LUMEN ET VIRTUS
ISSN: 2177-2789

AS (IN)EFICIÊNCIAS COMPROBATÓRIAS DA LEGISLAÇÃO BRASILEIRA E OS DESAFIOS DA PERSECUÇÃO PENAL NOS CRIMES DE INVASÃO DE DISPOSITIVOS INFORMÁTICOS: UMA ANÁLISE À LUZ DAS LEIS 12.737/2012 E 14.155/2021

THE (IN)EFFICIENCIES OF EVIDENCE IN BRAZILIAN LEGISLATION AND THE CHALLENGES OF CRIMINAL PROSECUTION IN CRIMES OF INVASION OF COMPUTER DEVICES: AN ANALYSIS IN LIGHT OF LAWS 12.737/2012 AND 14.155/2021

LAS (IN)EFICIENCIAS DE LA PRUEBA EN LA LEGISLACIÓN BRASILEÑA Y LOS DESAFÍOS DE LA PERSECUCIÓN PENAL EN LOS DELITOS DE INVASIÓN DE DISPOSITIVOS INFORMÁTICOS: UN ANÁLISIS A LA LUZ DE LAS LEYES 12.737/2012 Y 14.155/2021

https://doi.org/10.56238/levv16n51-001

Data de submissão: 05/07/2025 **Data de publicação:** 05/08/2025

Veronica Alkmim Rocha
Mestre em Desenvolvimento Social
Instituição: Universidade Estadual de Montes Claros (UNIMONTES)
E-mail: veronica.rocha@gmail.com

Mauro Charles Alkmim Rocha
Graduando em Direito
Instituição: Faculdades Integradas Pitágoras de Montes Claros (FIPMoc Afya)
E-mail: escritasscontabeis@hotmail.com

Elisângela Pereira da Silva
Graduanda em Direito
Instituição: Faculdades Integradas Pitágoras de Montes Claros (FIPMoc Afya)
E-mail: elisangela98948444@gmail.com

Flaubert de Oliveira Neres e Souza
Graduando em Direito
Instituição: Faculdades Integradas Pitágoras de Montes Claros (FIPMoc Afya)
E-mail: flaubertneres@gmail.com

José Gilberto Dias
Graduando em Direito
Instituição: Faculdades Integradas Pitágoras de Montes Claros (FIPMoc Afya)
E-mail: betodias2207@gmail.com

Josiane Oliveira Araújo
Bacharela em Direito
Instituição: Faculdades Integradas Pitágoras de Montes Claros (FIPMoc Afya)
E-mail: josiane240188@gmail.com

Victor Santos Amaral
Graduando em Direito
Instituição: Faculdades Integradas Pitágoras de Montes Claros (FIPMoc Afya)
E-mail: amaralvictordir@gmail.com

RESUMO
Este estudo investiga a eficácia das Leis 12.737/2012 e 14.155/2021 na contenção e persecução penal dos crimes de invasão de dispositivos informáticos no Brasil, abordando as persistentes ineficiências comprobatórias. Analisa-se a legislação vigente, a evolução do direito digital até a Lei Geral de Proteção de Dados (LGPD) e as lacunas enfrentadas pelas autoridades na prova de autoria e materialidade desses delitos. A metodologia adotada é qualitativa e quantitativa, de natureza exploratória e descritiva, fundamentada em uma extensa pesquisa bibliográfica de alto impacto e análise documental de normativos jurídicos. Complementarmente, foram examinados dados estatísticos públicos da SaferNet Brasil referentes aos anos de 2019 a 2021, contextualizando a incidência de crimes cibernéticos no país. Os resultados revelam que, apesar das alterações promovidas pela Lei 14.155/2021, o Brasil mantém-se em posição de destaque nos rankings globais de crimes cibernéticos, com desafios intrínsecos à natureza digital desses delitos dificultando a efetividade da lei. Conclui-se que a legislação atual, embora aprimorada, ainda se mostra insuficiente para mitigar o crescente número de ocorrências, demandando um constante aperfeiçoamento jurídico e operacional para uma efetiva responsabilização dos infratores e a proteção da sociedade digital.

Palavras-chave: Crimes Cibernéticos. Persecução Penal. Prova Digital. Invasão de Dispositivos. Legislação Brasileira.

ABSTRACT
This study investigates the effectiveness of Laws 12.737/2012 and 14.155/2021 in containing and prosecuting computer hacking crimes in Brazil, addressing persistent evidentiary inefficiencies. It analyzes current legislation, the evolution of digital law up to the General Data Protection Law (LGPD), and the gaps faced by authorities in proving authorship and materiality of these crimes. The methodology adopted is qualitative and quantitative, exploratory and descriptive in nature, based on extensive high-impact bibliographic research and documentary analysis of legal regulations. Additionally, public statistical data from SaferNet Brasil for the years 2019 to 2021 were examined, contextualizing the incidence of cybercrime in the country. The results reveal that, despite the changes introduced by Law 14.155/2021, Brazil remains prominent in global cybercrime rankings, with challenges inherent to the digital nature of these crimes hindering the effectiveness of the law. The conclusion is that current legislation, although improved, remains insufficient to mitigate the growing number of incidents, requiring ongoing legal and operational improvements to effectively hold offenders accountable and protect the digital society.

Keywords: Cybercrimes. Criminal Prosecution. Digital Evidence. Device Hacking. Brazilian Legislation.

RESUMEN
Este estudio investiga la efectividad de las Leyes 12.737/2012 y 14.155/2021 para contener y perseguir los delitos de ciberpiratería en Brasil, abordando las persistentes ineficiencias probatorias. Analiza la legislación vigente, la evolución del derecho digital hasta la Ley General de Protección de Datos (LGPD) y las lagunas que enfrentan las autoridades para probar la autoría y la materialidad de estos delitos. La metodología adoptada es cualitativa y cuantitativa, exploratoria y descriptiva, basada en una extensa investigación bibliográfica de alto impacto y en el análisis documental de la normativa legal. Además, se examinaron datos estadísticos públicos de SaferNet Brasil para los años 2019 a 2021, contextualizando la incidencia de los delitos informáticos en el país. Los resultados revelan que, a pesar de los cambios introducidos por la Ley 14.155/2021, Brasil se mantiene destacado en los rankings mundiales de ciberdelincuencia, con desafíos inherentes a la naturaleza digital de estos delitos

que dificultan la efectividad de la ley. La conclusión es que la legislación actual, aunque mejorada, sigue siendo insuficiente para mitigar el creciente número de incidentes, por lo que se requieren mejoras jurídicas y operativas constantes para responsabilizar eficazmente a los infractores y proteger la sociedad digital.

Palabras clave: Delitos Cibernéticos. Persecución Penal. Prueba Digital. Hackeo de Dispositivos. Legislación Brasileña.

