Cognitio Juris
ISSN 2236-3009

CRIMES CIBERNÉTICOS E A PROTEÇÃO DE DADOS: A LEGISLAÇÃO BRASILEIRA EM RELAÇÃO AOS CRIMES CIBERNÉTICOS COM BASE NA PROTEÇÃO DE DADOS PESSOAIS

CYBERCRIMES AND DATA PROTECTION: BRAZILIAN LEGISLATION REGARDING CYBERCRIMES BASED ON THE PROTECTION OF PERSONAL DATA

Artigo submetido em 18 de maio de 2026
Artigo aprovado em 20 de maio de 2026
Artigo publicado em 20 de maio de 2026

Cognitio Juris
Volume 16 – Número 59 – 2026
ISSN 2236-3009

.

Autor(es):
Antônio Jorge Dias
Delner do Carmo Azevedo

.

RESUMO: O avanço das tecnologias digitais e a ampliação do acesso à internet transformaram significativamente as relações sociais, econômicas e institucionais, criando possibilidades de comunicação e desenvolvimento. Contudo, tais transformações também

contribuíram para o surgimento de práticas ilícitas realizadas em ambiente virtual, conhecidas como crimes cibernéticos. Essas condutas representam riscos à privacidade, à segurança da informação e à proteção dos dados pessoais, exigindo do Estado mecanismos jurídicos eficazes para sua prevenção e repressão. O presente artigo científico tem como objetivo analisar criticamente a legislação brasileira relacionada aos crimes cibernéticos, especialmente no que se refere à proteção de dados pessoais. A pesquisa possui abordagem qualitativa, natureza descritiva e exploratória, fundamentada em revisão bibliográfica, análise legislativa e estudo doutrinário. O estudo examina a evolução normativa brasileira, com destaque para a Lei nº 12.737/2012, conhecida como Lei Carolina Dieckmann, o Marco Civil da Internet (Lei nº 12.965/2014), a Lei Geral de Proteção de Dados Pessoais – LGPD (Lei nº 13.709/2018) e a Lei nº 14.155/2021. Analisa-se ainda o reconhecimento constitucional da proteção de dados pessoais como direito fundamental por meio da Emenda Constitucional nº 115/2022. Os resultados demonstram que, embora o Brasil tenha avançado significativamente na regulamentação do ambiente digital, ainda persistem desafios relacionados à rápida evolução tecnológica, à atuação dos órgãos fiscalizadores, à cooperação internacional e à conscientização da população sobre segurança digital. Conclui-se que a efetividade do combate aos crimes cibernéticos depende da constante atualização legislativa, do fortalecimento institucional e da implementação de políticas públicas voltadas à educação digital e à proteção dos direitos fundamentais no ambiente virtual.

Palavras-chave: crimes cibernéticos. proteção de dados. LGPD. segurança digital. legislação brasileira.

ABSTRACT: The advancement of digital technologies and the expansion of internet access have significantly transformed social, economic, and institutional relations, creating new possibilities for communication and development. However, these transformations have also contributed to the emergence of illicit practices carried out in the virtual environment, known as cybercrimes. These behaviors represent risks to privacy, information security, and the protection of personal data, requiring effective legal mechanisms from the State for their

prevention and repression. This scientific article aims to critically analyze Brazilian legislation related to cybercrimes, especially regarding the protection of personal data. The research has a qualitative approach, a descriptive and exploratory nature, based on bibliographic review, legislative analysis, and doctrinal study. This study examines the evolution of Brazilian regulations, highlighting Law No. 12.737/2012, known as the Carolina Dieckmann Law, the Brazilian Internet Bill of Rights (Law No. 12.965/2014), the General Data Protection Law – LGPD (Law No. 13.709/2018), and Law No. 14.155/2021. It also analyzes the constitutional recognition of personal data protection as a fundamental right through Constitutional Amendment No. 115/2022. The results demonstrate that, although Brazil has made significant progress in regulating the digital environment, challenges persist related to rapid technological evolution, the actions of regulatory bodies, international cooperation, and public awareness of digital security. It concludes that the effectiveness of combating cybercrime depends on constant legislative updates, institutional strengthening, and the implementation of public policies focused on digital education and the protection of fundamental rights in the virtual environment.

Keywords: cybercrime, data protection, LGPD (Brazilian General Data Protection Law), digital security, Brazilian legislation.

