REVISTA DCS
FUNDADA EN 2000

A LEI CAROLINA DIECKMANN E OS CRIMES CIBERNÉTICOS NO BRASIL: CONTEXTO, TIPIFICAÇÃO E IMPACTOS

THE CAROLINA DIECKMANN LAW AND CYBERCRIMES IN BRAZIL: CONTEXT, TYPIFICATION AND IMPACTS

LA LEY CAROLINA DIECKMANN Y LOS DELITOS INFORMÁTICOS EN BRASIL: CONTEXTO, TIPIFICACIÓN E IMPACTOS

Ana Flávia Andrade Ferreira[1], Anna Julia Silva Moreira[2], Divino Cesar Matias Silva[3], Gabriel Inácio Estevam Castilho[4], Lucas Antônio Guimarães[5], Lucas Rafael Sousa Narciso[6], Ricardo Bandeira Ruas[7], Vitória Martins Freitas[8], Welton Narciso Dias Neto[9], Diego Santos Almeida Pinto[10]

DOI: 10.54899/dcs.v23i91.5859
Recibido: 11/05/2026 | Aceptado: 05/06/2026 | Publicación en línea: 12/06/2026.

RESUMO

O presente trabalho tem como tema a Lei n° 12.737/2012, conhecida como Lei Carolina Dieckmann, analisando seus reflexos na proteção de dados informáticos e no enfrentamento dos crimes cibernéticos no Brasil. O estudo buscou compreender como o avanço tecnológico e a crescente utilização da internet contribuiram para o aumento dos delitos informáticos, bem como avaliar a resposta da legislação vigente. A pesquisa adotou abordagem qualitativa, baseada em levantamento bibliográfico, reunindo fundamentos teóricos e normativos para analisar a eficácia e as limitações da referida lei. Constatou-se que, embra a Lei Carolina Dieckmann represente um marco ao tipificar a invasão de dispositivos informáticos, com a inclusão do artigos 154-A e 154-B no Código Penal, ainda apresenta lacunas relevantes, como a exigência de mecanismos de segurança no dispositivo invadido, o que restringe sua aplicação. Além disso, verificou-se que,

[1] Graduanda em Direito, Centro Universitário de Goiatuba (UNICERRADO), Goiatuba, Goiás, Brasil.
E-mail: anaflaviaferreira654@gmail.com
[2] Graduanda em Direito, Centro Universitário de Goiatuba (UNICERRADO), Goiatuba, Goiás, Brasil.
E-mail: annajuliamoressi@gmail.com
[3] Graduando em Direito, Centro Universitário de Goiatuba (UNICERRADO), Goiatuba, Goiás, Brasil.
E-mail: divino.silva@alunos.unicerrado.edu.br
[4] Graduando em Direito, Centro Universitário de Goiatuba (UNICERRADO), Goiatuba, Goiás, Brasil.
E-mail: gc256420@gmail.com
[5] Graduando em Direito, Centro Universitário de Goiatuba (UNICERRADO), Goiatuba, Goiás, Brasil.
E-mail: lucasguima220@gmail.com
[6] Graduando em Direito, Centro Universitário de Goiatuba (UNICERRADO), Goiatuba, Goiás, Brasil.
E-mail: sousanarcisolucasrafael@gmail.com
[7] Graduando em Direito, Centro Universitário de Goiatuba (UNICERRADO), Goiatuba, Goiás, Brasil.
E-mail: ricardo.ruas@alunos.unicerrado.edu.br
[8] Graduanda em Direito, Centro Universitário de Goiatuba (UNICERRADO), Goiatuba, Goiás, Brasil.
E-mail: martinsfreitasvitoria7@gmail.com
[9] Graduando em Direito, Centro Universitário de Goiatuba (UNICERRADO), Goiatuba, Goiás, Brasil.
E-mail: welton.neto@alunos.unicerrado.edu.br
[10] Mestre em Olericultura, Instituto Federal Goiano (IF GOIANO). Morrinhos, Goiás, Brasil.
E-mail: d01.santos@hotmail.com Orcid: https://orcid.org/0009-0001-1073-6885

mesmo com avanços legislativos posteriores, como o Marco Civil da Internet e a Lei Geral de Proteção de Dados, persistem desafios quanto à efetividade da persecução penal e à proteção das vítimas. Observou-se, ainda, que os crimes cibernéticos geram impactos significativos, causando prejuízos morais e patrimoniais, ampliando a sensação de impunidade e afetando principalmente grupos vulneráveis, o que compromete a segurança no ambiente digital. Conclui-se que é necessário fortalecer a legislação vogente, com maior clareza e rigor na tipificação penal, além de investir em políticas públicas de conscientização e prevenção, a fim de garantir a proteção da privacidade, da intimidade e dos dados pessoais, conforme os direitos fundamentais assegurados pela Constituição Federal.

Palavras-chave: Crimes Cibernéticos. Lei Carolina Dieckmann. Proteção de Dados. Invasão de Dispositivos Informáticos. Direito Digital.

ABSTRACT

This study addresses Law No. 12,737/2012, known as the Carolina Dieckmann Law, analyzing its impacts on the protection of computer data and the fight against cybercrimes in Brazil. The research aimed to understand how technological advancement and the increasing use of the internet have contributed to the rise of cyber offenses, as well as to evaluate the response of current legislation. The study adopted a qualitative approach, based on a bibliographic review, gathering theoretical and normative foundations to analyze the effectiveness and limitations of the law. It was found that, although the Carolina Dieckmann Law represents a milestone by criminalizing the invasion of computer devices, with the inclusion of Articles 154-A and 154-B in the Brazilian Penal Code, it still presents relevant gaps, such as the requeriment of security mechanisms in the invaded device, which restricts its application. Futhermore, even with subsequent legislative advances, such as the Civil Rigths Framework for the Internet and the General Data Protection Law, challenges remain regarding the effectiveness of criminal prosecution and the protection of victims. It was also observed cybercrimes generate significant impacts, causing moral and financial damages, increasing the sense of impunity, and especially affecting vulnerable groups, thereby compromising security in the digital environment. It is concluded that it is necessary to strengthen existing legislation, with greater clarity and rigor in criminal classification, as well as to invest in public policies of awareness and prevention, in order to ensure the protection of privacy, intimacy, and personal data, in accordance with the fundamental rights guaranteed by the Federal Constitution.

Keywords: Cybercrimes. Carolina Dieckmann Law. Data Protection. Computer Device Invasion. Digital Law.