1 INTRODUÇÃO

A rápida e contínua evolução tecnológica tem transformado profundamente as interações sociais, econômicas e políticas, culminando na consolidação da sociedade da informação e no ciberespaço como ambientes ubíquos de convivência humana. Paralelamente a essas inovações, observa-se um alarmante crescimento na incidência de crimes cibernéticos, que se manifestam de diversas formas, desde furtos de informações e fraudes online até invasões de dispositivos informáticos, causando prejuízos significativos a indivíduos e organizações em escala global (Castells, 2007; Wall, 2017).

Diante da complexidade e do caráter transnacional desses delitos, o legislador brasileiro tem buscado adaptar o ordenamento jurídico para coibir tais práticas. Nesse contexto, a promulgação da Lei nº 12.737/2012 (Lei Carolina Dieckmann) representou um marco ao tipificar os crimes informáticos no Código Penal. No entanto, a dinâmica do ambiente digital, marcada pela rápida obsolescência das tecnologias e pela sofisticação das técnicas criminosas, evidenciou a necessidade de constantes aprimoramentos. Reconhecendo essas lacunas, a Lei nº 14.155/2021 introduziu alterações significativas nos dispositivos que tratam dos crimes cibernéticos, incluindo o aumento das penas e a especificação de condutas criminosas.

Apesar dos esforços legislativos, um dos maiores desafios enfrentados pelo Estado na repressão desses ilícitos reside na dificuldade de comprovação da autoria e materialidade dos crimes. A natureza volátil das evidências digitais, a possibilidade de anonimato e a complexidade do rastreamento de atividades na rede configuram obstáculos substanciais para a persecução penal eficaz (Monteiro & Diniz, 2020; Brenner, 2010). Surge, então, a problemática central que norteia este estudo: as alterações promovidas pela Lei nº 14.155/2021 são suficientes para diminuir a incidência dos crimes cibernéticos de invasão de dispositivos informáticos no Brasil, considerando as persistentes ineficiências comprobatórias da legislação anterior (Lei nº 12.737/2012)?

Com o propósito de responder a essa questão, o presente artigo tem como objetivo geral investigar as (in)eficiências comprobatórias da Lei nº 12.737/2012 e das alterações da Lei nº 14.155/2021 no que concerne à invasão de dispositivos informáticos. Para tanto, busca-se alcançar os seguintes objetivos específicos: a) descrever a evolução da informática e o surgimento do Direito Digital, com ênfase na Lei Geral de Proteção de Dados (LGPD) como marco de proteção; b) identificar as lacunas e as dificuldades enfrentadas na comprovação da autoria e materialidade nos casos de invasão de dispositivos informáticos; e c) apresentar dados estatísticos relevantes sobre a incidência de crimes cibernéticos no Brasil.

A metodologia empregada neste estudo é de abordagem qualitativa e quantitativa, de natureza exploratória e descritiva. A pesquisa qualitativa pautou-se em um rigoroso levantamento bibliográfico, abrangendo doutrinas consolidadas e artigos científicos recentes de alto impacto (nacionais e

internacionais), bem como na análise documental de legislações pertinentes (Lei nº 12.737/2012, Lei nº 14.155/2021, Marco Civil da Internet e LGPD). A abordagem quantitativa envolveu a coleta e análise de dados estatísticos públicos de organizações reconhecidas, como a SaferNet Brasil, com foco nos relatórios de ocorrências de crimes cibernéticos dos anos de 2019 a 2021, visando contextualizar a problemática empírica.

2 REFERENCIAL TEÓRICO

O presente capítulo visa aprofundar a base teórica e normativa que sustenta a análise da efetividade da legislação brasileira no combate aos crimes de invasão de dispositivos informáticos. Serão abordadas a evolução da sociedade da informação e do direito digital, a relevância da Lei Geral de Proteção de Dados (LGPD), a conceituação e classificação dos crimes cibernéticos, a análise crítica das Leis nº 12.737/2012 e nº 14.155/2021 e os desafios inerentes à investigação e à prova digital.

2.1 O CENÁRIO DA SOCIEDADE DA INFORMAÇÃO E O SURGIMENTO DO DIREITO DIGITAL

A transição para a sociedade da informação, impulsionada pela revolução tecnológica e pelo advento da internet, reconfigurou as relações sociais, econômicas e políticas em escala global. Conforme Castells (2007), a internet, originalmente desenvolvida a partir de um projeto militar do governo dos Estados Unidos (ARPANET) na década de 1960, transcendeu suas aplicações iniciais para se tornar um ambiente ubíquo de interação humana a partir de meados dos anos 1990. Atualmente, a conectividade é onipresente, viabilizada por dispositivos cada vez mais sofisticados, como smartphones, tablets e uma miríade de outros aparelhos interconectados.

Nesse contexto de hiperconectividade, a Inteligência Artificial (IA) e a robótica emergem como novas fronteiras tecnológicas, prometendo otimizar processos e facilitar o cotidiano humano (Santos et al., 2021). Contudo, essa crescente dependência tecnológica acarreta vulnerabilidades significativas, abrindo espaço para a proliferação de condutas ilícitas no ambiente virtual. A complexidade do ciberespaço, caracterizada pela velocidade da informação, transnacionalidade e pela capacidade de anonimização, impôs ao sistema jurídico tradicional o desafio de adaptar seus paradigmas e criar um arcabouço normativo específico – o Direito Digital (Lessig, 2006; Wall, 2017).

2.2 A LEI GERAL DE PROTEÇÃO DE DADOS (LGPD) E A PROTEÇÃO DE DADOS PESSOAIS

A proteção de dados pessoais tornou-se um pilar fundamental do Direito Digital, especialmente diante da crescente coleta e tratamento de informações em plataformas digitais. A Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709/2018, representa um marco regulatório no Brasil, alinhando-se a legislações internacionais como o General Data Protection Regulation (GDPR)

europeu. Seu principal objetivo é garantir o direito fundamental à privacidade e à proteção de dados pessoais, estabelecendo regras claras sobre a coleta, armazenamento, tratamento e compartilhamento dessas informações por parte de entidades públicas e privadas (Doneda, 2019).

A vigência da LGPD, marcada por diversas prorrogações e alterações legislativas (como a MP 869/2018 convertida na Lei 13.853/2019 e a MP 959/2020), reflete a complexidade de sua implementação e a necessidade de adaptação do setor público e privado. Finalmente, com a entrada em vigor de suas sanções a partir de agosto de 2021, a lei passou a impor rigorosas obrigações e penalidades, que variam desde advertências até multas de até R$ 50 milhões, visando reeducar a cultura de tratamento de dados no país (Botelho, 2020; Dower, 2020).

