XXXII CONGRESSO NACIONAL DO CONPEDI SÃO PAULO - SP

INTERNET: DINÂMICAS DA SEGURANÇA PÚBLICA E INTERNACIONAL

DANIELLE JACON AYRES PINTO

GUSTAVO RABAY GUERRA

JOSÉ RENATO GAZIERO CELLA

JÉSSICA FACHIN

I61

Internet: dinâmicas da segurança pública internacional[Recurso eletrônico on-line] organização CONPEDI

Coordenadores: Danielle Jacon Ayres Pinto, Gustavo Rabay Guerra, José Renato Gaziero Cella, Jéssica Fachin – Florianópolis: CONPEDI, 2025.

Inclui bibliografia
ISBN: 978-65-5274-285-8
Modo de acesso: www.conpedi.org.br em publicações
Tema: Os Caminhos Da Internacionalização E O Futuro Do Direito

1. Direito – Estudo e ensino (Pós-graduação) – Encontros Nacionais. 2. Internet. 3. Segurança pública internacional. XXXII Congresso Nacional do CONPEDI São Paulo - SP (4: 2025: Florianópolis, Brasil).

CDU: 34

XXXII CONGRESSO NACIONAL DO CONPEDI SÃO PAULO - SP

INTERNET: DINÂMICAS DA SEGURANÇA PÚBLICA E INTERNACIONAL

Apresentação

No XXII Congresso Nacional do CONPEDI, realizado nos dias 26, 27 e 28 de novembro de 2025, o Grupo de Trabalho - GT “Internet: Dinâmicas da Segurança Pública e Internacional”, que teve lugar na tarde de 28 de novembro de 2025, destacou-se no evento não apenas pela qualidade dos trabalhos apresentados, mas pelos autores dos artigos, que são professores pesquisadores acompanhados de seus alunos pós-graduandos. Foram apresentados artigos objeto de um intenso debate presidido pelos coordenadores.

Esse fato demonstra a inquietude que os temas debatidos despertam na seara jurídica. Cientes desse fato, os programas de pós-graduação em direito empreendem um diálogo que suscita a interdisciplinaridade na pesquisa e se propõe a enfrentar os desafios que as novas tecnologias impõem ao direito. Para apresentar e discutir os trabalhos produzidos sob essa perspectiva.

Os artigos que ora são apresentados ao público têm a finalidade de fomentar a pesquisa e fortalecer o diálogo interdisciplinar em torno do tema “Internet: Dinâmicas da Segurança Pública e Internacional”. Trazem consigo, ainda, a expectativa de contribuir para os avanços do estudo desse tema no âmbito da pós-graduação em direito, apresentando respostas para uma realidade que se mostra em constante transformação.

Os Coordenadores

Prof. Dr. José Renato Gaziero Cella

Prof. Dra. Danielle Jacon Ayres Pinto

Prof. Dr. Gustavo Rabay Guerra

Prof. Dra. Jéssica Fachin

CIBERSEGURANÇA E COOPERAÇÃO INTERNACIONAL: CAMINHOS PARA A PROTEÇÃO DE INFRAESTRUTURAS CRÍTICAS

CYBERSECURITY AND INTERNATIONAL COOPERATION: PATHS TO PROTECT CRITICAL INFRASTRUCTURES

Felipe dos Santos Gasparoto
Carlos Henrique Gasparoto

Resumo

O artigo analisa a crescente vulnerabilidade das infraestruturas críticas diante da intensificação dos processos de digitalização e do aumento dos ciberataques. Inicialmente, destaca que setores como energia, saúde, transportes, telecomunicações e defesa passaram a ser alvos frequentes de ameaças sofisticadas, capazes de gerar impactos econômicos, sociais e políticos de grande magnitude. São mencionados casos emblemáticos, como o malware Stuxnet (2010) e o ataque de ransomware à Colonial Pipeline (2021), que evidenciam o potencial de desestabilização dessas ofensivas. No contexto brasileiro, observa-se que, apesar da existência de instrumentos normativos como o Marco Civil da Internet, a Lei Geral de Proteção de Dados, a Lei Carolina Dieckmann e a Política Nacional de Segurança da Informação, ainda há fragmentação regulatória, baixa integração institucional e reduzida participação do país em tratados internacionais, fatores que aumentam sua vulnerabilidade. Como resultado da análise, propõe-se um modelo regulatório baseado em três eixos: elaboração de legislação específica para proteção de infraestruturas críticas; fortalecimento da integração entre Estado, setor privado e sociedade civil; e intensificação da cooperação internacional, com adesão à Convenção de Budapeste e participação ativa em fóruns multilaterais. Conclui-se que a construção de um marco normativo robusto e alinhado a padrões globais é essencial para assegurar resiliência digital, continuidade dos serviços essenciais e fortalecimento da posição brasileira na governança internacional da cibersegurança.

Palavras-chave: Cibersegurança, Infraestruturas críticas, Cooperação internacional, Soberania digital, Defesa cibernética

Abstract/Resumen/Résumé

The article analyzes the growing vulnerability of critical infrastructures in the face of increasing digitalization processes and the rise of cyberattacks. Initially, it highlights that sectors such as energy, health, transportation, telecommunications, and defense have become frequent targets of sophisticated threats capable of generating economic, social, and political impacts of great magnitude. Emblematic cases are mentioned, such as the Stuxnet malware (2010) and the ransomware attack on Colonial Pipeline (2021), which demonstrate the destabilizing potential of such offensives. In the Brazilian context, it is observed that, despite

the existence of legal instruments such as the Internet Civil Framework, the General Data Protection Law, the Carolina Dieckmann Law, and the National Information Security Policy, there is still regulatory fragmentation, low institutional integration, and limited participation in international treaties, factors that increase the country's vulnerability. As a result of the analysis, a regulatory model is proposed based on three axes: drafting specific legislation for the protection of critical infrastructures; strengthening integration between the State, the private sector, and civil society; and intensifying international cooperation, with adherence to the Budapest Convention and active participation in multilateral forums. It is concluded that the construction of a robust regulatory framework aligned with global standards is essential to ensure digital resilience, continuity of essential services, and the strengthening of Brazil's position in international cybersecurity governance.

