeu a determinar à Comissão Europeia que avaliasse a necessidade de ampliar o escopo da NIS para outros serviços e setores críticos não cobertos por legislações específicas (EC, 2023a, p. 17-18).

Em nível global, as agências da União Europeia avaliam que o cenário se encontra volátil, em que os incidentes de cibersegurança, especialmente ataques de DDoS e resgates de *ramsonware*, aumentaram 150% entre os anos de 2022 e 2023 (EP, 2023, p. 3). Esse cenário deve se tornar ainda mais complexo com o desenvolvimento de novas tecnologias e com o aperfeiçoamento das já existentes, como a computação quântica e a inteligência artificial, demandando maior preparação e capacidade de resposta às ameaças associadas a esses elementos (EC, 2023a, p. 17-18).

Durante a discussão do projeto que culminou na aprovação da NIS 2, abriu-se tomada de subsídios entre julho e outubro de 2020 para a avaliação do impacto da NIS 1.

Foram apresentadas 206 (duzentas e seis) contribuições, das quais 182 (cento e oitenta e duas) provieram de respondentes localizados dentro da União Europeia. O tópico mais controverso foi a ausência de uma abordagem harmonizada entre os diversos países membros, especialmente no que diz respeito à definição de operadores dos serviços essenciais (EP, 2023, p. 3).

Por sua vez, na avaliação de impacto regulatório que culminou na aprovação da NIS 2, optou-se por uma nova regulação sistêmica, com o descarte de ideias como manutenção do *status quo*, mudanças não-legislativas e reforma parcial da NIS 1.

Igualmente, entendeu-se que o escopo da NIS 1 já se encontrava desatualizado em virtude da maior digitalização e interconectividade dos serviços, não refletindo mais todos os setores digitalizados que prestam serviços essenciais à economia e à sociedade como um todo (EP, 2023, p. 6). Destacou-se, ainda, que os países-membros não têm sistematicamente compartilhado informações entre si e que o monitoramento e o *enforcement* da NIS 1 vinham se revelando ineficientes (EP, 2023, p. 6-7).

Dentre as principais mudanças trazidas pela NIS 2, destacam-se (EP, 2023, p. 7-8):

1. estabelecimento de regras que garantam que todas as entidades públicas e privadas no mercado interno que desempenhem funções importantes para a economia e a sociedade como um todo sejam obrigados a tomar medidas adequadas de cibersegurança (art. 2º). Essa providência é adotada com o fim de aumentar o nível de resiliência cibernética de um conjunto mais abrangente de empresas;

2. ampliação significativa do escopo regulatório, com acréscimo de novos setores, como telecomunicações, plataformas de redes sociais e a administração pública (art. 2º);

3. previsão de que todas as entidades de médio e grande porte ativas nos setores abrangidos pelo *framework* da NIS 2 terão de cumprir as regras de segurança apresentadas na proposta (art. 2º);

4. eliminação da possibilidade de os Estados-Membros adaptarem os requisitos em certos casos, vez que isso levou a uma grande fragmentação na implementação da NIS 1 (art. 5º);

5. eliminação da distinção feita entre operadores de serviços essenciais e provedores de serviços digitais, que atualmente se enquadram em três categorias: plataformas de comércio *online*, motores de busca e prestadores de serviços em nuvem, tendo a nova regulação trabalhado apenas com entidades "essenciais e importantes" (art. 3º);

6. independentemente do porte, aplicação da Diretiva para prestadores de serviços de comunicação eletrônica ou prestadores de redes de comunicações eletrônicas. No entanto, as empresas que não se qualifiquem como empresas de tamanho médio ou superior recaem na categoria de serviços importantes, não essenciais. Dessa forma, aplica-se o regime de controle leve, somente *ex post*, a fim de atingir um equilíbrio entre as obrigações sobre essas entidades e sobre as autoridades competentes, nos termos do considerando 122 do preâmbulo da NIS 2;

7. abordagem, pela primeira vez, da cibersegurança da cadeia de suprimentos das TIC, de especial importância para a Internet das Coisas (art. 7º, 2., "a");

8. redução das inconsistências em termos de resiliência em todo o mercado interno nos setores já abrangidos pela NIS, através de um maior alinhamento com i) o âmbito da incidência efetiva da diretiva; ii) os requisitos de segurança e de comunicação de incidentes; iii) as disposições que regem a supervisão e aplicação nacionais; e iv) as capacidades das autoridades competentes relevantes dos Estados-Membros (arts. 7º e ss.);

9. inclusão de uma lista de elementos-chave que todas as empresas devem abordar ou implementar como parte das medidas que tomam, incluindo resposta a incidentes, segurança da cadeia de suprimentos, encriptação e divulgação de vulnerabilidades (art. 21);

10. abordagem, em duas fases, para a comunicação de incidentes. As empresas afetadas têm 24 horas, contados a partir do momento em que tomam conhecimento de um incidente, para apresentar um relatório inicial, seguido de um relatório final, mais extenso, no máximo um mês depois (art. 23);

11. no que diz respeito ao *enforcement*, fixação de uma lista mínima de sanções administrativas sempre que houver descumprimento das regras relativas à gestão de riscos de cibersegurança ou das suas obrigações de comunicação estabelecidas na Diretiva NIS. Tais sanções incluem instruções vinculativas, ordem para implementar as recomendações de uma auditoria de segurança, ordem para alinhar as medidas de segurança com os requisitos NIS e multas administrativas, de até 10 milhões de euros ou 2% do faturamento bruto das entidades em nível mundial, o que for maior (art. 34);

12. incremento do nível de conhecimento situacional conjunto e da capacidade coletiva de preparação e resposta, i) tomando medidas para aumentar o nível de confiança entre as autoridades competentes; ii) compartilhando mais informações; e iii) estabelecendo regras e procedimentos em caso de incidente ou crise de grande escala. Espera-se que as novas regras melhorem a forma como a UE previne, trata e responde a incidentes e crises de cibersegurança em grande escala, introduzindo responsabilidades claras, um planejamento adequado e uma maior cooperação da UE (art. 7º);

13. obrigação de os Estados-Membros adotarem uma estratégia nacional de cibersegurança, designarem equipes nacionais de resposta a incidentes de segurança (CSIRT), responsáveis pelo tratamento de riscos e incidentes, uma autoridade nacional competente em matéria de cibersegurança e um ponto único de contato (SPOC). O SPOC deve exercer a função de entidade de ligação para assegurar a cooperação transfronteiriça entre as autoridades dos Estados-Membros com as autoridades relevantes de outros Estados-Membros e, se for caso disso, com a Comissão e com a ENISA, (art. 7º) e deve assegurar a cooperação intersetorial com outras autoridades competentes em seu Estado-Membro (EC, 2023);

14. continuidade ao Grupo de Cooperação NIS para apoiar e facilitar a cooperação estratégica e o intercâmbio de informações entre os Estados-Membros e a Rede CSIRT, que promove uma cooperação operacional rápida e eficaz entre CSIRT nacionais (arts. 11 a 14).

Por sua vez, com a migração cada vez mais intensa das redes para modelos em nuvem que operem em *cloud computing* e *edge computing* - o qual deverá integrar praticamente as rotinas de qualquer empreendimento digital na Europa até o ano de 2025 (EC, 2023a, p. 13) - e, ainda, *em fog computing*, a ENISA desenvolveu estudo em que identificou alguns desafios para a cibersegurança em computação em nuvem, que envolvem aspectos tais como: controle de acesso, *accountability* (especialmente em ambientes *multicloud*), *compliance* (com atenção à necessidade de uma mesma organização atender a diversos regramentos quando operar internacionalmente), confidencialidade (devendo ser adotadas medidas para que se evite a extrusão de dados), resposta a incidentes de cibersegurança e integridade dos dados, dentre outros (ENISA, 2023, p. 22-23).

Dentre os riscos apontados, foram identificados os seguintes: *data breaches*, abuso de configurações equivocadas e controle inadequado de mudanças nos equipamentos de T.I., ausência de estratégia e de arquitetura de segurança em nuvem, administração insuficiente de credenciais de acesso, sequestro de contas,

ameaças internas, emprego abusivo de interfaces de API inseguras, dentre outros (ENISA, 2023, p. 23-24).

Igualmente, a Comissão Europeia reiterou a sua preocupação com cabos submarinos em virtude de diversos incidentes de conotações geopolíticas que evidenciaram o potencial de comprometimento dessas infraestruturas críticas, especialmente a partir do conflito Rússia-Ucrânia (EC, 2024, p. 21). Ademais, há preocupações envolvendo maior disponibilização de conectividade 5G, cobertura de acesso de um Gigabyte por segundo para todos, ampliação da produção de semicondutores que empreguem tecnologia de ponta para 20% e o emprego do primeiro computador quântico até 2025.

A Europa enfrenta desafios relacionados ao desenvolvimento de *hardware* proprietário e não dependente de capital humano, carecendo de um número de profissionais que varia entre 260.000 e 500.000, principalmente nas pequenas e nas médias empresas (EC, 2023a, p. 19), e demandando insumos presentes em países alheios à União. Além disso, há preocupações relativas às criptografias legadas que possam ser quebradas com a computação quântica e ao cumprimento de metas associadas à neutralização de carbono no setor.

Ainda no tema cibersegurança, é importante mencionar dois projetos.

O primeiro é o projeto *Cyber Resilience Act* (CRA), que procura estabelecer, no mercado europeu, obrigações e requisitos de segurança de produtos de *hardware* e *software* desde a concepção, compreendendo o seu desenvolvimento, manutenção e fim de ciclo de uso (EC, 2024, p. 21), com o potencial de ser um divisor de águas nos esforços da Comissão Europeia no combate aos ataques envolvendo a cadeia de suprimentos de produtos digitais (EC, 2023a, p. 18).

O segundo é o projeto *Cyber Solidarity Act*, que visa aprimora as práticas para detecção, preparação e resposta a ameaças cibernéticas (EC, 2023a, p. 19).

No que diz respeito à sustentabilidade do setor, a Comissão Europeia constatou que o setor de tecnologias da informação e comunicação representa: a) entre 7 e 9% do

consumo global de eletricidade, estimando-se sua elevação para 13% até 2030; b) cerca de 3% das emissões globais de gases com efeito de estufa; e c) quantidades crescentes de lixo eletrônico. Por outro lado, com o adequado tratamento, é possível que a tecnologia digital contribua para reduzir as emissões globais em 15% (EC, 2024, p. 34).

O cenário português

Em Portugal, observa-se uma estreita relação entre o Regulador de Telecomunicações, a Autoridade Nacional de Comunicações (ANACOM), e o órgão responsável pela Cibersegurança no país, o Centro Nacional de Cibersegurança (CNCS), especialmente no que diz respeito à segurança cibernética no setor de Telecomunicações.

O CNCS foi instituído pela Resolução do Conselho de Ministros nº 42/2012, de 13 de abril de 2012 (PORTUGAL, 2012). O CNCS tem sua atual configuração atualizada pelo Decreto-Lei nº 136/2017, de 6 de novembro de 2017, e desenvolve a sua missão com o objetivo de contribuir para uma utilização livre, confiável e segura do ciberespaço de interesse nacional com foco na segurança das interações entre pessoas, processos e tecnologias, desenvolvendo um conjunto de atividades dirigidas aos cidadãos e organizações.

O CNCS atua como coordenador operacional e Autoridade Nacional em matéria de cibersegurança, trabalhando em conjunto com entidades do Estado, operadores de infraestruturas críticas nacionais, operadores de serviços essenciais e prestadores de serviços digitais. Além disso, estende sua atuação para a sociedade em geral.

A ANACOM, por sua vez, enquanto órgão regulador dos setores postal e de comunicações eletrônicas, é dirigida pelo Conselho de Administração (CA), responsável por definir e acompanhar a estratégia da Autoridade, garantindo a direção dos serviços (PORTUGAL, 2024).

Vinculado diretamente ao Conselho de Administração da ANACOM, encontra-se o responsável por segurança, cuja missão é assegurar o cumprimento das obrigações da ANACOM relacionadas ao Regime Jurídico da Segurança do Ciberespaço. Esse responsável deve articular as matérias relativas à cibersegurança e à segurança das redes e serviços de comunicações eletrônicas, incluindo a segurança física, com as demais Unidades Orgânicas da ANACOM. A ANACOM é membro e participante ativa da Estratégia Nacional de Cibersegurança em Portugal.

Portugal estabeleceu seu Regime Jurídico da Segurança do Ciberespaço por meio da Lei n.º 46/2018, de 13 de agosto de 2018 (PORTUGAL, 2018), a qual transpôs a Diretiva (UE) 2016/1148 (NIS 1).

A Aplicação do Regime Jurídico da Segurança do Ciberespaço em Portugal foi, posteriormente, regulamentada pelo Decreto-Lei 65/2021, de 30 de julho de 2021 (PORTUGAL, 2021), no qual se prevê, entre os principais objetivos, a adoção de uma estratégia nacional de segurança de redes e dos sistemas de informação e a criação de uma rede de equipes de resposta a incidentes de segurança (CERT.PT).

Iniciativas portuguesas de destaque

Do Centro Nacional de Cibersegurança (CNCS):

1. Sensibilização e treinamento para promover comportamentos seguros e responsáveis no uso da tecnologia e do ciberespaço, incluindo formação especializada em cibersegurança;

2. Produção e disseminação de alertas, orientações e boas práticas para o uso (mais) seguro da tecnologia por parte dos cidadãos e das organizações, assim como de recomendações técnicas e produção de normativos e referenciais dirigidos em particular às organizações;

3. Oferta de capacitação formativa em alto nível para os desafios em cibersegurança;

4. Produção de conhecimento sobre o estado da cibersegurança nacional nas suas diversas vertentes, incluindo a definição do nível nacional de alerta de cibersegurança;

5. Publicação, em 2022, do Guia para Gestão dos Riscos em matérias de Segurança da Informação e Cibersegurança (PORTUGAL, 2022).

Da Autoridade Nacional de Comunicações (ANACOM):

1. Publicação do Regulamento nº 303/2019 da Autoridade, relativo à segurança e à integridade das redes e serviços de comunicações eletrônicas (PORTUGAL, 2019);

2. CSIRT – ANACOM - que tem como objetivos, entre outros, articular os trabalhos e atividades, no âmbito da Equipe de Resposta a Incidentes de Segurança, com o CNCS e com as principais partes interessadas dos setores regulados pela ANACOM e apoiar a Comissão de Planeamento Civil de Emergência das Comunicações na elaboração de planos, proposta de legislação e assessorar essa comissão em estudos e informações que venham a ser necessários no âmbito da sua atuação;

3. Participação em exercícios de cibersegurança como o Cyber Europe (ENISA, 2024) e o Exercício Nacional de Cibersegurança; e

4. Instituição de Grupo de trabalho CNCS–ANACOM para os trabalhos de desenvolvimento do esquema europeu de certificação de cibersegurança em matérias de segurança das redes 5G como parte do quadro nacional de Certificação de Cibersegurança.

3

Benchmark: Reino Unido (UK)

O principal marco regulatório de cibersegurança do Reino Unido é a Diretiva NIS 1, em que essa legislação foi recepcionada como legado do arcabouço legislativo incorporado ao país durante o período em que fez parte da União Europeia.

No entanto, como a sua saída da UE se deu antes da aprovação da Diretiva NIS 2, essa última não será aplicável.

A política de cibersegurança do Reino Unido envolve diversos ramos do governo com linhas de responsabilidade relativamente claras, dentre as quais citam-se (CLARK, 2024, p. 26-28):

1. o *Cabinet Office*, que é o proprietário e "supervisor" da política;
2. o *Department for Science, Innovation and Technology* (DSIT), responsável pela implantação da Diretiva NIS no Reino Unido;
3. o *Home Office*, responsável pela política em cibercrime;

4. o Ministério da Defesa (*Ministry of Defence*), a quem compete liderar o trabalho de detectar, interromper e dissuadir adversários que operam no ciberespaço, incluindo terroristas, grandes grupos criminosos cibernéticos e atores estatais, além de supervisionar a Força Cibernética Nacional;

5. o *Foreign, Commonwealth and Development Office* (FCDO), o qual é responsável pelas atividades internacionais de segurança cibernética do Reino Unido e supervisiona o Centro Nacional de Segurança Cibernética e, juntamente com o Ministério da Defesa, a Força Cibernética Nacional;

6. o *National Cyber Security Centre*, o qual é, nos termos da NIS e dos demais regulamentos britânicos: a) ponto de contato único com parceiros nacionais e internacionais; b) autoridade técnica, responsável por fornecer aconselhamento técnico especializado às autoridades competentes e outras organizações, não tendo, todavia, poderes para regulação direta; e c) Equipe de Resposta a Incidentes de Segurança Informática (CSIRT), responsável por monitorar e relatar incidentes cibernéticos, realizar avaliações de ameaças e fornecer alertas antecipados sobre ameaças cibernéticas; e

7. o *Information Commissioner's Office* - autoridade britânica de proteção de dados.

