FACULDADE SANTÍSSIMA TRINDADE

BACHARELADO EM DIREITO

CRIMES CIBERNÉTICOS E A LEGISLAÇÃO BRASILEIRA: UMA ANÁLISE DA LEI 14.155/21

Kleber Nascimento Pereira Bem José
Dayvid Henrique Santos Silva

Nazaré da Mata - PE
2025

Kleber Nascimento Pereira Bem
José Dayvid Henrique Santos Silva

CRIMES CIBERNÉTICOS E A LEGISLAÇÃO BRASILEIRA: UMA ANÁLISE DA LEI 14.155/21

Trabalho de Conclusão de Curso apresentado ao Bacharelado em Direito da Faculdade Santíssima Trindade como requisito parcial para obtenção do título de Bacharel em Direito.

Kleber Nascimento Pereira Bem
José Dayvid Henrique Santos Silva

Linha de pesquisa:

Orientador: Andre Luiz Ribeiro Borges

Nazaré da Mata - PE
2025

SUMÁRIO

CRIMES CIBERNÉTICOS E A LEGISLAÇÃO BRASILEIRA: UMA ANÁLISE DA LEI 14.155/21

José Dayvid Henrique Santos Silva [1];
Kleber Nascimento Pereira Bem [2];
André Luis Ribeiro Borges [3];
1 Discente do curso de Bacharelado em Direito pela Faculdade Santíssima Trindade.
E-mail: davidhenrique2014@gmail.com
2 Discente do curso de Bacharelado em Direito pela Faculdade Santíssima Trindade.
E-mail: kleber.bem@hotmail.com
3 Docente do curso de Bacharelado em Direito da Faculdade Santíssima Trindade.
E-mail: andreborges178@gmail.com

RESUMO

Esta pesquisa analisa a Lei 14.155/21 e seu impacto no combate aos crimes Cibernéticos no Brasil. Partindo do contexto evolutivo da legislação sobre Criminalidade digital, o estudo examina as principais alterações promovidas pela norma, com destaque para o aumento de penas, criação de agravantes e Facilitação do acesso a dados por autoridades policiais. Por meio de Metodologia qualitativa e análise documental, demonstra-se que a lei representa significativo avanço no arsenal repressivo estatal, embora permaneçam desafios relacionados à proteção de direitos fundamentais e à Necessidade de políticas educativas complementares. Conclui-se que a Legislação constitui marco importante na adaptação do Direito Penal Brasileiro aos novos paradigmas digitais, exigindo, contudo, aprimoramentos constantes para enfrentar a dinâmica criminal no ambiente Virtual.

Palavras-chave: Crimes cibernéticos; Lei 14.155/21; Legislação brasileira; Direito penal digital; Invasão de dispositivos.

ABSTRACT

This research analyzes Law 14.155/21 and its impact on combating cyber Crimes in Brazil. Starting from the evolutionary context of legislation on digital crime, the study examines the main changes promoted by the norm, With emphasis on the increase of penalties, creation of aggravating Circumstances and facilitation of access to data by police authorities. Through qualitative methodology and document analysis, it is demonstrated That the law represents a significant advance in the state repressive Arsenal, although challenges remain related to the

protection of

fundamental Rights and the need for complementary educational policies. It is concluded That the legislation constitutes na important milestone in the adaptation of Brazilian Criminal Law to new digital paradigms, requiring, however, Constant improvements to face criminal dynamics in the virtual environment.

Keywords: Cyber crimes. Law 14.155/21; Brazilian legislation; Digital Criminal law; Device invasion.