Keywords/Palabras-claves/Mots-clés: Cybersecurity, Critical infrastructures, International cooperation, Digital sovereignty, Cyber defense

1.Introdução

O avanço exponencial das tecnologias digitais e a crescente interconexão dos sistemas informacionais têm transformado profundamente a dinâmica social, econômica e política no cenário global. A digitalização de processos e a dependência de redes interligadas trouxeram ganhos expressivos de eficiência, mas também impuseram novos desafios, sobretudo relacionados à segurança cibernética. No contexto atual, as infraestruturas críticas — como energia, saúde, transportes, telecomunicações e defesa — tornaram-se especialmente vulneráveis, figurando como alvos frequentes de ciberataques com potencial de gerar impactos econômicos, sociais e geopolíticos de grande magnitude.

Segundo relatório da Cybersecurity Ventures (2024), estima-se que os prejuízos globais decorrentes de crimes cibernéticos ultrapassem US$ 10,5 trilhões até 2025, evidenciando que as ameaças digitais deixaram de ser um problema meramente técnico para se consolidarem como um desafio estratégico de segurança internacional. Casos emblemáticos, como os ataques de ransomware que paralisaram redes hospitalares na Europa, a interrupção de oleodutos nos Estados Unidos e invasões a sistemas governamentais em países da América Latina e da Ásia, demonstram que a cibersegurança está diretamente relacionada à soberania nacional, à proteção de dados e à estabilidade das nações.

No Brasil, o cenário não é diferente. De acordo com dados recentes da Agência Nacional de Proteção de Dados (ANPD) e do Centro de Estudos, Resposta e Tratamento de Incidentes Cibernéticos (CERT.br), houve um aumento superior a 200% nos incidentes de segurança digital entre 2020 e 2024, afetando diretamente serviços essenciais e setores estratégicos. A carência de uma regulamentação robusta e de mecanismos eficazes de cooperação internacional potencializa os riscos à segurança digital do país, colocando em evidência a necessidade urgente de criação de políticas públicas e estratégias normativas que integrem prevenção, monitoramento e resposta rápida a incidentes.

Nesse contexto, a cooperação jurídica internacional assume papel central na mitigação de ameaças e no enfrentamento de crimes cibernéticos que, por sua natureza transnacional, ultrapassam fronteiras físicas e desafiam a eficácia das legislações internas. A harmonização normativa, a troca de informações entre Estados e a adesão a instrumentos multilaterais — como a

Convenção de Budapeste sobre Crimes Cibernéticos — são elementos fundamentais para estruturar um sistema global de ciberdefesa cooperativa. A ausência do Brasil como signatário de tratados estratégicos, aliada à fragmentação de políticas internas, acentua a vulnerabilidade nacional frente a incidentes de grande escala.

A problemática que orienta este estudo pode ser assim definida: como criar um modelo regulatório e de cooperação internacional que garanta a proteção eficaz das infraestruturas críticas no Brasil? Parte-se da hipótese de que a inexistência de um marco normativo robusto e a fragilidade dos mecanismos de cooperação internacional ampliam significativamente os riscos à segurança digital, à estabilidade geopolítica e à própria soberania nacional.

Diante disso, a presente pesquisa busca analisar a importância da cibersegurança para a proteção das infraestruturas críticas brasileiras, discutindo os impactos da transformação digital, os desafios regulatórios e a necessidade de integração a padrões internacionais de governança digital. O objetivo é contribuir para o debate acadêmico e jurídico acerca da construção de políticas públicas eficazes e de estratégias multilaterais que assegurem a proteção dos sistemas essenciais à manutenção da ordem social e econômica.

2. Infraestruturas Críticas e Riscos Cibernéticos

2.1. Conceito de Infraestrutura Crítica

O conceito de infraestrutura crítica ocupa papel central nas discussões contemporâneas sobre segurança nacional e ciberdefesa. Em termos gerais, considera-se infraestrutura crítica todo sistema, ativo, serviço ou instalação que seja essencial para o funcionamento da sociedade, da economia e das instituições do Estado, de modo que qualquer comprometimento de sua integridade, disponibilidade ou confidencialidade pode gerar consequências graves para a ordem social, econômica e política.

No âmbito jurídico nacional, a definição foi incorporada de forma mais expressiva com a Estratégia Nacional de Segurança Cibernética (E-Ciber), aprovada pelo Decreto nº 10.222/2020, que classifica como críticas “as infraestruturas cujos serviços são indispensáveis para a segurança da sociedade e do Estado, bem como para o funcionamento regular da economia”. O mesmo decreto estabelece que a proteção dessas estruturas deve ser prioridade para a Administração Pública,

orientando órgãos e entidades federais a adotar medidas preventivas, normativas e operacionais para mitigar riscos.

Ainda no contexto brasileiro, a Lei nº 13.709/2018 — Lei Geral de Proteção de Dados (LGPD) —, embora não trate diretamente de infraestruturas críticas, impõe diretrizes para a segurança de dados pessoais, refletindo a importância de sistemas seguros e protegidos. Além disso, órgãos como a Agência Nacional de Energia Elétrica (ANEEL), a Agência Nacional de Aviação Civil (ANAC) e a Agência Nacional de Telecomunicações (ANATEL) já adotam normativas setoriais próprias para regulamentar padrões mínimos de proteção digital nos setores de sua competência.

No plano internacional, a definição de infraestrutura crítica é mais abrangente e consolidada. A Diretiva Europeia 2008/114/CE define como infraestruturas críticas "os ativos, sistemas ou partes destes que são essenciais para a manutenção de funções vitais para a sociedade, saúde, segurança, bem-estar econômico ou social, cuja interrupção teria um impacto significativo em pelo menos dois Estados-Membros". Já o Department of Homeland Security (DHS), dos Estados Unidos, identifica 16 setores estratégicos como críticos, incluindo:

Setor financeiro – bancos, sistemas de pagamento, bolsas de valores;

Energia – usinas hidrelétricas, redes de transmissão e distribuição;

Saúde – hospitais, laboratórios, sistemas de prontuário eletrônico;

Transportes e logística – portos, aeroportos, rodovias e ferrovias;

Telecomunicações e tecnologia da informação – provedores de internet, redes 5G, satélites;

Defesa e segurança pública – forças armadas, polícias e sistemas de inteligência.

Esses exemplos revelam a diversidade e a interdependência entre os setores críticos. Um ataque bem-sucedido contra um sistema bancário, por exemplo, pode gerar colapsos na economia nacional, assim como uma invasão a hospitais pode comprometer diretamente a vida de milhares de pessoas. Da mesma forma, um incidente de segurança em portos e aeroportos pode afetar a

logística internacional, demonstrando que o risco cibernético associado a essas estruturas não se limita ao ambiente nacional, mas assume contornos transnacionais e geopolíticos.