O país não dispõe de um regulador único de cibersegurança, cabendo aos reguladores setoriais promoverem essa articulação com o setor privado, incluindo os fornecedores de infraestruturas críticas. Assim, no setor de telecomunicações, essa regulação é feita pelo Office of Communications – Ofcom (CLARK, 2024, p. 26-28), e, no setor financeiro, pelo Financial Conduct Authority (FCA) e pelo Bank of England's Prudential Regulation Authority (CLARK, 2024, p. 26).

A atual Estratégia Britânica de Cibersegurança (The National Cyber Strategy 2022, ou NCS 2022), por sua vez, é construída em cima de cinco pilares, a saber (CLARK, 2024, p. 46):

1. fortalecer o ecossistema cibernético do Reino Unido, em que o governo deve exercer um papel de facilitador entre os diversos *stakeholders* (líderes da indústria, acadêmicos, inovadores, autoridades de *enforcement*, comunidade de segurança nacional *etc.*);

2. construir um Reino Unido digital robusto e próspero, por meio do qual se procura aumentar a resiliência cibernética em toda a sociedade, a partir de três premissas: a) compreender a natureza do risco cibernético b) proteger sistemas contra ataques cibernéticos, e c) garantir que os sistemas sejam capazes de minimizar o impacto de ataques cibernéticos bem-sucedidos e de se recuperar rapidamente deles;

3. assumir a liderança nas tecnologias vitais para o poder cibernético, tais como 5G, IA, *blockchain*, semicondutores, criptografia, dispositivos de Internet das Coisas, tecnologias quânticas, de forma a participar relevantemente na moldagem do consenso global relacionado a essas tecnologias, tidas como essenciais para cibersegurança;

4. promover a liderança e influência do Reino Unido numa escala global, para defender um ciberespaço livre, aberto, pacífico e seguro, evitando a disseminação de perspectivas autoritárias para o ciberespaço, por meio da articulação com organizações multilaterais e com o reforço de parcerias principalmente na África e no Indo-Pacífico; e

5. detectar, interromper e dissuadir adversários, por meio do aperfeiçoamento de capacidade cibernética de o Reino Unido ativamente identificar, perturbar e dissuadir adversários no ciberespaço, com uma atuação articulada dos diversos entes encarregados dessas atribuições e com o objetivo de aumentar os custos e riscos da realização de ataques cibernéticos.

Pode-se perceber que a atuação das autoridades no setor de cibersegurança tem se concentrado mais em orientar o setor privado no desenvolvimento de suas capacidades em cibersegurança, em vez de adotar uma abordagem mais incisiva, normalmente associada às políticas de comando-e-controle, especialmente quando comparada com o cenário institucional da União Europeia.

A NCSC, por sua vez, desenvolveu, alguns programas para promover as capacidades de cibersegurança das mais diversas organizações britânicas (CLARK, 2024, p. 34-35):

1. *Cyber Aware* - consiste em campanha de informação direcionada ao público em geral e a pequenas empresas sobre a relevância das ameaças cibernéticas e sobre como se protegerem. O NCSC disponibiliza uma ferramenta *online* em que pessoas e empresas podem verificar o quanto estão seguras;

2. *Cyber Essentials* – estabelece cinco controles básicos que organizações de todos os tamanhos podem adotar para fortalecer suas defesas contra ataques cibernéticos comuns: *firewalls*; configurações seguras; proteção contra *malware*; controle de acesso de usuários; e gerenciamento de atualizações de segurança. Com o *Cyber Essentials Plus*, as organizações podem ter um auditor para avaliar, de forma independente, se atendem aos padrões esperados;

3. 10 *Steps to Cyber Security* – coleção de orientações destinadas principalmente a organizações de médio a grande porte, em que se aponta como elas podem gerir os riscos cibernéticos, compreendê-los, implementar as medidas de mitigação adequadas e se preparar para incidentes cibernéticos;

4. *Cyber Assessment Framework* – que consiste numa coleção de orientações detalhadas, destinadas a prestadores de serviços essenciais, fornecendo uma abordagem sistemática e abrangente para avaliar até que ponto os riscos cibernéticos para funções essenciais se encontram devidamente gerenciados pela organização responsável;

5. *Active Cyber Defence* – um conjunto de ferramentas e serviços projetados para ajudar as organizações a se defenderem proativamente contra ataques cibernéticos comuns e não direcionados. Exemplificativamente, disponibiliza a ferramenta "*Exercise in a Box*", que fornece recursos que permitem a não especialistas testar a resposta da sua organização a um ataque cibernético.

No que diz respeito aos *data centers*, há uma percepção de que se deve evoluir no tema, pois são considerados infraestruturas críticas, consistindo num alvo atrativo para vários agentes hostis propensos a causar eventos que podem ser cruciais para a economia, para o setor público e para as rotinas diárias (DSIT, 2023, p. 10), em que muitos desses agentes estão localizados fora da jurisdição britânica.

O emprego dos *data centers* dos operadores de rede no setor de telecomunicações encontra-se no escopo regulatório do Telecommunications (Security) Act (TSA), de 2003, cujo *enforcement*, conforme já adiantado, compete ao Office of Communications (Ofcom) quando qualquer infraestrutura fornecida por fornecedores públicos de comunicações eletrônicas se ligue a *data centers* ou se encontre dentro deles (DSIT, 2023, p. 33).

Além disso, o Ofcom tem o papel de servir como autoridade designada para o *oversight* das infraestruturas digitais no que diz respeito ao *enforcement* da Diretiva NIS 1 (OFCOM, 2023).

O TSA, por sua vez, foi alterado pelo Telecommunications (Security) Act de 2021, por meio do qual se atribuíram ao Ofcom novas competências e poderes, incluindo a supervisão dos fornecedores de "alto risco", ou *high risk vendors*, desde que haja alguma diretiva emitida pelo Secretário de Estado que atribua algum poder de fiscalização ao Ofcom sobre os fornecedores (OFCOM, 2023).

O Ofcom tem a incumbência de assegurar que os prestadores adotem as medidas necessárias para incrementar os níveis de segurança e de capacidade de resiliência em suas redes e serviços contra eventos que possam comprometer sua integridade, incluindo aqueles relacionados a ataques cibernéticos (OFCOM, 2023).

Dentre essas medidas, compreendem-se aquelas de mitigação de riscos, de preparação para eventos, de resposta a incidentes e de recuperação da higidez das redes e serviços, sendo possível que as prestadoras sejam sancionadas em caso de descumprimento desses mandamentos, com multas e com imposição de medidas coercitivas (OFCOM, 2023).

O papel do Ofcom (regulador de telecomunicações britânico)

O emprego dos *data centers* dos operadores de rede no setor de telecomunicações encontra-se no escopo regulatório do Telecommunications (Security) Act (TSA), de 2003, cujo *enforcement*, conforme já adiantado, compete ao *Office of Communications* (Ofcom) quando qualquer infraestrutura fornecida por fornecedores públicos de comunicações eletrônicas se ligue a *data centers* ou se encontre dentro deles (DSIT, 2023, p. 33). Além disso, o Ofcom tem o papel de servir como autoridade designada para o *oversight* das infraestruturas digitais no que diz respeito ao *enforcement* da Diretiva NIS 1 (OFCOM, 2023).

O TSA, por sua vez, foi alterado pelo *Telecommunications (Security) Act* de 2021, por meio do qual se atribuíram ao Ofcom novas competências e poderes, incluindo a supervisão dos fornecedores de "alto risco", ou *high risk vendors*, desde que haja alguma diretiva emitida pelo Secretário de Estado aos fornecedores, conferindo alguma incumbência ao Ofcom nesse contexto (OFCOM, 2023).

Apesar de seu poder sancionador, o Ofcom visa empregar uma colaboração estreita com os diversos fornecedores nos serviços de telecomunicações para incrementar as suas capacidades em cibersegurança e, concomitantemente, estimular o cumprimento do TSA, com as alterações trazidas em 2021. Para essa finalidade, o Ofcom exige que as prestadoras façam o *disclosure* de algumas informações que considera importantes para o sucesso de suas políticas públicas voltadas à segurança e à integridade nos serviços de telecomunicações (OFCOM, 2023).

O Ofcom tem a incumbência de assegurar que os prestadores adotem as medidas necessárias para incrementar os níveis de segurança e de capacidade de resiliência em suas redes e serviços contra eventos que possam comprometer sua integridade, incluindo aqueles relacionados a ataques cibernéticos (OFCOM, 2023).

Dentre essas medidas, compreendem-se aquelas de mitigação de riscos, de preparação para eventos, de resposta a incidentes e de recuperação da higidez das redes e serviços, sendo possível que as prestadoras sejam sancionadas em caso de descumprimento desses mandamentos, com multas e imposição de medidas coercitivas (OFCOM, 2023).

Além disso, o Ofcom, em parceria com o *Department for Digital, Culture, Media & Sport* (DCMS) costuma realizar constantemente testes de penetração (chamados de testes TBEST) a partir do mapeamento das ameaças às organizações e da simulação de cenários de ameaças realistas (OFCOM, 2023).

Ainda, o Ofcom recomenda a assimilação das *guidelines* para provedores de infraestruturas críticas editada pelo *Electronic Communications Resilience and Response Group* (EC-RRG), um grupo de trabalho que envolve agentes dos setores público, incluindo o próprio Ofcom, e privado, cujo escopo é servir de ponto focal para a cooperação em matéria de resiliência no setor de telecomunicações (EC-RRG, 2018).

No que diz respeito ao cenário associado à NIS 1, conforme visto acima, o Ofcom é designado como autoridade para a infraestrutura digital, tendo competência para avaliar os seguintes serviços: Registros de nomes de domínio de nível superior (TLD); "*Resolver services*" de sistema de nomes de domínio (DNS); Serviço de hospedagem oficial de DNS; e Ponto de Troca de Internet (IXP).

Para promover a conformidade dos diversos provedores nos serviços de telecomunicações e nos serviços de infraestrutura digitais associados à NIS, o Ofcom editou diversos manuais (OFCOM, 2022; OFCOM, 2023a).

Mais recentemente, no ano de 2023, o DSIT encerrou um processo de tomada de subsídios e publicou o relatório para avaliação de regulamentação de *data centers* operados por terceiros, especialmente os de colocação e de co-hospedagem (DSIT, 2023, p. 11), embora ainda não haja consenso se *data centers* devam ser considerados formalmente como *Critical National Infrastructure* (CNI), isto é, infraestrutura crítica nacional.

O objetivo da referida tomada de subsídios é conceber um *framework* institucional para a criação de um arcabouço normativo para mitigar riscos e aumentar a resiliência de dados armazenados no Reino Unido, com um foco especial, mas não limitado a, em *data centers* operados por terceiros. Esses *data centers* não são diretamente regulados em aspectos de segurança e resiliência no Reino Unido,

encontrando-se fora de sua jurisdição em temas como administração de riscos, segurança física, cibersegurança das instalações, gestão de incidentes e melhorias na segurança da infraestrutura britânica (DSIT, 2023, p. 11, 12 e 16).

Acrescenta-se que, no que diz respeito aos *data centers*, o aumento da demanda por aplicações de inteligência artificial e de grandes modelos de linguagem são exemplos de fatores que vêm deflagrando recentemente mudanças na configuração do mercado a eles associados, cujos provedores estão oferecendo densidades mais altas de *rack* para atender às demandas de maior poder computacional.

Com isso, a sustentabilidade ambiental e o consumo de energia dos *data centers* continuam a ser críticos para fornecer operações confiáveis e, ao mesmo tempo, equilibrar a eficiência para minimizar o impacto e os custos ambientais (DSIT, 2023, p. 28-29).

Quanto ao ponto, o DSIT manifesta preocupações relacionadas à logística reversa de fim de ciclos de investimento e à pegada ambiental que a ampliação do uso de *data centers* pode gerar, principalmente quanto à emissão de gases de efeito estufa (DSIT, 2023, p. 67). O DSIT estima que existam entre 250 (duzentos e cinquenta) e 400 (quatrocentos) *data centers* de colocação operando atualmente no Reino Unido, representando cerca de 1,5 GW de consumo de eletricidade em aproximadamente meio milhão de metros quadrados de área útil (DSIT, 2023, p. 67).

> Por *data center*, deve-se compreender uma estrutura, ou grupo de estruturas, dedicada à hospedagem centralizada, à interligação e à operação de equipamentos de tecnologia da informação e de redes de telecomunicações, fornecendo serviços de armazenamento, processamento e transporte de dados, juntamente com todas as instalações e infraestruturas para distribuição de energia e controle ambiental e de resiliência e segurança necessárias (DSIT, 2023, p. 32, tradução livre).

Para o arcabouço regulatório, espera-se o tratamento dos seguintes temas: 01) estabelecimento de supervisão regulatória apropriada e serviços de *data centers* dentro do seu escopo; 02) fixação de uma base mínima de medidas de mitigação de

riscos de segurança e resiliência; 03) garantia de detecção e gerenciamento de incidentes e, quando forem significativos a partir de um certo gatilho, de que sejam reportados, sem prejuízo da avaliação do nível de *disclosure* adequado em situações que acarretem impacto significativo na economia, nos serviços essenciais ou nas infraestruturas nacionais críticas, que envolvam dados em massa ou sensíveis (dados não pessoais fora do escopo do GDPR), segurança pública, ou segurança nacional (DSIT, 2023, p. 25); 03) assegurar que o governo e os reguladores tenham as informações, a capacidade e os instrumentos para abordar os riscos locais e sistêmicos para a infraestrutura de dados atuais e emergentes, e que os clientes tenham percepção suficiente dos riscos e das medidas de mitigação necessárias, quando apropriado (DSIT, 2023, p. 57).

Dentre os diversos riscos à integridade do ecossistema digital que deverão ser tratados no arcabouço, citam-se: vulnerabilidades de *hardware*, vulnerabilidades de *software*, ataques físicos, ameaças de *insiders*, erros humanos, problemas na cadeia de suprimentos, desastres naturais – tais como incêndios, inundações e temperaturas extremas – concentração geográfica da infraestrutura, dos operadores ou do mercado, disrupções econômicas que possam resultar na insolvência de operadores de infraestruturas de dados, ampliação das superfícies de ataque em decorrência do uso mais intensivo de *edge computing etc*. No que diz respeito ao *edge computing*, é possível que se amplie o escopo de regulados, pois há uma percepção no sentido de mesmo pequenos *data centers* poderem ser vistos como um risco a ser considerado enquanto elemento de uma rede de comunicações mais abrangente.

O DSIT e outros entes governamentais intentam empregar uma linha mestra que envolva uma atuação dialogada com atores de segmentos relevantes da indústria, com a finalidade de explorar a construção de soluções coletivas e voluntárias e, ao mesmo tempo, o desenvolvimento de um arcabouço regulatório que assegure um nível mínimo de resiliência e segurança para o setor e que considere as dinâmicas de mercado e dos modelos de negócio a ele relacionados. Essa aproximação

dialogada está em sintonia com a *Resilience Framework* 2022, que prega uma abordagem de infraestruturas críticas e serviços essenciais baseada em *standards* amplamente reconhecidos pela comunidade em geral nos níveis interno e internacional, notadamente os institutos de padronização, indústria, *experts* e reguladores (DSIT, 2023, p. 48).

Igualmente, entende-se que a natureza das ameaças à segurança e à resiliência não torna viável uma prevenção de riscos ampla e completa, sendo necessária a promoção cuidadosa do equilíbrio dos custos de oportunidade entre segurança e resiliência, de um lado, e investimento e inovação, de outro, sem prejuízo da avaliação dos custos das intervenções ao pagador de impostos (DSIT, 2023, p. 19). Outra preocupação diz respeito à promoção de boas práticas, da transparência e da interoperabilidade entre os *frameworks* no Reino Unido e no exterior, com a finalidade, neste último caso, de minimizar os custos transfronteiriços de operação (DSIT, 2023, p. 48).

No que diz respeito a quem deve ser o regulador para promover as intervenções relacionadas à promoção da cibersegurança, o DSIT propõe atribuir essas funções a um ente que supervisione os requisitos mínimos de segurança e resiliência, que poderiam ser ampliados voluntariamente pelos regulados ou, ainda, heterarquicamente, caso se entenda que a indústria não esteja conseguindo mitigar riscos adequadamente mesmo quando cumprisse esses requisitos mínimos (DSIT, 2023, p. 19-20).

Por sua vez, os ramos seguintes estariam fora do escopo desse arcabouço: 01) redes e serviços de comunicações públicas, que continuariam regidos pelo *Telecommunications (Security) Act* (TSA); 02) a infraestrutura digital, que continuaria sob a égide da Diretiva NIS; 03) cabos submarinos, que, embora venham eventualmente a se conectar com *data centers*, fazem parte de uma política governamental específica que compreende a melhoria da segurança, resiliência e cobertura regulatória da infraestrutura da Internet, incluindo locais de aterrissagem de cabos, de forma a minimizar interrupções, encontrando-se em monitoramento e

revisão contínuos; e 04) o armazenamento e processamento de dados empresariais, quando operado dentro de sua estrutura e com a finalidade de fornecimento e gerenciamento de serviços utilizados pela própria empresa, sem que haja prestação de serviços a terceiros, e sem prejuízo da incidência de regulamentos setoriais específicos (DSIT, 2023, p. 33).