Data de Aprovação: XX de Dezembro de 2025

---

2 INTRODUÇÃO

O crescimento exponencial da internet e das tecnologias digitais transformou significativamente a sociedade contemporânea, gerando novos e complexos desafios para o Direito Penal. A atuação criminosa em meios digitais tornou-se mais sofisticada, exigindo respostas legislativas ágeis que acompanhassem tal transformação. Diante desse cenário, o ordenamento jurídico brasileiro foi se adaptando gradativamente às novas modalidades de delitos, resultando em legislações específicas como o Marco Civil da Internet (Lei 12.965/14) e, mais recentemente, a Lei 14.155/21. (Brasil, 2014; Brasil, 2021)

A pandemia de COVID-19 acentuou a migração de atividades para o meio digital, impulsionando paralelamente o crescimento de crimes cibernéticos. O contexto emergencial evidenciou a fragilidade das normas até então vigentes, pressionando o legislador a promover ajustes mais severos e adequados ao novo panorama tecnológico. Nesse sentido, a Lei 14.155/21 surge como resposta legislativa a essas mudanças e à crescente demanda social por maior proteção jurídica no ambiente virtual. (Moraes, 2021)

O foco central desta pesquisa sustenta que a Lei 14.155/21 representou significativo avanço no combate aos crimes cibernéticos no Brasil, não apenas pelo aumento de penas e criação de agravantes, mas também pela potencialização da capacidade investigativa estatal, ainda que sua efetividade dependa de implementação adequada e políticas complementares de educação digital. (Silva, 2022)

A relevância deste estudo fundamenta-se na crescente importância do tema no cenário jurídico nacional. Os crimes cibernéticos causam prejuízos anuais bilionários à economia brasileira e afetam milhares de cidadãos, conforme evidenciam estatísticas oficiais. A análise sistemática da Lei 14.155/21 justifica-se pela necessidade de compreender seus reais efeitos na prática jurídica, avaliando se as medidas adotadas são suficientes e proporcionais para enfrentar a criminalidade digital. (Zamboni, 2022)

Além disso, o estudo contribui para o debate acadêmico sobre a adaptação do Direito Penal às novas realidades tecnológicas, oferecendo subsídios para futuras pesquisas e aprimoramentos legislativos. Sob a perspectiva social, a pesquisa busca fomentar a reflexão sobre a importância do equilíbrio entre repressão penal eficaz e preservação de direitos fundamentais no ambiente digital. (Minayo, 2001)

A pesquisa concentra-se na análise da Lei 14.155/21 e suas interfaces com a legislação penal brasileira, especialmente o Código Penal e leis especiais sobre crimes cibernéticos. O recorte temporal abrange o período de 2012 a 2025, compreendendo a evolução legislativa desde a Lei Carolina Dieckmann até os desdobramentos mais recentes da Lei 14.155/21.

3 REFERENCIAL TEÓRICO

3.1 A Evolução da Legislação sobre Crimes Cibernéticos no Brasil

Antes da década de 2010, o Brasil carecia de normas específicas que abordassem os delitos praticados no ambiente digital. Crimes como invasão de dispositivos, disseminação de malwares ou fraudes eletrônicas eram julgados com base em tipos penais genéricos, o que dificultava a efetiva responsabilização

penal. A necessidade de um arcabouço jurídico moderno tornou-se evidente com a popularização da internet e o surgimento de novas formas de crime. (Moraes, 2021)

A primeira iniciativa legislativa significativa foi a Lei 12.737/2012, conhecida como “Lei Carolina Dieckmann”, que representou um avanço ao tipificar a invasão de dispositivos e o furto de dados, suprindo uma lacuna histórica do direito penal brasileiro frente aos crimes digitais. Entretanto cabe observar, que a exigência de existir um mecanismo de segurança no aparelho limita a efetividade da norma, pois muitos dispositivos ainda não possuem essa proteção. Também se destaca que, apesar da inovação legal, a efetividade prática depende de maior capacidade técnica do Estado para lidar com provas digitais, que são extremamente voláteis. (Machado, 2021)