1. INTRODUÇÃO

A sociedade contemporânea encontra-se profundamente marcada pela transformação digital e pela crescente utilização das tecnologias da informação e comunicação. Conforme destaca Queiroz (2024), a expansão tecnológica modificou significativamente as relações sociais e econômicas, criando desafios para o Direito Penal e para os mecanismos de proteção jurídica no ambiente virtual. A internet passou a integrar praticamente todas as atividades humanas, influenciando relações sociais, econômicas, profissionais e institucionais. O ambiente virtual tornou-se indispensável para o funcionamento da sociedade moderna, permitindo o compartilhamento instantâneo de informações, a realização de transações financeiras, o

armazenamento de dados pessoais e o desenvolvimento de inúmeras atividades cotidianas.

Entretanto, a expansão do espaço digital também contribuiu para o surgimento de novas modalidades criminosas, praticadas por meio de sistemas computacionais, dispositivos eletrônicos e redes de comunicação. Os crimes cibernéticos passaram a representar uma ameaça significativa à segurança da informação, à privacidade e à integridade dos dados pessoais dos usuários da internet. Segundo Lopes e Lopes (2023), o crescimento das práticas ilícitas no ambiente digital demonstra a necessidade de fortalecimento das políticas públicas de segurança cibernética e da modernização legislativa brasileira. Fraudes eletrônicas, invasão de dispositivos informáticos, vazamento de dados, crimes financeiros digitais, disseminação de fake news, extorsões virtuais e ataques a sistemas governamentais tornaram-se cada vez mais frequentes.

Nesse contexto, tornou-se indispensável a criação de instrumentos jurídicos capazes de regulamentar o ambiente virtual e garantir a proteção dos direitos fundamentais dos cidadãos. O ordenamento jurídico brasileiro passou por importantes transformações legislativas voltadas ao combate da criminalidade digital, destacando-se a promulgação da Lei nº 12.737/2012, conhecida como Lei Carolina Dieckmann, do Marco Civil da Internet (Lei nº 12.965/2014) e da Lei Geral de Proteção de Dados Pessoais – LGPD (Lei nº 13.709/2018).

A proteção de dados pessoais ganhou ainda maior relevância com a Emenda Constitucional nº 115/2022, que incluiu expressamente a proteção de dados no rol dos direitos e garantias fundamentais previstos na Constituição Federal. Essa mudança reforçou a importância da privacidade e da segurança das informações pessoais em uma sociedade cada vez mais dependente da tecnologia. Diante disso, o presente artigo científico busca responder ao seguinte problema de pesquisa: em que medida a legislação brasileira tem sido eficaz no combate aos crimes cibernéticos e na proteção de dados pessoais diante das constantes transformações tecnológicas?

O objetivo geral da pesquisa consiste em analisar criticamente a legislação brasileira relacionada aos crimes cibernéticos e à proteção de dados pessoais, identificando seus avanços, limitações e desafios contemporâneos. Como objetivos específicos, pretende-se identificar os principais crimes cibernéticos previstos no ordenamento jurídico brasileiro; examinar a evolução histórica da proteção de dados pessoais; analisar os desafios enfrentados pela legislação diante das inovações tecnológicas; e discutir a importância da conscientização digital e da atuação institucional no combate à criminalidade virtual.

A metodologia utilizada fundamenta-se em pesquisa bibliográfica, documental e legislativa, com abordagem qualitativa e natureza descritiva. Foram analisadas normas jurídicas, artigos científicos, doutrinas e publicações relacionadas ao Direito Digital e à proteção de dados pessoais. A relevância do tema justifica-se pelo crescimento exponencial dos crimes virtuais e pela necessidade de fortalecimento dos mecanismos jurídicos voltados à proteção dos direitos fundamentais no ambiente digital. Além disso, o estudo contribui para o aprofundamento das discussões acadêmicas sobre o Direito Digital e a efetividade da legislação brasileira diante das novas tecnologias.

- **CRIMES CIBERNÉTICOS NO ORDENAMENTO JURÍDICO BRASILEIRO**

O crescimento da internet e das tecnologias digitais modificou profundamente a dinâmica social e econômica contemporânea. A facilidade de comunicação e compartilhamento de informações trouxe inúmeros benefícios para a sociedade, porém também ampliou significativamente os riscos relacionados à criminalidade digital. Os crimes cibernéticos passaram a atingir não apenas indivíduos, mas também empresas, instituições financeiras e órgãos públicos, causando prejuízos econômicos, danos morais e violações aos direitos fundamentais.