RESUMEN

Este artículo se centra en la Ley N° 12.737/2012, conocida como Ley Carolina Dieckmann, analizando su impacto en la protección de datos informáticos y la lucha contra el cibercrimen en Brasil. El estudio buscó comprender cómo el avance tecnológico y el creciente uso de internet han contribuido al aumento de los ciberdelitos, así como evaluar la respuesta de la legislación vigente. La investigación adoptó un enfoque cualitativo, basado en una revisión bibliográfica, recopilando fundamentos teóricos y normativos para analizar la efectividad y las limitaciones de la ley mencionada. Se encontró que, si bien la Ley Carolina Dieckmann representa un hito en la criminalización de la intrusión en dispositivos informáticos, con la inclusión de los artículos 154-

A y 154-B en el Código Penal, aún presenta deficiencias relevantes, como el requisito de mecanismos de seguridad en el dispositivo invadido, lo que restringe su aplicación. Además, se constató que, incluso con avances legislativos posteriores como el Marco Civil de Internet (Marco Civil da Internet) y la Ley General de Protección de Datos (Lei Geral de Proteção de Dados), persisten desafíos en cuanto a la efectividad del enjuiciamiento penal y la protección de las víctimas. Asimismo, se observó que los ciberdelitos generan impactos significativos, causando daños morales y patrimoniales, incrementando la sensación de impunidad y afectando principalmente a los grupos vulnerables, comprometiendo así la seguridad en el entorno digital. Se concluye que es necesario fortalecer la legislación vigente, con mayor claridad y rigor en la clasificación penal, así como invertir en políticas de sensibilización pública y prevención, para garantizar la protección de la privacidad, la intimidad y los datos personales, de conformidad con los derechos fundamentales consagrados en la Constitución Federal.

Palabras clave: Ciberdelitos. Carolina Dieckmann Law. Protección de datos. Piratería informática. Derecho digital.

INTRODUÇÃO

Atualmente, os crimes informáticos impulsionados pelo avanço tecnológico e pela crescente interconectividade digital, configuram-se como um dos principais desafios ao Direito Penal contemporâneo, com reflexos diretos na proteção da privacidade e na segurança dos dados pessoais. Diante da ampliação do uso da internet e de dispositivos tecnológicos, observa-se o aumento significativo dessas práticas ilícitas, evidenciando a relevância do tema e a necessidade de respostas normativas eficazes.

Nesse contexto, o direito à privacidade, consagrado como direito fundamental pela Constituição Federal de 1988, especialmente em seu artigo 5°, assume papel central na tutela da dignidade humana e da liberdade individual, sendo essencial para a proteção de outros direitos, como a liberdade de expressão e de associação.

A relevância científica e social deste estudo está em compreender como a evolução tecnológica e a insuficiência normativa influenciam a ocorrência e a expansão dos crimes cibernéticos no Brasil, bem como seus impactos na sociedade. O aumento da circulação de informações e da coleta de dados pessoais, aliado à vulnerabilidade dos usuários e à constante transformação do ambiente digital, contribui para a prática de delitos que geram prejuízos morais e patrimoniais, além de intensificar a sensação de insegurança e impunidade. Conforme apontam

estudos doutrinários, a internet, ao espaço de desenvolvimento e inovação, também se tornou um ambiente propício à atuação criminosa, em razão das facilidades de anonimato e da complexidade na identificação dos agentes.

Nesse contexto, este trabalho dedica-se a analisar o impacto da Lei n° 12.737/2012, conhecida como Lei Carolina Dieckmann, tomando como eixo central a proteção de dados informáticos e a repressão aos crimes cibernéticos no Brasil.

Diante dessa perspectiva, a presente pesquisa busca responder à seguinte pergunta: é possivel que, diante das lacunas existentes na legislação , determinados crimes cibernéticos permaneçam impunes?

O objetivo geral deste estudo consiste em verificar de que forma a legislação vigente, especialmente a Lei Carolina Dieckmann, contribui para o enfrentamento de crimes cibernéticos, evidenciando seus reflexos para a proteção da privacidade e da segurança digital.

Para isso, foram delimitados os seguintes objetivos específicos: a) Descrever a evolução dos crimes informáticos e suas principais modalidades no contexto contemporâneo; b) Analisar os reflexos desses crimes para a sociedade, considerando os prejuízos morais, patrimoniais e a vulnerabilidade de determinados grupos; e c) Identificar possíveis limitações da legislação vigente, bem como alternativas para aprimorar a proteção jurídica no ambiente digital.

Parte-se da hipótese de que a exigência de lacunas normativas, como a exigência de mecanismos de segurança nos dispositivos invadidos, pode favorecer a impunidade em determinados casos, deixando bens jurídicos relevantes sem a devida tutela estatal. Dessa forma, entende-se que tais limitações possuem reflexs diretos na efetividade da persecução penal e na proteção dos direitos fundamentais, impactando a segurança jurídica e a confiança social no ambiente digital.

Assim, para viabilizar o desenvolvimento da hipótese, caracterizou-se a pesquisa com finalidade básica estratégica, de objetivo descritivo, abordagem qualitativa, fundamentada no método hipotético-dedutivo e utilizando procedimentos bibliográfics e documentais, possibilitando uma análise crítica acerca da relação entre evolução tecnológica, legislação penal e crimes cibernéticos no Brasil.

O presente artigo divide-se em três seções. A primeira apresenta a fundamentação teórica sobre os crimes informáticos, abordando o direito à privacidade, a evolução tecnológica e as principais modalidades delitivas no ambiente digital.

A segunda seção analisa os reflexos desses crimes para a sociedade, considerando os

impactos sobre as vítimas, a segurança digital e a efetividade da atuação estatal.

A terceira e última seção apresenta alternativas para o aprimoramento da proteção jurídica, incluindo o fortalecimento da legislação, a atuação integrada dos órgãos de persecução penal e a promoção de políticas de conscientização e prevenção.

Por fim, conclui-se que os objetivos propostos foram alcançados e que a análise realizada corrobora a hipótese de que a insuficiência normativa e os desafios impostos pela evolução tecnológica podem favorecer a ocorrência e, em alguns casos, a impunidade dos crimes cibernéticos no Brasil.

Nesse contexto, torna-se pertinente considerar medidas que promovam o aprimoramento da legislação, o fortalecimento da fiscalização e o investimento em educação digital, com vistas a garantir maior efetividade na proteção da privacidade, da intimidade e dos dados pessoais, bem como a segurança no ambiente virtual.

REFERENCIAL TEÓRICO

Conforme a teoria de John Locke, a propriedade é concebida como um direito fundamental de origem natural, decorrente do trabalho humano e relacionado às ideias de estado de natureza, contrato social e sociedade civil. Ao longo da história, esse direito passou por diversas reinterpretações, especialmente com a superação do absolutismo e a ascensão do liberalismo.

Diante desse contexto, torna-se relevante compreender como a concepção lockeana de propriedade se relaciona com os direitos fundamentais na atualidade. Embora permaneça garantida nos ordenamentos jurídicos, a propriedade passou a sofrer limitações, exigindo a conciliação entre interesses individuais e coletivos. Assim, o referencial teórico busca analisar as bases filosóficas da propriedade em Locke, seu desenvolvimento histórico e seus desdobramentos no cenário jurídico contemporâneo.