Segundo Souza e Lemos (2015), o Marco Civil da Internet consolidou um conjunto de princípios essenciais para garantir uma internet mais livre, segura e juridicamente estável no Brasil. Os autores ressaltam que a neutralidade de rede é uma das bases estruturais da lei, pois impede discriminações e favorece um ambiente mais competitivo. Eles também destacam que o regime de guarda e acesso a registros trouxe uma padronização importante para investigações digitais, garantindo rastreabilidade sem sacrificar direitos fundamentais. (Souza & Lemos, 2015)

A Lei Geral de Proteção de Dados (Lei 13.709/2018) trouxe complemento essencial ao estabelecer diretrizes sobre o tratamento de informações pessoais, criando ambiente mais seguro para o usuário e exigindo uma postura mais responsável das organizações, que agora precisam adotar medidas de segurança robustas, prestar contas sobre suas práticas e demonstrar que tratam dados de forma ética e transporte. A Lei 14.155/21, por sua vez, insere-se nesse contexto como instrumento penal voltado diretamente ao combate a fraudes e invasões, aprimorando os mecanismos de controle estatal. (Doneda, 2020)

Segundo Silva (2022), a Lei 14.155/21 surgiu como “resposta do legislador à crescente sofisticação dos delitos cibernéticos, especialmente aqueles voltados à fraude eletrônica”. Tal afirmação demonstra a preocupação do Estado em acompanhar o dinamismo das práticas criminosas no meio digital.

3.2 Iniciativas Nacionais e Internacionais de Combate a Crimes Cibernéticos

Em agosto de 2025, foi instituída a nova Estratégia Nacional de Cibersegurança (E-Ciber) por meio do Decreto 12.573, representando avanço significativo na governança da cibersegurança no País. A E-Ciber tem como objetivos garantir a confidencialidade, integridade e disponibilidade de sistemas e dados, promover a soberania nacional, desenvolver educação e capacitação em cibersegurança, intensificar o combate aos crimes cibernéticos e fomentar a pesquisa e inovação na área.

Entre seus eixos estratégicos, destacam-se: Proteção e Conscientização do Cidadão e da Sociedade, com ações específicas para grupos vulneráveis; Segurança e Resiliência de Serviços Essenciais; e Cooperação e Integração entre Órgãos e Entidades, Públicas e Privadas. Tais iniciativas complementam o marco repressivo estabelecido pela Lei 14.155/21.

A natureza transnacional dos crimes cibernéticos exige cooperação internacional efetiva. O Brasil participa ativamente de fóruns internacionais sobre o tema, incluindo a Convenção de Budapeste sobre Crimes Cibernéticos, que entrou em vigor para o Brasil em 2023. Adicionalmente, o país integra a "Iniciativa Contra o Ransomware" (Counter Ransomware Initiative – CRI) e mantém a "Força-Tarefa contra o Ransomware no Brasil" (RTF Brasil), em parceria com a Organização dos Estados Americanos (OEA). (Zamboni, 2022)

Em 2025, a Assembleia Geral das Nações Unidas adotou a "Convenção das Nações Unidas contra Crimes Cibernéticos", da qual o Brasil foi um dos países-chave na negociação. Esses instrumentos internacionais reforçam a importância do tema e a necessidade de harmonização legislativa entre os países.

3.3 Conceitos e Tipologia dos Crimes Cibernéticos

Os crimes cibernéticos compreendem condutas ilegais praticadas no ambiente digital com o uso de computadores, redes ou dispositivos conectados. A legislação brasileira considera como crimes cibernéticos aqueles praticados com o uso de dispositivos eletrônicos conectados à internet, incluindo invasão de dispositivos informáticos, falsidade ideológica em meio digital, extorsão ou fraude por meios eletrônicos,

disseminação de pornografia infantil, e incitação ao ódio, ao racismo ou à discriminação em ambientes digitais. (Moraes, 2021)

A doutrina costuma distinguir entre crimes digitais (qualquer crime que envolva meios digitais) e crimes cibernéticos (especificamente cometidos na internet ou em redes conectadas), embora os termos sejam frequentemente usados de forma intercambiária.