A LGPD, em seu Art. 5º, I, define "dados pessoais" como toda informação relacionada a pessoa natural identificada ou identificável, abrangendo, por exemplo, nome completo, CPF, RG e endereço. O inciso II do mesmo artigo conceitua "dados pessoais sensíveis" como aqueles que revelam origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, ou dado genético ou biométrico. A lei também estabelece, no Art. 14, §2º, requisitos específicos para o tratamento de dados de crianças, exigindo o consentimento específico dos pais ou responsáveis. A Autoridade Nacional de Proteção de Dados (ANPD), regulamentada pelo Decreto nº 10.474/2020, é o órgão central responsável por fiscalizar e implementar as diretrizes da LGPD, emitindo normas e promovendo a conscientização sobre a proteção de dados pessoais.

2.3 O MARCO CIVIL DA INTERNET (LEI Nº 12.965/2014) E A RESPONSABILIDADE NA REDE

O Marco Civil da Internet (Lei nº 12.965/2014) é um diploma legal fundamental no Brasil, estabelecendo princípios, garantias, direitos e deveres para o uso da internet. Ao definir a internet como "o sistema constituído do conjunto de protocolos lógicos, estruturado em escala mundial para uso público e irrestrito, com a finalidade de possibilitar a comunicação de dados entre terminais por meio de diferentes redes" (BRASIL, 2014), a lei busca regulamentar um ambiente que, por sua natureza, facilita tanto a comunicação quanto a prática de condutas ilícitas.

Embora o Marco Civil tenha sido criado com o intuito de preencher lacunas regulatórias e garantir a liberdade de expressão e a privacidade dos usuários, ele também impôs desafios à persecução penal de crimes cibernéticos. A exigência de ordem judicial para acesso a registros de conexão e acesso (Art. 15), embora essencial para a proteção da privacidade, pode gerar morosidade e dificuldades na obtenção de dados cruciais para a investigação, impactando a celeridade na identificação de infratores (Miranda & Santos, 2018; Lemos, 2017).

2.4 CRIMES CIBERNÉTICOS: CONCEITUAÇÃO E CLASSIFICAÇÕES

A expansão do uso da informática e da internet gerou uma nova categoria de ilícitos, denominados genericamente como crimes cibernéticos, crimes informáticos, crimes digitais ou crimes eletrônicos. Embora a terminologia possa variar, a essência desses delitos reside na utilização da rede de computadores ou de dispositivos informáticos como meio ou fim para a prática de condutas típicas, antijurídicas e culpáveis, que lesam bens jurídicos protegidos pelo ordenamento penal (Silva, 2015; Wall, 2017).

Para uma compreensão mais aprofundada, os crimes cibernéticos são comumente classificados da seguinte forma:

- **Crimes Próprios ou Puros:** São aqueles cuja prática depende intrinsecamente do uso da tecnologia da informação, não possuindo correspondência no mundo físico. O próprio sistema informático é o objeto ou instrumento do crime. Exemplos incluem a invasão de dispositivos informáticos (hacking) e a criação e disseminação de vírus ou outros códigos maliciosos (Malaquias, 2012; Britz, 2013).
- **Crimes Impróprios ou Mistos:** Caracterizam-se pelo uso do computador ou da internet como um meio para a prática de delitos já previstos na legislação penal tradicional. O bem jurídico tutelado não é tecnológico, mas o ambiente digital facilita a execução da conduta. Exemplos comuns incluem calúnia, injúria, difamação (crimes contra a honra praticados online), furto mediante fraude eletrônica e estelionato virtual (Crespo, 2015; Nucci, 2014).
- **Crimes Comuns:** São aqueles que podem ser praticados por qualquer pessoa, com ou sem o uso da internet. A internet, neste caso, é apenas um instrumento facilitador, sem ser essencial para a tipificação do delito.

Os agentes que atuam no ambiente cibernético também possuem classificações diversas. Além dos Hackers, indivíduos com alta capacidade técnica que podem tanto desenvolver soluções de segurança quanto explorar vulnerabilidades (Mishra & Mishra, 2013), existem os Crackers (que invadem sistemas para fins ilícitos, quebram proteções de softwares), Phreakers (especialistas em telefonia para fins criminosos), Desenvolvedores de Vírus/Malwares e Piratas de Programas, entre outros (Vianna, 2001). A compreensão dessas tipologias e atores é fundamental para a análise da eficácia da legislação penal.

2.5 OS CRIMES DE INVASÃO DE DISPOSITIVOS INFORMÁTICOS: ANÁLISE DA LEI Nº 12.737/2012 E AS ALTERAÇÕES DA LEI Nº 14.155/2021

A Lei nº 12.737/2012, conhecida como "Lei Carolina Dieckmann", representou a primeira tentativa significativa do legislador brasileiro de tipificar crimes informáticos. Sua promulgação foi

catalisada por eventos de grande repercussão, como a exposição indevida de fotos íntimas da atriz Carolina Dieckmann, cujo caso evidenciou a lacuna normativa para a proteção da privacidade e da intimidade no ambiente digital. Antes dessa lei, a tipificação de condutas como a invasão de dispositivos e o vazamento de dados era um desafio, sendo frequentemente enquadradas de forma precária em crimes como extorsão, difamação ou furto (Garcia, 2017).

A redação original do Art. 154-A do Código Penal, introduzido pela Lei nº 12.737/2012, definia o crime de invasão de dispositivo informático alheio com a ressalva "mediante violação indevida de mecanismo de segurança". Essa exigência gerou intensos debates na doutrina e jurisprudência, pois, na prática, inviabilizava a punição de invasões ocorridas em dispositivos sem senhas ou proteções ativas, ou quando a invasão se dava por vulnerabilidades não "violadas" ativamente pelo agente (Kummer, 2017; Greco, 2018). Tal limitação reduzia drasticamente a efetividade da norma, conferindo-lhe um caráter de delito de menor potencial ofensivo, com penas de detenção de três meses a um ano.

Diante da crescente sofisticação dos crimes cibernéticos e da necessidade de fortalecer o combate a essas condutas, a Lei nº 14.155/2021, sancionada em 28 de maio de 2021, promoveu alterações significativas. As principais modificações incluíram:

- **Aumento das Penas para Invasão de Dispositivo Informático:** A pena para o caput do Art. 154-A do CP foi elevada de detenção para reclusão, de um a quatro anos, e multa, retirando o caráter de delito de menor potencial ofensivo.
- **Exclusão da Exigência de "Violação de Mecanismo de Segurança":** A nova redação do Art. 154-A suprimiu a expressão "mediante violação indevida de mecanismo de segurança", ampliando o escopo de aplicação do tipo penal e permitindo a punição de invasões mesmo em dispositivos desprotegidos.
- **Qualificadoras Específicas:** Foram estabelecidos aumentos de pena para os casos em que a invasão resultar em prejuízo econômico (§2º), ou na obtenção/divulgação/comercialização de comunicações eletrônicas privadas, segredos comerciais ou informações sigilosas (§3º e §4º). Também foram previstas qualificadoras para crimes praticados contra autoridades públicas (§5º).
- **Alterações no Furto e Estelionato:** A Lei nº 14.155/2021 também modificou os artigos 155 (§4º-B, §4º-C) e 171 (§2º-A, §2º-B) do Código Penal, criando novas modalidades qualificadas de furto e estelionato praticados por meio eletrônico ou informático, com penas mais severas, e estabelecendo a competência pelo domicílio da vítima (§4º do Art. 70 do CPP).