Portanto, compreender o conceito jurídico e técnico de infraestruturas críticas é essencial para a formulação de políticas públicas eficazes e para o desenho de um modelo regulatório integrado à realidade global. A proteção desses ativos exige um arcabouço normativo sólido, atualizado e alinhado aos padrões internacionais, de forma a permitir que os Estados sejam capazes de prevenir, detectar e responder a incidentes cibernéticos de alta complexidade.

2.2. Ameaças e Vulnerabilidades

A crescente dependência de sistemas digitais e interconectados ampliou de forma significativa a superfície de exposição das infraestruturas críticas a ameaças cibernéticas cada vez mais sofisticadas. A digitalização de serviços essenciais — como sistemas bancários, redes elétricas, hospitais, portos e aeroportos — trouxe benefícios inegáveis em termos de eficiência e integração, mas, paralelamente, criou um ambiente de maior vulnerabilidade diante da atuação de agentes maliciosos que exploram fragilidades técnicas, humanas e organizacionais.

Entre os principais tipos de ciberataques que afetam essas estruturas, destacam-se:

a) Ransomware

Trata-se de um tipo de software malicioso que sequestra dados ou bloqueia o acesso a sistemas, exigindo o pagamento de resgate — geralmente em criptomoedas — para a liberação. No contexto de infraestruturas críticas, um ataque de ransomware pode resultar na paralisação total de serviços essenciais, como ocorreu em diversos hospitais da Alemanha e da França, onde operações cirúrgicas foram canceladas devido à indisponibilidade de sistemas de prontuários eletrônicos.

b) Phishing e Engenharia Social

Os ataques de phishing consistem no envio de mensagens fraudulentas, frequentemente via e-mail, que induzem usuários a fornecer dados sensíveis, como senhas, informações bancárias ou credenciais de acesso a redes corporativas. Em ambientes de alta complexidade, como centrais de operação de redes elétricas e sistemas de controle de tráfego aéreo, esse tipo de vulnerabilidade pode comprometer completamente a integridade de processos críticos.

c) Ataques de Negação de Serviço Distribuído (DDoS)

Os ataques DDoS têm por objetivo sobrecarregar servidores e redes, inviabilizando o acesso a serviços essenciais. Um exemplo recorrente ocorre no setor financeiro, onde sistemas bancários enfrentam instabilidades devido ao tráfego artificial gerado por redes de computadores comprometidos (botnets). No caso das infraestruturas críticas, ataques DDoS podem interromper o funcionamento de portos, aeroportos e redes de telecomunicações, afetando diretamente a logística e a comunicação nacional e internacional.

d) Espionagem Digital e Sabotagem

A espionagem digital envolve a infiltração em sistemas estratégicos com o objetivo de extrair dados sensíveis, enquanto a sabotagem busca causar danos diretos à integridade física ou lógica das estruturas. Trata-se de uma ameaça frequentemente associada à cibersegurança geopolítica, na qual Estados-nação utilizam ataques cibernéticos para obter vantagem estratégica.

Casos Emblemáticos

Alguns episódios marcantes ilustram a gravidade das ameaças e suas consequências para as infraestruturas críticas:

Stuxnet (2010) – Considerado um dos ataques mais sofisticados da história, o malware Stuxnet foi utilizado para sabotar o programa nuclear iraniano, danificando centrífugas utilizadas no enriquecimento de urânio. O caso demonstrou a capacidade de um ciberataque direcionado causar danos físicos concretos a equipamentos estratégicos, inaugurando uma nova era de guerra cibernética.

Colonial Pipeline (2021) – O maior oleoduto dos Estados Unidos, responsável pelo fornecimento de cerca de 45% do combustível da costa leste, sofreu um ataque de ransomware que paralisou suas operações por vários dias. O incidente provocou escassez de combustíveis, aumento de preços e prejuízos bilionários, evidenciando a vulnerabilidade de sistemas logísticos complexos e altamente interconectados.

Esses casos ilustram que os impactos dos ciberataques não se restringem ao ambiente digital, alcançando a esfera econômica, social e até mesmo a segurança nacional. Um ataque

direcionado contra sistemas bancários pode paralisar a economia de um país; uma invasão a redes elétricas pode gerar blecautes em larga escala; a paralisação de hospitais pode comprometer a vida de milhares de pacientes; e a interrupção de portos e aeroportos pode desestabilizar cadeias globais de suprimento.

A Complexidade do Cenário Brasileiro

No Brasil, embora a Estratégia Nacional de Segurança Cibernética (E-Ciber) e outras iniciativas recentes tenham buscado estabelecer diretrizes para a proteção de infraestruturas críticas, os dados do Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br) revelam que os incidentes envolvendo ransomware, DDoS e phishing cresceram mais de 200% entre 2020 e 2024. A falta de um marco normativo robusto, associada à carência de investimentos em tecnologias de proteção e à fragilidade da cooperação internacional, amplia os riscos e evidencia a necessidade de políticas públicas mais eficazes e integradas.

Dessa forma, compreender os tipos de ameaças, seus mecanismos de ataque e os impactos potenciais é etapa fundamental para a construção de um modelo regulatório sólido e de estratégias coordenadas de defesa, capazes de proteger ativos estratégicos e garantir a continuidade dos serviços essenciais.

2.3. Impactos Econômicos, Sociais e Políticos

A crescente incidência de ciberataques contra infraestruturas críticas tem produzido efeitos que transcendem o ambiente digital, gerando consequências econômicas, sociais e políticas de grande magnitude. A proteção desses sistemas estratégicos deixou de ser apenas uma questão técnica e passou a ocupar posição central na agenda de segurança nacional e na formulação de políticas públicas voltadas à defesa cibernética.

a) Impactos Econômicos e Custos Financeiros

Os ataques cibernéticos contra setores essenciais acarretam prejuízos bilionários e provocam desestabilizações nas cadeias produtivas e logísticas. Segundo estimativa da Cybersecurity Ventures (2024), os danos financeiros globais decorrentes de crimes cibernéticos podem ultrapassar US$ 10,5 trilhões até 2025, demonstrando que a cibersegurança é também um problema de grande relevância econômica.

No caso brasileiro, os impactos são igualmente preocupantes. Relatórios do Centro de Estudos, Resposta e Tratamento de Incidentes Cibernéticos (CERT.br) indicam que empresas de energia, bancos, hospitais e plataformas de logística vêm sofrendo perdas significativas decorrentes de ransomware, phishing e ataques de negação de serviço. Quando incidentes dessa natureza atingem redes elétricas, sistemas bancários ou portos e aeroportos, os reflexos se espalham por toda a economia, ocasionando desabastecimento, aumento de custos operacionais e queda da produtividade nacional.