Os seguintes serviços igualmente deverão ficar de fora do arcabouço, mas ressalva-se que a perspectiva de abordagem pelo Governo Britânico será influenciada pelo *feedback* obtido na tomada de subsídios: 01) os serviços de *cloud computing*, os quais, atendidos determinados requisitos, são regulamentos pela Diretiva NIS, sendo considerados *Relevant Digital Service Providers* (RDSP) e; 02) serviços gerenciados (*managed services*), em que se propõe que, quando portarem determinadas características, sejam regulamentados pela Diretiva NIS como um RDSP (DSIT, 2023, p. 34).

Pode ser percebido que o Reino Unido vem promovendo uma abordagem junto ao setor regulado que envolve mais o diálogo do que a imposição verticalizada de medidas de comando-e-controle.

Embora a tomada de subsídios realizada no ano de 2023 contemple a possibilidade de um regulador com poderes sancionatórios no que diz respeito a *data centers*, entende-se que o diálogo voltado a uma construção conjunta dos padrões mínimos de cibersegurança com o setor privado deve ser a premissa fundamental.

Por sua vez, não pode ser esquecido que a Diretiva NIS 1 continuará em vigência no Reino Unido mesmo após o início da Diretiva NIS 2 na União Europeia, com possibilidade de multas de até 17 (dezessete) milhões de libras tanto para os provedores de serviços essenciais quanto para os provedores de serviços digitais relevantes. Neste último caso, as multas são aplicadas pelo ICO (*Information Commissioner's Office*), que é equivalente à Autoridade Nacional de Proteção de Dados brasileira.

Ainda no que diz respeito ao tema, o Reino Unido considera avaliar a adoção de novas ações em seu arcabouço regulatório para incrementar a cibersegurança, tais como (CLARK, 2024, p. 52):

01) Reforma do *Computer Misuse Act* 1990, para estimular o *ethical hacking*, ou *hacking* "do bem", que tem o potencial de ser útil para um ambiente digital mais seguro, embora o regramento atual possa desestimular profissionais a identificar vulnerabilidades sob o receio de terem os seus comportamentos avaliados como ilegais. Por outro lado, há o risco de que eventual flexibilização na legislação estimule o emprego de técnicas mais perigosas por profissionais sem os conhecimentos necessários;

02) possível proibição de pagamentos de resgastes em eventos que envolvam *ransomware*, ante a premissa de que o pagamento de resgates poderia sinalizar um estímulo a ações dessa natureza;

03) ampliação do rol de sujeitos obrigados a notificar incidentes de segurança, considerando que, atualmente, apenas entidades sujeitas à NIS estão obrigadas a fazê-lo;

04) ampliação do escopo da NIS para compreender MSPs, outras infraestruturas críticas e entidades das quais os provedores de serviços essenciais sujeitos à NIS dependem para fornecer suas atividades;

05) estabelecimento de deveres de ciberproteção por fabricantes de produtos e provedores de serviços, com a promoção de ações de *security by default*, sem que esse "fardo" recaia sobre os próprios consumidores; e

06) incremento da governança e *accountability* para estimular práticas de divulgação, tanto internamente como externamente, de incidentes de segurança que ocorram nas empresas, em que, em 2021, apenas 37% delas divulgaram publicamente os incidentes de segurança que ali desenvolveram.

4

Benchmark: Estados Unidos (EUA)

No cenário institucional norte-americano, existe uma diversa e ampla gama de agências com competências diferentes e complementares em segurança cibernética, destacando-se, para fins do presente trabalho, três instituições.

A primeira delas é o *National Institute of Standards and Technology* (NIST), cujo principal papel, na área de cibersegurança, é desenvolver padrões, diretrizes, melhores práticas e outros recursos de segurança cibernética para atender às necessidades da indústria dos EUA, das agências federais e do público em geral. O NIST ainda desenvolve estudos e relatórios para fortalecer as práticas e rotinas de cibersegurança das diversas entidades, públicas ou privadas, além de pesquisas de longo prazo de cunho mais estratégico para antecipar os impactos futuros de novas tecnologias.

A segunda entidade é o *Cibersecurity and Infrastructure Agency* (CISA) - Agência de Segurança Cibernética e de Infraestrutura – com a missão de liderar o esforço nacional para compreender, gerenciar e reduzir o risco à infraestrutura física e cibernética dos Estados Unidos.

A terceira é a *Federal Communications Commission* (FCC), sobre a qual será falada em tópico específico.

Um dos marcos mais relevantes para a promoção da cibersegurança nos Estudos Unidos é o *Cibersecurity Framework* (CSF), que tem como foco uma audiência ampla, independentemente de seu conhecimento e do nível de maturidade de seus programas de cibersegurança, não se direcionando exclusivamente às infraestruturas críticas. O CSF busca possuir uma perspectiva de neutralidade quanto a setor, país ou tecnologia, sem uma abordagem "*one-size-fits-all*".

Embora o CSF tenha sido produzido pelo NIST, tanto ele quanto o CISA emitiram *guidances* para a sua implantação (CISA, 2020; NIST, 2024). Todavia, tendo em vista que o NIST emitiu novo *guidance* em 2024, que se encontra em sua versão 2.0, será utilizado tal documento como referência para a abordagem do arcabouço norte-americano.

Os riscos que o CSF visa endereçar são relacionados aos seguintes setores: finanças, privacidade, cadeia de suprimentos, reputação, tecnologia e de natureza física.

O CSF 2.0 apresenta funções-núcleo, que se constituem nos objetivos que a organização deve atingir na adoção de medidas de promoção de cibersegurança, a saber: governar, identificar, proteger, detectar, responder e recuperar-se (*govern, identify, protect, detect, respond, and recover*). A partir daí, cada organização passa a desenhar o leque de ações que entende necessárias para o atingimento desses objetivos. Interessante notar que uma das grandes inovações do CSF 2.0 foi justamente a inclusão da função de governança, antes inexistente.

A sua matriz é assim representada (NIST, 2024, p. 3), em que, a partir da função, detalham-se as categorias e subcategorias de ações associadas a cada uma das funções-núcleo referidas:

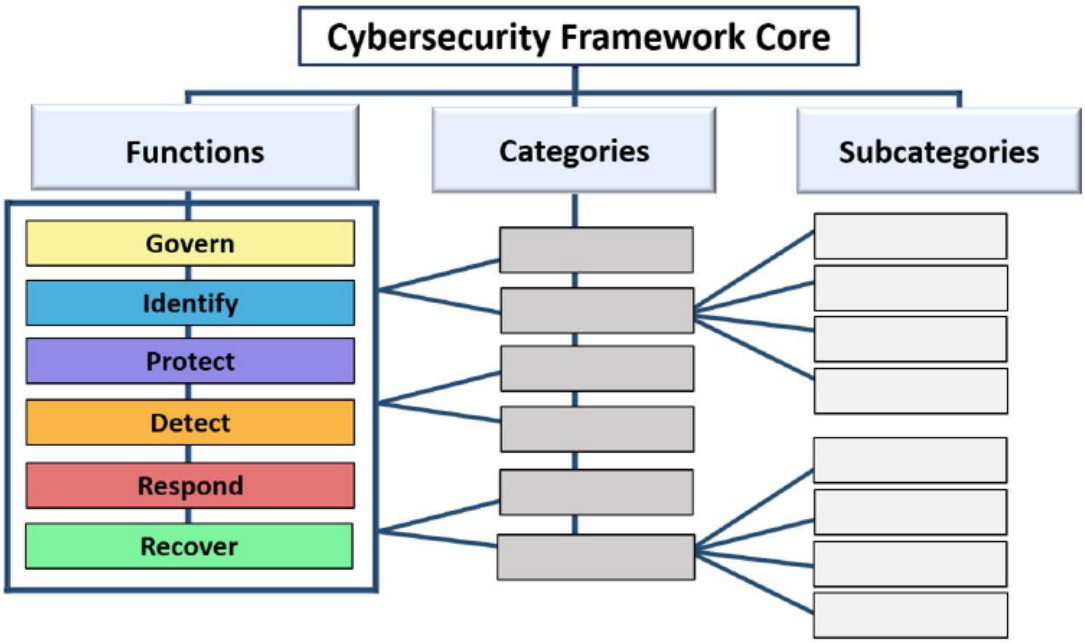


Fig. 1. CSF Core structure

O núcleo desses objetivos pode ser assim resumido (NIST, 2024, p. 3-4):

1. governar: a estratégia, as expectativas e a política de gestão de riscos de segurança cibernética da organização são estabelecidas, comunicadas e monitoradas;

2. identificar: os atuais riscos de segurança cibernética da organização são elencados e compreendidos;

3. proteger: são utilizadas salvaguardas para gerenciar os riscos de cibersegurança da organização;

4. detectar: possíveis ataques e comprometimentos de cibersegurança são encontrados e analisados, com a descoberta e análise oportunas de anomalias, indicadores de comprometimento e outros eventos potencialmente adversos que podem indicar a ocorrência de ataques e incidentes de segurança cibernética;

5. responder: ações em relação a um incidente de segurança cibernética detectado são adotadas, de forma a conter os efeitos de incidentes de cibersegurança, por meio do gerenciamento, análise, mitigação, produção de relatórios e comunicação de incidentes;

6. recuperar-se: os ativos e operações afetados por um incidente de cibersegurança são restaurados e normalizados, sem prejuízo da restauração das operações para reduzir os efeitos do incidente e da comunicação adequada durante os esforços de recuperação.

Note-se que a função "governar" é central a todos os demais aspectos do CSF, conforme se depreende da figura abaixo, extraída do próprio *framework* em estudo (NIST, 2024, p. 3-4), apenas destacando-se que as funções "governar", "identificar", "proteger" e "detectar" são exercidas em caráter permanente, enquanto as de "responder" e "recuperar-se" são exercidas episodicamente, quando há a ocorrência de incidentes de segurança:

Fig. 2. CSF Functions

Além disso, o CSF estabelece quatro camadas de nível de maturidade de segurança (*tiers*), quais sejam, 01) parcial; 02) informada quanto a riscos; 03) repetível; e 04) adaptativa (NIST, 2024, p. 8):

Fig. 4. CSF Tiers for cybersecurity risk governance and management

Para facilitar a implementação do *framework*, a NIST elaborou um *Quick Start Guide*, que consiste em orientações acessíveis aos usuários, com o NIST aberto a *inputs* e discussões da academia, de governos, das empresas e da comunidade em geral (NIST, 2024, p. 17).

Além disso, incentiva a comunicação e o intercâmbio entre esses diversos *players* para melhor afinar as expectativas de cibersegurança, o planejamento e a alocação de recursos (NIST, 2024, p. 10):

Fig. 5. Using the CSF to improve risk management communication

Igualmente, o CSF pontua enfaticamente que existe um espaço de intersecção entre cibersegurança e proteção à privacidade, e a essencialidade da primeira para a proteção da última, ainda que cada uma delas possua domínios próprios. Igualmente, entende que é importante que se promova o adequado *oversight* sobre os fornecedores de *hardware* e *software* nas diversas cadeias de suprimentos, inclusive no que diz respeito aos riscos associados à inteligência artificial e a outras tecnologias emergentes (NIST, 2024, p. 13):

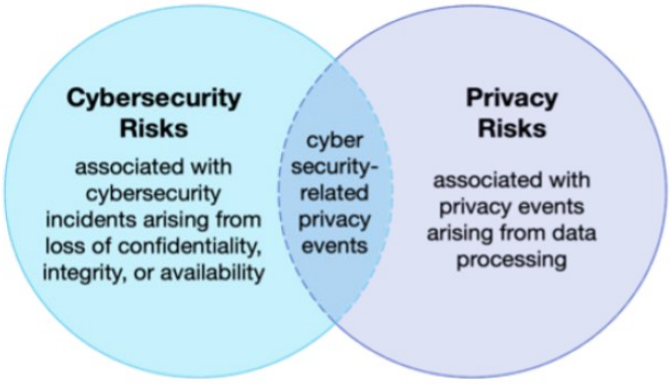


Fig. 6. Cybersecurity and privacy risk relationship

Como se pode ver, embora haja um alinhamento entre as prioridades a serem alcançadas nos arcabouços norte-americano, britânico e europeu em escala comunitária, notadamente no que diz respeito à proteção à privacidade e à preservação da integridade do ecossistema digital contra ameaças presentes e futuras, o cenário norte-americano se diferencia pelo seu foco mais acentuado no diálogo e na horizontalidade, enquanto os demais ambientes estudados carregam um tom de maior verticalidade e maior foco numa proteção mais enfática do indivíduo, mas com o potencial *tradeoff* de inibir investimentos em pesquisa e desenvolvimento e o florescimento de novas tecnologias.

Essa constatação, aliás, reflete a trajetória institucional das matrizes europeia e norte-americana, em que esta última se mostrou mais amigável a um ciclo contínuo de destruição criativa, especialmente em decorrência do espaço "quase libertário" associado ao Vale do Silício. Isso ocorreu notadamente após o advento do *Communications Decency Act* de 1996, que consolidou a sua aversão a intervenções governamentais, pondo maior crédito na capacidade de o setor privado e de os mercados conseguirem, com o tempo, mitigar os eventuais infortúnios associados ao surgimento de novas tecnologias. No entanto, essa crença tem perdido força mais recentemente, em decorrência de incidentes como o da Cambridge Analytica, da Equifax e da Solar Winds (BRADFORD, 2023, p. 33 *et seq.*).

O papel da *Federal Communications Commission* na cibersegurança das telecomunicações

No que diz respeito às ações da FCC para a promoção da cibersegurança no setor de telecomunicações, destaca-se o papel de sua Divisão de Cibersegurança e de Confiabilidade das Comunicações - *Cybersecurity and Communications Reliability Division* (CCR) – que é encarregada de assegurar a higidez das redes de comunicações, especialmente durante os períodos de emergência, com um foco especial em comunicações de emergência – 911 e afins – no desempenho da rede durante desastres e nas ameaças à rede (FCC, 2024).

Nesse ponto, a CCR divulga uma série de regras, manuais e recomendações de boas práticas sobre respostas a desastres e emergências, sobre alertas de emergência e sobre cibersegurança. Neste último caso, endereçam-se temas como *ramsonware*, orientações, ferramentas para pequenas empresas *etc.* (FCC, 2022).

A CCR realiza o monitoramento e a análise das redes de comunicações para identificar tendências e ações que a FCC pode tomar para prevenir e mitigar riscos, além de prestar assistência nas atividades de resposta e de recuperação, quando necessário.

Além disso, a CCR atua na preparação e resposta a desastres, coletando informações sobre o estado operacional da infraestrutura de comunicações para apoiar os esforços governamentais de assistência a catástrofes e para monitorar a restauração e recuperação. De igual forma, supervisiona e monitora os esforços da indústria para fortalecer a resiliência da rede sem fio (FCC, 2024).

Nesse aspecto, destaca-se o papel do *Disaster Information Reporting System* (DIRS) - Sistema de Relatórios de Informações sobre Desastres – de adesão voluntária pelos provedores, cuja finalidade é coletar informações sobre o *status* da infraestrutura de provedores de serviços de telefonia fixa, sem fio, transmissão, cabo, VoIP interconectado e banda larga.

Em momentos de crise, o DIRS permite que os provedores de comunicações relatem rapidamente degradações de serviço e solicitem assistência. Por sua vez, a FCC compila os dados e fornece informações sobre o *status* da rede aos agentes federais de gestão de emergências e publica relatórios de informações agregadas sobre restauração (FCC, 2024a).

Outra iniciativa para momentos de crise que merece destaque é o *Mandatory Disaster Response Initiative*, com vigência a partir de 1º de maio de 2024, que impõe que determinados provedores de serviços sem fio (equivalentes ao SMP no Brasil), em síntese, adotem, quando ordenado em hipóteses específicas na própria norma, as seguintes medidas para mitigação de efeitos de desastres: fornecimento mútuo de *roaming* quando uma rede estiver inoperante, sempre que isso for tecnicamente viável; celebração de acordos de cooperação mútua para compartilhamento da infraestrutura física e articulação antes e durante as emergências; melhorar a preparação em nível municipal; melhorar a prontidão do consumidor; e ampliar a conscientização do público em geral e as comunicações dos *stakeholders* sobre os períodos de recuperação (FCC, 2024b).

Por fim, a CCR monitora os riscos e vulnerabilidades das redes de comunicações e da cadeia de suprimentos, procedendo a avaliações detalhadas em empresas que possam representar uma ameaça potencial a essa cadeia e à integridade das redes de comunicações dos EUA (FCC, 2024).

