Nota técnica:

Minuta de Anteprojeto da Lei Geral de Cibersegurança do Comitê Nacional de Cibersegurança (CNCiber)[1]

A minuta de anteprojeto de Lei Geral de Cibersegurança, elaborada pelo Comitê Nacional de Cibersegurança (CNCiber), busca estruturar um marco normativo mais abrangente para a política de cibersegurança no Brasil. O texto parte de um diagnóstico já conhecido: o aumento da digitalização vem acompanhado de riscos crescentes, enquanto a resposta institucional ainda é fragmentada. Nesse contexto, a proposta tenta organizar princípios, objetivos e instrumentos que deem mais coerência à atuação estatal e à articulação com o setor privado.

Entre os princípios elencados, aparecem a soberania nacional, a privacidade, o sigilo das comunicações, a resiliência institucional e a cooperação entre diferentes atores. Também há referência à promoção da inovação e ao desenvolvimento tecnológico nacional. No campo dos direitos, o texto reafirma garantias como liberdade de expressão, acesso à informação, proteção de dados pessoais e inviolabilidade das comunicações - esta última alinhada ao art. 5º da Constituição, que só admite restrição mediante ordem judicial.

Nesta nota técnica, o objetivo é examinar pontos sensíveis da minuta sob a perspectiva da governança da Internet, da proteção de direitos fundamentais e da coerência sistêmica com o ordenamento brasileiro vigente, em particular, o Marco Civil da Internet (MCI), a Lei Geral de Proteção de Dados (LGPD) e o arranjo multissetorial consolidado em torno do Comitê Gestor da Internet no Brasil (CGI.br). A análise não pretende esgotar a discussão sobre o anteprojeto, mas oferecer subsídios para o aperfeiçoamento da proposta nos pontos em que o texto, em sua redação atual, pode gerar insegurança jurídica, sobreposição regulatória ou redução do nível de proteção a direitos.

1. Escopo de aplicação

[1] Esta contribuição técnica foi elaborada por Luiza Dutra (Instituto de Referência em Internet e Sociedade — IRIS) com revisão interna do Grupo de Trabalho sobre Criptografia da Internet Society Capítulo Brasil (ISOC Brasil), representado por Thobias Prado e Pedro Amaral, e de Fernanda Rodrigues e Rafaela Ferreira (IRIS).

Apesar da pretensão estruturante, alguns pontos da minuta deixam dúvidas importantes. Um deles é o próprio alcance da lei. O art. 6º estabelece como agentes obrigados os operadores de infraestruturas críticas, os provedores de serviços essenciais e os entes federativos com mais de cem mil habitantes — e estende a aplicação aos fornecedores diretos e indiretos da cadeia de suprimentos desses agentes. A lista de serviços essenciais, no parágrafo único do art. 2º, abrange dezesseis setores, incluindo a categoria "infraestruturas digitais", que reúne data centers, serviços de nuvem, provedores de infraestrutura de tráfego da Internet, DNS, registros de TLD (Top-Level Domain), CDNs (Content Delivery Networks), prestadores de serviços de confiança e provedores de serviços gerenciados.

A minuta não especifica, porém, como - ou até que ponto - esse desenho se aplica ao restante dos prestadores de serviço que atuam na camada de aplicação. Essa indefinição pode gerar lacunas ou sobreposições com outros marcos já existentes, como o Marco Civil da Internet, a LGPD e regimes setoriais já consolidados. A questão se torna ainda mais sensível quando se observa que a minuta cria uma autoridade nacional de cibersegurança com competências regulatórias, de fiscalização e sancionatórias amplas, sem um mapeamento claro de como essas competências dialogam com as da ANPD, da Anatel, do Banco Central e do CGI.br/NIC.br. O resultado é a possibilidade de descoordenação regulatória num ambiente já caracterizado por uma multiplicidade de instâncias com poder normativo sobre temas correlatos.

O texto reconhece parte desse problema em pontos isolados, o art. 6º, §4º ressalva as competências do Banco Central e do Conselho Monetário Nacional para o setor financeiro; o art. 19 prevê cooperação técnica contínua entre BCB (Banco Central do Brasil), CMN (Conselho Monetário Nacional), CNCiber (Comitê Nacional de Cibersegurança), autoridade nacional e GSI (Gabinete de Segurança Institucional da Presidência da República). Mas a solução é pontual, e não sistêmica de forma a gerar insegurança jurídica e duplicidade de obrigações para os agentes regulados.