CRIMES CIBERNÉTICOS

Os crimes cibernéticos consistem em condutas ilícitas praticadas por meio de sistemas informáticos, dispositivos eletrônicos ou redes digitais, especialmente a internet, sendo um reflexo direto do avanço tecnológico e da crescente digitalização das relações sociais. Tais delitos

podem ter como finalidade a violação de bens jurídicos como a privacidade, a intimidade, o patrimônio e a honra, assumindo tanto a forma de crimes próprios — que dependem do meio digital para sua execução — quanto crimes impróprios, que correspondem a infrações já previstas no ordenamento jurídico, mas praticadas no ambiente virtual.

Além disso, os crimes cibernéticos apresentam características específicas, como o anonimato dos agentes, a dificuldade de produção de provas e a possibilidade de atuação transnacional, fatores que dificultam a investigação e a responsabilização penal. Nesse contexto, sua crescente incidência evidencia a necessidade de constante atualização legislativa e de mecanismos eficazes de prevenção e repressão no ambiente digital.

Os Primeiros Crimes Cibernéticos

A compreensão da Lei nº 12.737/2012 exige, primordialmente, o resgate da trajetória técnica e comportamental que culminou na necessidade de tipificação penal dessas condutas. O crime cibernético não constitui um fenômeno isolado, mas sim um desdobramento direto da evolução das redes de comunicação e da crescente digitalização das relações sociais.

A gênese da criminalidade digital remonta ao fenômeno conhecido como phreaking. Na década de 1970, indivíduos denominados phreakers identificaram que o sistema de telefonia operava por meio de sinais de áudio. A partir da replicação da frequência de 2600 Hz, com o uso de dispositivos como a chamada Blue Box, tornava-se possível assumir o controle de centrais telefônicas. Embora tais práticas não envolvessem diretamente dados digitais, esse período foi fundamental para o desenvolvimento da lógica de exploração de vulnerabilidades sistêmicas com o objetivo de obtenção de vantagens ilícitas, característica que permanece presente nos crimes cibernéticos contemporâneos (Lévy, 1999).

Com o avanço das redes computacionais interconectadas, um dos primeiros grandes marcos de vulnerabilidade ocorreu em 1988, com o episódio do Morris Worm. Desenvolvido por Robert Tappan Morris, o programa tinha como finalidade inicial mensurar a dimensão da rede. Contudo, em razão de uma falha em sua programação, ocorreu uma replicação descontrolada, que comprometeu aproximadamente 10% da internet existente à época. Esse evento evidenciou, de forma inédita, a fragilidade das redes baseadas em relações de confiança e impulsionou a criação dos primeiros centros especializados em segurança da informação, constituindo um divisor de águas na história da cibersegurança (Hafner; Lyon, 1996).

A partir da década de 1990, com a expansão comercial da internet, observa-se uma mudança significativa no perfil dos agentes envolvidos em práticas ilícitas. O que antes era predominantemente motivado por curiosidade técnica passou a assumir caráter econômico e estruturado. O caso de Vladimir Levin, em 1994, ilustra esse novo cenário, uma vez que o agente invadiu sistemas bancários do Citibank e realizou transferências ilícitas que somaram aproximadamente 10 milhões de dólares. Nesse contexto, o anonimato proporcionado pela rede passou a ser utilizado como mecanismo de ocultação da autoria, favorecendo a prática de delitos patrimoniais, como estelionato e furto, o que evidenciou a defasagem do Código Penal brasileiro de 1940 diante das novas dinâmicas tecnológicas (cassanti, 2014).

Dessa forma, verifica-se que a evolução dos crimes cibernéticos acompanha diretamente o desenvolvimento tecnológico, passando de práticas experimentais para condutas altamente estruturadas e lucrativas. Esse processo evidencia a necessidade de constante atualização do ordenamento jurídico, a fim de garantir respostas eficazes às novas modalidades delitivas que emergem no ambiente digital.

Aumento dos Crimes Cibernéticos no Brasil

Os crimes cibernéticos têm aumentado significativamente no Brasil nos últimos anos, tem acompanhado diretamente o processo de digitalização da sociedade e a ampliação do acesso à internet. Com a popularização das redes sociais, dos serviços bancários digitais e das plataformas de comunicação, o ambiente virtual passou a ser amplamente utilizado tanto para atividades lícitas quanto para a prática de condutas ilícitas, o que contribui para o crescimento das ocorrências relacionadas à criminalidade informática.

Em 2025, houve crescimento de cerca de 28% nas denúncias, com mais de 87 mil casos registrados, e esse aumento mostra que o ambiente digital se tornou um espaço cada vez mais utilizado para práticas criminosas.

O crescimento está ligado principalmente à popularização da internet e das redes sociais. Os principais tipos de crimes praticados são:

- Fraudes eletrônicas e golpes online
- Invasão de dispositivos (hackeamento)
- Roubo e vazamento de dados pessoais
- Crimes contra a honra (difamação, injúria)

- Exploração sexual e pornografia infantil (um dos que mais crescem).

Em 2025, a maior parte das denúncias envolveu exploração sexual infantil online.

Os fatores que explicam esse aumento estão ligados ao avanço tecnológico rápido, facilidade no anonimato, dificuldade de identificação dos criminosos, aumento de usuários conectados.

Tais condutas refletem a sofisticação crescente dos meios utilizados pelos agentes criminosos e a dificuldade de identificação e responsabilização no ambiente digital.

De acordo com dados e relatórios de instituições especializadas em segurança digital, como a SaferNet Brasil e órgãos de segurança pública, tem-se verificado uma tendência de crescimento nas denúncias relacionadas a crimes cibernéticos nos últimos anos, especialmente aqueles envolvendo fraudes financeiras e exposição indevida de dados pessoais. Esse cenário evidencia não apenas a expansão quantitativa dessas ocorrências, mas também sua diversificação qualitativa, com o surgimento de novas modalidades delitivas.

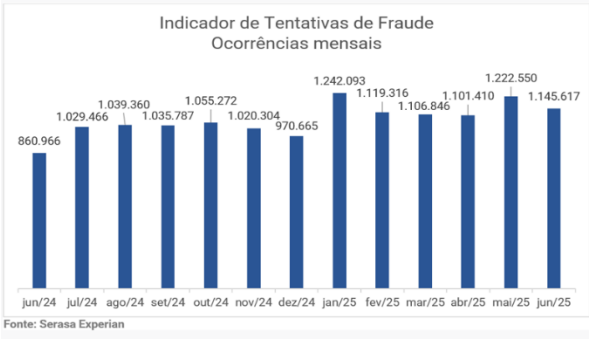
Além disso, o aumento da conectividade e o uso massivo de dispositivos móveis contribuem para a ampliação da vulnerabilidade dos usuários, que muitas vezes não possuem conhecimento técnico suficiente para identificar riscos e tentativas de fraude. Esse fator, aliado ao anonimato proporcionado pela rede, favorece a atuação de criminosos e dificulta o trabalho de investigação e repressão por parte das autoridades competentes, como a Polícia Federal.