Apesar desses avanços, a efetividade da Lei nº 14.155/2021 na prática ainda é objeto de discussão na doutrina. Embora o endurecimento das penas e a ampliação do alcance do Art. 154-A

representem um passo importante, a proporcionalidade das sanções e a capacidade real de inibição da criminalidade cibernética são temas que merecem análise contínua (Lima, 2022; Ramagem, 2022). A lei busca coibir, mas os desafios intrínsecos à investigação digital persistem, como será abordado na próxima seção.

2.6 OS DESAFIOS DA INVESTIGAÇÃO E PROVA DIGITAL EM CRIMES CIBERNÉTICOS

A investigação e a prova em crimes cibernéticos apresentam complexidades notáveis, que transcendem as dificuldades inerentes à persecução penal tradicional. A principal barreira reside na natureza fluida e volátil das evidências digitais, bem como na capacidade dos criminosos de utilizar ferramentas de anonimização e técnicas de ocultação de rastros. A identificação da autoria, em particular, emerge como um dos maiores desafios, frequentemente levando à morosidade ou ao arquivamento de inquéritos (Brenner, 2010; Grabosky & Smith, 2010).

A rastreabilidade dos IPs (Internet Protocols), que funcionam como identificadores dos dispositivos conectados à rede, é um ponto crítico. Embora os provedores de conexão e de aplicações devam manter registros de acesso, o acesso a essas informações pela polícia para fins de investigação depende de ordem judicial, conforme estabelecido pelo Marco Civil da Internet (Art. 15). Historicamente, essa exigência, embora protetiva da privacidade, tem sido apontada por autoridades policiais como um fator de lentidão no processo investigativo, com provedores que demoram a responder ou exigem o cumprimento de rigorosos trâmites judiciais (Gomes, 2016).

Estudos comparativos internacionais demonstram a discrepância no tempo de resolução de crimes cibernéticos. Enquanto em alguns países a identificação da autoria pode ocorrer em poucos dias, no Brasil, o processo pode se estender por semanas ou meses, culminando muitas vezes no arquivamento do caso por falta de elementos comprobatórios. Essa disparidade evidencia a necessidade de maior investimento em recursos tecnológicos, capacitação de profissionais especializados em forense digital e aprimoramento dos protocolos de cooperação entre as autoridades policiais, o judiciário e os provedores de internet (Norton, 2020; ITU, 2020).

Além das questões de celeridade e acesso à prova, a complexidade tecnológica dos crimes cibernéticos exige um conhecimento técnico especializado das forças policiais e do Ministério Público. A compreensão de termos como backdoor (tipo específico de trojan que permite acesso remoto a um sistema infectado) e outras vulnerabilidades é essencial para a correta qualificação dos delitos e a coleta de evidências digitais que sejam válidas em juízo. A ausência de recursos orçamentários adequados e a escassez de profissionais qualificados no campo da cibersegurança e da investigação digital são problemas recorrentes que impactam diretamente a efetividade da repressão a esses crimes (OECD, 2017).

3 METODOLOGIA

A presente pesquisa adota uma abordagem quali-quantitativa, buscando integrar a profundidade da análise descritiva com a objetividade dos dados empíricos. Quanto à sua natureza, o estudo classifica-se como exploratório e descritivo, dado que visa aprofundar a compreensão sobre as ineficiências legislativas e os desafios comprobatórios em crimes cibernéticos, ao mesmo tempo em que descreve a incidência desses delitos no contexto brasileiro.

Os procedimentos técnicos empregados na coleta e análise de dados foram os seguintes:

3.1 PESQUISA BIBLIOGRÁFICA

Realizou-se um rigoroso levantamento bibliográfico em bases de dados científicas reconhecidas, como Scopus, Web of Science, Google Scholar e bases de dados jurídicas, para identificar e analisar a literatura pertinente. Foram consultados livros, artigos científicos publicados em periódicos de alto impacto (nacionais e internacionais), teses e dissertações de programas de pós-graduação em Direito, Criminologia Cibernética e Segurança da Informação. Priorizou-se a seleção de obras clássicas da área e, em particular, publicações dos últimos três anos, a fim de garantir a atualização com o estado da arte e a diversidade de perspectivas teóricas e empíricas sobre o tema dos crimes cibernéticos e do direito digital.

3.2 PESQUISA DOCUMENTAL

A pesquisa documental envolveu a análise crítica de um conjunto de normativos jurídicos fundamentais para a temática. Foram examinadas a Lei nº 12.737/2012 (que tipificou os delitos informáticos), a Lei nº 14.155/2021 (que alterou o Código Penal, aumentando penas e aprimorando tipificações de crimes cibernéticos), o Marco Civil da Internet (Lei nº 12.965/2014) (que estabelece princípios para o uso da internet no Brasil) e a Lei Geral de Proteção de Dados Pessoais (LGPD - Lei nº 13.709/2018) (que regulamenta o tratamento de dados pessoais no país). Adicionalmente, foram consultados relatórios e documentos oficiais de organizações nacionais e internacionais de cibersegurança e órgãos de aplicação da lei, como a Interpol e a SaferNet Brasil.

3.3 COLETA E ANÁLISE DE DADOS QUANTITATIVOS

Para contextualizar a incidência e o perfil dos crimes cibernéticos, foram coletados e analisados dados estatísticos públicos da SaferNet Brasil. Especificamente, foram examinados os relatórios anuais e os dados disponíveis no site da organização, focando nas ocorrências e tipos de atendimentos relacionados a crimes cibernéticos no período compreendido entre os anos de 2019 e 2021. A análise desses dados foi de caráter descritivo, visando identificar tendências, volumes e a categorização dos delitos reportados, que serão apresentados em quadros e gráficos na seção de Resultados e Discussão.

3.4 ANÁLISE DOS DADOS

A análise dos dados qualitativos, provenientes da pesquisa bibliográfica e documental, foi realizada por meio de análise de conteúdo e análise documental, buscando identificar conceitos-chave, argumentos doutrinários e jurisprudenciais, lacunas legislativas e desafios operacionais na investigação de crimes digitais. Os dados quantitativos, por sua vez, foram submetidos a uma análise estatística descritiva, permitindo a visualização de padrões e a interpretação do panorama da criminalidade cibernética no período estudado, correlacionando-os com o arcabouço teórico e normativo.