A crescente dependência das tecnologias da informação tornou os dados pessoais um dos bens mais valiosos da atualidade. Informações relacionadas à identidade, localização, hábitos

de consumo, dados bancários e registros pessoais passaram a ser constantemente coletadas e armazenadas em sistemas digitais. Nesse cenário, a proteção dessas informações tornou-se elemento essencial para preservação da privacidade, da dignidade humana e da segurança jurídica.

Diante desse contexto, o ordenamento jurídico brasileiro precisou adaptar-se às novas demandas sociais e tecnológicas, desenvolvendo normas específicas voltadas à regulamentação do ambiente virtual e ao combate das práticas ilícitas realizadas por meios eletrônicos.

2.1. Conceito e Características dos Crimes Cibernéticos

Os crimes cibernéticos podem ser definidos como infrações penais praticadas por meio de dispositivos eletrônicos, sistemas informatizados ou redes de computadores, tendo como finalidade obter vantagem ilícita, causar danos ou violar direitos de terceiros. Essas práticas criminosas utilizam a tecnologia como instrumento para execução das condutas ilícitas.

A criminalidade digital apresenta características específicas que dificultam sua repressão e investigação. Entre essas características destacam-se a rapidez na propagação das informações, o anonimato proporcionado pela internet, a dimensão transnacional dos delitos e a dificuldade de identificação dos autores.

Os crimes cibernéticos podem ser classificados em crimes próprios e impróprios. Os crimes próprios são aqueles que dependem necessariamente do uso de sistemas informatizados para sua prática, como a invasão de dispositivos informáticos. Já os crimes impróprios correspondem a infrações tradicionais praticadas com auxílio da tecnologia, como estelionato, ameaça e difamação realizados em ambiente virtual.

Com o aumento da utilização das plataformas digitais, tornou-se comum a ocorrência de golpes financeiros, clonagem de aplicativos de mensagens, fraudes bancárias eletrônicas,

ataques hackers, vazamentos de dados e crimes contra a honra praticados nas redes sociais. Tais condutas demonstram que o ambiente virtual se tornou espaço propício para a atuação criminosa.

Além disso, o avanço da inteligência artificial, do armazenamento em nuvem e do compartilhamento massivo de informações ampliou os riscos relacionados à segurança digital e à proteção da privacidade dos indivíduos.

2.2 Evolução da Legislação Brasileira Sobre Crimes Cibernéticos

A legislação brasileira relacionada aos crimes cibernéticos desenvolveu-se de forma gradual, acompanhando a expansão das tecnologias digitais e o aumento das infrações praticadas no ambiente virtual.

Um dos principais marcos legislativos foi a promulgação da Lei nº 12.737/2012, conhecida como Lei Carolina Dieckmann. Essa norma surgiu após a divulgação indevida de fotografias íntimas da atriz Carolina Dieckmann, vítima de invasão de dispositivo informático. A lei alterou o Código Penal Brasileiro para tipificar a invasão de dispositivos eletrônicos com a finalidade de obter, adulterar ou destruir dados sem autorização do titular.

A Lei Carolina Dieckmann representou importante avanço no combate aos delitos informáticos, pois reconheceu juridicamente a necessidade de proteção dos sistemas eletrônicos e das informações digitais. Conforme Corrêia (2022), a promulgação da referida norma representou um marco inicial na consolidação da legislação brasileira voltada aos crimes cibernéticos.

Posteriormente, foi promulgada a Lei nº 12.965/2014, denominada Marco Civil da Internet. Essa legislação estabeleceu princípios, direitos, garantias e deveres para o uso da internet no Brasil, assegurando direitos fundamentais como a liberdade de expressão, a privacidade e a proteção de dados pessoais.

O Marco Civil da Internet também disciplinou a responsabilidade dos provedores de aplicações e serviços digitais, estabelecendo regras sobre guarda de registros, proteção da privacidade e fornecimento de dados mediante ordem judicial. Outro importante avanço legislativo ocorreu com a Lei nº 14.155/2021, responsável por aumentar as penas aplicadas aos crimes de invasão de dispositivos informáticos e fraudes eletrônicas. Essa legislação alterou dispositivos do Código Penal e do Código de Processo Penal, tornando mais rigorosa a repressão aos crimes praticados em ambiente virtual.