2. A racionalidade atuarial e os efeitos da gestão de riscos sobre a regulação

Outro aspecto que chama atenção é a centralidade da lógica de gestão de riscos, presente em pontos estruturantes da minuta — notadamente nas definições do art. 3º, XIX (gestão de riscos cibernéticos) e XXIV (risco cibernético), nos deveres do art. 8º (estabelecimento, manutenção e revisão contínua de processos de gestão de riscos pelos agentes obrigados) e na competência da autoridade nacional para definir metodologias e níveis de tolerância ao risco (art. 17, II e III). . Embora esse modelo seja comum em políticas de cibersegurança, sua adoção sem parâmetros

mais bem definidos pode abrir espaço para interpretações muito amplas e para uma distribuição desigual de responsabilidades. Na prática, isso pode significar tanto insegurança jurídica quanto maior discricionariedade regulatória.

Nesse ponto, é importante observar que a centralidade da gestão de riscos no anteprojeto não é apenas uma escolha técnica neutra, mas parte de uma racionalidade mais ampla de organização da segurança digital. Essa lógica tende a deslocar a atenção da análise de eventos concretos para a antecipação de comportamentos e cenários futuros, estruturando a regulação a partir de níveis de risco, probabilidades e categorias de perigosidade.[2]

É justamente aqui que se torna necessário atenção para não se cair em uma lógica de risco em que a própria governança passa a operar por mecanismos de predição e classificação contínua de sujeitos, sistemas e setores. Nessa abordagem, aquilo que é tratado como "risco" deixa de ser apenas um instrumento de gestão e passa a organizar a própria forma como se distribuem responsabilidades, vigilância e intervenção institucional.[3]

No caso da minuta, isso se conecta diretamente com o art. 18, ao permitir que autoridades setoriais flexibilizem, dispensem ou ampliem o rigor das normas gerais estabelecidas pela autoridade nacional de cibersegurança. Ainda que a intenção seja acomodar especificidades setoriais, essa arquitetura pode aprofundar um modelo no qual diferentes regimes de risco coexistem e se ajustam de forma altamente discricionária, sem parâmetros suficientemente uniformes.

O problema não é a existência de flexibilidade regulatória em si, mas o risco de que essa flexibilidade opere dentro de uma racionalidade predominantemente atuarial, em que a regulação passa a ser guiada por classificações de risco cada vez mais abertas, com efeitos diretos sobre o nível de proteção aplicado a diferentes setores e, em última instância, sobre direitos fundamentais.

3. O poder cautelar do art. 17, XIII e a interface com o Marco Civil da Internet

A racionalidade da gestão de riscos encontra sua expressão mais sensível no art. 17, XIII, que confere à autoridade nacional de cibersegurança competência para determinar, em caráter cautelar, por até setenta e duas horas, o bloqueio de

---

[2] DIETER, Maurício Stegemann. *Política criminal atuarial: a criminologia do fim da história*. 2012. Tese (Doutorado em Direito) – Universidade Federal do Paraná, Curitiba, 2012.

[3] HARCOURT, Bernard E. The shaping of chance: actuarial models and criminal profiling at the turn of the twenty-first century. *The University of Chicago Law Review*, Chicago, v. 70, n. 1, p. 105-128, 2003. Disponível em: JSTOR. Acesso em: 13 maio 2026. DOI: 10.2307/1600548.

tráfego, a remoção de artefatos maliciosos, a desconexão ou o desligamento de ciberativos. Os requisitos são dois: risco iminente de dano irreparável à confidencialidade, integridade, autenticidade ou disponibilidade de ciberativos, ou à estabilidade do ciberespaço nacional; e elevada possibilidade de aplicação de sanção por prática de atividade ilícita relacionada à cibersegurança.

O instrumento pode ter função legítima em hipóteses muito específicas, contenção de ataques em andamento contra infraestruturas críticas, por exemplo. Mas a redação atual concede um poder amplo a uma autoridade administrativa, sobre objetos de natureza técnica e comunicacional, com parâmetros substantivos pouco delimitados e sem previsão expressa de controle judicial. A noção de "estabilidade do ciberespaço nacional" é, em particular, suficientemente aberta para acomodar interpretações que vão muito além da contenção de ataques pontuais.

Esse desenho se choca com pilares centrais do Marco Civil da Internet (MCI). A neutralidade de rede, prevista no art. 9º, veda o tratamento isonômico de pacotes baseado em conteúdo, origem, destino, terminal ou aplicação, ressalvadas hipóteses muito específicas previstas em regulamentação. Os arts. 10 e 11 disciplinam a guarda e o tratamento de registros, comunicações e dados pessoais, e ancoram um regime de proteção que tem o controle judicial como elemento estruturante. A exigência constitucional de ordem judicial para restringir o sigilo das comunicações, recordada na própria minuta no art. 4º, III, é o parâmetro mais alto do ordenamento brasileiro nessa matéria. Conferir a uma autoridade administrativa o poder de bloquear tráfego ou desligar ciberativos sem homologação judicial automática introduz uma assimetria difícil de sustentar à luz desse arranjo.