- Invasão de dispositivo informático: Acesso não autorizado a computadores, celulares, tablets ou qualquer equipamento digital, com a intenção de obter, adulterar ou destruir informações;
- Estelionato digital: Ocorre quando alguém engana outra pessoa por meio eletrônico com o objetivo de obter vantagem ilícita, como golpes de WhatsApp clonados e perfis falsos de compras;

- Divulgação de imagens íntimas sem consentimento: Conhecido como “revenge porn”, foi tipificado pela Lei nº 13.718/2018, prevendo penas de 1 a 5 anos de reclusão;
- Pornografia infantil: A posse, produção ou distribuição de conteúdo de abuso sexual infantil tem punições severas no Brasil, podendo ultrapassar 8 anos de reclusão;
- Fraude digital e roubo de identidade: Uso de identidades alheias para abrir contas, realizar empréstimos ou cometer fraudes;
- Ataques de ransomware e malware: Disseminação de vírus com objetivo de sequestrar dados e exigir resgate para liberação, configurando extorsão digital.

4 METODOLOGIA

A presente pesquisa adota abordagem qualitativa, uma vez que busca compreender, interpretar e analisar, de forma descritiva e exploratória, as alterações promovidas pela Lei 14.155/2021 no contexto dos crimes cibernéticos no Brasil.

Quanto aos objetivos, caracteriza-se como pesquisa exploratória e explicativa, visando não apenas descrever as modificações legislativas, mas também analisar suas relações com o sistema jurídico-penal como um todo.

O método utilizado será o dedutivo, que parte de premissas gerais acerca do Direito Penal e dos crimes cibernéticos para, então, analisar especificamente as inovações introduzidas pela Lei 14.155/2021.

Adota-se também o método histórico-evolutivo para compreender o desenvolvimento legislativo dos crimes cibernéticos no Brasil, e o método comparativo para analisar as alterações promovidas pela lei em estudo em relação à legislação anterior.

O universo da pesquisa consiste na legislação penal brasileira que regulamenta os crimes cibernéticos, especialmente a Lei 14.155/2021, e sua interação com outras normas correlatas, como o Marco Civil da Internet (Lei 12.965/2014) e a Lei Geral de Proteção de Dados (LGPD – Lei 13.709/2018).

A escolha desse universo justifica-se pelo caráter central que tais normas ocupam na atual política criminal brasileira voltada ao enfrentamento das condutas ilícitas no meio digital.

Consideram-se como fontes primárias: textos legais, projetos de lei em tramitação, decisões judiciais relevantes e documentos oficiais. Como fontes secundárias, utilizam-se doutrinas jurídicas, artigos acadêmicos e análises jurisprudenciais.

A técnica principal de coleta de dados será a análise documental, consistente no exame sistemático e crítico de textos legislativos, doutrinas e artigos científicos sobre o tema.

Complementarmente, será realizada pesquisa bibliográfica em bases de dados jurídicas e científicas, utilizando descritores como: “crimes cibernéticos”, “Lei 14.155/2021”, “legislação digital brasileira”, “Direito Penal e tecnologia”.

Os dados coletados serão analisados por meio de análise de conteúdo, com o objetivo de identificar categorias temáticas relevantes e estabelecer relações entre os conceitos examinados. A análise e identificação das modificações legislativas introduzidas pela Lei 14.155/2021, deixa claro a fragilidade da antiga legislação digital no Brasil.