Dessa forma, o crescimento dos crimes cibernéticos no Brasil deve ser compreendido como um fenômeno multifatorial, que envolve tanto aspectos tecnológicos quanto sociais, exigindo respostas estatais cada vez mais integradas, bem como o fortalecimento de políticas públicas de prevenção e educação digital.

Gráficos demonstram o aumento de delitos cibernéticos:

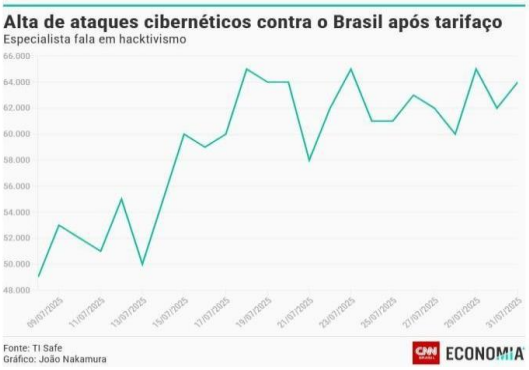
Principais condutas criminosas na internet

Quadro1. Indicador de tentaivas de fraudes



Fonte: Serasa

Quadro 2. Ataques cibernéticos



Fonte: CNN Economia

Atualmente, as condutas criminosas no ambiente digital deixaram de ser apenas invasões técnicas complexas para se tornarem, em grande parte, jogos de manipulação psicológica e engenharia social.

No topo da lista de ocorrências estão as fraudes financeiras, especialmente aquelas que exploram a rapidez do Pix e a confiança nas redes sociais. Golpes que utilizam perfis falsos no WhatsApp ou que simulam centrais telefônicas bancárias tornaram-se rotineiros, afetando cerca de um quarto da população brasileira no último ano.

O uso de deepfakes — vídeos ou áudios gerados por IA que imitam perfeitamente a voz e o rosto de familiares ou figuras públicas — elevou o patamar do estelionato digital, tornando cada vez mais difícil para o usuário comum distinguir o que é real do que é fabricado.

Além do prejuízo financeiro, a internet continua sendo um terreno fértil para crimes contra a honra, como a calúnia, a injúria e a difamação. O suposto anonimato das redes sociais encoraja ataques que podem destruir reputações em questão de segundos. Casos de cyberstalking (perseguição obsessiva digital) e a disseminação de discursos de ódio também registram altas, exigindo uma atuação mais firme das autoridades.

Paralelamente, crimes de invasão de dispositivo, tipificados pela Lei Carolina Dieckmann, evoluíram para o sequestro de dados (ransomware), onde criminosos bloqueiam o acesso a arquivos pessoais ou empresariais exigindo resgates em criptomoedas.

Para combater esse avanço, a legislação brasileira tem se modernizado com leis que endurecem as penas para fraudes eletrônicas e garantem a proteção de dados pessoais através da LGPD.

No entanto, a principal barreira contra o crime cibernético ainda é a prevenção: a desconfiança diante de links suspeitos, o uso de autenticação em duas etapas e a conscientização sobre as novas tecnologias são ferramentas essenciais para navegar com segurança em um mundo

cada vez mais conectado e vulnerável.

Tipificação dos Delitos Cibernéticos

A tipificação dos delitos cibernéticos no ordenamento jurídico brasileiro está diretamente relacionada às transformações provocadas pelo avanço das tecnologias da informação. A ampliação do uso da internet e de dispositivos digitais não apenas facilitou a comunicação, mas também possibilitou o surgimento de novas formas de prática criminosa, muitas vezes não previstas originalmente pelo legislador penal.

Nesse contexto, o Direito Penal passou a enfrentar o desafio de adequar suas normas à realidade virtual, buscando proteger bens jurídicos como a privacidade, a intimidade e o patrimônio. Conforme destaca Souza Filho (2024), o ordenamento jurídico brasileiro ainda apresenta lacunas relevantes no tratamento dos crimes cibernéticos, especialmente diante da rapidez com que essas condutas evoluem.

Novas normas passaram a complementar a proteção no ambiente digital, como a Lei nº 12.965/2014 (Marco Civil da Internet), que estabelece princípios, garantias e deveres para o uso da internet no Brasil (Brasil, 2014), e a Lei nº 13.709/2018 (Lei Geral de Proteção de Dados), que disciplina o tratamento de dados pessoais (Brasil, 2018). Ainda que não tenham natureza estritamente penal, tais legislações contribuem para a estrutura normativa de enfrentamento das condutas ilícitas no meio digital.

No âmbito doutrinário, os delitos cibernéticos costumam ser classificados em crimes próprios e impróprios. Os crimes próprios são aqueles que dependem necessariamente do meio informático para sua execução, como a invasão de sistemas e a disseminação de softwares maliciosos. Já os crimes impróprios correspondem a condutas previstas no ordenamento jurídico, mas que passam a ser praticadas por meio digital, como o estelionato, a difamação e a ameaça.

Por outro lado, autores especializados em direito digital destacam que a complexidade do ambiente virtual exige constante atualização legislativa. Nesse sentido, Pinheiro (2021) aponta que a dinâmica das relações digitais e a sofisticação das práticas ilícitas dificultam a atuação estatal, especialmente no que se refere à identificação dos autores e à produção de provas.

Além das dificuldades relacionadas à tipificação, a persecução penal desses delitos enfrenta desafios específicos, como a identificação dos autores, a volatilidade das provas digitais e a transnacionalidade das condutas. Esses fatores dificultam a aplicação da lei e exigem não

apenas o aprimoramento legislativo, mas também mecanismos de cooperação internacional.

Dessa forma, embora o Brasil tenha avançado na tipificação dos delitos cibernéticos, ainda se verifica a necessidade de constante atualização normativa. A complexidade e a dinamicidade do ambiente digital impõem ao Direito Penal o desafio de equilibrar a proteção eficaz dos bens jurídicos com a garantia dos direitos fundamentais.

Tratamento Legislativo Dos Crimes Cibernéticos no Brasil

O tratamento legislativo dos crimes cibernéticos no Brasil estrutura-se a partir de um conjunto de diplomas normativos que, embora não componham um sistema penal digital unificado, formam a base jurídica responsável pela tipificação, prevenção e repressão das condutas ilícitas praticadas no ambiente virtual.

Nesse contexto, a Lei n.º 12.737/2012, conhecida como Lei Carolina Dieckmann, representa o marco inicial da criminalização específica de delitos informáticos no ordenamento jurídico brasileiro. A referida legislação introduziu no Código Penal os artigos 154-A e 154-B, tipificando a conduta de invasão de dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança, com o objetivo de obter, adulterar ou destruir dados ou informações.