Igualmente, destaca-se o papel do *Communications Security, Reliability, and Interoperability Council* (CSRIC) – Conselho de Segurança, Confiabilidade e Interoperabilidade de Comunicações - que tem a atribuição de fornecer recomendações à FCC para que ela possa assegurar a segurança, a confiabilidade e a interoperabilidade dos sistemas de comunicações, entradas em temas associados à segurança pública e à segurança interna, como alertas de emergência, números de emergência *etc.*

Essas recomendações abordam temas como prevenção e enfrentamento de eventos prejudiciais à cibersegurança, o desenvolvimento de práticas aprimoradas para melhorar a confiabilidade geral das comunicações, a disponibilidade e o desempenho dos serviços de comunicações e alertas de emergência durante desastres naturais, ataques terroristas, ataques à segurança cibernética, além de outros eventos que possam resultar em comprometimento excepcional da infraestrutura de comunicações (FCC, 2023).

Assim como ocorre com o NIST e com o CISA, a atuação da FCC na promoção da cibersegurança no setor de telecomunicações é preponderantemente horizontal, sendo raras as situações em que se imponha algum comando (como ocorre na *Mandatory Disaster Response Initiative*) em face das prestadoras.

Outra iniciativa voluntária desenvolvida pela FCC (2024c), é relacionada à etiquetagem de produtos de internet das coisas, denominado de *Cybersecurity Labeling for Internet of Things Program* , de participação voluntária pelos regulados. Nesse programa, produtos que cumprirem os *standards* de cibersegurança estabelecidos pela FCC poderão usar o selo respectivo (*U.S. Cyber Trust Mark)* identificando esse atendimento. O objeto do programa são os produtos de Internet das Coisas sem fio destinados aos consumidores, podendo abranger câmeras de segurança doméstica, dispositivos de compras ativados por voz, aparelhos conectados à Internet, rastreadores de *fitness*, controles de portas de garagem e babás eletrônicas. Além da supervisão pela FCC, os fornecedores deverão periodicamente proceder a verificações de conformidade por meio de laboratórios acreditados pela referida Agência.

5 *Benchmark:* Israel

Israel é um dos expoentes mundiais no desenvolvimento de aplicações de cibersegurança.

Esse protagonismo é decorrente de uma visão estratégica do governo israelense, que visa promover a vocação do país em liderar a exploração das potencialidades da cibersegurança para fomentar o crescimento econômico e promover os interesses nacionais no tema (STATE OF ISRAEL, 2017, p 5).

A entidade de referência para a execução da estratégia de cibersegurança israelense é o *Israel National Cyber Directorate* (INCD), que resulta da junção de dois entes governamentais que anteriormente detinham dimensões distintas dessa política: o *Israel National Cyber Bureau* (INCB), criado em 2012, com a incumbência de conceber políticas de cibersegurança e promover a construção de capacidades no país; e a *National Cyber Security Authority* (NCSA), encarregada de desenvolver as ações de cibersegurança do governo de Israel propriamente ditas (STATE OF ISRAEL, 2017, p 6-7).

Por sua vez, o panorama israelense é caracterizado por uma presença constante de ataques provenientes de diversos atores, que já focaram praticamente todos os setores da sua economia, várias de suas agências governamentais, e, principalmente, suas infraestruturas críticas (FREILICH *et alii*, 2023, p. 93 *et seq.*).

A estratégia israelense de cibersegurança compreende uma abordagem em três camadas, concebidas em uma perspectiva integrada para proporcionar uma abordagem holística do tema (STATE OF ISRAEL, 2017, p. 12-13), a saber:

1. Primeira camada de atuação: busca **aumentar a robustez em capacidades de cibersegurança** das organizações e dos processos, garantindo que continuem operando em uma rotina permanente de ameaças, com prevenção e respostas à maior parte dos ataques. Seus instrumentos focam na prevenção e geralmente consistem na disseminação de boas práticas, recomendações, guias, regulações, inclusive para infraestruturas críticas e incentivos (STATE OF ISRAEL, 2017, p. 15), em que o próprio governo procura adotar os melhores *standards* possíveis para sinalizar uma "liderança pelo exemplo" (STATE OF ISRAEL, 2017, p. 9-10);

2. Segunda camada: compreende a **ciberresiliência sistêmica**, consistente na habilidade de confrontar ciberataques antes, durante e após os incidentes. Diferentemente da primeira camada, seus instrumentos focam nas respostas do *Computer Emergency Response Team* (CERT) nacional, liderado pelo NCSA. A atuação do CERT é desenvolvida em cooperação com o setor privado e envolve o compartilhamento de informações relevantes, a promoção desse compartilhamento pelos demais *stakeholders*, e o auxílio a organizações durante os incidentes (STATE OF ISRAEL, 2017, p. 11); e

3. Terceira camada: envolve a **ciberdefesa**, desenvolvida a nível nacional, incluindo campanhas contra os autores de ataques (com ações de inteligência, prevenção, repressão e inibição) e campanhas de defesa nacional (com operações de defesa, resposta a incidentes nacionais e avaliação de situações).

Dentre as recomendações expedidas pelo INCD, cita-se a relacionada à redução de riscos de cibersegurança em câmeras de monitoramento, emitidas em 2018. Nessas recomendações, o INCD alerta que a ausência de adoção de práticas apropriadas pode resultar em extrusão e/ou descaracterização de dados, engenharias sociais, perdas de acesso, entre outros efeitos indesejado.

Essa recomendação abrange os cuidados desde o momento anterior à aquisição, compreendendo as etapas de escolha (especialmente no que diz respeito às configurações do equipamento quanto ao uso de redes e à gestão de *software* por intermediários), instalação, manutenção e atualização de *software* (STATE OF ISRAEL, 2018).

Igualmente, o INCD expediu *guidelines* voltadas à cibersegurança a respeito de serviços em nuvem, envolvendo pontos como o desenho de matrizes de responsabilidades compartilhadas entre clientes e provedores de serviços, considerando o modelo de contratação (IaaS, PaaS, SaaS etc.), controles de segurança que devem ser implementados pelos *Chief Information Security Officers* (CISOs), práticas a serem desenvolvidas junto aos *Cloud Access Security Brokers* (CASBs), e práticas para identificação, proteção e detecção de riscos, além de resposta e recuperação após incidentes (STATE OF ISRAEL, 2017a).

Mais recentemente, o INCD expediu recomendações associadas ao conflito envolvendo Israel e Hamas. Nelas, o INCD faz um inventário das atividades dos diversos atores responsáveis pelas ameaças, das organizações no ciberfronte, dos ativos em risco, dos instrumentos empregados, da evolução da atividade cibercriminosa - tratada como uma consequência "natural" do conflito. Além disso, traz percepções e orientações para o cenário atual, inclusive no que diz respeito a aquisição de equipamentos destinados a se conectarem à rede (STATE OF ISRAEL, 2024).

Pouco tempo antes, no final de 2023, o Knesset (o Parlamento Israelense), no contexto do conflito em estudo, aprovou proposição, com vigência temporária por sete meses, autorizando, dentre outros, o INCD a expedir ordens diretas a provedores de serviços digitais e de armazenamento de dados para que adotem medidas voltadas a detectar, prevenir e conter ciberataques (KNESSET, 2023).

Em 2021, o INCD também expediu recomendações relacionadas à cadeia de suprimentos (STATE OF ISRAEL, 2021, p. 4-6), a partir da identificação dos seguintes problemas, que devem ser solucionados para um funcionamento mais saudável do mercado:

1. Ausência de padronização da terminologia empregada entre provedores de produtos e serviços de cibersegurança e seus adquirentes, em que há dificuldades na condução de questionários para identificação de riscos enfrentados por cada um deles;

2. Dificuldade na administração do número excessivo de questionários que as organizações necessitam enviar aos seus provedores, num processo que rotineiramente demanda a contratação de um *expert* em segurança, o qual necessitará empregar tempo precioso para essa atividade; e

3. Provedores, por sua vez, são demandados a responder inúmeros questionários encaminhados pelos seus clientes, em que esses questionários não são uniformizados e cujo conteúdo é disperso, relacionados a deveres específicos de cada um deles.

Com isso, o INCD entendeu que é importante desenvolver uma linguagem uniforme para a padronização de requisitos e construir um instrumento apto a inspirar confiança no mercado, especialmente no que diz respeito às rotinas de inspeção e aos padrões de demonstração de cumprimento desses requisitos (STATE OF ISRAEL, 2021, p. 7).

Para essa finalidade, o INCD editou um regulamento (a Metodologia Nacional para a Proteção da Cadeia de Suprimentos), focada na regulação das atividades de cibersegurança dessa cadeia na economia israelense, na qual são apresentadas rotinas a serem seguidas por clientes, provedores de serviços de cibersegurança e instituições governamentais, em que estas últimas exercem um papel de supervisor das práticas de um sistema de acreditação de profissionais de *compliance*, voltados a proporcionar a confiança esperada na economia digital.

Igualmente, essa regulação trata do nível de serviços oferecidos pelo Estado e de recomendações aos provedores de produtos e serviços de cibersegurança sobre processos de gestão de riscos na cadeia de suprimentos e sobre ciberdefesa.

Embora o trabalho do INCD não seja imune a críticas, há uma percepção de que a estratégia de cibersegurança israelense tem rendido bons frutos, em que o INCD vem ocupando uma posição de destaque na economia e na promoção da segurança nacional desse país, que se encontra mais bem defendido atualmente (FREILICH *et alii*, 2023, p. 189).

A visão estratégica que vem sendo imprimida nessa abordagem é decorrente de um nível elevado de cooperação desenvolvido entre diferentes segmentos da sociedade israelense, com instituições de governo (civis e militares), indústrias, setor

privado, academia *etc.*, unidas por uma perspectiva cultural de autopreservação (FREILICH *et alii*, 2023, p. 189).

Ainda assim, Israel enfrenta vários desafios na construção de suas capacidades, tais como (FREILICH *et alii*, 2023, p. 212-218):

1. diminuir a escassez de profissionais de alta performance (cientistas de dados, engenheiros, programadores *etc.*), em que o país compete com as gigantes de tecnologia no processo de captação desses profissionais;

2. perda de relevância em pesquisa e desenvolvimento, pois houve diminuição do percentual do orçamento governamental destinado a essa finalidade nas últimas décadas, em que as multinacionais do setor privado podem acabar encontrando oportunidades de fomento mais atrativas em outros locais;

3. fuga de cérebros em que, ainda que as estatísticas de emigração em Israel sejam baixas para os padrões da OCDE, muitos dos emigrantes são trabalhadores altamente qualificados;

4. diminuição da velocidade de aparecimento de novas empresas no setor, inclusive multinacionais, o que levou o país a mudar o foco dos investimentos para a inteligência artificial, em que uma força tarefa recomendou a criação de uma autoridade semelhante ao INCD para o tema;

5. limitações de escala do país para exercer uma posição de liderança na computação quântica, em que o risco da ausência de independência das capacidades nesse ponto pode eventualmente implicar em impossibilidade de aquisição dessa tecnologia no exterior;

6. maior escrutínio da comunidade internacional no que diz respeito ao uso de programas de exploração de vulnerabilidades para monitoramento de dissidentes políticos por clientes governamentais de fornecedores israelenses, levantando problemas relacionados ao descumprimento do Acordo de Wassenaar, num cenário em que, ainda que Israel não seja dele signatário para ciberexportações, muitos dos países com quem desenvolve relações diplomáticas são participes desse acordo, acrescentando-se que algumas de suas diretrizes estão incorporadas no próprio Direito Interno israelense.

6

Benchmark: OCDE

Ao lado da governança e regulação do tema na União Europeia, Reino Unido e Estados Unidos, é importante destacar o trabalho da OCDE na matéria, uma vez que notoriamente guia o desenvolvimento de políticas públicas e regulatórias que não se limitam apenas aos países desenvolvidos.

A OCDE trabalha com a terminologia "*segurança digital*", a fim de ressaltar as perspectivas sociais e econômicas desse fenômeno (OCDE, 2002b, p. 11).

A OCDE é precursora nos trabalhos relacionados à segurança das TICs, remontando ao início da Década de 90, com a edição das Diretrizes para a Segurança dos Sistemas de Informação (OCDE, 1992).

Posteriormente, evoluiu-se para as Diretrizes da OCDE para a Segurança das Redes e Sistemas de Informação (OCDE, 2002) e, na sequência, para a Recomendação da OCDE sobre Gerenciamento de Riscos de Segurança Digital para Prosperidade Econômica e Social (OCDE, 2015).

Após processo de revisão realizado no âmbito do Grupo de Trabalho de Segurança Digital – denominado Grupo de Trabalho de Segurança na Economia Digital, cujas

atividades se desenvolveram até o final do ano de 2023 – foi aprovado novo conjunto de recomendações em 2022, em cujo desenvolvimento a Anatel, no exercício das suas competências de representação internacional, sob coordenação do Poder Executivo, acompanhou e participou ativamente.

O atual arcabouço da OCDE conta com as seguintes Recomendações

1. Recomendação sobre Gerenciamento de Riscos de Segurança Digital (OCDE 2022a);
2. Recomendação sobre Estratégias Nacionais de Segurança Digital (OCDE, 2022c);
3. Recomendação sobre a Segurança Digital de Produtos e Serviços (OCDE, 2022d);
4. Recomendação sobre o Tratamento de Vulnerabilidades de Segurança Digital (OCDE, 2022e);
5. Recomendação sobre Segurança Digital de Atividades Críticas (OCDE, 2019); e
6. Diretrizes sobre Política de Criptografia (OCDE, 1997).

O Brasil aderiu às cinco primeiras recomendações, demonstrando o compromisso político de implementação das diretrizes constantes desses documentos, que não possuem caráter vinculante.

Destaca-se o conteúdo das quatro primeiras recomendações, aderidas pelo Brasil em setembro de 2022.

A Recomendação de Gerenciamento de Riscos preza por uma abordagem fundamentada nos princípios gerais de cultura de segurança digital; responsabilidade de todos os atores de acordo com seus papéis, contexto e

habilidade de agir; gestão dos riscos consistente com direitos humanos e valores fundamentais; e cooperação.

Além disso, como princípios operacionais, recomenda que os líderes e tomadores de decisão garantam que o risco digital seja gerenciado como risco estratégico; que os riscos sejam tratados com base em avaliações contínuas; que as medidas de segurança sejam apropriadas a esses riscos; que a inovação seja considerada; e que um plano de preparação e continuidade seja adotado, implementado e testado, para garantir a resiliência (OCDE, 2022a).

Esses princípios gerais e operacionais são a base que ilumina todas as recomendações da OCDE, e são resultantes do amadurecimento e aprimoramento das diretrizes estabelecidas ao longo das últimas décadas pela referida organização internacional.

A segunda recomendação tem seu foco nas Estratégias Nacionais de Segurança Digital, recomendando que o arcabouço institucional estabeleça uma coordenação intragovernamental, garanta o apoio de mais alto nível do governo e estabeleça responsabilidades claras.

Segundo essa Recomendação, a Estratégia deve ser direcionada a todos os atores e adaptada para PMEs e indivíduos, articulando suas responsabilidades, com base nos seus papéis, habilidade de agir e contexto. Além disso, deve abordar conscientização e capacitação, resposta a incidentes e coordenação de vulnerabilidades, padrões de gestão de risco, indústria, pesquisa e inovação em segurança digital, engajamento na proteção dos indivíduos e de pequenas e médias empresas, transformação digital setorial, parcerias e cooperação internacional.

Recomenda-se, ainda, a adoção de políticas e iniciativas para implementação da Estratégia, com alocação dos recursos necessários, engajamento com outros atores, sem prejuízo da avalição, revisão e aprimoramento regulares da Estratégia e das suas políticas de implementação (OCDE, 2022c).

A Recomendação sobre a Segurança Digital de Produtos e Serviços está diretamente relacionada às competências da Agência no processo de conformidade dos equipamentos para telecomunicações.

No nível doméstico, conclama os aderentes a adotarem medidas para intensificar a cooperação por meio da integração de políticas no contexto de outras políticas de segurança e transformação digitais; alavancar a comunidade multissetorial no apoio ao desenvolvimento e à implementação de políticas; estabelecer uma abordagem integrada de governo para aumentar a segurança dos produtos e serviços digitais e a cooperação interagências; promover a capacitação em segurança digital; e encorajar fornecedores a colaborar e coordenar a resposta a incidentes e o compartilhamento de informações.

No nível internacional, recomenda considerar padrões internacionais no desenvolvimento de políticas; compartilhar boas práticas sobre políticas e iniciativas nacionais e regionais; aumentar a cooperação transfronteiriça; encorajar fornecedores e usuários a colaborarem e coordenarem as respostas a incidentes e a compartilharem informações; promover a interoperabilidade de arcabouços legais, incluindo requisitos, certificações e selos; e fomentar ações de capacitação em países em desenvolvimento.

No tocante ao dever de cuidado dos fornecedores, recomenda o desenho de políticas que fomentem o *security-by-design*, o *security-by-default,* o tratamento e a coordenação de vulnerabilidades, a cooperação na cadeia de suprimentos dos proprietários de código, a avaliação do nível de segurança digital dos produtos e serviços, e a adoção de políticas claras, responsáveis e transparentes sobre o fim de suporte/ciclo de vida do produto e/ou serviço digital.