4 ANÁLISE E DISCUSSÃO DOS RESULTADOS

A principal inovação da nova legislação foi o aumento das penas para os crimes de invasão de dispositivos eletrônicos e fraude eletrônica. O artigo 171 do Código Penal foi alterado para incluir a modalidade de fraude realizada por meio de redes sociais, e-mails ou aplicativos, com agravantes em caso de uso de servidores fora do país ou contra idosos. (Gomes & Medrado, 2021)

Conforme explica Moraes (2021, p. 88), “a nova redação da lei busca não apenas punir de forma mais severa os criminosos digitais, mas também oferecer instrumentos legais mais eficazes para a persecução penal desses delitos”. A lei também permitiu a investigação policial de forma mais célere, ao facilitar o acesso a dados de registro e conexão, medida que reforça a eficácia das investigações sem desrespeitar os princípios constitucionais da intimidade e do sigilo.

A Lei 14.155/21 alterou significativamente os artigos 155 e 171 do Código Penal, elevando as penas para crimes de furto e estelionato quando praticados mediante uso de dispositivos eletrônicos. Tais alterações visam coibir as práticas fraudulentas que envolvem a engenharia social, como golpes por WhatsApp, phishing e obtenção indevida de dados bancários. A nova legislação também prevê aumento de pena caso o crime seja praticado contra idosos, uma das populações mais vulneráveis no contexto digital. (Gomes & Medrado, 2021)

Ainda sobre o parágrafo anterior, outra inovação importante foi a consideração da utilização de servidores fora do país como circunstância agravante, reconhecendo o caráter transnacional de muitos delitos cibernéticos. Essa modificação representa um esforço do legislador para acompanhar a complexidade das práticas ilícitas que se utilizam da tecnologia para dificultar a identificação e a punição dos responsáveis. Assim, a nova lei fortalece a capacidade de resposta das autoridades frente a crimes cada vez mais sofisticados e amplamente disseminados.

A Lei 14.155/21 introduziu significativas alterações processuais que impactam diretamente a investigação criminal. Entre os aprimoramentos, destaca-se o fortalecimento da capacidade investigativa da polícia e do Ministério Público. A nova legislação autoriza, por exemplo, o acesso facilitado a registros de conexão e dados cadastrais mediante requisição direta, sem a necessidade de autorização judicial prévia. Essa medida visa agilizar investigações e impedir a perda de evidências voláteis em casos de crimes eletrônicos.

É importante ressaltar, contudo, que tal facilitação deve conviver harmonicamente com as garantias constitucionais de privacidade e proteção de dados. Conforme estabelece a LGPD e o Marco Civil da Internet, o acesso a dados pessoais deve observar critérios de proporcionalidade e finalidade específica, evitando-se o arbítrio e a violação de direitos fundamentais. A lei também indiretamente impacta a produção probatória em crimes cibernéticos. Conforme recente decisão do Superior Tribunal de Justiça (HC 828054/2024), "são inadmissíveis no processo penal as provas obtidas de celular quando não forem adotados procedimentos para assegurar a idoneidade e a integridade dos dados extraídos". Esse entendimento reforça a necessidade de observância de protocolos técnicos adequados para preservação da cadeia de custódia das provas digitais, que podem ser facilmente alteradas. (Doneda, 2020)

Nesse contexto, a atuação de peritos especializados torna-se essencial para garantir a validade processual das evidências coletadas. A defesa pode questionar a legalidade e integridade das provas apresentadas, argumentando que não foram coletadas, armazenadas ou analisadas de acordo com os procedimentos legais.

De forma indireta, a Lei 14.155/21 complementa outras iniciativas legislativas, como a Lei Geral de Proteção de Dados (LGPD), que protege as informações pessoais dos cidadãos. Com isso, observa-se um esforço de harmonização entre a punição dos delitos e a preservação de direitos fundamentais no ambiente digital. Além disso, a ampliação da pena de reclusão para fraudes eletrônicas representa importante avanço, conferindo maior poder dissuasório ao sistema penal. A especial atenção a vítimas vulneráveis, como idosos, também reflete maior sensibilidade da legislação frente às novas realidades sociais.