3.5 LIMITAÇÕES DO ESTUDO

É importante reconhecer as limitações inerentes a este estudo. Não foi possível obter acesso direto a bases de dados específicas da Polícia Civil ou de outros órgãos de segurança pública sobre a totalidade dos inquéritos e condenações por crimes de invasão de dispositivos informáticos. Contudo, essa limitação foi mitigada pela utilização de fontes de dados públicas e reconhecidas (SaferNet Brasil), bem como pela profundidade da pesquisa bibliográfica e documental, que permitiu uma compreensão abrangente da problemática e dos desafios enfrentados na persecução penal desses delitos no Brasil.

4 ANÁLISE DOS RESULTADOS E DISCUSSÃO

Esta seção apresenta os dados empíricos coletados e promove um diálogo crítico com o referencial teórico estabelecido, buscando responder ao problema de pesquisa sobre a efetividade das Leis nº 12.737/2012 e nº 14.155/2021 na contenção dos crimes de invasão de dispositivos informáticos e na superação dos desafios comprobatórios.

Inicialmente, cumpre reiterar que, embora a pesquisa bibliográfica e documental tenha sido ampla, a obtenção de dados brutos e detalhados de bases de dados específicas da Polícia Civil não foi possível devido ao caráter sigiloso das informações. Contudo, essa lacuna foi suprida pela análise de relatórios e dados estatísticos públicos de instituições de referência no campo da cibersegurança, que fornecem um panorama consistente da incidência dos crimes cibernéticos no Brasil.

4.1 PANORAMA DA CRIMINALIDADE CIBERNÉTICA NO BRASIL: DADOS E TENDÊNCIAS

Estudos e relatórios recentes evidenciam a crescente e preocupante incidência de ataques e crimes cibernéticos no Brasil. Uma consultoria alemã, por exemplo, apontou que o país ocupou a 5ª posição global em ataques cibernéticos em 2021, registrando 91 milhões de ocorrências somente no primeiro trimestre daquele ano, superando os números de 2020. Além disso, a empresa holandesa de cibersegurança Surfshark destacou que o Brasil foi o 6º país mais afetado por vazamentos de dados em

2021, com estimativas indicando que aproximadamente uma em cada cinco pessoas teve seus dados comprometidos (Revista IstoÉ, 2021). Casos notórios de vazamento de dados envolvendo grandes empresas e órgãos governamentais, como Facebook, JBS, Renner e Ifood, reforçam a magnitude do problema e a vulnerabilidade do ambiente digital brasileiro.

Para uma análise mais detalhada da percepção e registro de ocorrências, foram examinados os indicadores anuais da SaferNet Brasil, organização que atua na promoção de direitos humanos na internet e no combate a crimes cibernéticos. Os dados referentes aos anos de 2019, 2020 e 2021 revelam a posição do Brasil no ranking global de registros de crimes cibernéticos, conforme sintetizado na Tabela 1:

Tabela 1: Posição do Brasil no Ranking Global de Crimes Cibernéticos (2019-2021)

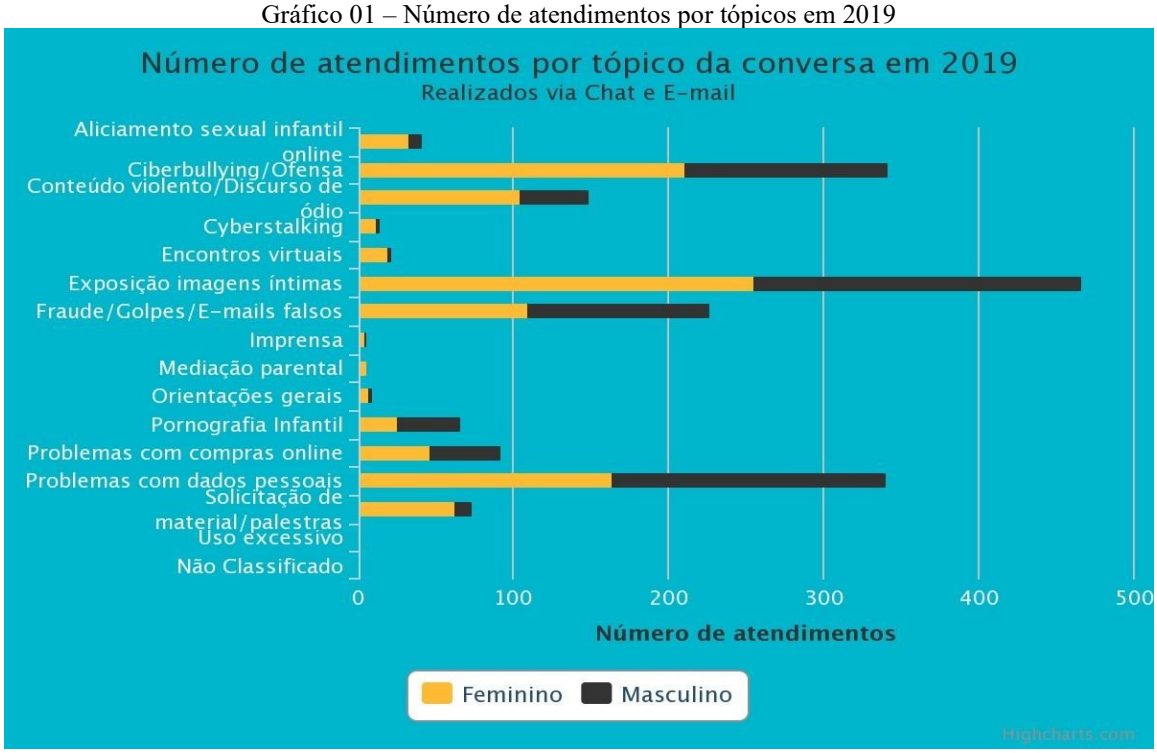
Ano	Posição do Brasil no Ranking Global de Crimes Cibernéticos
2019	6º lugar
2020	6º lugar
2021	10º lugar

Fonte: Adaptado de SaferNet Brasil (2019, 2020, 2021)

Os dados da Tabela 1 indicam que, apesar da promulgação da Lei nº 12.737/2012 em 2012, o Brasil permaneceu em uma posição alarmantemente alta no ranking de ocorrências de crimes cibernéticos até 2020. O 6º lugar mantido por anos, mesmo com uma legislação específica, sugere que a Lei nº 12.737/2012 não operou como uma ferramenta de repressão ou prevenção suficientemente eficaz. A redução para o 10º lugar em 2021, ano da sanção da Lei nº 14.155/2021, pode ser um indicativo inicial de um efeito legislativo, porém, essa posição ainda representa um nível elevado de criminalidade cibernética, demandando uma análise mais aprofundada de outros fatores.