A recomendação dedica, ainda, uma parte à transparência e ao compartilhamento de informações, sugerindo aos aderentes que adotem políticas para incentivar os fornecedores a utilizarem avaliações de terceiro; serem transparentes; cooperarem e compartilharem informações com autoridades públicas e outros atores; permitirem que usuários avançados acessem e modifiquem configurações de segurança; e

encorajem pesquisadores, quando apropriado, a atestar produtos e serviços, preferencialmente com a consideração de padrões internacionais no desenvolvimento de selos.

Por fim, recomenda adotar políticas proporcionais ao risco e promover inovação, pesquisa e desenvolvimento para aumentar a segurança digital de produtos e serviços (OCDE, 2022d).

O último destaque do arcabouço é a Recomendação sobre o Tratamento de Vulnerabilidades de Segurança Digital.

O texto aderido propõe tornar claras as responsabilidades, garantindo que todos os atores estejam cientes de que seus produtos e sistemas de informação possam conter alguma vulnerabilidade; e que são responsáveis, com base no seu papel, contexto e habilidade de agir, por endereçar essas vulnerabilidades e compartilhar informações, clarificando os papéis de proprietários de código, proprietários de sistemas, proprietários de vulnerabilidades e pesquisadores de vulnerabilidades.

Ademais, recomenda o encorajamento e proteção de pesquisadores de vulnerabilidades, a disseminação de boas práticas e o aprimoramento da cooperação nacional e internacional (OCDE, 2022e).

As recomendações da OCDE são importantes subsídios ao processo regulamentar da Agência e é possível apontar o alinhamento do R-Ciber, com as suas recentes alterações, aos princípios de gestão de riscos recomendados.

Salienta-se que a assimetria regulatória adotada para o controle *ex ante* atende diretamente ao pressuposto de que a responsabilidade dos atores na gestão desses riscos deve considerar o papel, contexto e a habilidade de agir de cada ator.

Outro exemplo de alinhamento são os atos de conformidade específicos de segurança cibernética, aprovados pela Agência após a aprovação do R-Ciber no ano de 2020.

O Ato nº 77, de 05 de janeiro de 2021, aprovou os Requisitos de Segurança Cibernética para Equipamentos para Telecomunicações e expressamente cita

trabalho da OCDE sobre a segurança digital de produtos nas referências. O ato discute expressamente os aspectos tratados na recomendação e fixa, como requisitos para homologação de equipamentos, a existência de políticas claras de suporte do produto, um processo de Divulgação Coordenada de Vulnerabilidades, dentre outros.

Após um processo de revisão e amadurecimento do Ato nº 77 durante discussões desenvolvidas no GT-Ciber, aprovou-se o Ato 2.436, de 7 de março de 2023, que estabelece requisitos mandatórios mínimos de segurança cibernética para avaliação da conformidade de equipamentos CPE (*Customer Premises Equipment),* reforçando-se o alinhamento da Anatel com a Recomendação em estudo.

Observa-se que o primeiro ato, de 2021, adota uma abordagem voluntária, enquanto o segundo emprega uma perspectiva mais mandatória.

De qualquer forma, ambos os atos alinham-se à Recomendação sobre Segurança Digital de Produtos e Serviços, na qual se entende que os aderentes devem adotar políticas que sejam embasadas inicialmente numa abordagem dialogada, a partir de medidas voluntárias, sem prejuízo do uso de medidas mandatórias, caso necessárias (OCDE, 2022d).

7

Benchmark:

União Internacional de Telecomunicações (UIT)

A UIT é a agência especializada das Nações Unidas para as TICs e possui um extenso trabalho na área de segurança cibernética.

O desenvolvimento dessas ações e trabalhos atendem ao seu papel de agência facilitadora da Linha de Ação C5 do Plano de Genebra da Cúpula Mundial para a Sociedade da Informação, o qual trata da construção de confiança e segurança no uso dessas tecnologias (CGI.br, 2014).

A UIT é responsável por auxiliar os países a construírem suas capacidades de segurança cibernética, com iniciativas relacionadas aos seguintes aspectos, dentre várias outras atividades:

1. estabelecimento de padrões técnicos de segurança cibernética;

2. assistência para criação e aprimoramento de CSIRTs e desenvolvimento de Estratégias Nacionais de Segurança Cibernética;

3. elaboração de indicadores (*Global Cybersecurity Index*);

4. desenvolvimento de diretrizes para a proteção das crianças no ambiente digital;

5. realização de simulações (*cyberdrills*); e

6. enfrentamento das tecnologias emergentes (*AI for Good*).

Destaca-se igualmente o trabalho do Setor de Desenvolvimento em segurança cibernética (ITU, 2024) e o trabalho de desenvolvimento de padrões de segurança cibernética (ITU, 2024a).

A Anatel engaja-se fortemente nesses trabalhos, exercendo a representação brasileira sob coordenação do Poder Executivo.

Além disso, criou um Subgrupo específico no âmbito do GT-Ciber para internalizar, fomentar e construir os posicionamentos brasileiros para serem apresentados nas discussões realizadas nas diversas instâncias da organização.

Em 2023, a Anatel, representando o Brasil na UIT, apresentou iniciativa exitosa que resultou na Decisão nº 639 (C23), cujo foco é a construção de um repositório informativo para ajudar os Estados-Membros a desenvolverem a sua capacidade de cibersegurança e resiliência cibernética.

Por meio de tal Decisão, instruiu-se o Secretário-Geral e os seus três Diretores a:

1. desenvolverem um recurso informativo para os Estados Membros, que inclua, no âmbito de cada um dos pilares da Agenda Global de Cibersegurança (GCA): a. exemplos de melhores práticas existentes; b. fontes de aconselhamento, assistência e orientação da UIT e de outras organizações relevantes para que os países reforcem a sua segurança cibernética e a sua resiliência cibernética; c. informações sobre programas de capacitação que a UIT e outras organizações relevantes estão fornecendo; e

2. manterem e atualizarem regularmente tal repositório, para ter em conta novos desafios, novos desenvolvimentos e novas atividades relacionadas com a UIT, bem como novas atividades lideradas por outras organizações que possam ajudar os Membros a reforçar a sua capacidade de segurança cibernética e de resiliência cibernética.

Nota-se que o mandato da organização transborda à regulação setorial. Porém, podem ser ressaltados alguns esforços recentes específicos nessa área.

A publicação *Global Digital Regulatory Outlook 2023* (ITU, 2023) apresenta a segurança cibernética como um dos nove temas no radar de todos os reguladores e como um pilar da transformação digital.

Ao tratar das opções regulatórias, o texto destaca os diferentes mandatos dos reguladores das TICs/Telecomunicações e a ausência de uma abordagem única. Aponta que, mesmo nos casos de mandato limitado, existe um papel para esses reguladores.

Como possíveis áreas de atuação, a publicação cita: medidas de governança para as prestadoras de serviços; promoção de boas práticas para detecção e mitigação de ameaças; promoção de compartilhamento de informações; proteção de infraestrutura crítica; desenvolvimento de esquemas de certificação e de etiquetagem; e fomento da conscientização.

A publicação enfatiza a necessidade de regulação colaborativa e a possibilidade da combinação de regulação tradicional com novas ferramentas colaborativas para enfrentar os desafios desse fenômeno (ITU, 2023).

A segunda e mais recente iniciativa é o "*Guiding Principles for ICT regulators to enhance cyber resilience*", disponível na Plataforma de Regulação Digital - iniciativa da UIT em colaboração com o Banco Mundial (BENUSSI *et alii*, 2024).

A publicação traz uma abrangente contextualização da segurança cibernética para as TICs e apresenta os desafios, os principais ativos, riscos e vulnerabilidades, um mapeamento do ecossistema de segurança cibernética, um rol de práticas regulatórias e os princípios orientadores.

São detalhados 19 (dezenove) princípios orientadores que abrangem: Estratégias Nacionais e regulação setorial, colaboração multissetorial, simulações, práticas de promoção de gestão de riscos, conscientização, investimento em pesquisa e desenvolvimento em segurança cibernética, e higiene cibernética, melhores práticas e padrões.

Embora anterior ao documento, constata-se a sinergia do R-Ciber e os princípios nele consagrados, enfatizando-se, no texto, diversas experiências brasileiras nacionais e setoriais, incluindo a atuação da Anatel na temática (BENUSSI *et alii*, 2024).

Por fim, ainda merece atenção o Relatório "*Cybersecurity Assurance Practices*", o qual reconhece o momento propício ao desenvolvimento de esquemas de certificação, de etiquetagem e de requisitos, consolidando as discussões e contribuições no tema em seis principais conclusões:

1. diferentes níveis de criticidade requerem diferentes níveis de garantia;
2. o engajamento multissetorial pode funcionar como um caminho efetivo para impulsionar essas práticas;
3. deve-se considerar uma abordagem regulatória evolutiva;
4. as práticas não podem ser estáticas, demandando revisão e adaptação ao longo do tempo;

5. há a necessidade de esforços para educar os consumidores sobre a importância de segurança cibernética e da escolha de produtos mais seguros; e

6. é importante buscar sinergia e harmonização internacional e acordos de reciprocidade.

O Relatório ainda conta com um rol exemplificativo de práticas da Arábia Saudita, Austrália, Brasil, Coreia do Sul, Reino Unido e Singapura (ITU, 2023a).

8

Adaptação e Implementação no Contexto Brasileiro

Várias das medidas em discussão na Europa e nos Estados Unidos e citadas neste trabalho pressupõem discussões em termos de governança e coordenação nacionais que estão acontecendo nesse momento no âmbito do CNCiber.

No que diz respeito à Anatel, a recente revisão do R-Ciber trouxe medidas oportunas.

Dentre elas, citam-se a ampliação da abrangência dos controles *ex ante* para inclusão de novos prestadores e operadores de infraestruturas críticas – com o destaque para os de cabos submarinos - o que foi feito no art. 2º-B recentemente adicionado.

Igualmente, destaca-se a discussão, reflexão e amadurecimento sobre a incorporação de novos elementos normativos no R-Ciber, tais como *data centers*, inteligência artificial e computação em nuvem, revela-se oportuna.

Quanto ao ponto, atualizou-se o art. 14 do R-Ciber, para determinar que as políticas de segurança cibernética das prestadoras também contemplem aspectos relacionados a *data centers* e à computação em nuvem, em medida de regulação **indireta** do tema.

Por sua vez, a Anatel já manifestou preocupação quanto à regulamentação direta de *data centers* e de serviços computação em nuvem, pois atualmente é necessária a edição de regramento específico em segurança cibernética para esses setores (OLIVEIRA, 2022).

No entanto, essa discussão encontra-se em maturação, tanto em seu âmbito interno quanto perante a sociedade brasileira.

Mesmo no cenário internacional, esses temas emergentes ainda não são abordados uniformemente. Muitos países atualmente estão avaliando quais medidas de intervenção são necessárias, e em que grau.

A Anatel – especialmente por meio da relatoria do Conselheiro Alexandre Freire na revisão do R-Ciber e por meio de sua atuação como Presidente do Comitê de Infraestrutura de Telecomunicações, além da atuação do próprio GT-Ciber – tem fomentado a produção de estudos e informações a respeito do tema, tanto em seu ambiente *interna corporis,* como perante a comunidade em geral (acadêmica, de prestadores de serviços de telecomunicações, de fornecedores de soluções *etc.*).

Reconhecendo a premente necessidade de elaboração de diagnóstico e de estudos técnicos voltados ao fortalecimento das medidas de segurança cibernética, o Conselheiro Diretor Alexandre Freire, durante a relatoria do R-Ciber, determinou a realização das seguintes diligências pela área técnica, voltadas à obtenção de insumos para uma futura regulação direta de *data centers* e de *cloud computing* e de utilização de inteligência artificial ante os riscos que pode trazer para as diversas camadas da rede:

1. Diagnóstico da utilização de *data centers* e *cloud computing* pelas prestadoras de telecomunicações (Ofício nº 86/2023/AF-ANATEL);

2. Realização de estudos sobre os impactos do uso de inteligência artificial na integridade da infraestrutura de telecomunicações (Ofício nº 15/2024/AF-ANATEL);

3. Produção de estudo sobre segurança física e cibernética dos cabos submarinos (Ofício nº 18/2024/AF-ANATEL);

4. Apresentação de estudo sobre aplicações de inteligência artificial generativa e seus impactos para a integridade do ecossistema digital (Ofício nº 30/2023/AF-ANATEL).

Além disso, o Centro de Altos Estudos em Comunicações Digitais e Inovações Tecnológicas da Anatel (CEADI), realizou, em 2023, o *Workshop* Regulação & Segurança Cibernética, em que diversos profissionais e acadêmicos de destaque na área de cibersegurança debateram o tema, ainda durante a relatoria do R-Ciber.

Como consectários dessas diligências e discussões, espera-se a realização de tomadas de subsídios, consultas internas, consultas públicas, eventos acadêmicos *etc*. em que a Anatel deverá ter uma percepção mais acurada desses novos temas, notadamente no que se relaciona à regulação direta de *cloud computing* e de *data centers* e de aplicações de inteligência artificial para preservação da integridade do ecossistema digital nas suas diversas camadas.

Em que pese esses temas não terem sido incluídos no texto final da revisão do R-Ciber, eles devem ser amadurecidos, tendo o próprio Conselheiro Alexandre Freire, durante a relatoria da revisão da Agenda Regulatória 2023-2024, em alerta regulatório, destacado que a Anatel futuramente os enfrentará.

Na esfera internacional, a Anatel se encontra alinhada com as práticas estimuladas pela OCDE e pela UIT.

Aliás, em algumas ocasiões, incorporou adiantadamente algumas de suas recomendações, antes mesmo da edição de ato formal pela UIT, em tópicos cujo debate já se encontrava suficientemente amadurecido.

No entanto, há uma série de desafios a serem superados, os quais serão vistos no capítulo a seguir.

9

Desafios e Oportunidades Futuras

Pode ser percebido que todos os países, mesmo os desenvolvidos, apresentam desafios significativos a serem superados na construção das suas capacidades de cibersegurança e resiliência cibernética.

O caráter dinâmico dos riscos e a relevância do tema como eixo viabilizador da transformação digital e, consequentemente, do desenvolvimento dos países e do bem-estar das suas populações, demandam uma revisão permanente das medidas adotadas, tanto *ex ante* como *ex post*, sejam elas de adoção voluntária, sejam elas impostas coercitivamente.

Os desafios que países com diferentes níveis de desenvolvimento e maturidade em cibersegurança enfrentam são diversos, porém não menos complexos.

Apenas para ilustrar algumas dessas dificuldades, destaca-se o notório déficit de capital humano apto a lidar com ameaças de cibersegurança em todo o mundo.

Mesmo em regiões com maior circulação de riqueza, como a Europa e os Estados Unidos, identifica-se uma carência de profissionais qualificados, com um déficit global estimado em 4 (quatro) milhões de profissionais (ISC, 2023).

Ainda, é importante considerar as tecnologias emergentes, como, por exemplo, a computação quântica, que apresentam significativos riscos para criptografias, tecnologias e sistemas legados, sendo imperioso promover a adequada gestão desses riscos.

Mais imediatamente, devem ser considerados os riscos cibernéticos associados à Inteligência Artificial, dado que está claro ser uma tecnologia muito rica e de fácil acesso, permitindo a agentes mal-intencionados a produção de artifícios maliciosos e engenhosos. Trata-se de uma solução que traz uma espécie de assessoramento muito qualificado e acessível, tanto para a promoção do bem-estar das pessoas como para a concretização de prejuízos em seu desfavor, e suas implicações precisam ser acompanhadas.

A evolução das redes de telefonia, notadamente a próxima geração 6G, trará um novo período de parametrizações internacionais, com oportunidade para uma dedicação mais qualificada à segurança. Afinal de contas, identifica-se uma dependência cada vez maior de muitas indústrias em relação ao ecossistema digital para a execução de seus distintos processos de produção, gerenciamento e de circulação de bens e serviços.

A proteção e a gestão de riscos nas infraestruturas críticas, como cabos submarinos, *data centers* e serviços de computação em nuvem, inclusive de forma diretas, entre outras, são igualmente temas de enorme importância.

Outro desafio é o necessário domínio técnico-científico de toda a cadeia que envolve o ecossistema digital para que um país possa defender sua soberania e seus interesses. Ou seja, é importante deter conhecimento profundo desde a pesquisa e fabricação de *chips* (*hardwares*) até a programação adequada e eficaz das aplicações

e algoritmos atuais e emergentes (*softwares*), perpassando por diversos elementos e camadas de redes do citado ecossistema.

A evolução impõe o amadurecimento contínuo de todos os atores envolvidos no ambiente da cibersegurança, pois não basta ter a tecnologia segura; é necessário que os usuários internalizem as boas práticas, especialmente as relacionadas à higiene cibernética.