Casos como o ataque à Colonial Pipeline (2021), que paralisou cerca de 45% do fornecimento de combustíveis na costa leste dos Estados Unidos, ilustram o efeito dominó que um único incidente pode gerar, afetando não apenas uma empresa, mas toda a infraestrutura econômica de um país. Essa realidade evidencia a necessidade de investimentos maciços em segurança digital e da criação de mecanismos regulatórios claros e integrados, capazes de reduzir riscos e proteger ativos estratégicos.

b) Impactos Sociais e Direitos Fundamentais

Os ciberataques contra infraestruturas críticas também produzem consequências diretas para a sociedade, afetando o exercício de direitos fundamentais e o acesso a serviços básicos. A interrupção de hospitais, por exemplo, pode inviabilizar tratamentos médicos, colocando vidas em risco imediato; falhas em sistemas de telecomunicações podem prejudicar a comunicação em situações de emergência; e ataques a redes de abastecimento de água e energia comprometem diretamente a qualidade de vida da população.

Além disso, a exposição de dados pessoais decorrente de falhas de segurança digital gera impactos significativos à privacidade e à dignidade humana, trazendo à tona a importância da Lei Geral de Proteção de Dados Pessoais (LGPD – Lei nº 13.709/2018), que estabelece normas para o tratamento de informações sensíveis. No entanto, a crescente sofisticação dos ataques demonstra que a legislação existente, embora relevante, ainda é insuficiente para lidar com a complexidade e a velocidade das ameaças atuais.

c) Impactos Políticos e Soberania Nacional

O crescimento dos incidentes cibernéticos contra infraestruturas críticas expõe diretamente questões relacionadas à soberania nacional e à segurança do Estado. Em um contexto de interdependência digital, países que não possuem estratégias robustas de cibersegurança e mecanismos eficazes de cooperação internacional tornam-se mais vulneráveis a ataques coordenados, inclusive perpetrados por outros Estados-nação.

A Estratégia Nacional de Segurança Cibernética (E-Ciber), instituída pelo Decreto nº 10.222/2020, reconhece a importância da proteção de sistemas estratégicos para a defesa nacional e estabelece diretrizes para a mitigação de riscos. Entretanto, a ausência de um marco normativo abrangente, aliado à falta de alinhamento com tratados internacionais — como a Convenção de Budapeste sobre Crimes Cibernéticos —, limita a capacidade do Brasil de responder de forma rápida e eficiente a ameaças globais.

A relação entre segurança digital, proteção de dados e defesa nacional é, portanto, indissociável. Um ataque direcionado contra redes elétricas, sistemas bancários ou plataformas de logística não compromete apenas o funcionamento de serviços essenciais, mas também fragiliza a capacidade do Estado de proteger seus cidadãos e de assegurar sua integridade territorial. Nesse sentido, a criação de políticas públicas integradas e de um modelo regulatório alinhado às normas internacionais é essencial para fortalecer a soberania e garantir a resiliência das infraestruturas críticas brasileiras.

3. Panorama Jurídico Nacional

3.1. Legislação Brasileira Aplicável

A crescente complexidade das ameaças cibernéticas e a vulnerabilidade das infraestruturas críticas demandam um arcabouço normativo robusto que assegure a proteção de dados, a segurança digital e a preservação da soberania nacional. No Brasil, o ordenamento jurídico ainda se encontra em processo de consolidação no campo da cibersegurança, apresentando avanços significativos, mas também lacunas que dificultam uma atuação coordenada entre os diferentes setores da Administração Pública, empresas privadas e órgãos de controle.

Entre as principais normas aplicáveis ao tema, destacam-se o Marco Civil da Internet (Lei nº 12.965/2014), a Lei Geral de Proteção de Dados Pessoais – LGPD (Lei nº 13.709/2018), a Lei nº 12.737/2012 — conhecida como Lei Carolina Dieckmann — e o Decreto nº 9.637/2018, que institui a Política Nacional de Segurança da Informação (PNSI).

a) Marco Civil da Internet (Lei nº 12.965/2014)

O Marco Civil da Internet estabelece princípios, garantias, direitos e deveres para o uso da rede no Brasil, representando um marco normativo fundamental para a regulação da esfera digital. Seu objetivo central é assegurar a neutralidade da rede, a proteção à privacidade e a inviolabilidade das comunicações dos usuários, bem como definir responsabilidades para provedores de aplicações e serviços.

O artigo 10 da lei determina que os provedores devem guardar sigilo sobre os dados pessoais e o conteúdo das comunicações privadas, salvo mediante ordem judicial. Já o artigo 13 prevê a obrigatoriedade de guarda de registros de conexão e acesso, permitindo que autoridades competentes realizem investigações de crimes digitais.

Para a proteção de infraestruturas críticas, o Marco Civil é relevante por estabelecer um equilíbrio entre liberdade e segurança no ambiente digital, criando mecanismos que permitem o monitoramento de incidentes e a cooperação entre órgãos públicos, empresas e usuários. No entanto, o dispositivo não estabelece, por si só, diretrizes específicas para a defesa cibernética, o que exige a integração com outras normas mais especializadas.

b) Lei Geral de Proteção de Dados Pessoais – LGPD (Lei nº 13.709/2018)

A LGPD representa um dos avanços mais significativos na regulação do tratamento de dados pessoais no Brasil, alinhando-se às melhores práticas internacionais, como o Regulamento Geral sobre a Proteção de Dados (GDPR) da União Europeia. A lei estabelece regras para a coleta, o armazenamento, o compartilhamento e o tratamento de dados pessoais, aplicando-se tanto a entidades públicas quanto privadas.

Nos artigos 46 a 50, a LGPD impõe obrigações de segurança da informação, exigindo que os controladores e operadores adotem medidas técnicas e administrativas aptas a proteger os dados contra acessos não autorizados, destruição acidental, perda, alteração ou qualquer forma de tratamento ilícito.

Em casos de incidentes que possam gerar riscos ou danos relevantes aos titulares, a lei prevê, em seu artigo 48, a obrigatoriedade de comunicação à Autoridade Nacional de Proteção de Dados (ANPD), que pode determinar providências como notificação dos afetados, aplicação de sanções e recomendações de melhoria nos processos de segurança.