Além dessas normas, destaca-se a adesão do Brasil à Convenção de Budapeste sobre Crimes Cibernéticos, tratado internacional voltado à cooperação entre os países no combate à criminalidade digital transnacional.

- **A PROTEÇÃO DE DADOS PESSOAIS COMO DIREITO FUNDAMENTAL**

A proteção de dados pessoais consolidou-se como uma das principais preocupações jurídicas da sociedade contemporânea. Em razão do intenso fluxo de informações no ambiente digital, tornou-se indispensável estabelecer mecanismos legais capazes de garantir maior controle dos indivíduos sobre seus próprios dados.

Com o avanço das plataformas digitais, redes sociais, serviços bancários eletrônicos e sistemas de armazenamento em nuvem, os dados pessoais passaram a ser amplamente utilizados por empresas e instituições públicas para fins econômicos, administrativos e comerciais. Essa realidade ampliou os riscos relacionados ao uso indevido das informações pessoais, à exposição da privacidade e à ocorrência de vazamentos de dados.

A necessidade de proteção jurídica tornou-se ainda mais evidente diante do aumento expressivo dos crimes virtuais envolvendo roubo de identidade, fraudes financeiras e comercialização indevida de informações pessoais. Assim, a proteção de dados passou a ser compreendida como instrumento essencial para garantia da liberdade individual, da privacidade e da segurança digital.

3.1 Lei Geral de Proteção de Dados Pessoais – LGPD

A proteção de dados pessoais ganhou destaque no ordenamento jurídico brasileiro com a promulgação da Lei nº 13.709/2018, conhecida como Lei Geral de Proteção de Dados Pessoais – LGPD. De acordo com Silva e Novais (2023), a LGPD consolidou princípios fundamentais relacionados à privacidade, à transparência e à responsabilização no tratamento de dados pessoais.

A LGPD estabelece normas para o tratamento de dados pessoais realizados por pessoas físicas, empresas e órgãos públicos, visando proteger os direitos fundamentais de liberdade, privacidade e livre desenvolvimento da personalidade da pessoa natural.

A legislação determina princípios fundamentais para o tratamento de dados, entre os quais se destacam a finalidade, adequação, necessidade, transparência, segurança e responsabilização. Nesse sentido, Damião e Novais (2024) afirmam que a LGPD fortaleceu significativamente a tutela jurídica das informações pessoais e ampliou a responsabilidade das instituições públicas e privadas.

Além disso, a LGPD assegura aos titulares diversos direitos relacionados aos seus dados pessoais, incluindo:

Entre os principais direitos assegurados aos titulares de dados pessoais pela LGPD destacam-se o direito de acesso às informações armazenadas, a possibilidade de correção de dados incompletos ou desatualizados, o direito à exclusão de informações desnecessárias, a portabilidade dos dados, a revogação do consentimento previamente concedido e o direito de ser informado sobre eventual compartilhamento das informações pessoais com terceiros.

A legislação aplica-se a qualquer operação de tratamento de dados realizada no território nacional ou que envolva dados coletados no Brasil, independentemente da localização da empresa responsável pelo tratamento.

A criação da Autoridade Nacional de Proteção de Dados – ANPD representou importante instrumento de fiscalização e aplicação das normas previstas na LGPD. A ANPD possui competência para regulamentar, fiscalizar e aplicar sanções administrativas em casos de descumprimento da legislação.

3.2 A Proteção de Dados Como Direito Fundamental

A proteção de dados pessoais foi elevada à categoria de direito fundamental por meio da Emenda Constitucional nº 115/2022, que incluiu expressamente essa garantia no artigo 5º da Constituição Federal. Tal reconhecimento constitucional reforça a compreensão de que a proteção das informações pessoais constitui elemento indispensável para preservação da dignidade da pessoa humana e da liberdade individual.

O reconhecimento constitucional da proteção de dados demonstra a importância da privacidade e da segurança da informação na sociedade contemporânea. Em uma realidade marcada pela coleta massiva de informações pessoais, a proteção de dados tornou-se essencial para preservação da dignidade humana e da autonomia individual.