Percebe-se claramente que não se trata de um desafio a ser endereçado a curto e médio prazos, mas sim, de um projeto de nação a longo prazo, que já está provocando imensas transformações no setor produtivo, o qual cada vez mais se expande para o ambiente digital.

Portanto, é essencial a promoção de investimentos substanciais nos setores que envolvem a higidez de todo o ecossistema digital, pois, no mundo contemporâneo, a soberania cibernética é um dos pilares para a manutenção da soberania nacional e o será cada vez mais, considerando o ritmo da transformação digital, apoiada principalmente pela conectividade fornecida pelo setor de telecomunicações.

Consoante a extensa parte introdutória, procurou-se assentar a criticidade e a relevância do papel do setor de telecomunicações e, especialmente, do regulador, para a promoção da cibersegurança e da resiliência cibernética no país.

Esse papel faz com que as ações adotadas no setor se projetem de forma muito positiva para todo o ecossistema digital. É justamente por isso, e considerando as novas e emergentes tecnologias e riscos de segurança cibernética, que o Conselho Diretor aprovou a inclusão do novo item 29 da Agenda Regulatória 2023-2024, com o intuito de avaliar a revisão do R-Ciber, de modo a atualizá-lo para contemplar novos elementos, tecnologias e pontos de criticidade, sendo essa revisão concluída em sessão realizada em 04 de julho de 2024.

O presente trabalho constituiu-se em importante subsídio para essa revisão, estabelecendo-se como elemento de fomento ao debate público de um tema tão

relevante para o desenvolvimento do país e para a proteção e resiliência cibernética do nosso ecossistema digital.

Por fim, ainda que a presente etapa de revisão do R-Ciber tenha sido concluída, e rememorando o que foi exposto na apresentação, esse tema será revisitado, possibilitando reflexões que podem resultar em nova proposta regulatória.

Os riscos da inteligência artificial – especialmente da generativa – para a integridade do ecossistema digital e as iniciativas da Anatel

A inteligência artificial (IA), até pouco tempo conhecida principalmente pelo emprego, dentre outros, de modelos preditivos, classificatórios e recomendatórios, já vinha proporcionando notáveis ganhos de eficiência por meio de decisões automatizadas a partir de modelos que envolvem aprendizado de máquinas e uma amostragem massiva de dados.

O advento da IA generativa, por sua vez, vem se constituindo num novo e relevante salto no uso dessa tecnologia.

As ferramentas de IA Generativa compreendem os recursos que permitam criar novos conteúdos (textos, imagens, áudios e vídeos) a partir de prévio treinamento baseado em dados e de comandos do usuário realizados em linguagem natural, inclusive com o uso de informações em tempo real (OCDE, 2023, p. 6).

Suas aplicações podem envolver as mais diversas finalidades, como a realização de compras, de reservas *etc.*, e já podem ser vistas, inclusive, no mercado de valores mobiliários, com o emprego dos preços de ações e de conteúdo de notícias nos dados que embasarão a decisão a ser tomada em alguma operação (LORENZ *et alii*, 2023, p. 6 e 10).

Pessoas, governos e mercados no mundo inteiro já reconheceram as potencialidades de ganhos de eficiência que o uso da IA generativa pode proporcionar.

Aliás, observa-se o aporte de diversos investimentos de capital de risco (*venture capital*) para iniciativas focadas na modelagem de códigos de programação, na produção de material artístico e criativo (imagens, vídeos, composições, música, *marketing*, filmes *etc.*), no desenvolvimento de conteúdo educativo (cursos, ementas, informativos, cartas de recomendação, dentre outros), no aperfeiçoamento de motores de pesquisa a partir de interações conversacionais e, até mesmo, na descoberta de novos medicamentos com o emprego de modelagem química generativa (LORENZ *et alii*, 2023, p. 12-13).

No entanto, a utilização de IA Generativa não é vista como um processo isento de riscos (OCDE, 2023, p. 11), os quais precisam ser devidamente endereçados.

Conforme será visto a seguir, eles compreendem, dentre outros, as implicações da dificuldade de se distinguir a origem "artificial" da informação, problemas de vieses, além dos riscos do uso adversarial (KISSINGER *et alii*, 2021, p. 63-66).

No âmbito da autorregulação, destacam-se as recentes normas ISO/IEC 24027:2024, cujo objeto é a mitigação de vieses algorítmicos, e ISO/IEC 42001:2023, voltada à gestão de sistemas de inteligência artificial.

Não à toa, os integrantes do G7 deram início ao *Hiroshima AI Process Comprehensive Policy Framework*, o qual atualmente conta com a adesão de mais de quarenta países, para a criação de um *framework* internacional que inclui princípios orientadores e um código de conduta destinado a promover sistemas avançados de IA seguros, protegidos e confiáveis (OCDE, 2023).

Assim, estudos e arcabouços vêm sendo patrocinados recentemente, por exemplo, pela OCDE – destacando-se o trabalho seminal *Initial Policy Considerations For Generative Artificial Intelligence* (LORENZ *et alii*, 2023) – e pelos Estados Unidos, notadamente pelo NIST (NIST, 2023; NIST, 2024a), com o *Artificial Intelligence Risk Management Framework* (AI RMF 1.0) e o seu *companion document* – o *Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile* (ainda em fase de revisão pela referida agência) – em que se identificam vários riscos associados ao uso de IA Generativa, mas ressalvando que a extensão total desses riscos ainda não é conhecida (NIST, 2024a, p. 3).

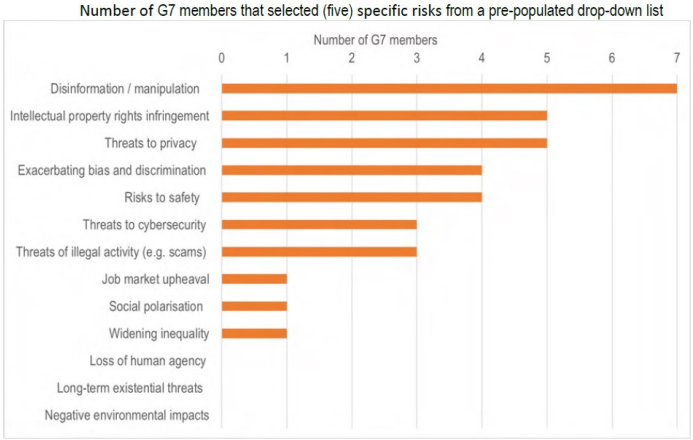
O primeiro desses riscos é a fundamentação dos modelos de linguagem natural em probabilidades, e não no contexto do uso dessa linguagem, o que, diferentemente da conversa humana, torna mais difícil para os modelos checarem a veracidade das informações que geram (LORENZ *et alii*, 2023, p. 14).

O segundo deles relaciona-se à crescente dificuldade de se distinguir se um determinado conteúdo foi gerado por um humano ou por uma ferramenta de IA generativa.

O terceiro se relaciona ao comportamento amplamente "autônomo" de várias das ferramentas de IA Generativa, em que elas podem retroalimentar a sua capacidade de tomar decisões por conta própria para criar ou propagar desinformação, para executar ações indesejadas ou, ainda, para que os *bots* ajam e se identifiquem como humanos (LORENZ *et alii*, 2023, p. 11), o que se denomina de risco de "integridade da informação" (NIST, 2024a, p. 7-8). Nesse cenário, contempla-se, ainda, o chamado risco de "confabulação", em que a ferramenta de IA apresenta conteúdo errôneo ou falso para atender ao *prompt* do usuário, como resultado "lógico" da construção de sua programação (NIST, 2024a, p. 5).

No Processo de Hiroshima, cada um dos países integrantes do G7 escolheu cinco riscos associados ao uso de IA Generativa, em que a desinformação/manipulação da informação aparece como unanimidade, consoante se extrai do gráfico abaixo (OCDE, 2023, p. 14):

FIGURE 2.2. TOP FIVE *RISKS* PRESENTED BY GENERATIVE AI IN ACHIEVING NATIONAL AND REGIONAL GOALS



Note: The figure aggregates responses from seven respondents to the question: "*From your country or region's perspective, what are the top five risks generative AI presents to achieving national and regional goals? (Please select five options)*".

Isso faz surgir incertezas sobre a extensão das repercussões sociais e econômicas de tais ferramentas.

Indaga-se, por exemplo, se, atualmente, a IA Generativa já pode ser considerada como uma forma de Inteligência Artificial Geral, em que os próprios dados de treinamento podem perpetuar a propagação de vieses, de discriminações e de informações incorretas (LORENZ *et alii*, 2023, p. 17).

Um instrumento que tem sido utilizado para mitigar esse risco é o emprego de *red teams*, em que equipes adotam uma abordagem agressiva para investigar o modelo de IA Generativa em busca de falhas e vulnerabilidades (LORENZ *et alii*, 2023, p. 17-18), prática essa que, aliás, vem sendo estimulada pela Casa Branca (THE WHITE HOUSE, 2023).

No entanto, o emprego desse e de outros instrumentos de supervisão humana, inclusive checagem de fatos e educação de usuários, têm limites de escala, de custos e de qualidade do *feedback* (LORENZ *et alii*, 2023, p. 15), sendo necessário pensar em como utilizar a IA Generativa para "policiar" ela mesma.

Outra prática seria a confrontação de modelos de IA Generativa entre si (idênticos ou não) para a detecção de *deepfakes*, de ações de desinformação *etc.*

Um dos exemplos mais curiosos desses eventos indesejados é o de *jailbreaks*, em que os modelos baseados em linguagem natural são intencionalmente explorados para responder de forma inapropriada às suas instruções, com o emprego de técnicas adversariais de *machine learning*.

Usos adversariais podem compreender, até mesmo, um acesso mais facilitado a processos de síntese e análise necessários para a confecção não convencional de armas químicas, biológicas, radiológicas e nucleares e sobre outros vinte e três materiais biológicos considerados perigosos (NIST, 2024a, p. 4-5).

Esses usos adversariais podem servir para, por exemplo, propagar conteúdo inapropriado, como incitação ao crime, ao terrorismo, à autolesão, à automutilação e ao suicídio; conteúdo obsceno, degradante ou abusivo, especialmente por meio de *deepfakes* (como a divulgação de pornografia infantil, que é proibida em qualquer hipótese, e a exposição não consentida de conteúdo íntimo adulto); e conteúdo de linguagem tóxica, enviesada ou homogeneizada, que podem servir para reforçar discursos de ódio e inibir a promoção da diversidade (NIST, 2024a, p. 5-6, 9-10).

Por sinal, a NIST norte-americana desenvolveu uma *guideline* para orientar indivíduos e organizações responsáveis por projetar, desenvolver, implantar, avaliar e governar sistemas de IA a lidar com essas técnicas adversariais, assim compreendidas como aquelas que têm pelo menos um dos seguintes objetivos em relação a uma ferramenta de IA, preditiva ou generativa: 1. torná-lo indisponível; 2. comprometer sua integridade; ou 3. comprometer a privacidade dos dados empregados no modelo (VASSILEV *et alii*, 2024).

De igual forma, o *companion document* da NIST acima mencionado deverá trazer *checklists* para a identificação de riscos no ciclo de vida do uso de ferramentas de IA Generativa, as medidas respectivas de mitigação (NIST, 2024a, p. 11-62) e orientações para a própria governança no uso dessas ferramentas no que diz respeito à estrutura da organização que a desenvolve, à consideração de terceiros interessados sobre a ferramenta, a rotinas *pre-deployment*, à procedência do conteúdo gerado, com auditabilidade dos dados e *feedback* público estruturado, e à comunicação de incidentes (NIST, 2024a, p. 63-69).

No que diz respeito à geração de imagens sintéticas, conceberam-se outras medidas para mitigar o risco de desinformação, como a utilização de marcas d'água e de outros sinais distintivos, restrição a usos de código e a elaboração de *guidelines*.

Ainda assim, não há garantias de que essas medidas serão efetivas. Aliás, as marcas d'água podem ser utilizadas para ataques de *spoofing* (LORENZ *et alii*, 2023, p. 17), prática esta já endereçada pela Anatel em outras de suas políticas voltadas à inibição de golpes e fraudes perpetradas nos serviços de telecomunicações (*online* ou não), mas que deve ganhar progressivamente novas camadas de sofisticação com o uso de recursos de IA Generativa.

Esse cenário é agravado pela opacidade algorítmica e pela complexidade das ferramentas de IA Generativa como um todo, o que pode limitar as possibilidades de contenção do seu comportamento (OCDE, 2024, p. 39-40), e amplificar os riscos de prejuízos financeiros em virtude do emprego de instrumentos mais eficientes de engenharias sociais, de *phishing*, de *smishing etc.* (OCDE, 2023a, p. 21).

Outro evento de desinformação a ser considerado são os "ataques de paráfrase", em que o refraseamento de textos por aplicações de IA Generativa pode servir para dificultar a efetividade dos algoritmos de detecção de informações incorretas (LORENZ *et alii*, 2023, p. 16-17).

Por sua vez, recentemente, o Parlamento Europeu (2024), nas discussões relacionadas à regulamentação do uso de IA na UE, sinalizou que estabelecerá obrigações específicas para sistemas de IA de alto risco, assim entendidos aqueles que podem causar danos significativos à saúde, à segurança, aos direitos fundamentais, ao meio ambiente, à democracia e ao Estado de Direito.

Ainda segundo o Parlamento Europeu (2024), os exemplos de utilização de IA de alto risco compreendem as situações relacionadas a infraestruturas críticas, educação e formação profissional, emprego, serviços públicos e privados essenciais (por exemplo, cuidados de saúde e serviços bancários), determinados sistemas de aplicação da lei, migração e gestão de fronteiras, justiça e processos democráticos (por exemplo, com a finalidade de influenciar eleições).

Dentre as obrigações cuja implementação é estudada para a gestão desses sistemas, o Parlamento Europeu considera as seguintes (2024): avaliação e redução de riscos identificados, manutenção de registros de utilização, transparência e precisão e garantia de supervisão humana.

O quarto é relacionado aos riscos aos direitos fundamentais e à democracia em decorrência de uma vigilância excessiva das pessoas por ferramentas de IA (preditivas, generativas *etc.*). Tal risco também pode decorrer de um desempoderamento coletivo que o uso de IA pode proporcionar, pois são capazes de redistribuir configurações de poder e os benefícios coletivos que esse uso pode trazer à sociedade como um todo (LORENZ *et alii*, 2023, p. 26-27).

O quinto risco é o de ciberataques automatizados e personalizados, nos quais instrumentos de IA generativa podem, em um círculo vicioso, ser treinados para operações cada vez mais sofisticadas (LORENZ et alii, 2023, p. 7). Nesse sentido, os países do G7, no Processo de Hiroshima, declararam que esses riscos de cibersegurança associados a esses instrumentos são uma preocupação (OCDE, 2023, p. 24). Em publicação recente, conseguiu-se demonstrar, para fins de prova de conceito com intuito informacional, que é possível, por exemplo, empregar o Chat GPT para que um *malware* possa tanto reescrever seu próprio código e diminuir as chances de detecção de antivírus como reescrever o e-mail de propagação para conseguir mais facilmente engajar o usuário na abertura dessa mensagem (ZIMMERMAN; ZOLLIKOFER, 2024).

O sexto risco é o de violação a direitos de propriedade intelectual, em que diversas ferramentas de aplicação de IA baseadas em linguagem natural incluíram marcas, patentes, canções, filmes, fotos e outros elementos protegidos por *copyright* em seus dados de treinamento sem o consentimento dos seus titulares. Esse risco também pode ocorrer pela geração de conteúdo semelhante, ainda que não idêntico, àquele protegido por *copyright* (NIST, 2024a, p. 8-9). Esse ponto tem sido objeto de preocupação específica na Organização Mundial de Propriedade Intelectual (OMPI), nos EUA e na Europa (OCDE, 2023, p. 23; LORENZ *et alii*, 2023, p. 19-20).

O sétimo risco é associado aos impactos da IA Generativa no mercado de trabalho.

Uma vertente desse risco é relacionada ao excesso de dependência em relação a essas ferramentas, que tende a ser crescente à medida que sua assertividade aumenta, como resultado da sofisticação dos processos de treinamento dos modelos baseados em linguagem natural.

É possível, inclusive, que isso comprometa o desenvolvimento de competências e habilidades pelas pessoas, que podem passar a ficar cada vez mais habituadas ao uso da IA Generativa. De igual forma, não se ignora a possibilidade de perda dessas competências e habilidades pelo desuso. E esse processo tende a se intensificar com o aumento das capacidades das ferramentas baseadas em linguagem natural.

Há indícios de que ferramentas de IA tendem a gerar efeitos mais pronunciados em ocupações que demandem competências mais elementares. Anota-se, ainda, que ferramentas de IA Generativa têm apresentado desempenho notável em testes de aptidão profissional, como os *Bar exams* nos Estados Unidos (LORENZ *et alii*, 2023, p. 27).