Além da tipificação básica, a norma prevê formas qualificadas do delito, especialmente quando da invasão resulta a obtenção de conteúdos de comunicações privadas, segredos comerciais ou industriais, informações sigilosas ou ainda o controle remoto não autorizado do dispositivo invadido. Apesar de sua relevância histórica, a Lei n.º 12.737/2012 é objeto de críticas doutrinárias, sobretudo quanto à redação técnica e à limitação inicial das penas, consideradas desproporcionais frente à gravidade das condutas praticadas no ambiente digital.

Em seguida, o Marco Civil da Internet (Lei n.º 12.965/2014) instituiu um paradigma regulatório de natureza principiológica para o uso da internet no Brasil. Embora não possua natureza penal, sua relevância no campo dos crimes cibernéticos é indireta e significativa, uma vez que estabelece diretrizes sobre a responsabilidade civil de provedores, a guarda de registros de acesso e a proteção de direitos fundamentais no ambiente virtual. Tais disposições impactam diretamente a produção de provas em investigações criminais e a delimitação da licitude de medidas investigativas no meio digital.

A Lei Geral de Proteção de Dados Pessoais (Lei n.º 13.709/2018) acrescenta outro eixo

normativo relevante ao sistema, ao regulamentar o tratamento de dados pessoais por pessoas físicas e jurídicas, públicas ou privadas. Embora não contenha tipos penais próprios, sua interface com o Direito Penal é evidente, pois violações graves a seus dispositivos podem se relacionar a crimes já previstos no Código Penal, como delitos contra a honra, a privacidade e o patrimônio, além de influenciar a configuração de circunstâncias qualificadoras e agravantes em determinadas hipóteses.

Posteriormente, a Lei n° 14.155/2021 representou avanço relevante no enfrentamento das fraudes digitais, ao agravar as penas dos crimes de invasão de dispositivo informáticos, furto e estelionato quando cometidos por meio de dispositivos eletrônicos, redes de computadores ou qualquer outro meio digital. A norma surgiu como resposta ao aumento expressivo de golpes virtuais no país, especialmente aqueles envolvendo fraudes bancárias e transferências eletrônicas indevidas, reforçando a maior reprovabilidade da conduta quando praticada no ambiente digital.

Mais recentemente, o Decreto Legislativo n.º 37/2023 aprovou a adesão do Brasil à Convenção sobre o Cibercrime do Conselho da Europa (Convenção de Budapeste), considerada o principal instrumento internacional de cooperação no combate aos crimes cibernéticos. A incorporação desse tratado representa um avanço relevante na harmonização normativa internacional, especialmente no que se refere à tipificação de condutas, à cooperação jurídica entre Estados e ao aprimoramento dos mecanismos de obtenção de prova digital.

Dessa forma, observa-se que o arcabouço normativo brasileiro relativo aos crimes cibernéticos evidencia um processo gradual de especialização legislativa. Contudo, ainda se caracteriza por fragmentação normativa e pela necessidade de constante atualização, em razão da rápida evolução tecnológica e da sofisticação das condutas criminosas no ambiente digital.

LEI CAROLINA DIECKMANN (LEI N° 12.737/2012)

A Lei nº 12.737/2012, conhecida como Lei Carolina Dieckmann, representa um marco na legislação brasileira ao tipificar os crimes informáticos, especialmente a invasão de dispositivos eletrônicos sem autorização. A norma introduziu os artigos 154-A e 154-B no Código Penal, estabelecendo punições para a obtenção, adulteração ou destruição de dados sem consentimento do titular . Sua criação foi motivada pela necessidade de proteção da privacidade e dos dados pessoais no ambiente digital, diante do aumento dos crimes cibernéticos no Brasil.

Determinantes do Contexto de Criação da Lei Carolina Dieckmann, Tipificação Penal e Impactos da Legislação

Os crimes informáticos constituem um fenômeno cada vez mais recorrente nas sociedades contemporâneas, especialmente naquelas marcadas pelo intenso desenvolvimento tecnológico e pela ampla difusão da internet. No Brasil, esse cenário representa um dos principais desafios ao Direito Penal moderno, uma vez que a expansão do ambiente digital possibilitou novas formas de interação social, mas também ampliou significativamente as oportunidades para a prática de condutas ilícitas. Entre os fatores mais relevantes que impulsionam esse contexto destacam-se o crescimento exponencial da conectividade, a popularização de dispositivos eletrônicos, a insuficiência normativa inicial e a dificuldade de adaptação das instituições estatais às novas dinâmicas do ciberespaço. sonegação fiscal é um fenômeno recorrente em diversos países, especialmente naqueles que possuem elevada carga tributária e falhas estruturais na administração pública. No Brasil, essa prática representa um dos principais desafios para o Estado, comprometendo a arrecadação e refletindo diretamente na oferta de serviços essenciais. Entre os fatores mais relevantes estão a alta carga de impostos, a complexidade do sistema tributário e a percepção de ineficiência na gestão dos recursos públicos.

A origem desse ambiente digital remonta à criação da internet a partir da ARPANET, desenvolvida nos Estados Unidos na década de 1960, inicialmente com fins militares e estratégicos. Posteriormente, essa tecnologia evoluiu e se expandiu globalmente, chegando ao Brasil de forma mais ampla a partir da década de 1990. A partir desse momento, consolidou-se um novo espaço de interação denominado ciberespaço, caracterizado por sua natureza imaterial, descentralizada e em constante expansão. Nesse ambiente, surgem também conceitos como cibercultura, que corresponde às práticas sociais desenvolvidas no meio digital, e cibercrime, que se refere às condutas ilícitas praticadas por meio de sistemas informáticos ou da internet.

Nesse contexto, os crimes informáticos passam a assumir múltiplas formas, incluindo invasão de dispositivos, furto e vazamento de dados, fraudes eletrônicas, disseminação de conteúdos ilícitos, entre outros. A facilidade de acesso à internet, aliada à possibilidade de anonimato e à utilização de tecnologias avançadas, contribui para a atuação de agentes que exploram vulnerabilidades técnicas e humanas.

A divisão da internet em diferentes camadas — como surface web, deep web e dark web— intensifica esse cenário, uma vez que determinadas áreas oferecem maior grau de

anonimatoe menor controle estatal, favorecendo a prática de atividades ilícitas.

É importante distinguir, no plano conceitual, os crimes informáticos dos crimes cibernéticos. Enquanto os primeiros abrangem todas as condutas ilícitas que envolvem o uso de sistemas computacionais, os segundos referem-se especificamente àquelas realizadas por meio da internet. Ademais, termos como “hacker” e “cracker” não possuem, em sua origem, conotação necessariamente criminosa, sendo utilizados para designar indivíduos com habilidades técnicas em informática, os quais podem atuar tanto de forma lícita quanto ilícita. Essa distinção é fundamental para evitar generalizações e permitir uma análise mais precisa do fenômeno.