A LGPD se torna particularmente importante para a proteção de infraestruturas críticas ao estabelecer padrões de governança digital, uma vez que essas estruturas operam com grandes volumes de dados sensíveis e estão expostas a riscos que podem comprometer diretamente serviços essenciais.

c) Lei nº 12.737/2012 – Lei Carolina Dieckmann

A chamada Lei Carolina Dieckmann, promulgada após um caso amplamente divulgado de invasão e divulgação de dados pessoais da atriz, modificou o Código Penal Brasileiro para tipificar condutas relacionadas à invasão de dispositivos informáticos e à violação de dados pessoais.

O artigo 154-A, introduzido pela norma, estabelece como crime a invasão de dispositivo alheio mediante violação de mecanismos de segurança, com pena de detenção de três meses a um ano e multa. A sanção é aumentada se houver obtenção de conteúdos privados, segredos comerciais ou informações sigilosas.

Embora a lei tenha representado um avanço, ela é frequentemente criticada por limitar-se a tipos penais básicos, sem abarcar a complexidade dos ataques cibernéticos modernos, como ransomware, espionagem digital e ataques de negação de serviço. Dessa forma, a norma precisa ser interpretada em conjunto com legislações mais recentes e com políticas públicas voltadas à defesa cibernética.

d) Decreto nº 9.637/2018 – Política Nacional de Segurança da Informação (PNSI)

O Decreto nº 9.637/2018 instituiu a Política Nacional de Segurança da Informação, estabelecendo diretrizes para a proteção de dados e de sistemas de informação considerados estratégicos para o Estado brasileiro. Entre seus objetivos principais, destacam-se:

Estabelecer normas para segurança cibernética e defesa digital;

Preservar a integridade, confidencialidade e disponibilidade das informações;

Organizar a atuação integrada entre órgãos governamentais e entidades privadas;

Incentivar a pesquisa e o desenvolvimento tecnológico voltados à cibersegurança.

O decreto também cria o Comitê Gestor de Segurança da Informação (CGSI), responsável por coordenar ações e propor estratégias para enfrentar incidentes e ameaças cibernéticas, inclusive no contexto das infraestruturas críticas.

Apesar de representar um avanço, a PNSI ainda enfrenta desafios relacionados à implementação efetiva das medidas propostas e à necessidade de integração com normas internacionais e padrões globais de segurança cibernética.

O conjunto dessas normas compõe a base regulatória brasileira para a proteção do ambiente digital e das infraestruturas críticas. No entanto, verifica-se que, embora existam avanços significativos, ainda há fragmentação normativa e ausência de harmonização legislativa com padrões internacionais, o que limita a eficácia das medidas de prevenção e resposta a incidentes cibernéticos.

3.2. Atuação da ANPD e Órgãos Reguladores

A crescente sofisticação dos ciberataques e o aumento da dependência de infraestruturas críticas para a manutenção da ordem social, econômica e política exigem a atuação coordenada de órgãos públicos e entidades reguladoras. No Brasil, essa responsabilidade está distribuída entre diferentes instituições, com destaque para a Autoridade Nacional de Proteção de Dados (ANPD), o Gabinete de Segurança Institucional da Presidência da República (GSI), a Polícia Federal e o Ministério da Defesa. Cada uma dessas entidades exerce funções complementares que visam prevenir, mitigar e responder a incidentes de segurança cibernética, compondo um ecossistema regulatório ainda em consolidação.

a) A Autoridade Nacional de Proteção de Dados (ANPD)

Criada pela Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018), a ANPD é o órgão central responsável por zelar pela proteção dos dados pessoais e pela implementação efetiva da LGPD. Entre suas atribuições, destacam-se:

Fiscalização e aplicação de sanções administrativas em caso de incidentes de segurança que envolvam dados pessoais;

Elaboração de normas e diretrizes técnicas para a adoção de boas práticas de proteção de dados;

Gestão de incidentes relevantes, inclusive aqueles que afetam infraestruturas críticas, determinando obrigações de comunicação, mitigação e reparação;

Promoção da cooperação institucional com órgãos reguladores, empresas privadas e entidades internacionais.

Nos termos do artigo 48 da LGPD, em caso de incidentes de segurança que possam acarretar risco ou dano relevante, a ANPD deve ser imediatamente comunicada pelos controladores de dados. Essa comunicação permite a adoção de medidas coordenadas para mitigar impactos, preservar direitos fundamentais e, quando necessário, notificar os titulares afetados.

Em casos envolvendo infraestruturas críticas, a atuação da ANPD assume caráter estratégico, uma vez que a indisponibilidade de serviços essenciais ou a exposição de dados sensíveis pode comprometer a continuidade de operações vitais para o país.

b) Gabinete de Segurança Institucional da Presidência da República (GSI)

O Gabinete de Segurança Institucional (GSI), vinculado diretamente à Presidência da República, desempenha papel fundamental na coordenação da segurança cibernética nacional, especialmente em situações que envolvem ativos e sistemas considerados estratégicos para a defesa e soberania do Estado.

Por meio do Departamento de Segurança da Informação (DSI/GSI), o órgão atua na formulação de políticas, na proposição de normas e na implementação de estratégias preventivas para a proteção de infraestruturas críticas. Além disso, o GSI é responsável pela coordenação da Política Nacional de Segurança da Informação (PNSI), estabelecida pelo Decreto nº 9.637/2018, integrando esforços entre diferentes esferas do governo e entidades privadas.

O GSI também mantém interlocução direta com outros órgãos estratégicos, como a ANPD, o CERT.br e o Centro de Defesa Cibernética do Exército Brasileiro (CDCiber), garantindo que incidentes de alta gravidade sejam tratados de forma integrada, com compartilhamento rápido de informações e definição de respostas coordenadas.

c) Polícia Federal

A Polícia Federal atua na investigação de crimes cibernéticos e na persecução penal de condutas tipificadas pelo ordenamento jurídico brasileiro, especialmente aquelas previstas na Lei nº 12.737/2012 (Lei Carolina Dieckmann), na LGPD e no Código Penal. Entre suas funções, destacam-se:

Investigação de ataques cibernéticos a órgãos públicos e infraestruturas críticas;

Atuação contra organizações criminosas transnacionais envolvidas em espionagem, fraudes digitais e sabotagem;

Cooperação com agências internacionais, como a Interpol e a Europol, em casos que envolvem múltiplas jurisdições;

Fornecimento de perícia técnica para identificação de vulnerabilidades e mecanismos de ataque.