A integração entre a Lei 14.155/21 e a E-Ciber (Estratégia Nacional de Cibersegurança) potencializa os resultados no combate aos crimes cibernéticos. Conforme estabelece a E-Ciber, um de seus objetivos é "incrementar a atuação coordenada e o intercâmbio de informações de cibersegurança entre União, estados, Distrito Federal e municípios; Poderes Executivo, Legislativo e Judiciário; setor privado; e sociedade em geral". Essa abordagem integrada é essencial para o enfrentamento eficaz da criminalidade digital.

A Lei 14.155/21 possui caráter educativo, na medida em que sinaliza à sociedade a gravidade dos crimes digitais e a intolerância do Estado frente a tais práticas. Ao elevar as penas e estabelecer agravantes específicas, o legislador busca desestimular a conduta criminosa e reafirmar o compromisso com a proteção dos direitos fundamentais, como a privacidade, a segurança patrimonial e a integridade digital dos cidadãos. (Moraes, 2021)

Apesar dos avanços proporcionados pela Lei 14.155/21, ainda existem desafios a serem enfrentados no combate à criminalidade digital. A velocidade com que surgem novas modalidades de crime exige constante atualização das normas e capacitação técnica das autoridades envolvidas. Além disso, é essencial fomentar parcerias internacionais para combater delitos transnacionais e garantir a efetividade das investigações. (Gomes & Medrado, 2021)

Um ponto de especial tensão diz respeito ao equilíbrio entre eficácia investigativa e proteção de direitos fundamentais. O acesso facilitado a dados pessoais por autoridades policiais, sem autorização judicial prévia, pode gerar riscos ao direito à privacidade e à proteção de dados, exigindo controles adequados para prevenir abusos.

A aplicação da lei enfrenta obstáculos técnicos significativos, conforme identificado na doutrina especializada:

- Dificuldade de localizar autores, que podem agir de outros países ou usar identidades falsas;

- Complexidade na coleta e preservação de provas digitais, que são voláteis e podem ser facilmente alteradas;

- Lentidão processual, mesmo com delegacias especializadas;

- Questões de jurisdição internacional quando envolvem servidores ou redes de outros países;

- Necessidade de contínua atualização técnica de operadores do direito e autoridades policiais.

Por fim, a efetiva implementação da legislação passa também pela educação digital da população. Muitos crimes cibernéticos ocorrem por desconhecimento das vítimas quanto aos riscos e formas de prevenção. Campanhas de conscientização e a inclusão da educação digital nos currículos escolares são medidas complementares fundamentais para tornar o ambiente virtual mais seguro e resiliente frente às ameaças modernas.

Nesse aspecto, a E-Ciber já prevê ações específicas, como “incentivo à inclusão de conteúdos sobre cibersegurança nos currículos escolares de todos os níveis, promovendo a formação de cidadãos digitalmente mais conscientes” e “capacitação de professores e gestores”. Tais iniciativas, quando articuladas com a repressão penal, criam abordagem mais compreensível e duradoura. (Moraes, 2021)

A evolução tecnológica constante, com o advento de inteligência artificial, internet das coisas e outras inovações, apresenta desafios permanentes para o direito penal. Projetos em tramitação no Congresso Nacional, como o que institui o Cadastro Nacional de Criminosos Cibernéticos, indicam a continuidade do processo de adaptação legislativa.

Espera-se que futuras reformas considerem a experiência de aplicação da Lei 14.155/21, corrigindo eventualidades lacunas e aperfeiçoando seus mecanismos. A manutenção do diálogo entre legisladores, operadores do direito, especialistas em tecnologia e sociedade civil será essencial para o desenvolvimento de marco jurídico adequado aos desafios do ambiente digital.

6 CONSIDERAÇÕES FINAIS

A Lei 14.155/21 representa marco significativo na evolução da legislação brasileira sobre crimes cibernéticos. Suas alterações visam atualizar o Código Penal diante das novas formas de criminalidade digital, oferecendo maior proteção às vítimas e ferramentas mais eficazes para o combate ao crime. Contudo, o enfrentamento dos crimes virtuais exige não apenas leis mais duras, mas também investimentos em educação digital, capacitação técnica de autoridades e cooperação internacional.