A evolução tecnológica contínua tem imposto desafios significativos ao Direito, especialmente no que diz respeito à tipificação penal dessas condutas. Durante muito tempo, o ordenamento jurídico brasileiro não possuía normas específicas para tratar dos crimes informáticos, o que exigia a aplicação analógica de dispositivos do Código Penal, muitas vezes de forma insuficiente. Diante desse cenário, tornou-se evidente a necessidade de criação de uma legislação própria, capaz de responder às demandas emergentes do ambiente digital.

É nesse contexto que surge a Lei n.º 12.737/2012, conhecida como Lei Carolina Dieckmann, responsável por introduzir no Código Penal os artigos 154-A e 154-B, tipificando a invasão de dispositivos informáticos. A criação dessa norma representou um marco inicial na tentativa de adequar o sistema jurídico brasileiro às novas realidades tecnológicas, conferindo maior proteção aos dados e às informações pessoais dos indivíduos.

A criação da Lei Carolina Dieckmann está diretamente relacionada à necessidade de proteção de direitos fundamentais, especialmente o direito à privacidade e à intimidade.

Esses direitos possuem profunda fundamentação histórica e filosófica, com destaque para as contribuições de John Locke, que, no contexto do liberalismo, defendeu a liberdade individual e o direito do indivíduo de controlar sua própria vida e suas informações. Ao longo do tempo, esses direitos foram incorporados aos ordenamentos jurídicos modernos, sendo reconhecidos como essenciais para a dignidade da pessoa humana.

No Brasil, a Constituição Federal de 1988 consagra, em seu artigo 5º, a inviolabilidade da intimidade, da vida privada, da honra e da imagem, assegurando o direito à reparação em caso de violação. Contudo, a efetivação desses direitos no ambiente digital enfrenta desafios consideráveis, especialmente diante da massiva coleta de dados, da exposição constante nas redes e da dificuldade de controle sobre as informações compartilhadas.

Além disso, a proteção da privacidade no contexto digital também encontra respaldo em

instrumentos internacionais e em legislações complementares, como o Marco Civil da Internet e a Lei Geral de Proteção de Dados (LGPD), que ampliam a regulamentação sobre o uso e o tratamento de dados pessoais. Ainda assim, a constante evolução tecnológica exige atualização contínua das normas e das práticas institucionais.

Outro fator determinante nesse cenário é a dificuldade de investigação e responsabilização dos autores de crimes cibernéticos. A utilização de ferramentas de criptografia, redes privadas e outros mecanismos de ocultação dificulta a identificação dos agentes, contribuindo para a sensação de impunidade. Além disso, a atuação desses crimes muitas vezes ultrapassa fronteiras nacionais, exigindo cooperação internacional e estratégias mais sofisticadas de enfrentamento.

Por fim, observa-se que o problema dos crimes informáticos não se limita à existência de condutas ilícitas, mas envolve uma complexa relação entre tecnologia, direito e sociedade. A evolução constante do ambiente digital exige do Estado não apenas a criação de normas mais eficazes, mas também o fortalecimento das instituições responsáveis pela investigação e repressão desses delitos, bem como a promoção de políticas públicas voltadas à educação digital e à conscientização dos usuários.

Dessa forma, compreender o contexto de criação da Lei Carolina Dieckmann, bem como a tipificação penal das condutas e os impactos práticos da legislação, permite uma análise mais ampla e crítica da proteção jurídica no ambiente digital. Esses elementos evidenciam a necessidade de constante adaptação do Direito às transformações tecnológicas, de modo a garantir a efetiva tutela dos direitos fundamentais e a segurança das relações no ciberespaço.

Sua criação está diretamente relacionada à crescente incidência de delitos praticados no ambiente digital, impulsionados pelo avanço tecnológico e pela ampliação do uso da internet. No Brasil, essa realidade passou a exigir respostas normativas específicas, uma vez que, até então, muitas dessas condutas não eram devidamente tipificadas, o que dificultava a responsabilização dos agentes e contribuía para a sensação de impunidade.

De acordo com a doutrina, a referida lei surgiu como instrumento destinado a suprir lacunas existentes no Direito Penal, especialmente no que se refere à invasão de dispositivos informáticos. Conforme destacado por Monteiro (2022), antes de sua promulgação, o simples acesso indevido a dispositivos eletrônicos não era considerado crime, sendo tratado, em muitos casos, apenas como ato preparatório.

Com o advento da lei, passou-se a reconhecer essa conduta como ilícita, ampliando as

possibilidades de punição e fortalecendo a tutela jurídica no ambiente digital.

O contexto de criação da Lei Carolina Dieckmann está intimamente ligado a um caso concreto de grande repercussão nacional, envolvendo a divulgação não autorizada de imagens íntimas da atriz Carolina Dieckmann, após a invasão de seu dispositivo eletrônico. O episódio evidenciou a vulnerabilidade dos usuários e a ausência de mecanismos legais adequados para a proteção da privacidade no meio digital, impulsionando o debate público e jurídico sobre a necessidade de regulamentação específica.

É importante destacar que a prática de invasão e subtração de dados já ocorria

anteriormente, porém carecia de amparo legal específico. Com a crescente digitalização da vida cotidiana, os indivíduos passaram a compartilhar grandes volumes de informações pessoais online, o que intensificou as preocupações relacionadas à segurança e ao uso indevido desses dados. Nesse cenário, a proteção da privacidade e da intimidade assume papel central, sendo considerada essencial para a garantia da liberdade individual e da autonomia dos sujeitos.

Os danos causados pelos crimes cibernéticos não se limitam ao aspecto patrimonial, mas atingem também a esfera psicológica das vítimas, gerando sentimentos de vulnerabilidade, exposição e, muitas vezes, impunidade. A divulgação indevida de informações pessoais ou imagens íntimas pode causar prejuízos irreparáveis, reforçando a importância de mecanismos legais eficazes para a proteção dos indivíduos no ambiente digital. Nesse sentido, a denúncia e a atuação dos órgãos de persecução penal tornam-se fundamentais para a efetividade da legislação.

A legislação também se articula com outros diplomas normativos, como a Lei de Acesso à Informação (Lei n.º 12.527/2011), que estabelece diretrizes para o tratamento de dados pessoais com respeito à intimidade e à privacidade.

Ademais, alterações posteriores, como a promovida pela Lei n.º 14.155/2021, reforçaram o combate aos crimes cibernéticos, ampliando as hipóteses de incidência e aumentando as penalidades, especialmente em casos que envolvem fraudes eletrônicas e prejuízos a instituições financeiras.

No plano jurisprudencial, os tribunais superiores têm consolidado o entendimento sobre a aplicação da lei, reconhecendo a importância da representação da vítima para a persecução penal e reafirmando a tipificação das condutas previstas no artigo 154-A do Código Penal.

Esse movimento contribui para a uniformização da interpretação e para o fortalecimento da segurança jurídica.

Por fim, observa-se que, embora a Lei Carolina Dieckmann represente um avanço

significativo, sua efetividade ainda enfrenta desafios diante da constante evolução tecnológica e da sofisticação dos crimes cibernéticos. A ampliação do uso da internet, aliada à exposição voluntária de informações pessoais pelos próprios usuários, contribui para a intensificação dos riscos e para a complexidade na proteção da privacidade.