Além do ranking geral, é fundamental observar os tipos de atendimentos e infrações mais recorrentes, que fornecem insights sobre as modalidades de crimes cibernéticos que mais afetam a população. Os Gráficos 1, 2 e 3 a seguir, adaptados dos relatórios da SaferNet Brasil, ilustram o número de atendimentos por tópicos em cada ano:

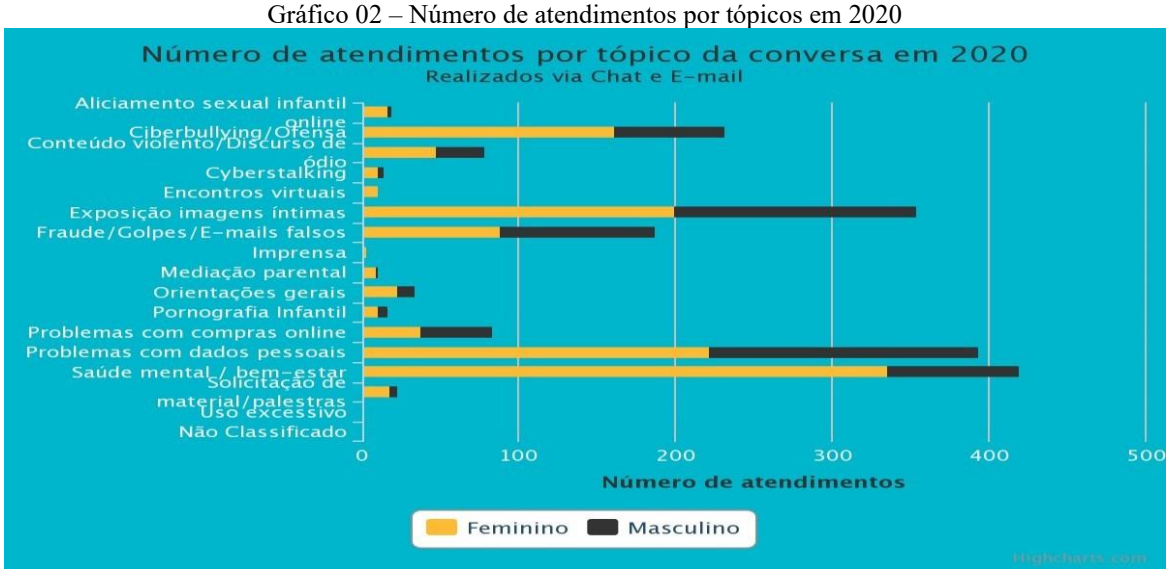
Gráfico 01 – Número de atendimentos por tópicos em 2019



Fonte: site safenet - https://indicadores.safernet.org.br/helpline/helplineviz/pt/ acesso em junho/2022

Em 2019, a "exposição de imagens íntimas" destacou-se como o tópico com maior número de registros, aproximando-se de 500 ocorrências, seguido por "ciberbullying/ofensa" e "problemas com dados pessoais" (ambos acima de 300 registros), e "fraudes/golpes/e-mails falsos" (acima de 200). Esses dados corroboram a preocupação com a proteção da privacidade e intimidade, temas que foram impulsionados, em parte, pela "Lei Carolina Dieckmann" (Lei nº 12.737/2012), mas que ainda persistiam em alta incidência.

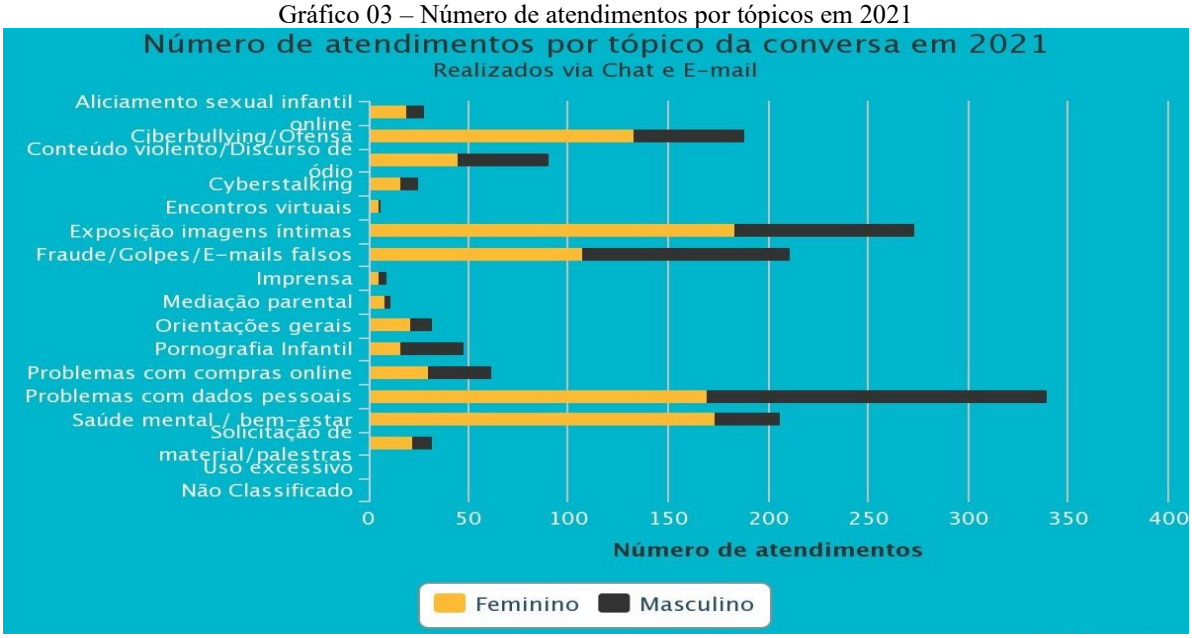
Gráfico 02 – Número de atendimentos por tópicos em 2020



Fonte: site safenet - https://indicadores.safernet.org.br/helpline/helplineviz/pt/ acesso em junho/2022

O ano de 2020 foi marcado pelo início da pandemia de COVID-19 e pelo consequente isolamento social, que intensificou a utilização de meios eletrônicos para diversas atividades. Embora o Brasil tenha mantido a 6ª posição no ranking geral de crimes cibernéticos, os tipos de ocorrências apresentaram uma mudança notável. "Saúde mental/bem-estar" (com mais de 400 atendimentos) e "Problemas com dados pessoais" (próximo a 400 registros) emergiram como as principais preocupações, refletindo o aumento da vulnerabilidade e da dependência digital da população durante o período de confinamento. A "exposição de imagens íntimas" e o "ciberbullying/ofensa" também se mantiveram com números expressivos.

Gráfico 03 – Número de atendimentos por tópicos em 2021



Fonte: site safenet https://indicadores.safernet.org.br/helpline/helplineviz/pt/ acesso em junho/2022

Em 2021, ano de transição e flexibilização das medidas de isolamento, bem como da sanção da Lei nº 14.155/2021, houve uma leve alteração no cenário. "Problemas com dados pessoais" tornou-se o principal tópico de atendimento (aproximadamente 350 registros), reforçando a relevância da LGPD. "Exposição de imagens íntimas" (mais de 250 registros) permaneceu em segundo lugar, enquanto "saúde mental/bem-estar" e "fraude/golpes/e-mails falsos" (ambos acima de 200 registros) continuaram a representar volumes significativos. A queda do Brasil para a 10ª posição geral em 2021, embora positiva, ainda sinaliza um panorama desafiador e uma criminalidade cibernética em patamares elevados.