Os dados pessoais passaram a possuir relevante valor econômico e estratégico, sendo frequentemente utilizados para fins comerciais, políticos e institucionais. Dessa forma, o uso inadequado dessas informações pode resultar em graves violações aos direitos fundamentais dos cidadãos.

A constitucionalização da proteção de dados fortaleceu a atuação da LGPD e ampliou a responsabilidade do Estado na garantia da segurança digital e da privacidade dos indivíduos.

- **DESAFIOS DA LEGISLAÇÃO BRASILEIRA FRENTE ÀS INOVAÇÕES TECNOLÓGICAS**

As constantes transformações tecnológicas representam um dos maiores desafios enfrentados pelo Direito contemporâneo. Conforme observa Conceição (2024), a velocidade

das inovações digitais dificulta a atualização das normas jurídicas e amplia os desafios relacionados à fiscalização e responsabilização dos agentes envolvidos em crimes virtuais. O desenvolvimento acelerado das ferramentas digitais, da inteligência artificial e dos sistemas de comunicação virtual modifica rapidamente as relações sociais, criando formas de interação e, consequentemente, novas possibilidades de práticas criminosas.

A legislação brasileira, embora tenha avançado significativamente nos últimos anos, ainda enfrenta dificuldades para acompanhar a velocidade das mudanças tecnológicas. O processo legislativo tradicional costuma ser mais lento que o surgimento de novas tecnologias, fazendo com que determinadas condutas ilícitas permaneçam temporariamente sem regulamentação específica.

Além disso, os crimes cibernéticos apresentam características particulares que dificultam sua investigação e repressão, especialmente em razão da atuação transnacional dos criminosos e da facilidade de ocultação da identidade dos autores. Essas circunstâncias exigem não apenas atualização legislativa constante, mas também cooperação internacional eficiente e investimentos em tecnologia e capacitação profissional.

4.1 Limitações da Legislação e Dificuldades de Fiscalização

Apesar dos avanços normativos observados nos últimos anos, a legislação brasileira ainda enfrenta dificuldades para acompanhar a rápida evolução tecnológica.

As tecnologias digitais desenvolvem-se em velocidade muito superior à capacidade de atualização das normas jurídicas. Novas ferramentas, plataformas digitais e modalidades de interação virtual surgem constantemente, criando desafios inéditos para o Direito.

Entre os principais obstáculos enfrentados pela legislação brasileira estão as dificuldades relacionadas à investigação de crimes transnacionais, o anonimato proporcionado pelo ambiente virtual, a insuficiência estrutural e tecnológica de determinados órgãos

fiscalizadores, além da complexidade relacionada à coleta e preservação de provas digitais. Soma-se a isso o constante surgimento de novas modalidades de golpes virtuais, que acompanham a rápida evolução tecnológica e desafiam continuamente o sistema jurídico brasileiro.

A atuação dos criminosos em diferentes países dificulta a responsabilização penal e exige cooperação internacional eficiente entre autoridades públicas.

Além disso, muitas empresas ainda apresentam falhas na proteção de dados pessoais, permitindo vazamentos de informações e exposição indevida dos usuários.

4.2 Educação Digital e Segurança da Informação

A conscientização da população sobre segurança digital constitui importante mecanismo de prevenção aos crimes cibernéticos.

Muitos usuários da internet adotam práticas inseguras, como utilização de senhas fracas, compartilhamento excessivo de informações pessoais e acesso a redes públicas sem proteção adequada.

A ausência de educação digital favorece a atuação criminosa e amplia os riscos de fraudes eletrônicas e vazamentos de dados. Para Corrêia (2022), a conscientização social sobre segurança da informação constitui instrumento indispensável para prevenção da criminalidade cibernética e fortalecimento da proteção de dados pessoais.

Diante disso, torna-se necessária a implementação de políticas públicas voltadas à educação tecnológica e à conscientização social sobre proteção de dados pessoais. A segurança digital não depende apenas da existência de leis, mas também da adoção de práticas preventivas por parte dos usuários, empresas e instituições públicas.

Nesse contexto, destaca-se a importância do investimento em tecnologia, capacitação

profissional e fortalecimento dos mecanismos de fiscalização e investigação digital.

- **CONSIDERAÇÕES FINAIS**

A criminalidade cibernética tornou-se uma das principais preocupações do Direito moderno, especialmente em razão da intensa digitalização das relações sociais e econômicas. O ambiente virtual passou a desempenhar papel fundamental na vida cotidiana, permitindo a realização de inúmeras atividades por meios eletrônicos. Entretanto, essa transformação também ampliou significativamente os riscos relacionados à privacidade, à segurança da informação e à proteção de dados pessoais.