Não se trata de afastar o instrumento, mas de submetê-lo a parâmetros compatíveis com a moldura constitucional e com o MCIl. Hipóteses materiais taxativas, dever de fundamentação técnica, homologação judicial em prazo curto, vedação expressa ao bloqueio de protocolos ou aplicações específicas e publicização periódica das medidas adotadas são salvaguardas mínimas para que o poder cautelar não se converta em ferramenta de discricionariedade ampla sobre a infraestrutura comunicacional.

4. A ausência da criptografia como pilar estruturante

Talvez a lacuna mais relevante do texto seja a ausência de qualquer referência explícita à criptografia como elemento estruturante da cibersegurança. O anteprojeto menciona confidencialidade, integridade e autenticidade como objetivos, mas evita nomear o principal mecanismo técnico que sustenta esses

atributos. Essa escolha não parece neutra. Afastar a criptografia como pilar nominado da cibersegurança, ainda que se preserve a menção a confidencialidade, integridade e autenticidade, mantém em aberto o espaço normativo para que regulamentações infralegais, da autoridade nacional ou das autoridades setoriais, venham a impor, sob argumentos de auditoria, rastreabilidade ou cooperação investigativa, requisitos que enfraqueçam protocolos criptográficos, instituam mecanismos de acesso excepcional ou exijam custódia de chaves. O silêncio do texto, nesse sentido, indica uma escolha de arquitetura normativa que desloca para o plano regulamentar uma decisão estrutural sobre o nível de proteção dos sistemas brasileiros.

A criptografia não é apenas uma ferramenta técnica entre outras. Ela é o que permite proteger infraestruturas críticas, evitar vazamentos de dados em larga escala e garantir o sigilo das comunicações. Também é fundamental para a própria segurança do Estado e de empresas. Ao contrário do que ainda aparece em certos debates, a criptografia não inviabiliza investigações. O que ela faz é impedir que a fragilização dos sistemas seja tratada como solução. Sem ela, o custo da investigação recai sobre toda a sociedade, na forma de maior exposição a ataques e abusos.[4]

Ignorar esse papel acaba reforçando uma oposição artificial entre segurança e privacidade, quando, na prática, uma depende da outra.[5] A ausência de um reconhecimento mais claro da criptografia enfraquece o próprio objetivo do anteprojeto de criar um ambiente digital seguro e confiável.

O silêncio da Minuta nesta matéria abre espaço para que regulamentações infralegais, da autoridade nacional ou das autoridades setoriais previstas no art. 18, imponham requisitos de acesso excepcional, custódia de chaves ou enfraquecimento deliberado de protocolos criptográficos, sob argumentos de auditoria, rastreabilidade ou interesse investigativo. O resultado seria a redução do nível geral de proteção dos sistemas brasileiros, com impacto sobre cidadãos, empresas e órgãos públicos. A experiência comparada, incluindo a Ley Marco de Ciberseguridad chilena, de 2024, aponta caminhos para reconhecer a criptografia

[4] DUTRA, Luiza; PRADO, Thobias. Por que a criptografia é uma questão feminista? Instituto de Referência em Internet e Sociedade, [s.d.]. Disponível em: https://irisbh.com.br/por-que-a-criptografia-e-uma-questao-feminista/. Acesso em: 13 maio 2026.

[5] DUTRA, Luiza; PRADO, Thobias. O Estado que quer a chave-mestra. Internet Society Brasil Blog, 30 mar. 2026. Disponível em: https://www.isoc.org.br/post/o-estado-que-quer-a-chave-mestra. Acesso em: 13 maio 2026.

forte como pilar normativo, vedar *backdoors* e exigências de custódia de chaves, e estabelecer requisitos mínimos para proteção de dados em trânsito e em repouso e para a integridade da infraestrutura da Internet, como adoção de DNSSEC, RPKI e versões atualizadas dos protocolos de transporte e de IP.

5. Prevenção, repressão e o déficit de salvaguardas

O texto adota uma abordagem bastante orientada à prevenção, detecção e repressão de incidentes e crimes cibernéticos, o que é compreensível, mas não vem acompanhado do mesmo nível de detalhamento em relação a salvaguardas. Faltam referências mais concretas a limites, controles e garantias.

Não há, por exemplo, previsão especificada de devido processo em medidas relacionadas à cibersegurança, nem parâmetros sobre coleta e compartilhamento de dados, nem diretrizes mais explícitas de necessidade e proporcionalidade. Também não aparecem mecanismos de transparência ou de auditoria independente. Em um contexto marcado por históricos de vigilância e expansão de capacidades tecnológicas de monitoramento, essa ausência não é trivial.