4.2 DISCUSSÃO CRÍTICA SOBRE A EFETIVIDADE DA LEGISLAÇÃO E OS DESAFIOS COMPROBATÓRIOS

Os resultados apresentados confirmam a persistente e alta incidência de crimes cibernéticos no Brasil, levantando questionamentos sobre a real efetividade das leis penais no combate a essas

infrações. A Lei nº 12.737/2012, em seus sete anos de vigência antes das alterações de 2021, mostrou-se insuficiente para coibir a criminalidade, como evidenciado pela manutenção do Brasil entre as principais vítimas de ataques cibernéticos e vazamento de dados. A exigência original de "violação indevida de mecanismo de segurança" no Art. 154-A do CP, amplamente criticada pela doutrina (Greco, 2018), dificultava a tipificação e a consequente punição de grande parte das invasões.

As alterações da Lei nº 14.155/2021, embora representem um avanço no endurecimento das penas e na ampliação do escopo do Art. 154-A, não parecem ter gerado, de imediato, uma redução drástica no volume de ocorrências. A passagem do Brasil da 6ª para a 10ª posição em 2021, embora um sinal positivo, ainda o mantém em um patamar de alta vulnerabilidade. Esse cenário sugere que a efetividade legislativa não se limita apenas ao aumento de penas, mas depende crucialmente da capacidade de persecução penal, especialmente no que tange à prova da autoria e materialidade dos delitos.

A dificuldade na investigação dos crimes cibernéticos, como discutido por Brenner (2010) e Grabosky & Smith (2010), é um fator predominante. A obtenção e o rastreamento de IPs, embora tecnicamente possíveis, esbarram na morosidade do sistema judicial e nas respostas, por vezes lentas, dos provedores de internet, conforme relatado em discussões como as da CPI de crimes cibernéticos em 2016 (Gomes, 2016). A natureza transnacional de muitos ataques e a utilização de redes anônimas (como a dark web ou o uso de VPNs e proxies para mascarar a localização) tornam a identificação dos autores um desafio complexo que exige cooperação internacional e ferramentas de investigação forense digital mais sofisticadas (ITU, 2020; OECD, 2017).

A análise dos atendimentos da SaferNet reforça que problemas com dados pessoais e a exposição de imagens íntimas continuam a ser pautas de grande preocupação. A LGPD, embora fundamental, atua mais na prevenção e na responsabilização cível e administrativa das empresas que tratam dados, mas não resolve diretamente o desafio da identificação do criminoso que invade e utiliza esses dados de forma ilícita. A persistência de fraudes e golpes online, mesmo com o aumento das penas de estelionato eletrônico pela Lei nº 14.155/2021, demonstra a adaptabilidade dos criminosos e a necessidade de estratégias mais abrangentes que envolvam educação digital, cibersegurança e cooperação multidisciplinar.

O legislador brasileiro, ao realizar alterações no Código Penal de forma reativa a eventos de grande visibilidade, como o "Caso Carolina Dieckmann", pode ter negligenciado uma análise mais profunda das lacunas operacionais e tecnológicas que dificultam a aplicação efetiva da lei. A ineficácia percebida na contenção dos crimes cibernéticos não se deve apenas à pena cominada, mas principalmente à complexidade da prova digital e à falta de recursos humanos e tecnológicos adequados para as forças de segurança.

5 CONSIDERAÇÕES FINAIS

O presente estudo propôs-se a investigar as (in)eficiências comprobatórias da Lei nº 12.737/2012 e as alterações promovidas pela Lei nº 14.155/2021, sobre a invasão de dispositivos informáticos no Brasil, buscando identificar lacunas e possíveis soluções para mitigar a crescente criminalidade cibernética. Para tanto, analisou-se a evolução do Direito Digital, a relevância da Lei Geral de Proteção de Dados (LGPD) e os desafios inerentes à investigação e prova digital, com base em pesquisa bibliográfica, documental e dados estatísticos da SaferNet Brasil.

Os resultados da pesquisa evidenciaram que a promulgação da Lei nº 12.737/2012, embora tenha representado um marco na tipificação dos crimes informáticos – impulsionada por eventos de grande repercussão social –, revelou-se insuficiente em sua aplicação prática. A exigência da "violação indevida de mecanismo de segurança" em sua redação original, conforme analisado no referencial teórico, gerou uma lacuna que dificultava a efetiva responsabilização dos infratores e a percepção de uma pena proporcional ao dano causado.

A Lei nº 12.965/2014, o "Marco Civil da Internet", ao estabelecer direitos e garantias, também introduziu a necessidade de ordem judicial para acesso a registros de conexão e acesso. Embora fundamental para a proteção da privacidade, essa exigência, na prática, gerou morosidade e desafios adicionais às investigações policiais, conforme apontado em relatórios e debates sobre o tema.

As alterações trazidas pela Lei nº 14.155/2021, que endureceram as penas para a invasão de dispositivos informáticos e reformularam os tipos penais de furto e estelionato eletrônico, representam um avanço legislativo significativo. A exclusão da exigência de "violação de mecanismo de segurança" no Art. 154-A do Código Penal é um ponto crucial que amplia o alcance da norma.

Contudo, a análise dos dados da SaferNet Brasil revelou que, apesar dessas mudanças e da entrada em vigor das sanções da LGPD, a incidência de crimes cibernéticos no Brasil, embora tenha mostrado uma leve redução de posição no ranking global em 2021 (de 6º para 10º lugar), ainda se mantém em patamares alarmantes. A persistência de problemas com dados pessoais, exposição de imagens íntimas e fraudes/golpes continua a demandar atenção, indicando que a simples elevação das penas pode não ser suficiente para conter a criminalidade.

A problemática central deste estudo — se as alterações da Lei nº 14.155/2021 são suficientes para diminuir a incidência dos crimes cibernéticos de invasão de dispositivos informáticos no Brasil, considerando as persistentes ineficiências comprobatórias da legislação anterior — pode ser respondida com a conclusão de que, embora a nova lei represente um aprimoramento e uma tentativa de adequação à realidade tecnológica, sua efetividade plena ainda é comprometida pelos desafios estruturais e operacionais da investigação e prova digital. A dificuldade na obtenção célere de dados para identificação da autoria, a complexidade tecnológica dos delitos e a necessidade de capacitação

especializada dos agentes de segurança pública e do sistema de justiça são obstáculos que persistem, limitando a capacidade preventiva e repressiva da legislação.