Metodologia de Aplicação da Lei Carolina Dieckmann

A internet contemporânea, consolidada em praticamente todos os estratos da sociedade brasileira, constitui um vetor de evolução comunicativa, audiovisual e instantânea. Contudo, o uso nocivo dessas conexões demonstra que o progresso tecnológico é ambivalente, trazendo riscos latentes.

Nesse sentido, embora o ciberespaço tenha sido outrora percebido como um território anômico (sem leis), a Lei Carolina Dieckmann (Lei nº 12.737/2012) surgiu como um marco divisório no Direito Digital, tipificando a invasão de dispositivo informático.

Atualmente, essa legislação não opera de forma isolada, mas atua como o alicerce de um ecossistema complexo de combate aos crimes cibernéticos. Com os avanços tecnológicos sem precedentes, novos mecanismos de suporte foram integrados a esse ordenamento, seguindo uma metodologia de proteção integral. A Lei Geral de Proteção de Dados (LGPD - Lei nº 13.709/2018), por exemplo, subsidia decisões judiciais e estabelece um controle rigoroso sobre a segurança informacional, agindo de forma preventiva e punitiva nas esferas administrativa e civil, responsabilizando organizações por negligência na guarda de ativos digitais.

Sob a ótica da metodologia de aplicação da lei, esse conjunto normativo se aprimora continuamente mediante o enfrentamento de novos conflitos digitais, exigindo Inteligência e Análise de Dados para rastrear autores de delitos, muitas vezes ocultos sob o anonimato da rede. A aplicação da norma ocorre de forma integrada: no caso do vazamento de imagens íntimas, embora existam dispositivos específicos para crimes contra a honra e a dignidade sexual, a Lei Carolina Dieckmann permanece como o ponto de partida metodológico sempre que a obtenção do material decorrer da violação (invasão) de um dispositivo informático.

Portanto, o cenário atual em 2026 demonstra que a persecução penal de crimes digitais não se resume apenas à punição, mas à utilização de perícias técnicas para garantir a cadeia de custódia das evidências eletrônicas, assegurando que o combate à criminalidade tecnológica seja eficaz, justo e fundamentado na legalidade.

Conclui-se que a eficácia da Lei Carolina Dieckmann reside em sua natureza preventiva. Ao punir a tentativa, independentemente da consumação do delito, a legislação estabelece uma base de segurança mais robusta, mitigando riscos e evitando danos mais graves.

Reflexos da Aplicação da Lei Carolina Dieckmann

A aplicação da Lei n.º 12.737/2012, conhecida como Lei Carolina Dieckmann, trouxe importantes reflexos para o Direito e para a sociedade, principalmente no que se refere à proteção da privacidade e ao combate aos crimes informáticos. Ao incluir os artigos 154-A e 154-B no Código Penal, a lei passou a prever de forma específica a invasão de dispositivos eletrônicos, o que representou um avanço diante das lacunas que existiam anteriormente.

No âmbito jurídico, um dos principais efeitos da lei foi permitir a responsabilização penal de condutas que antes não eram claramente tipificadas. Com isso, o Estado passou a ter mais instrumentos para atuar nesses casos, contribuindo para a redução da impunidade e para o fortalecimento da segurança jurídica.

Já no plano social, a lei reforça a proteção de direitos fundamentais, como a intimidade e a vida privada, que são frequentemente violados no ambiente digital. Além disso, sua existência ajuda a conscientizar a população sobre os riscos e as consequências dos crimes cibernéticos, exercendo também uma função preventiva.

No entanto, a aplicação da lei ainda apresenta limitações. A exigência de mecanismos de segurança no dispositivo invadido pode dificultar sua utilização em alguns casos, o que acaba restringindo sua efetividade. Além disso, a dificuldade de identificar os autores desses crimes, devido ao anonimato na internet, ainda contribui para a sensação de impunidade.

Dessa forma, embora a Lei Carolina Dieckmann represente um avanço importante, seus reflexos ainda são limitados diante das constantes mudanças tecnológicas. Por isso, torna-se necessário o aprimoramento da legislação e o fortalecimento das medidas de prevenção, para garantir uma proteção mais efetiva no ambiente digital.

METODOLOGIA

A metodologia corresponde ao processo sistemático de planejamento e execução das etapas de pesquisa, que busca alcançar respostas claras e verdadeiras sobre um tema, registrando

os métodos utilizados ao longo do caminho para garantir que os objetivos sejam atingidos de forma eficiente (Marconi; Lakatos, 2003).

A presente pesquisa caracteriza-se como um estudo de natureza básica estratégica, uma vez que busca analisar a aplicação da Lei n° 12.737/2012 (Lei Carolina Dieckmann) no contexto dos crimes cibernéticos no Brasil, bem como seus reflexos na proteção de dados e na tutela da privacidade no ambiente digital.

Quanto aos objetivos, trata-se de uma pesquisa descritiva e exploratória, pois visa descrever o funcionamento da legislação vigente e explorar suas limitações diante da evolução das práticas criminosas no meio virtual. Nesse sentido, busca-se compreender a relação entre o avanço tecnológico e a necessidade de atualização normativa no ordenamento jurídico brasileiro.

No que se refere à abordagem, adotou-se o método qualitativo, uma vez que a análise fundamenta-se na interpretação de dados teóricos, doutrinários e normativos, sem utilização de mensuração estatística. Dessa forma, privilegia-se a compreensão crítica do fenômeno estudado.

Quanto aos procedimentos técnicos, foi realizada pesquisa bibliográfica e documental, com base em livros, artigos científicos, legislações, doutrinas de Direito Penal e Direito Digital, além de relatórios de instituições relacionadas à segurança da informação. O método utilizado foi o hipotético-dedutivo, partindo da hipótese de que a legislação brasileira, embora tenha avançado com a tipificação dos crimes informáticos, ainda apresenta limitações quanto à sua efetividade prática.

RESULTADOS E DISCUSSÃO

Esta seção apresenta e discute os resultados obtidos a partir da análise de dados secundários, coletados em fontes oficiais. Os resultados obtidos indicam que a Lei n.º 12.737/2012 (Lei Carolina Dieckmann) representou um marco relevante no ordenamento jurídico brasileiro, ao possibilitar a tipificação específica da invasão de dispositivos informáticos. Tal inovação contribuiu para o fortalecimento da tutela penal no enfrentamento dos crimes cibernéticos.

Entretanto, verifica-se que sua aplicação ainda encontra limitações relevantes, especialmente em razão da exigência de violação de mecanismo de segurança para a configuração do tipo penal, o que pode restringir sua incidência em determinadas situações concretas.

Constata-se, ainda, que a persecução penal dos crimes cibernéticos é dificultada por fatores como o anonimato dos agentes, a sofisticação tecnológica e a transnacionalidade das condutas, elementos que comprometem a identificação dos autores e a efetividade das investigações.