A Polícia Federal integra a Rede Nacional de Segurança Cibernética (RNSC), o que possibilita maior integração com órgãos como o GSI, a ANPD e o CERT.br, criando um ambiente mais favorável à resposta rápida e à prevenção de incidentes de grande escala.

d) Ministério da Defesa e Centro de Defesa Cibernética (CDCiber)

O Ministério da Defesa, por meio do Centro de Defesa Cibernética (CDCiber), é responsável por coordenar ações de ciberdefesa no âmbito militar, atuando na proteção de redes estratégicas e sistemas de comunicação das Forças Armadas. Além disso, o CDCiber desenvolve exercícios de simulação de ataques e resposta a incidentes, promovendo a capacitação técnica de equipes especializadas.

O papel do CDCiber vai além da proteção militar, estendendo-se à defesa de infraestruturas críticas civis quando estas estão diretamente relacionadas à segurança nacional. Nesse sentido, há integração com o GSI, a ANPD e a Polícia Federal para identificar ameaças, prevenir incidentes e coordenar respostas a ataques de grande impacto.

e) A Necessidade de Atuação Integrada

Apesar da existência de órgãos com atribuições específicas, o Brasil ainda enfrenta desafios significativos para consolidar uma estrutura de governança digital integrada. A fragmentação de competências e a ausência de um marco regulatório unificado dificultam a adoção de protocolos claros para prevenção e resposta a incidentes que envolvem infraestruturas críticas.

A atuação conjunta entre ANPD, GSI, Polícia Federal e Ministério da Defesa é essencial para enfrentar ameaças cibernéticas de alta complexidade, especialmente aquelas com potencial transnacional. O fortalecimento dessa integração exige cooperação institucional contínua, investimentos em tecnologia, capacitação profissional e adesão a tratados internacionais que facilitem a troca de informações e a padronização de procedimentos.

4. Cooperação Internacional e Governança Global

A natureza transnacional das ameaças cibernéticas exige uma abordagem coordenada entre os Estados, uma vez que ciberataques contra infraestruturas críticas não se limitam às fronteiras nacionais e podem gerar efeitos em cadeia sobre sistemas interdependentes em diversas regiões do mundo. O fortalecimento da cooperação internacional e da governança global em cibersegurança tornou-se, assim, uma prioridade estratégica para a proteção de ativos essenciais, envolvendo tanto tratados multilaterais quanto iniciativas regionais e boas práticas de colaboração institucional.

O principal marco jurídico internacional é a Convenção de Budapeste sobre Crimes Cibernéticos (2001), elaborada pelo Conselho da Europa. Este tratado estabelece diretrizes para a tipificação penal de condutas cibernéticas, define mecanismos de cooperação jurídica internacional e promove o intercâmbio de informações entre os Estados signatários. Atualmente, é considerado o instrumento internacional mais abrangente no enfrentamento de crimes digitais, ainda que o Brasil não seja signatário.

Além da Convenção de Budapeste, outros instrumentos internacionais também merecem destaque:

Diretiva Europeia 2008/114/CE – Estabelece normas de proteção de infraestruturas críticas na União Europeia, prevendo mecanismos de cooperação entre os Estados-membros;

Estratégia Global de Cibersegurança da União Internacional de Telecomunicações (UIT/ONU) – Propõe um modelo de governança global baseado em cinco pilares: medidas legais, técnicas, organizacionais, de capacitação e cooperação internacional;

Normas do Grupo dos Sete (G7) e do Grupo dos Vinte (G20) – Ambos os fóruns vêm aprovando recomendações conjuntas sobre proteção de infraestruturas críticas, combate a ransomware e incentivo ao compartilhamento de informações;

Tratados Interamericanos de Cooperação (OEA) – Por meio do Comité Interamericano contra el Terrorismo (CICTE), a OEA promove iniciativas regionais de fortalecimento da resiliência cibernética nos países da América Latina e Caribe.

b) Mecanismos de Integração Regional e Multilateral

A interdependência global dos sistemas críticos torna indispensável a criação de mecanismos de integração entre Estados e organizações internacionais. Entre os mais relevantes, destacam-se:

Fóruns de Cooperação Internacional – como a Global Forum on Cyber Expertise (GFCE) e a Internet Governance Forum (IGF), que promovem o diálogo entre governos, empresas e sociedade civil sobre práticas regulatórias e técnicas;

Parcerias Estratégicas de Segurança Digital – exemplos incluem acordos bilaterais de compartilhamento de informações em tempo real sobre incidentes cibernéticos, como os celebrados entre Estados Unidos, União Europeia e países asiáticos;

Exercícios Internacionais de Simulação de Ciberataques – programas como o Locked Shields, coordenado pelo Cooperative Cyber Defence Centre of Excellence (CCDCOE) da OTAN, testam a capacidade de resposta conjunta em cenários de ataque contra infraestruturas críticas;

Redes de Resposta a Incidentes (CSIRTs e CERTs) – entidades técnicas que atuam no monitoramento, prevenção e resposta a incidentes em âmbito global, promovendo a troca de informações e boas práticas entre países.

Para o Brasil, a adesão a esses mecanismos representa não apenas uma estratégia de defesa digital, mas também uma oportunidade de aproximação diplomática, fortalecendo sua posição na governança internacional da cibersegurança.

c) Boas Práticas Globais para Proteção de Infraestruturas Críticas

Diversos países e organismos internacionais têm desenvolvido modelos regulatórios e estratégicos que podem servir de referência para o aprimoramento do sistema brasileiro de proteção às infraestruturas críticas:

Estados Unidos – O Cybersecurity and Infrastructure Security Agency (CISA) coordena a proteção de 16 setores considerados críticos, promovendo a integração entre governo e setor privado. Além disso, o país adota normas técnicas como o NIST Cybersecurity Framework, que se tornou referência global em gestão de riscos cibernéticos;

União Europeia – A criação da Agência da União Europeia para a Cibersegurança (ENISA) fortaleceu a coordenação regional, especialmente após a adoção da Diretiva NIS

(Network and Information Security), que estabelece obrigações específicas para operadores de serviços essenciais;

Japão – Implementou políticas de resiliência cibernética voltadas às Olimpíadas de Tóquio (2020), com forte ênfase em integração público-privada e na capacitação de profissionais de segurança digital;

Estônia – Considerada referência internacional em governança digital, o país desenvolveu um modelo de Estado eletrônico resiliente, no qual a proteção de infraestruturas críticas é priorizada por meio de sistemas de redundância, descentralização de servidores e programas de educação digital da sociedade.