Em suma, embora a hipótese de um decréscimo nas ocorrências (observado na queda da posição do Brasil no ranking SaferNet em 2021) possa ter sido parcialmente confirmada, os objetivos deste estudo foram alcançados ao evidenciar que a legislação brasileira, apesar de aprimorada, ainda necessita de complementos que transcendam o aumento de penas. É imperativo o investimento contínuo em:

- **Aprimoramento técnico-operacional:** Capacitação de profissionais para investigação forense digital e aquisição de tecnologias avançadas.
- **Cooperação interinstitucional:** Fortalecimento dos laços entre autoridades policiais, judiciário e provedores de serviços de internet, tanto nacional quanto internacionalmente.
- **Educação digital:** Campanhas de conscientização e programas de letramento digital para a população, visando reduzir a vulnerabilidade dos usuários.
- **Ajustes normativos:** Avaliação contínua da legislação para cobrir novas modalidades de crimes e fechar lacunas não endereçadas, garantindo a proteção do bem jurídico tutelado no ambiente digital.

Sugere-se, para pesquisas futuras, um estudo longitudinal que possa acompanhar os impactos da Lei nº 14.155/2021 em um período de tempo mais estendido, bem como a realização de estudos de caso com foco na persecução penal de crimes de invasão de dispositivos, a fim de identificar boas práticas e gargalos específicos no processo investigativo e judicial.

REFERÊNCIAS

BRASIL. Decreto nº 10.474, de 26 de agosto de 2020. Aprova a estrutura regimental e o quadro demonstrativo dos cargos em comissão e das funções de confiança da Autoridade Nacional de Proteção de Dados (ANPD). Diário Oficial da União, Brasília, DF, 27 ago. 2020.

BRASIL. Lei nº 12.737, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Diário Oficial da União, Brasília, DF, 3 dez. 2012.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Diário Oficial da União, Brasília, DF, 24 abr. 2014.

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.

BRASIL. Lei nº 13.853, de 8 de julho de 2019. Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados (ANPD). Diário Oficial da União, Brasília, DF, 9 jul. 2019.

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 tornar mais graves os crimes de furto qualificado e de estelionato cometidos com o uso de dispositivos eletrônicos ou informáticos. Diário Oficial da União, Brasília, DF, 28 mai. 2021.

BOTELHO, J. A LGPD e o Direito ao Esquecimento. [S.l.]: [s.n.], 2020.

BRENNER, S. W. Cybercrime: The Investigation, Prosecution and Defense of a Computer-Related Crime. 2. ed. Durham, NC: Carolina Academic Press, 2010.

BRITZ, G. Cybercrime and Penal Law. Heidelberg: Springer, 2013.

CASTELLS, M. A galáxia da internet: reflexões sobre internet, negócios e sociedade. Tradução de Rodrigo Espanha. 2. ed. Lisboa: Fundação Calouste Gulbenkian, 2007.

CRESPO, M. Crimes Informáticos. [S.l.]: [s.n.], 2015.

DONEDA, D. Da proteção de dados pessoais no Brasil. 2. ed. Rio de Janeiro: Forense; São Paulo: Método, 2019.

DOWER, N. LGPD na prática. [S.l.]: [s.n.], 2020.

FERREIRA, S. P. Crimes Cibernéticos: A ineficácia da legislação brasileira. 2021. Trabalho de Conclusão de Curso (Graduação em Direito) – Pontifícia Universidade Católica de Goiás, Goiânia, 2021. Disponível em: https://repositorio.pucgoias.edu.br/jspui/handle/123456789/1709. Acesso em: 27 jun. 2022.

GARCIA, J. C. Crimes Digitais. [S.l.]: [s.n.], 2017.

GOMES, H. S. CPI de crimes cibernéticos quer prisão de quem invadir redes sociais. G1/Globo.com, [Rio de Janeiro], 1 abr. 2016. Disponível em: https://g1.globo.com/tecnologia/noticia/2016/04/cpi-de-crimes-ciberneticos-quer-prisao-de-quem-invadir-redes-sociais.html. Acesso em: 23 jun. 2022.

GRABOSKY, P. N.; SMITH, R. G. Cybercrime: The Challenges for Law Enforcement. [S.l.]: [s.n.], 2010.

GRECO, R. Curso de Direito Penal: Parte Especial. 15. ed. Niterói: Impetus, 2018. v. 2.

INSTITUTO NACIONAL DE TELECOMUNICAÇÕES (ITU). Global Cybersecurity Index 2020. Genebra: ITU, 2020. Disponível em: https://www.itu.int/en/publications/ITU-D/Pages/default.aspx.

KUMMER, D. Direito Penal Informático. [S.l.]: [s.n.], 2017.

LEMOS, R. A Lei e o Algoritmo: como o Marco Civil da Internet está reconfigurando as relações de poder. [S.l.]: [s.n.], 2017.

LESSIG, L. Code: Version 2.0. New York: Basic Books, 2006.

LIMA, R. Manual de Direito Penal. [S.l.]: [s.n.], 2022.

MALAQUIAS, L. C. Crimes Cibernéticos. [S.l.]: [s.n.], 2012.

MIRANDA, F.; SANTOS, C. A. G. O Marco Civil da Internet e a investigação criminal. Revista Brasileira de Ciências Criminais, [S.l.], v. [volume], n. [número], p. [páginas], 2018.

MISHRA, S. K.; MISHRA, K. K. Cyber Security: Principles and Practices. [S.l.]: [s.n.], 2013.

NORTON. Norton Cyber Safety Insights Report 2020: Brazil. [S.l.]: [s.n.], 2020.

NUCCI, G. S. Código Penal Comentado. 14. ed. Rio de Janeiro: Forense, 2014.

OLIVEIRA, W. K. de; DUARTE, E.; FRANÇA, G. V. A. de; GARCIA, L. P. Como o Brasil pode deter a COVID-19. Revista de Saúde Pública, São Paulo, v. [volume], n. [número], p. [páginas], 2020. Disponível em: http://scielo.org.

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (OECD). Digital Economy Outlook 2017. Paris: OECD Publishing, 2017. Disponível em: https://www.oecd.org/en/publications/reports.html.

RAMAGEM, F. Crimes Cibernéticos: Teoria e Prática. [S.l.]: [s.n.], 2022.

REVISTA ISTOÉ. Edição 1279. [Reportagem sobre ciberataques no Brasil]. 24 jun. 2021.

SAFERNET BRASIL. Indicadores. [S.l.], [2019, 2020, 2021]. Disponível em: https://indicadores.safernet.org.br/helpline/helplineviz/pt/. Acesso em: 27 jun. 2022.

SANTOS, S. E. F. et al. A inteligência artificial e virtualização em ambientes virtuais de ensino e aprendizagem. [Nome da Revista/Periódico], [S.l.], v. [volume], n. [número], p. 2-19, 2021.

SILVA, D. Crimes Cibernéticos. [S.l.]: [s.n.], 2015.

VIANNA, A. Segurança de Dados e Informações. [S.l.]: [s.n.], 2001.

WALL, D. S. Cybercrime, Society and the State: Global Trends and Implications. [S.l.]: [s.n.], 2017.