Ademais, é possível que a IA como um todo, não apenas a generativa, promova uma substituição massiva de empregos, com o potencial de criar uma espiral de desaceleração econômica decorrente da diminuição de circulação de riqueza que essa substituição pode proporcionar (ROUBINI, 2023, p. 238 *et seq.*).

O oitavo está relacionado à pegada ambiental e ao consumo dos recursos naturais necessários para as quantidades imensas de poder computacional que são exigidas para a aprendizagem profunda de máquina (LORENZ *et alii*, 2023, p. 27-28; NIST, 2024a, p. 6-7), em que se estima que o treinamento de um único modelo transformador de IA generativa pode emitir tanto carbono quanto o gerado por um passageiro em trezentos voos de ida e volta entre as cidades de São Francisco e Nova York (STRUBELL *et alii*, 2019).

Aliás, com essa percepção, o Conselheiro Diretor Alexandre Freire, durante a instrução do processo de revisão do R-Ciber, determinou, por meio do Ofício nº 16/2024/AF-ANATEL, a realização de estudo relacionado à pegada ambiental decorrente do uso de *data centers* em seus mais diversos matizes: consumo de energia, de água, depleção de recursos naturais para a produção de novos componentes mais sofisticados *etc.*

O nono risco é o de desalinhamento de propósitos, em que os sucessivos processos de aperfeiçoamento e aprendizagem das ferramentas de IA Generativa podem fazer com que elas passem a operar com outras finalidades, distintas daquelas que idealizaram a sua aplicação (LORENZ *et alii*, 2023, p. 27-28).

À luz dos riscos potenciais da inteligência artificial para a infraestrutura das telecomunicações, durante a relatoria do processo de Revisão do R-Ciber, o Conselheiro Diretor Alexandre Freire, por meio do Ofício nº 15/2024/AF-ANATEL, determinou diligência à sua área técnica, para a produção de diagnósticos e de estudos voltados ao fortalecimento das medidas de segurança cibernética.

Em resposta, a área técnica, no Informe nº 30/2024/SUE, além de destacar os potenciais usos e vantagens das ferramentas de IA, inclusive na segurança das redes, pontua tanto os riscos de amplificação de ameaças já existentes como o de surgimento de novas outras, num contexto que merece especial atenção em virtude da presença de infraestruturas críticas nas redes de telecomunicações.

Igualmente, identificou, dentre outros, os seguintes pontos de preocupação: opacidade algorítmica, envenenamento de dados e emprego de IA Generativa nos ataques à infraestrutura de rede.

No Informe em comento, são citados, como exemplos de pontos de atenção: a modulação e demodulação de sinal com recursos de IA no uso do espectro; o uso de veículos autônomos orientados por sistemas de IA, que podem conter alguma vulnerabilidade e podem ser influenciados com algum tipo de padrão semântico inesperado a partir de amostras adversariais (intencionais ou não); o emprego de arquiteturas *Open Ran*, com uma gestão por *software* e com o emprego de IA cada vez mais intensos na sua orquestração, o que aumenta a superfície de ataque na infraestrutura de conectividade e, por consequência, pode criar novas vulnerabilidades.

Ao proceder a um levantamento junto aos prestadores quanto ao uso de IA, a área técnica, no Informe em comento, noticia que "as iniciativas concretas das prestadoras no combate aos riscos da IA são limitadas ao uso interno de tais ferramentas, sob o argumento da possibilidade de vazamento ou espionagem de informações sensíveis – não apenas informações pessoais de usuários, como também estratégias comerciais", e acrescenta que a "proibição de uso pelos colaboradores de ferramentas de IA generativa disponibilizadas por terceiros, eventualmente seguida da oferta de alternativa desenvolvida internamente, figura como ação mais assertiva registrada".

Anota-se, ainda, que não há uniformidade nas iniciativas de governança das prestadoras e que elas alegam que vêm desenvolvendo ações de capacitação de seus colaboradores.

No que diz respeito à segurança e resposta a incidentes, as prestadoras informam adotar o funcionamento de *Security Operation Centers - SOC*. No entanto, a área técnica destaca que os processos de governança e os manuais ainda teriam um caráter generalista.

Os riscos da IA, especialmente da generativa, para a segurança das redes, como se pode ver, ainda demandam um maior estudo para uma compreensão mais precisa do que é possível ser feito, de modo que se preservem a integridade do ecossistema digital e os direitos dos consumidores, mas com o espaço necessário para que se estimule devidamente a inovação em uma seara cada vez mais disruptiva, em que os reguladores no mundo inteiro ainda estão procedendo a diversas avaliações de cenário para calibrarem e harmonizarem suas abordagens.

Além dessas diligências, a Anatel e o seu Centro de Altos Estudos em Comunicações Digitais e Inovações Tecnológicas (Ceadi), presidido pelo Conselheiro Diretor Alexandre Freire, promoveram diversos eventos voltados ao aprimoramento da compreensão sobre o tema, destacando-se os seguintes:

1. em outubro de 2023, o "Ciclo de Palestras sobre Tecnologias Emergentes e as Comunicações do Futuro - Desafios Legais em Inteligência Artificial (IA)", que contou com a participação das Professoras Dora Kaufman e Laura Schertel Mendes, dentre outros;

2. em março de 2024, o simpósio "Infraconnect", realizado em conjunto com a Agência Nacional de Transportes Terrestres (ANTT), em que se discutiram, dentre outros pontos, as relações entre os impactos da IA, as redes de telecomunicações e a cadeia de logística; e

3. em abril de 2024, o simpósio "Tecnologias Emergentes e as Comunicações do Futuro: Aplicações de Inteligência Artificial no mercado", que contou com a presença dos Professores Priscila Solís e Anderson Rocha, dentre outros.

Por sua vez, o Ceadi firmou parceria com o Instituto Tecnológico da Aeronáutica (ITA) para a entrega de produtos (*workshops*, estudos *etc.*) voltados a "elucidar e trazer contribuições sobre o uso de IA em diferentes ambientes de telecomunicações para torná-los mais eficientes, seguros e adaptados às necessidades em constante evolução", sendo composto por seis eixos, com previsão de conclusão para dezembro de 2025:

1. estimação do Índice de Qualidade de Serviço (IQS);

2. avaliação da relação entre qualidade de serviço (QoS) e capacidade da infraestrutura;

3. detecção e mitigação de ameaças à cibersegurança com uso de IA e *Machine Learning* (ML);

4. monitoramento de espectro;

5. monitoramento eficaz dos *marketplaces*; e

6. análise de redes sociais para detecção de interrupção de serviços com base na satisfação do usuário.

Além disso, o Ceadi vem promovendo diversas ações de capacitação dos servidores da Anatel, vez que a IA é um tema de fronteira, demandando o aperfeiçoamento do seu capital humano para adequadamente endereçar os desafios que ela já traz para o setor de telecomunicações.

Dentre as ações empreendidas, cita-se a parceria desenvolvida entre o Ceadi e a Kennedy School da Universidade de Harvard (Processo nº 53500.084654/2023-16), em que oito servidores da Anatel participaram do curso de aperfeiçoamento "Cybersecurity: The intersection of policy and technology".

Na Anatel, mesmo após a aprovação da revisão do R-Ciber, esses estudos serão continuados pelo Comitê de Infraestrutura de Telecomunicações, presidido pelo Conselheiro Diretor Alexandre Freire, e pelas suas diversas Superintendências competentes para o trato da matéria, com vistas à avaliação de novas inserções relacionadas à cibersegurança das redes na suas agendas regulatórias futuras.

Referências

AYRES PINTO, Danielle Jacon; GRASSI, Jéssica Maria. Guerra cibernética, ameaças às infraestruturas críticas e a defesa cibernética do Brasil. **Revista Brasileira de Estudos de Defesa**, Brasil, v. 7, p. 103-131, 2020. Disponível em: https://rbed.abedef.org/rbed/article/view/75178. Acesso em: 29 maio 2024.

AYRES PINTO, Danielle Jacon; MEDEIROS, Sabrina Evangelista. Cabos submarinos e segurança cibernética no Atlântico. **Atlantic Centre**, n. 11, mar. 2022. Disponível em: https://www.researchgate.net/publication/360199322_Cabos_submarinos_e_seguranca_cibernetica_no_Atlantico. Acesso em: 3 jun. 2024.

BENUSSI, Nicolò; BOTEVA, Mirela; MARZIONNA, Barbara Marchiori de Assis; ONYETT, Jake Stephen; TESAURO, Giulia. **Guiding principles for ICT regulators to enhance cyber resilience**. 2024. Disponível em https://digitalregulation.org/guiding-principles-for-ict-regulators-to-enhance-cyber-resilience/ Acesso em: 29 maio 2024.

BRADFORD, Anu. **Digital Empires.** Oxford: Oxford University Press, 2023.

BRASIL. Agência Nacional de Telecomunicações. **Ato nº 6539, de 18 de outubro de 2019**. Diário Oficial da União: Seção 1, Brasília, DF, Ano 157, v. 204, p. 14, 21 out. 2019. Disponível em https://www.in.gov.br/web/dou/-/ato-n-6.539-de-18-de-outubro-de-2019-222818608. Acesso em: 20 abr. 2024

_____. Agência Nacional de Telecomunicações. **Resolução nº 740, de 21 de dezembro de 2020**. Aprova o Regulamento de Segurança Cibernética Aplicada ao Setor de Telecomunicações. Diário Oficial da União: Seção 1, Brasília, DF, Ano 158, v. 246, p. 55-57. 24 dez. 2020a. Disponível em: https://www.in.gov.br/web/dou/-/resolucao-n-740-de-21-de-dezembro-de-2020-296152776. Acesso em: 20 abr. 2024.

_____. Agência Nacional de Telecomunicações**. Anatel torna públicos documentos preparatórios da revisão do Regulamento de Segurança Cibernética**. 2023a. Disponível em: https://www.gov.br/anatel/pt-br/assuntos/noticias/anatel-torna-publicos-documentos-preparatorios-da-revisao-do-regulamento-de-seguranca-cibernetica. Acesso em: 25 abr. 2024.

_____. Agência Nacional de Telecomunicações (Anatel). **Análise nº 4/2024/AF, no processo nª 53500.023403/2022-76**. Relator: Conselheiro Alexandre Freire. Brasília, 2024c. Disponível em: https://sei.anatel.gov.br/sei/modulos/pesquisa/md_pesq_documento_consulta_externa.php?8-74Kn1tDR89f1Q7RjX8EYU46IzCFD26Q9Xx5QNDbqYKt8cnnVHZauBP_NyhM1CSBcgVEn7mux3ovGt01wPurwqzRzDpDr8_hhPaviUHAJMWnN5WxM53TLMbSWsufdYS. Acesso em 20 maio 2024.

_____. Ministério da Ciência, Tecnologia e Inovação. **Estratégia Brasileira para a Transformação Digital (E-Digital)**. Ciclo 2022-2026. Brasília, 2022. Disponível em: https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/transformacaodigital/arquivosestrategiadigital/e-digital_ciclo_2022-2026.pdfhttps://www.gov.br/mcti/pt-br/acompanhe-o-mcti/transformacaodigital/arquivosestrategiadigital/e-digital_ciclo_2022-2026.pdf. Acesso em: 25 abr. 2024.

BRASIL. Ministério da Gestão e da Inovação em Serviços Públicos. Estratégias e Governança Digital. Transformação Digital. Central de Qualidade. **Painel de monitoramento de serviços federais.** 2024a. Disponível em: https://www.gov.br/governodigital/pt-br/estrategias-e-governanca-digital/transformacao-digital/central-de-qualidade/painel-de-monitoramento-de-servicos-federais#ancora-geral. Acesso em 25 abr. 2024.

_____. Presidência da República. **Decreto nº 9.637, de 26 de dezembro de 2018**. Institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação, e altera o Decreto nº 2.295, de 4 de agosto de 1997,

que regulamenta o disposto no art. 24,caput,inciso IX, da Lei nº 8.666, de 21 de junho de 1993, e dispõe sobre a dispensa de licitação nos casos que possam comprometer a segurança nacional.. Disponível em: https://www.in.gov.br/web/dou/-/decreto-n-9-637-de-26-de-dezembro-de-2018-56969938. Acesso em: 22 maio 2024.

_____. Presidência da República. **Decreto nº 10.222, de 5 de fevereiro de 2020**. Aprova a Estratégia Nacional de Segurança Cibernética. Diário Oficial da União: Seção 1, Brasília, DF, Ano 157, v. 26, p. 6, 06 fev. 2020. Disponível em: https://www.in.gov.br/web/dou/-/decreto-n-10.222-de-5-de-fevereiro-de-2020-241828419. Acesso em: 22 maio 2024.

_____. Presidência da República. Gabinete de Segurança Institucional. **Portaria GSI/PR nº 93, de 18 de outubro de 2021**. Aprova o glossário de segurança da informação. Diário Oficial da União: Seção 1, Brasília, DF, Ano 159, v. 197, p. 36. 19 out. 2021. Disponível em: https://www.in.gov.br/en/web/dou/-/portaria-gsi/pr-n-93-de-18-de-outubro-de-2021-353056370. Acesso em: 22 maio 2024.

_____. Presidência da República. **Decreto nº 11.856, de 26 de dezembro de 2023**. Institui a Política Nacional de Cibersegurança e o Comitê Nacional de Cibersegurança. Diário Oficial da União: Seção 1, Brasília, DF, Ano 159, v. 245, p. 10, 27 dez. 2023. Disponível em: https://www.in.gov.br/web/dou/-/decreto-n-11.856-de-26-de-dezembro-de-2023-533845289. Acesso em: 22 maio 2024.

_____. Presidência da República. Gabinete de Segurança Institucional. **Portaria nº 6, de 9 de fevereiro de 2024**. Diário Oficial da União: Seção 2, Brasília, DF, Ano 165, v. 39, p. 4. 14 fev. 2024. Disponível em: https://www.in.gov.br/web/dou/-/portaria-n-6-de-9-de-fevereiro-de-2024-542752145. Acesso em: 22 maio 2024.

_____. Presidência da República. Gabinete de Segurança Institucional. **Comitê Nacional de Cibersegurança**. 2024b. Disponível em: https://www.gov.br/gsi/pt-br/colegiados-do-gsi/comite-nacional-de-ciberseguranca-cnciber. Acesso em: 22 maio 2024.

CLARK, Adam. **Cybersecurity in the UK**. London: House of Commons Library, 2024. Disponível em: https://researchbriefings.files.parliament.uk/documents/CBP-9821/CBP-9821.pdf. Acesso em: 30 abr. 2024.

COPENHAGEN ECONOMICS. **The Economic Impact of the forthcoming Equiano Subsea Cable in Portugal**: Forecasting the effect of enhanced connectivity infrastructure on trade and growth. 2021. Disponível em: https://copenhageneconomics.com/wp-content/uploads/2021/12/copenhagen-economics-impact-of-forthcoming-equiano-subsea-cable_may2021.pdf. Acesso em: 25 mar. 2023.

CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY (CISA). **Cybersecurity Framework Implementation Guidance.** 2020. Disponível em: https://www.cisa.gov/sites/default/files/publications/Commercial_Facilities_Sector_Cybersecurity_Framework_Implementation_Guidance_FINAL_508.pdf. Acesso em: 04 maio 2024.

COMITÊ GESTOR DA INTERNET NO BRASIL (CGI.br). Documentos da Cúpula Mundial sobre a Sociedade da Informação. **Cadernos CGI.br Referências**, São Paulo, v. 1, 2014. Disponível em: https://www.cgi.br/media/docs/publicacoes/1/CadernosCGIbr_DocumentosCMSI.pdf. Acesso em: 29 maio 2024.

DINIZ, Augusto. Nvidia é o grande expoente do fenômeno que é a inteligência artificial, diz analista. **Infomoney**, 23 maio 2024. Disponível em: https://www.infomoney.com.br/mercados/nvidia-grande-expoente-fenomeno-inteligencia-artificial-analista/. Acesso em: 24 maio 2024.

ELECTRONIC COMMUNICATIONS RESILIENCE AND RESPONSE GROUP (EC-RRG). **Resilience Guidelines for Providers of Critical National Telecommunications Infrastructure**. 2018. Disponível em : https://assets.publishing.service.gov.uk/media/5b8d385bed915d1ebd71502c/EC-RRG_Resilience_Guidelines_v2.0.pdf. Acesso em: 28 maio 2024.

EUROPEAN COMMISSION (EC). **Directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive) – FAQs.** Bruxelas, 2023. Disponível em: https://digital-strategy.ec.europa.eu/en/faqs/directive-measures-high-common-level-cybersecurity-across-union-nis2-directive-faqs. Acesso em: 23 mar. 2024.

_____. **Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions.** Bruxelas, 2023a. Disponível em: https://data.consilium.europa.eu/doc/document/ST-13558-2023-INIT/en/pdf. Acesso em: 23 mar. 2024.

_____. **White Paper: How to master Europe's digital infrastructure needs?** Bruxelas, 2024. Disponível em: https://ec.europa.eu/newsroom/dae/redirection/document/102533. Acesso em: 23 mar. 2024.