Essas boas práticas evidenciam que a proteção das infraestruturas críticas não depende apenas da criação de normas jurídicas, mas também da integração institucional, do investimento em inovação tecnológica e da cooperação internacional estruturada.

d) Desafios para o Brasil

Embora o Brasil tenha avançado na construção de diretrizes internas, como a Política Nacional de Segurança da Informação (PNSI) e a Estratégia Nacional de Segurança Cibernética (E-Ciber), sua baixa participação em tratados internacionais e a ausência de mecanismos multilaterais efetivos de cooperação limitam a capacidade nacional de enfrentar ataques de grande escala.

A adesão à Convenção de Budapeste, a intensificação da cooperação com a OEA e a participação ativa em fóruns internacionais como o GFCE e o IGF configuram-se como passos fundamentais para consolidar a presença brasileira no cenário da governança global da cibersegurança.

Assim, a cooperação internacional e a governança global apresentam-se como elementos indispensáveis para a construção de um modelo regulatório eficaz e integrado, capaz de enfrentar os riscos cibernéticos que ameaçam as infraestruturas críticas. Ao alinhar-se às boas práticas internacionais e fortalecer sua atuação multilateral, o Brasil poderá aumentar sua resiliência digital, proteger sua soberania e contribuir para a estabilidade da segurança internacional.

5. Proposta de Modelo Regulatório e de Cooperação Internacional

A análise dos capítulos anteriores evidenciou que a ausência de um marco normativo específico voltado à proteção das infraestruturas críticas e a fragilidade da cooperação internacional constituem fatores que ampliam a vulnerabilidade do Brasil diante de ciberataques de alta complexidade. Diante desse cenário, impõe-se a necessidade de formular um modelo regulatório integrado que, ao mesmo tempo, fortaleça a governança digital nacional e posicione o país de forma mais ativa na governança global da cibersegurança.

Tal modelo deve ser concebido a partir de três eixos fundamentais: (I) a criação de um marco normativo robusto, específico para a proteção de infraestruturas críticas; (II) a integração de políticas públicas, setor privado e sociedade civil, com base em uma governança colaborativa; e (III) a adesão e fortalecimento de mecanismos de cooperação internacional, alinhados às boas práticas já consolidadas em outros países e organismos multilaterais.

a) Criação de um Marco Normativo Específico para Infraestruturas Críticas

A primeira medida essencial consiste na aprovação de uma legislação própria, destinada à proteção de infraestruturas críticas em âmbito nacional. Essa legislação deveria:

Definir quais setores e ativos devem ser classificados como críticos, com base em critérios técnicos e jurídicos claros;

Estabelecer padrões mínimos de segurança cibernética, inspirados em frameworks internacionais, como o NIST Cybersecurity Framework e a Diretiva NIS da União Europeia;

Criar protocolos unificados de prevenção, monitoramento e resposta a incidentes, aplicáveis a todos os operadores de serviços essenciais;

Instituir sanções administrativas e penais proporcionais para condutas que fragilizem a segurança das infraestruturas críticas;

Prever a criação de um centro nacional de coordenação de incidentes cibernéticos, responsável por articular a atuação entre órgãos públicos, setor privado e autoridades internacionais.

b) Integração de Políticas Públicas, Setor Privado e Sociedade Civil

O segundo eixo da proposta refere-se à necessidade de superar a atual fragmentação institucional por meio de uma governança digital colaborativa. Para tanto, seria necessária a criação de:

Parcerias público-privadas (PPPs) em cibersegurança, com o compartilhamento de informações sobre vulnerabilidades e ameaças em tempo real;

Centros integrados de resposta a incidentes (CSIRTs nacionais setoriais), vinculados ao modelo central de governança, de modo a garantir a rápida contenção e mitigação de ataques;

Programas de capacitação e conscientização social, voltados para empresas, órgãos públicos e cidadãos, a fim de construir uma cultura de segurança digital;

Planos nacionais de resiliência cibernética, com diretrizes para continuidade dos serviços essenciais mesmo em situações de crise.

Essa integração deve assegurar a participação não apenas do Estado e das grandes corporações, mas também de instituições acadêmicas, organizações da sociedade civil e pequenas e médias empresas, que frequentemente operam em cadeias interdependentes e igualmente expostas a riscos cibernéticos.

c) Fortalecimento da Cooperação Internacional

O terceiro eixo do modelo regulatório proposto consiste na intensificação da participação do Brasil em iniciativas internacionais de cibersegurança, especialmente por meio da:

Adesão à Convenção de Budapeste, o que permitiria maior alinhamento jurídico-penal e cooperação investigativa em crimes cibernéticos transnacionais;

Participação ativa em fóruns multilaterais, como o Internet Governance Forum (IGF), a Global Forum on Cyber Expertise (GFCE) e os programas da OEA/CICTE, ampliando a capacidade diplomática do país;

Estabelecimento de acordos bilaterais e regionais de compartilhamento de informações e de investigações conjuntas sobre ataques a infraestruturas críticas;

Cooperação com organismos internacionais de defesa, como a OTAN/CCDCOE, em exercícios de simulação de ataques (cyber drills), visando ao desenvolvimento da resiliência nacional;

Incentivo à harmonização de padrões técnicos e jurídicos entre países, reduzindo as assimetrias que dificultam a responsabilização de agentes maliciosos em âmbito transnacional.

Dessa forma, o modelo regulatório e de cooperação internacional aqui proposto busca não apenas fortalecer a resiliência interna do Brasil, mas também inserir o país em uma rede global de proteção cibernética, capaz de enfrentar as ameaças que desafiam a estabilidade econômica, social e política em escala planetária.

6. Conclusão

A presente pesquisa buscou analisar os desafios da cibersegurança no contexto da proteção de infraestruturas críticas, ressaltando a importância da integração entre marcos regulatórios nacionais, políticas públicas multissetoriais e mecanismos de cooperação internacional.

Constatou-se que a crescente digitalização de setores estratégicos — como energia, saúde, transportes, telecomunicações e defesa — ampliou significativamente a superfície de exposição a ciberataques complexos, capazes de gerar impactos não apenas econômicos, mas também sociais e políticos de grande magnitude. Os casos emblemáticos de Stuxnet (2010) e Colonial Pipeline (2021) ilustram como ataques direcionados podem comprometer serviços essenciais e afetar diretamente a soberania nacional e a estabilidade internacional.