A questão se torna ainda mais visível quando se observa o desenho da notificação obrigatória de ciberincidentes prevista no art. 10, III, e o subsequente compartilhamento de informações com o Centro Nacional de Cibersegurança a que se refere o art. 11, II. A minuta prevê, no art. 10, §2º, que a autoridade competente resguardará o sigilo das informações sobre o incidente notificado, mas não articula esse fluxo com os comandos da LGPD em hipóteses nas quais o incidente envolva dados pessoais — situação que será regra, e não exceção, para a maior parte dos serviços essenciais listados no parágrafo único do art. 2º. A ausência de critérios sobre minimização, anonimização, finalidade e prazo de retenção das informações compartilhadas com o CNCiber é uma lacuna que precisará ser endereçada para evitar duplicidade e divergência de obrigações entre o regime de cibersegurança e o regime de proteção de dados.

O déficit de salvaguardas também se manifesta na ausência de um regime claro de proteção a pesquisadores de segurança. A minuta menciona, no art. 2º, XX, a "invasão ética" como prática autorizada e regulamentada de identificação, teste e exploração de vulnerabilidades, e o art. 17, VII e VIII, atribui à autoridade competência para normatizar esses procedimentos e estimular a divulgação coordenada de vulnerabilidades. São avanços, mas o texto não institui um regime legal de *safe harbor* para pesquisadores de boa-fé que atuem dentro de políticas publicadas de divulgação coordenada. Sem essa proteção, a pesquisa

independente em segurança, que é parte indispensável da cadeia de defesa cibernética, permanece exposta a riscos jurídicos que tendem a desestimular a detecção e a correção precoces de vulnerabilidades.

6. Cooperação internacional e proteção de direitos

O anteprojeto também menciona a cooperação internacional em cibersegurança como uma de suas diretrizes, o que é positivo, mas levanta outra camada de atenção. A troca de informações entre países precisa estar ancorada em garantias de direitos humanos e proteção de dados, sob risco de ampliar práticas de compartilhamento pouco transparentes.

Nesse contexto, o art. 17, IX, da minuta prevê que a cooperação internacional se dará em coordenação com o Ministério das Relações Exteriores, o que é adequado do ponto de vista institucional. Falta, contudo, a previsão expressa de critérios substantivos para essa cooperação, em particular, a observância dos princípios de finalidade, necessidade e minimização no compartilhamento de dados, e a vedação ao compartilhamento que possa subsidiar práticas incompatíveis com o ordenamento brasileiro de proteção de direitos. A ausência desses critérios deixa margem para arranjos pouco transparentes, especialmente em um cenário internacional no qual diferentes países adotam padrões muito heterogêneos de proteção de dados e de garantias processuais.

7. Governança e o lugar do modelo multissetorial

Um último ponto merece atenção pela importância que tem na trajetória brasileira de governança da Internet: o desenho da participação multissetorial na minuta. O Conselho Nacional de Cibersegurança previsto no art. 23 reúne mais de trinta assentos, mas com forte preponderância do Poder Executivo federal, que conta com quinze representantes, em comparação a somente três da sociedade civil, três de instituições científicas, tecnológicas e de inovação, três do setor empresarial e um do CGI.br. Essa composição não corresponde ao padrão multissetorial paritário consolidado no Brasil em torno do próprio CGI.br, que tem sido referência internacional para o modelo de governança colaborativa da Internet.

O modelo multissetorial é, ele próprio, uma forma de produzir qualidade regulatória em ambientes tecnicamente complexos e em rápida transformação, e é a forma como o Brasil tem projetado, no plano internacional, uma posição de liderança no

debate sobre Internet aberta[6]. Reduzir a participação multissetorial a uma minoria consultiva no Conselho Nacional de Cibersegurança fragiliza, no longo prazo, a própria capacidade do arcabouço de cibersegurança de manter sintonia com a evolução técnica e social do ecossistema digital.

Considerações finais

No conjunto, a proposta representa um passo importante ao tentar consolidar uma política nacional de cibersegurança mais estruturada. Ainda assim, o texto ganha força se avançar em alguns pontos-chave: I) deixar mais claro seu escopo de aplicação, II) reduzir margens para fragmentação regulatória, III) incorporar salvaguardas mais robustas, IV) reconhecer explicitamente a criptografia como um pilar da segurança digital, e V) maior paridade na própria composição do conselho.

Mais do que um detalhe técnico, essa escolha diz respeito ao tipo de ambiente digital que se quer construir. Um marco de cibersegurança que não trate a criptografia como elemento central corre o risco de fragilizar exatamente aquilo que pretende proteger: a segurança, a confiança e os direitos no espaço digital.

[6] Sobre o caráter qualitativo do modelo multissetorial como mecanismo de produção regulatória em ambientes tecnicamente complexos, ver: ALMEIDA, Virgílio A. F.; GETSCHKO, Demi; AFONSO, Carlos. The origin and evolution of multistakeholder models. IEEE Internet Computing, v. 19, n. 1, p. 74-79, 2015.