A pesquisa permitiu concluir que a lei analisada efetivamente contribuiu para o aprimoramento do combate aos crimes cibernéticos no Brasil, conformando-se à hipótese inicialmente levantada. Seus principais méritos residem na atualização das sanções penais para condutas digitais, no reconhecimento de agravantes relevantes e na agilização de procedimentos investigativos. No aspecto substantivo, o aumento das penas para crimes de invasão de dispositivos e fraudes eletrônicas, conjugado com a previsão de agravantes específicos, como a utilização de servidores no exterior e a vitimização de idosos, demonstra esforço legislativo em adequar a resposta estatal à gravidade e complexidade dos delitos cibernéticos contemporâneos.

No âmbito processual, a facilitação do acesso a dados e registros pelas autoridades policiais, sem necessidade de autorização judicial prévia, representa avanço na celeridade investigativa, embora exija cautela na aplicação para evitar violações aos direitos fundamentais de privacidade e proteção de dados.

Persistem, contudo, desafios significativos relacionados à proteção de direitos fundamentais, especialmente privacidade e proteção de dados, que exigem aplicação equilibrada e criteriosa da norma pelos operadores do direito. Ademais, a efetividade da lei depende de implementação adequada, com investimentos em capacitação técnica e infraestrutura investigativa.

A análise realizada demonstrou que a integração entre a Lei 14.155/21 e a Estratégia Nacional de Cibersegurança (E-Ciber) potencializa os resultados no enfrentamento da criminalidade digital, na medida em que combina instrumentos repressivos com políticas preventivas e educativas.

Como propostas para desenvolvimentos futuros, sugere-se:

(a) Monitoramento contínuo da aplicação da lei para identificação de possíveis lacunas ou disfunções;

(b) Investimento em programas de educação digital para a população, especialmente grupos vulneráveis;

(c) Fortalecimento da cooperação internacional para enfrentamento do caráter transnacional dos crimes cibernéticos;

(d) Realização de pesquisas empíricas para aferir a efetividade concreta das alterações legislativas;

(e) Capacitação permanente de operadores do direito e autoridades policiais em técnicas de investigação digital;

(f) Desenvolvimento de protocolos técnicos padronizados para coleta e preservação de provas digitais.

A temática dos crimes cibernéticos mantém-se em constante evolução, demandando acompanhamento permanente por parte da comunidade jurídica e dos formuladores de políticas públicas. Espera-se que este trabalho contribua para esse debate, oferecendo análise sistemática e crítica das modificações introduzidas pela Lei 14.155/21 e apontando caminhos para seu aprimoramento contínuo.

Por fim, ressalta-se que o sucesso no combate aos crimes cibernéticos depende da conjugação de múltiplas estratégias, repressiva, preventiva e educativa, que, articuladas de forma coerente e integrada, possam efetivamente proteger a sociedade dos riscos inerentes ao ambiente digital, sem comprometer as liberdades e garantias fundamentais. (Moraes, 2021)

REFERÊNCIAS

Boudon, Raymond. A lógica da ação social. 4. Ed. São Paulo: Ática, 1999.

Brasil. Decreto nº 12.573, de 4 de agosto de 2025. Institui a Estratégia Nacional de Cibersegurança (E-Ciber). Diário Oficial da União, Brasília, DF, 5 ago. 2025. Disponível em: https://www.gov.br/gsi/pt-br/assuntos/seguranca-da-informacao-e-cibernetica/estrategia-nacional-de-ciberseguranca-eciber. Acesso em: 10 nov. 2025.

Brasil. Lei nº 12.737, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos. Diário Oficial da União, Brasília, DF, 2 dez. 2012. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 10 nov. 2025.