No Brasil, o arcabouço normativo vigente, embora conte com instrumentos relevantes — como o Marco Civil da Internet (Lei nº 12.965/2014), a Lei Geral de Proteção de Dados (Lei nº 13.709/2018), a Lei nº 12.737/2012 (Lei Carolina Dieckmann) e o Decreto nº 9.637/2018, que institui a Política Nacional de Segurança da Informação —, ainda se revela fragmentado e insuficiente para enfrentar os riscos que incidem sobre as infraestruturas críticas. Além disso, a baixa integração institucional entre órgãos reguladores e a restrita participação do Brasil em tratados internacionais limitam a eficácia da resposta a incidentes cibernéticos de caráter transnacional.

Partindo desse diagnóstico, a hipótese levantada na introdução foi confirmada: a ausência de um marco normativo robusto e a fragilidade da cooperação internacional efetivamente ampliam os riscos à segurança digital, à estabilidade geopolítica e à soberania nacional. Como resposta a essa problemática, propôs-se um modelo regulatório e de cooperação internacional assentado em três eixos: (i) criação de um marco normativo específico para a proteção de infraestruturas críticas; (ii) integração de políticas públicas, setor privado e sociedade civil em um modelo de governança colaborativa; e (iii) fortalecimento da cooperação internacional, com destaque para a adesão à Convenção de Budapeste e a participação ativa em fóruns multilaterais.

A relevância do tema é incontestável. Do ponto de vista jurídico, contribui para o debate sobre a necessidade de atualização legislativa e alinhamento às normas internacionais. No plano social e econômico, assegura a continuidade dos serviços essenciais, a proteção de dados pessoais e a defesa da vida e da dignidade humana. Já sob a ótica geopolítica, fortalece a posição do Brasil como ator estratégico na governança global da cibersegurança.

Assim, conclui-se que a construção de um marco regulatório sólido e integrado representa não apenas uma medida de proteção interna, mas também um passo fundamental para consolidar o Brasil como parceiro confiável na defesa internacional contra ameaças cibernéticas. A efetividade dessa agenda dependerá da cooperação entre Estado, setor privado, sociedade civil e comunidade internacional, configurando-se como um dos maiores desafios contemporâneos do Direito e da política global no século XXI.

Referências

ALMEIDA, Cláudia. Perícia forense e detecção de manipulações digitais. Rio de Janeiro: Lumen Juris, 2023.

BADARÓ, Gustavo Henrique. Provas ilícitas e cadeia de custódia. São Paulo: Revista dos Tribunais, 2022.

BITTAR, Eduardo. Prova digital no processo penal. 2. ed. São Paulo: RT, 2023.

BRASIL. Código de Processo Civil. Lei nº 13.105, de 16 de março de 2015. Disponível em: http://www.planalto.gov.br. Acesso em: 15 ago. 2025.

BRASIL. Código de Processo Penal. Decreto-Lei nº 3.689, de 3 de outubro de 1941. Alterado pela Lei nº 13.964, de 24 de dezembro de 2019. Disponível em: http://www.planalto.gov.br. Acesso em: 10 ago. 2025.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Marco Civil da Internet. Disponível em: http://www.planalto.gov.br. Acesso em: 09 ago. 2025.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais. Disponível em: http://www.planalto.gov.br. Acesso em: 05 ago. 2025.

BRASIL. Medida Provisória nº 2.200-2, de 24 de agosto de 2001. Institui a Infraestrutura de Chaves Públicas Brasileira – ICP-Brasil. Disponível em: http://www.planalto.gov.br. Acesso em: 15 ago. 2025.

CAPEZ, Fernando. Crimes Digitais e Provas Eletrônicas. São Paulo: Saraiva, 2022.

CHESNEY, Robert; CITRON, Danielle. Deep Fakes and the Liar's Dividend. California Law Review, v. 107, n. 2, 2019. Disponível em: https://papers.ssrn.com. Acesso em: 18 ago. 2025.

FONSECA, Rodrigo. Perícia digital e autenticação de arquivos. Porto Alegre: Bookman, 2021.

GALDINO, Gustavo. Deepfakes e o desafio probatório no processo penal comparado. Coimbra: Almedina, 2023.

GOMES, Anderson. Blockchain, certificação digital e provas eletrônicas. São Paulo: Saraiva, 2023.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. ISO/IEC 27037:2012 — Guidelines for identification, collection, acquisition, and preservation of digital evidence. Geneva: ISO, 2012.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. ISO/IEC 27041-27043:2015 — Information security incident investigation standards. Geneva: ISO, 2015.

LOPES JR., Aury. Direito Processual Penal. 19. ed. São Paulo: Saraiva, 2023.

MICROSOFT. Video Authenticator. Disponível em: https://www.microsoft.com. Acesso em: 10 ago. 2025.

NUCCI, Guilherme de Souza. Código de Processo Penal Comentado. 19. ed. Rio de Janeiro: Forense, 2023.

PACELLI, Eugênio. Curso de Processo Penal. 27. ed. Rio de Janeiro: Atlas, 2023.

ROSA, Alexandre Morais da. Provas Digitais e Processo Penal. São Paulo: RT, 2022.

SOUZA, Marcos Vinícius. Provas digitais e processo penal: desafios contemporâneos. São Paulo: Thomson Reuters, 2022.

UNITED STATES. Federal Rules of Evidence. Rule 901. Disponível em: https://www.law.cornell.edu/rules/fre/rule_901. Acesso em: 11 ago. 2025.

UNITED STATES. United States v. Browne, 834 F.3d 403 (3d Cir. 2016). Disponível em: https://casetext.com/case/united-states-v-browne. Acesso em: 11 ago. 2025.

UNITED STATES. United States v. Thomas, 327 F. Supp. 3d 1161 (E.D. Va. 2019). Disponível em: https://casetext.com/case/united-states-v-thomas-135. Acesso em: 11 ago. 2025.

UNITED STATES. United States v. Vayner, 769 F.3d 125 (2d Cir. 2014). Disponível em: https://casetext.com/case/united-states-v-vayner. Acesso em: 11 ago. 2025.

UNIÃO EUROPEIA. Regulamento (UE) 2016/679. Regulamento Geral sobre a Proteção de Dados (GDPR). Disponível em: . Acesso em: 15 ago. 2025.

UNIÃO EUROPEIA. Tribunal de Justiça da União Europeia. Digital Rights Ireland Ltd v. Minister for Communications, C-293/12 e C-594/12, 2014. Disponível em: . Acesso em: 15 ago. 2025.

TRIBUNAL EUROPEU DE DIREITOS HUMANOS. Benedik v. Slovenia. Application no. 62357/14. Julgado em 24 abr. 2018. Disponível em: https://hudoc.echr.coe.int. Acesso em: 28 ago. 2025.