Por fim, observa-se a expansão contínua dos crimes cibernéticos no contexto brasileiro, o que evidencia a necessidade de constante atualização normativa e de aprimoramento dos mecanismos institucionais de prevenção, investigação e repressão dessas práticas.

enfrentadas, sobretudo no que se refere à efetividade da aplicação da lei, à adaptação às novas tecnologias e ao fortalecimento da capacidade investigativa do Estado.

CONCLUSÃO

O presente estudo teve como objetivo analisar a Lei n.º 12.737/2012 (Lei Carolina Dieckmann) e sua relevância no enfrentamento dos crimes cibernéticos no Brasil, bem como compreender seus impactos na proteção de dados, na tutela da privacidade e na responsabilização de condutas praticadas no ambiente digital.

A partir da análise realizada, conclui-se que a referida legislação representou um importante marco inicial na criminalização de condutas informáticas, especialmente ao introduzir no Código Penal a tipificação da invasão de dispositivo informático. Esse avanço possibilitou maior proteção aos bens jurídicos relacionados à intimidade, à privacidade e à segurança da informação, fortalecendo a atuação do Estado no combate à criminalidade digital.

Contudo, verificou-se que a efetividade da Lei Carolina Dieckmann ainda enfrenta limitações significativas, tanto de ordem técnica quanto interpretativa. A exigência de mecanismos de segurança para configuração do delito, aliada às dificuldades de investigação dos crimes cibernéticos, evidencia a necessidade de constante aperfeiçoamento legislativo e institucional.

Além disso, observou-se que o crescimento acelerado dos crimes cibernéticos, associado à evolução tecnológica e à ampliação do uso da internet, exige respostas mais integradas e eficientes por parte do ordenamento jurídico brasileiro. Nesse sentido, a atuação isolada de normas específicas mostra-se insuficiente diante da complexidade do fenômeno digital contemporâneo.

Dessa forma, conclui-se que, embora a Lei Carolina Dieckmann tenha representado um

avanço relevante no Direito Penal brasileiro, ainda se faz necessário o fortalecimento do arcabouço normativo, o aprimoramento dos mecanismos de investigação e a implementação de políticas públicas voltadas à educação digital e à prevenção de crimes cibernéticos.

Por fim, reforça-se que a proteção dos direitos fundamentais no ambiente digital, especialmente a privacidade e a proteção de dados pessoais, depende não apenas da existência de leis, mas também de sua efetiva aplicação e constante atualização frente às transformações tecnológicas.

REFERÊNCIAS

ABNT/CB-21. **Projeto ABNT NBR ISO/IEC 27001:2013**. Disponível em: https://www.academia.edu/36290737/ABNT_CB_21_PROJETO_ABNT_NBR_ISO_IEC_27001_SET_2013_N%C3%83O_TEM_VALOR_NORMATIVO. Acesso em: 11 abr. 2026.

BRASIL. Decreto-Lei nº 2.848, de 7 de dezembro de 1940. **Código Penal**. Disponível em: http://www.planalto.gov.br. Acesso em: 24 mar. 2026.

BRASIL. Lei nº 12.737, de 30 de novembro de 2012. **Dispõe sobre a tipificação de crimes informáticos**. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 24 mar. 2026.

BRASIL. Lei nº 12.737, de 30 de novembro de 2012. **Dispõe sobre a tipificação criminal de delitos informáticos**. Disponível em: http://www.planalto.gov.br. Acesso em: 25 mar. 2026.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. **Marco Civil da Internet**. Disponível em: http://www.planalto.gov.br. Acesso em: 7 abr. 2026.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD)**. Disponível em: http://www.planalto.gov.br. Acesso em: 8 abr. 2026.

BRASIL. Lei nº 14.155, de 27 de maio de 2021. **Altera dispositivos do Código Penal relacionados a crimes cibernéticos**. Disponível em: http://www.planalto.gov.br. Acesso em: 9 abr. 2026.

CASSANTI, M. A. **Crimes cibernéticos: estratégias de prevenção e investigação**. 1. ed. Curitiba: Juruá, 2014.

CERT.BR. **Relatórios de incidentes de segurança na internet no Brasil**. Disponível em: https://www.cert.br. Acesso em: 2 abr. 2026.

HAFNER, K.; LYON, M. **Where wizards stay up late: the origins of the Internet**. New York: Simon & Schuster, 1996.

JUSBRASIL. **Crimes virtuais: uma análise acerca da ineficácia da legislação e os desafios de sua persecução penal**. Disponível em: https://www.jusbrasil.com.br/artigos/crimes-virtuais-

uma-analise-acerca-da-in-eficacia-da-legislacao-e-os-desafios-de-sua-persecucao-penal/1220973039. Acesso em: 12 abr. 2026.

LÉVY, P. **Cibercultura**. Tradução de Carlos Irineu da Costa. São Paulo: Editora 34, 1999.

LIMA, M. G. **Direito digital: análise da Lei 12.737/2012 e seus reflexos no ordenamento jurídico brasileiro**. 2. ed. Rio de Janeiro: Lumen Juris, 2016.

MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA. **Dados e políticas de enfrentamento aos crimes cibernéticos**. Disponível em: https://www.gov.br/mj. Acesso em: 31 mar. 2026.

POLÍCIA FEDERAL. **Relatórios e estatísticas de crimes cibernéticos no Brasil**. Disponível em: https://www.gov.br/pf. Acesso em: 29 mar. 2026.

ROSSINI, A. E. S. **Informática, telemática e direito penal**. São Paulo: Memória Jurídica, 2004.

SAFERNET BRASIL. **Indicadores de denúncias de crimes cibernéticos no Brasil**. Disponível em: https://www.safernet.org.br. Acesso em: 27 mar. 2026.

SERASA EXPERIAN. **Recorde: quase 7 milhões de tentativas de fraude foram registradas no 1º semestre de 2025; setor bancário é principal alvo**. São Paulo, 2025. Disponível em: https://www.serasaexperian.com.br/sala-de-imprensa/indicadores/recorde-quase-7-milhoes-de-tentativas-de-fraude-foram-registradas-no-1-semestre-de-2025-setor-bancario-e-principal-alvo. Acesso em: 25 mar. 2026.

SOUZA FILHO, L. C. C. de. **Análise dos crimes cibernéticos à luz da Lei Carolina Dieckmann: a persistência de carência normativa**. Recife: Faculdade Damas da Instrução Cristã, 2024. Disponível em: https://revistas.faculdadedamas.edu.br/index.php/academico/article/view/2577/1927. Acesso em: 2 abr. 2026.

UNITED NATIONS OFFICE ON DRUGS AND CRIME (UNODC). **Comprehensive study on cybercrime**. New York: United Nations, 2013. Disponível em: https://www.unodc.org. Acesso em: 4 abr. 2026.