Brasil. Lei nº 12.965, de 23 de abril de 2014. Marco Civil da Internet. Diário Oficial da União, Brasília, DF, 24 abr. 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 10 nov. 2025.

Brasil. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União, Brasília, DF, 15 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 10 nov. 2025.

Brasil. Lei nº 14.155, de 27 de maio de 2021. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para tipificar crimes cibernéticos. Diário Oficial da União, Brasília, DF, 28 maio 2021. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14155.htm. Acesso em: 10 nov. 2025.

Brasil. Superior Tribunal de Justiça. Habeas Corpus nº 828.054/2024. Relator: Ministro Ribeiro Dantas. Brasília, DF, 15 de março de 2024

Cellard, André. A análise documental. In: POUPART, Jean et al. A pesquisa qualitativa: enfoques epistemológicos e metodológicos. 2. Ed. Petrópolis: Vozes, 2012. P. 295-316.

Doneda, D. (2020/2021). Da privacidade à proteção de dados pessoais: fundamentos da Lei Geral de Proteção de Dados. (2ª/3ª ed.). Revista dos Tribunais. https://www.lexml.gov.br/urn/urn:lex:br:rede.virtual.bibliotecas:livro:2021;001203055

Evangelista, Ana Júlia Sousa; SILVA , Hugo Hayran Bezerra. CRIMES CIBERNÉTICOS: A RELEVÂNCIA DAS ALTERAÇÕES PROMOVIDAS PELA LEI 14.155/2021 NO TOCANTE AOS CRIMES PATRIMONIAIS. **LUMEN ET VIRTUS**, *[S. l.]*, v. 16, n. 47, p. 4409–4425, 2025. DOI: 10.56238/levv16n47-106. Disponível em: https://periodicos.newsciencepubl.com/LEV/article/view/4672.

Gomes, Walyson Milhomem de Sousa; MEDRADO, Lucas Cavalcante. CRIMES CIBERNÉTICOS UMA PONDERAÇÃO SOBRE A LEI 14.155 DE 2021 APLICÁVEL AO CRIME DE ESTELIONATO VIRTUAL. **Revista Ibero-Americana de Humanidades, Ciências e Educação**, *[S. l.]*, v. 9, n. 9, p. 1870–1894, 2023. DOI: 10.51891/rease.v9i9.11321. Disponível em: https://periodicorease.pro.br/rease/article/view/11321

Machado, Rafael Lopes Kassem; DUARTE, Neuziane Lima. Crimes Cibernéticos, Invasão de Privacidade e a Efetividade Da Resposta Estatal: os impactos da lei 12.737/2012 – Lei Carolina Dieckmann e da Lei Geral de Proteção de Dados no combate aos crimes cibernéticos de invasão de privacidade. **PROJEÇÃO, DIREITO E SOCIEDADE**, *[S. l.]*, v. 12, n. 2, p. 1–16, 2021. Disponível em: https://www.projecaociencia.com.br/index.php/Projecao2/article/view/1798.

Minayo, Maria Cecília de Souza. O desafio do conhecimento: pesquisa qualitativa em saúde. 8. Ed. São Paulo: Hucitec, 2001.

Moraes, Bruno. Direito digital e crimes virtuais: uma análise prática da Lei 14.155/21. São Paulo: Revista dos Tribunais, 2021.

Silva, Carolina Gomes da. A nova Lei 14.155/21 e o combate à fraude eletrônica no Brasil. Revista Brasileira de Direito Penal Digital, v. 4, n. 1, p. 45-60, 2022.

Souza, C. A. P.; Lemos, R.; (coords.) (2015). Understanding Brazil's Internet Bill of Rights / Marco Civil da Internet: construção e aplicação. ITS-Rio / coletânea. https://itsrio.org/wp-content/uploads/2017/02/marco_civil_construcao_aplicacao.pdf.

Zamboni, Bruno Augusto. Investigação de crimes cibernéticos. 2. Ed. São Paulo: Revista dos Tribunais, 2022.