EUROPEAN PARLIAMENT (EP). **The NIS2 Directive -** A high common level of cybersecurity in the EU. 2023. Disponível em: https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/689333/EPRS_BRI(2021)689333_EN.pdf. Acesso em: 23 mar. 2024.

_____. **Artificial Intelligence Act:** MEPs adopt landmark law. 2024. Disponível em: https://www.europarl.europa.eu/news/en/press-room/20240308IPR19015/artificial-intelligence-act-meps-adopt-landmark-law. Acesso em: 02 jul. 2024.

EUROPEAN UNION AGENCY FOR CYBERSECURITY (ENISA). **Cloud cybersecurity market analysis**. 2023. Disponível em : https://www.enisa.europa.eu/publications/cloud-cybersecurity-market-analysis/@@download/fullReport. Acesso em: 28 mar. 2024.

_____. **Home Topics. Training and Exercises. Cyber Exercises. Cyber Europe**. 2024. Disponível em: https://www.enisa.europa.eu/topics/training-and-exercises/cyber-exercises/cyber-europe-programme. Acesso em: 31 maio 2024.

FEDERAL COMMUNICATIONS COMISSION (FCC). **Network Reliability Resources**. 2022. Disponível em: https://www.fcc.gov/network-reliability-resources. Acesso em 30 maio 2024.

_____. **Communications Security, Reliability, and Interoperability Council**. 2023. Disponível em: https://www.fcc.gov/about-fcc/advisory-committees/communications-security-reliability-and-interoperability-council-0. Acesso em: 30 maio 2024.

_____. **Cybersecurity and Communications Reliability Division, Public Safety and Homeland Security Bureau**. 2024. Disponível em: https://www.fcc.gov/cybersecurity-and-communications-reliability-division-public-safety-and-homeland-security-bureau. Acesso em: 30 maio 2024.

_____. **Disaster Information Reporting System (DIRS)**. 2024a. Disponível em: https://www.fcc.gov/general/disaster-information-reporting-system-dirs-0#block-menu-block-4s. Acesso em: 30 maio 2024.

_____. **Wireless Network Resiliency During Disasters**. 2024b. Disponível em: https://www.fcc.gov/wireless-network-resiliency-during-disasters. Acesso em: 30 maio 2024.

_____. **FCC creates voluntary cybersecurity labeling program for smart products**. 2024c. Disponível em: https://docs.fcc.gov/public/attachments/DOC-401201A1.pdf. Acesso em: 30 maio 2024.

FREILICH, Charles; COHEN, D. Matthew S.; SIBONI, Gabi. **Israel and the Cyber Threat**: How the Startup Nation Became a Global Cyber Power. Oxford: Oxford University Press, 2023. Edição do Kindle.

FREITAS, Luciano Charlita de; GUTERRES, Egon, Cervieri; MORAIS, Leonardo Euler de; MOURA FILHO, Ronaldo Neves de; TALOUKI, Mariana Almeida de Sousa. Regulamentação da segurança cibernética das telecomunicações no Brasil: um balanço de incentivos em um contexto de neutralidade tecnológica, **Revista Latinoamericana de Economía y Sociedad Digital**, n. 2, ago. 2021. Disponível em: https://revistalatam.digital/article/210216-3/. Acesso em: 28 maio 2024.

HUREL, Louise Marie. Cibersegurança no Brasil: uma análise da estratégia nacional. **Instituto Igarapé - Artigo Estratégico 54**, Abr. 2021. Disponível em: https://igarape.org.br/wp-content/uploads/2021/04/AE-54_Seguranca-cibernetica-no-Brasil.pdf. Acesso em: 03 jun. 2024.

INTERNATIONAL TELECOMMUNICATIONS UNION (ITU). **Mandate**. 2022. Disponível em: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/about-cybersecurity.aspx. Acesso em: 28 maio 2024.

_____. **Global Digital Regulatory Outlook 2023:** Policy and regulation to spur digital transformation. Genebra: ITU Publications, 2023. Disponível em: https://www.itu.int/dms_pub/itu-d/opb/pref/D-PREF-BB.REG_OUT01-2023-PDF-E.pdf. Acesso em: 29 maio 2024.

_____. **Cybersecurity Assurance Practices**. 2023a. Disponível em: https://www.itu.int/dms_pub/itu-d/opb/stg/d-stg-sg02.03.2-2023-pdf-e.pdf. Acesso em: 29 maio 2024.

_____. **ITU-D Cybersecurity**. 2024. Disponível em: https://www.itu.int/itu-d/sites/cybersecurity/. Acesso em: 28 maio 2024.

_____. **SG17 - Security**. 2024a. Disponível em: https://www.itu.int/en/ITU-T/studygroups/2022-2024/17/Pages/default.aspx. Acesso em: 28 maio 2024.

ISC2. **Cybersecurity Workforce Study**: How the Economy, Skills Gap and Artificial Intelligence are Challenging the Global Cybersecurity Workforce. 2023. Disponível em: https://media.isc2.org/-/media/Project/ISC2/Main/Media/documents/research/ISC2_Cybersecurity_Wo

rkforce_Study_2023.pdf?rev=28b46de71ce24e6ab7705f6e3da8637e. Acesso em 20 maio 2024.

KISSINGER, Henry A; SCHMIDT, Eric; HUTTENLOCHER, Daniel. **The Age of AI**: And Our Human Future. New York: Little, Brown and Company, 2021. Edição do Kindle.

KNESSET. **Approved in final readings: Bill authorizing Cyber Directorate, Israeli Security Agency and Director of Security of the Defense Establishment to instruct digital or storage service supplier to take measures to detect, prevent, or contain cyber-attack**. 2023. Disponível em: https://main.knesset.gov.il/en/news/pressreleases/pages/press261223q.aspx. Acesso em 01 jul. 2024.

LORENZ, Philippe; PERSET, Karine; BERRYHILL, Jamie. **Initial policy considerations for generative artificial intelligence**, OECD Artificial Intelligence Papers, No. 1. Paris OECD Publishing, Paris, 2023. Disponível em: https://doi.org/10.1787/fae2d1e6-en. Acesso em 20 fev. 2024.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). **Artificial Intelligence Risk Management Framework (AI RMF 1.0).** 2023. Disponível em: https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf. Acesso em: 16 jul. 2024.

_____. **The NIST Cybersecurity Framework (CSF) 2.0.** 2024. Disponível em: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf. Acesso em: 02 maio. 2024.

_____. **Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile** (initial public draft). 2024a. Disponível em : https://airc.nist.gov/docs/NIST.AI.600-1.GenAI-Profile.ipd.pdf. Acesso em: 16 jul. 2024.

OLIVEIRA, Cristina Godoy Bernardo de. Desafios de regulação do digital e da inteligência artificial no Brasil. **Revista USP**, n. 135, out.-dez. 2022. Disponível em: https://www.revistas.usp.br/revusp/article/view/206257/189893. Acesso em: 3 jun. 2024.

ORGANIZAÇÃO DOS ESTADOS AMERICANOS (OEA). **Revisão da Capacidade de Cibersegurança** – República Federativa do Brasil. 2020. Disponível em: https://www.gov.br/gsi/pt-br/ssic/estrategia-nacional-de-seguranca-cibernetica-e-ciber/cmm-report-brazil-2023_final_pt.pdf/@@download/file. Acesso em: 25 abr. 2024.

ORGANIZAÇÃO PARA A COOPERAÇÃO E DESENVOLVIMENTO ECNONÔMICO (OCDE). **OECD Guidelines for the Security of Information Systems**. Paris, 1992. Disponível em: https://web-archive.oecd.org/2012-06-14/83193-oecdguidelinesforthesecurityofinformationsystems1992.htm. Acesso em: 28 maio 2024.

____. **Recommendation of the Council concerning Guidelines for Cryptography Policy**. Paris, 1997. Disponível em: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0289. Acesso em: 28 maio 2024.

____. **OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security**. Paris, 2002. Disponível em: https://web-archive.oecd.org/2015-10-28/80523-oecdguidelinesforthesecurityofinformationsystemsandnetworkstowardsacultureofsecurity.htm. Acesso em: 28 maio 2024.

____. **Recommendation of the Council on Digital Security of Critical Activities**. Paris, 2019. Disponível em: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0456. Acesso em: 28 maio 2024.

____.**Recommendation of the Council on Digital Security Risk Management**. Paris, 2022a. Disponível em: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0479. Acesso em: 26 abr. 2024.

____. **OECD Policy Framework on Digital Security**. Cybersecurity for Prosperity. Paris: OECD publishing, 2022b. Disponível em: https://read.oecd-ilibrary.org/science-and-

technology/oecd-policy-framework-on-digital-security_a69df866-en#page2. Acesso em: 28 mai. 2024.

____. **Recommendation of the Council on National Digital Security Strategies**. Paris, 2022c. Disponível em: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0480. Acesso em: 28 maio 2024.

____. **Recommendation of the Council on the Digital Security of Products and Services**. Paris, 2022d. Disponível em: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0481. Acesso em: 28 maio 2024.

____. **Recommendation of the Council on the Treatment of Digital Security Vulnerabilities**. Paris, 2022e. Disponível em: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0482. Acesso em: 28 maio 2024.

_____. **G7 Hiroshima Process on Generative Artificial Intelligence (AI)**: Towards a G7 Common Understanding on Generative AI. Paris: OECD Publishing, 2023. Disponível em: https://doi.org/10.1787/bf3c0c60-en. Acesso em 10 jul. 2024.

_____. **Generative artificial intelligence in finance -** OECD Artificial Intelligence Papers, No. 9. Paris: OECD Publishing, 2023a. Disponível em: https://doi.org/10.1787/ac7149cc-en. Acesso em 10 jul. 2024.

_____. **AI, data governance and privacy: Synergies and areas of international co-operation** - OECD Artificial Intelligence Papers, No. 22. Paris: OECD Publishing, 2024. Disponível em: https://doi.org/10.1787/2476b1a4-en. Acesso em 10 jul. 2024.

OFFICE OF COMMUNICATIONS (OFCOM). **Ofcom guidance on resilience requirements imposed by or under sections 105A to D of the Communications Act 2003**. Disponível em: https://www.ofcom.org.uk/__data/assets/pdf_file/0022/253750/Ofcom-guidance-on-resilience-requirements-imposed-by-or-under-sections-105A-to-D-of-the-Communications-Act-2003.pdf. Acesso em: 28 maio 2024.

_____. **Our network security and network resilience work**. 2023. Disponível em: https://www.ofcom.org.uk/phones-telecoms-and-internet/information-for-industry/network-security-and-resilience/our-work. Acesso em: 28 maio 2024.

_____. **Guidance for the digital infrastructure Subsector** - Statutory guidance under the Network and Information Systems Regulations 2018: Revised NIS Guidance. 2023a. Disponível em: https://www.ofcom.org.uk/__data/assets/pdf_file/0019/262090/Ofcom-Network-and-Information-Systems-Guidance.pdf. Acesso em: 28 maio 2024.

PORTUGAL. **Resolução do Conselho de Ministros nº 42/2012**. 2012. Disponível em: https://diariodarepublica.pt/dr/detalhe/resolucao-conselho-ministros/42-2012-552560. Acesso em: 31 maio 2024.

_____. **Decreto-Lei nº 136/2017**. 2017. Disponível em: https://diariodarepublica.pt/dr/detalhe/decreto-lei/136-2017-114152775. Acesso em 31 maio 2024.

_____. **Lei nº 46/2018**. 2018. Disponível em: https://diariodarepublica.pt/dr/detalhe/lei/46-2018-116029384. Acesso em: 31 maio 2024.

_____. Autoridade Nacional de Comunicações. **Regulamento nº 303/2019**. 2019. Disponível em: https://www.anacom.pt/render.jsp?contentId=1469920. Acesso em: 31 maio 2024.

_____. **Decreto-Lei nº 65/2021**. 2021. Disponível em: https://diariodarepublica.pt/dr/detalhe/decreto-lei/65-2021-168697988. Acesso em: 31 maio 2024.

_____. Centro Nacional de Cibersegurança. **Guia para Gestão dos Riscos em matérias de Segurança da Informação e Cibersegurança**. 2022. Disponível em: https://www.cncs.gov.pt/docs/guia-de-gestao-dos-riscos11.pdf. Acesso em: 31 maio 2024.

_____. Autoridade Nacional de Comunicações. **O Conselho de Administração**. 2024. Disponível em: https://www.anacom.pt/render.jsp?categoryId=377881. Acesso em: 31 maio 2024.

STATE OF ISRAEL. Prime Minister's Office .National Cyber Directorate. **National Cyber Security Strategy In Brief**. 2017. Disponível em: https://cyber.haifa.ac.il/images/pdf/cyber_english_A5_final.pdf. Acesso em: 20 jun. 2024.

_____. Prime Minister's Office .National Cyber Directorate. **Use of Cloud Services** - Addendum to the Cyber Defense Methodology for an Organization. 2017a. Disponível em: https://www.gov.il/BlobFolder/policy/cloud_services/en/Use%20of%20Cloud%20Services%20En.pdf. Acesso em: 20 jun. 2024.

_____. Prime Minister's Office. National Cyber Directorate. **Best Practice : Reducing cyber security risks in video surveillance cameras**. 2018. Disponível em: https://www.gov.il/BlobFolder/policy/iotcameras/en/Security%20Cameras_575480_Sharon3_EN_WEB%20-%20%D7%9E%D7%95%D7%A0%D7%92%D7%A9.pdf. Acesso em: 20 jun. 2024.

_____. Prime Minister's Office. National Cyber Directorate. **Regulating Supply Chain Cyber Defense in the Israeli Economy**. 2021. Disponível em: https://www.gov.il/BlobFolder/generalpage/expsupplychain/en/Supply%20chain.pdf. Acesso em: 20 jun. 2024.

_____. Prime Minister's Office. National Cyber Directorate **Iron Swords" War in Cyber Sphere :** Insights, Recommendations and Mitigations. 2024. Disponível em: https://www.gov.il/BlobFolder/reports/publish_2412/en/report2412en.pdf. Acesso em: 20 jun. 2024.

ROUBINI, Nouriel. **Mega-ameaças**: dez perigosas tendências que ameaçam nosso futuro e como sobreviver a elas. Trad. Maria de Fátima Oliva do Couto. São Paulo: Planeta do Brasil, 2023. Formato kindle.

STATISTA.COM. **Nvidia specialized market revenue worldwide from fiscal year 2019 to 2025, by quarter**. 2024. Disponível em: https://www.statista.com/statistics/1120484/nvidia-quarterly-revenue-by-specialized-market/. Acesso em: 24 maio 2024.

STRUBELL, Emma; GANESH, Ananya; MCCALLUM, Andrew. **Energy and Policy Considerations for Deep Learning in NLP**. 2019. Disponível em: https://arxiv.org/pdf/1906.02243. Acesso em 16 jul. 2024.

TAKAHASHI, Tadao (org.). **Sociedade da informação no Brasil**: Livro Verde. Brasília: Ministério da Ciência e Tecnologia, 2000. Disponível em: http://livroaberto.ibict.br/bitstream/1/434/1/Livro%20Verde.pdf. Acesso em: 24 abr. 2024.

THE WHITE HOUSE. **Fact Sheet: President Biden Issues Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence**. Washington, 2023. Disponível em : https://www.whitehouse.gov/briefing-room/statements-releases/2023/10/30/fact-sheet-president-biden-issues-executive-order-on-safe-secure-and-trustworthy-artificial-intelligence/. Acesso em 30 jun. 2024.

UK DEPARTMENT FOR SCIENCE, INNOVATION AND TECHNOLOGY (DSIT). **Protecting and enhancing the security and resilience of UK data infrastructure**. Londres: 2023. Disponível em: https://assets.publishing.service.gov.uk/media/657ab6f6254aaa000d050ce2/protecting_and_enhancing_the_security_and_resilience_of_UK_data_infrastructure.pdf. Acesso em: 25 mar. 2024.

VASSILEV, Apostol; OPREA, Alina; FORDYCE, Alie; ANDERSON, Hyrum. **Adversarial Machine Learning**: A Taxonomy and Terminology of Attacks and Mitigations - NIST Artifcial Intelligence (AI) Report, NIST Trustworthy and Responsible AI. NIST AI 100-2e2023. Gaithersburg, MD: National Institute of Standards and Technology, 2024. Disponível em: https://doi.org/10.6028/NIST.AI.100-2e2023. Acesso em 10 jul. 2024.

WORLD ECONOMIC FORUM (WEF). **The Global Risks Report.** 2024. Disponível em: https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2024.pdf. Acesso em: 25 abr. 2024.

ZIMMERMAN, Benjamin; ZOLLIKOFER, David. **Synthetic Cancer - Augmenting Worms with LLMs**. 2024. Disponível em: https://arxiv.org/pdf/2406.19570. Acesso em 13 jul. 2024.

Siga a Anatel

ANATEL