O crescimento dos crimes virtuais demonstra que a evolução tecnológica exige respostas jurídicas cada vez mais eficazes e atualizadas. Fraudes eletrônicas, invasões de sistemas, vazamentos de dados e ataques virtuais representam ameaças concretas aos direitos fundamentais dos cidadãos e evidenciam a necessidade de fortalecimento da proteção jurídica no ambiente digital.

Nesse contexto, a legislação brasileira passou por importantes avanços normativos, especialmente com a criação de leis voltadas à regulamentação do uso da internet e à proteção de dados pessoais. Todavia, a rápida evolução tecnológica continua impondo desafios constantes ao sistema jurídico, exigindo atuação integrada entre Estado, instituições públicas, empresas privadas e sociedade civil.

Os crimes cibernéticos representam um dos principais desafios jurídicos da sociedade contemporânea, especialmente diante da crescente digitalização das relações humanas e do aumento da dependência tecnológica.

A expansão do ambiente virtual trouxe inúmeros benefícios para a sociedade, mas também ampliou os riscos relacionados à privacidade, à segurança da informação e à proteção de dados pessoais. O aumento das fraudes eletrônicas, invasões de dispositivos informáticos e

vazamentos de dados evidencia a necessidade de fortalecimento dos mecanismos jurídicos de proteção digital.

O estudo demonstrou que o Brasil avançou significativamente na construção de um arcabouço normativo voltado ao combate da criminalidade cibernética e à proteção de dados pessoais. Entretanto, conforme ressaltam Silva e Novais (2023), a efetividade dessas normas depende da atuação eficiente dos órgãos fiscalizadores e da constante atualização legislativa diante das transformações tecnológicas. A Lei Carolina Dieckmann, o Marco Civil da Internet, a LGPD e a Lei nº 14.155/2021 representam importantes instrumentos jurídicos de proteção no ambiente virtual.

Além disso, a inclusão da proteção de dados pessoais no rol dos direitos fundamentais da Constituição Federal reforçou a importância da privacidade e da segurança digital como garantias essenciais da dignidade da pessoa humana.

Entretanto, verificou-se que ainda existem desafios relevantes relacionados à efetividade das normas jurídicas diante das constantes transformações tecnológicas. A rápida evolução das tecnologias digitais exige atualização legislativa contínua, fortalecimento institucional e cooperação internacional eficiente. Observou-se também que a prevenção dos crimes cibernéticos depende não apenas da atuação estatal, mas igualmente da conscientização da população sobre segurança digital. A educação tecnológica e a adoção de práticas preventivas são fundamentais para redução dos riscos no ambiente virtual.

Dessa forma, conclui-se que o enfrentamento da criminalidade digital exige atuação integrada entre Estado, empresas e sociedade civil, com investimentos em tecnologia, capacitação profissional, fiscalização eficiente e fortalecimento da cultura de proteção de dados pessoais. Somente por meio da combinação entre legislação adequada, educação digital e cooperação internacional será possível garantir maior segurança jurídica e efetiva proteção dos direitos fundamentais no ambiente virtual.

- **REFERÊNCIAS**

BRASIL. **Constituição da República Federativa do Brasil de 1988.** Brasília, DF: Presidência da República, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 18 maio 2026.

BRASIL. **Lei nº 12.737, de 30 de novembro de 2012.** Dispõe sobre a tipificação criminal de delitos informáticos. Brasília, DF: Presidência da República, 2012. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 18 maio 2026.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, DF: Presidência da República, 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 18 maio 2026.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 18 maio 2026.

BRASIL. **Lei nº 14.155, de 27 de maio de 2021.** Altera o Código Penal para tornar mais graves os crimes de violação de dispositivo informático e furto e estelionato cometidos de forma eletrônica ou pela internet. Brasília, DF: Presidência da República, 2021.

CONCEIÇÃO, Victória Corrêa da. **A Lei Geral de Proteção de Dados no Brasil e os possíveis crimes cibernéticos. 2024.** Trabalho de Conclusão de Curso (Graduação em Direito) – Universidade de Santa Cruz do Sul, Capão da Canoa, 2024.

CORRÊIA, Bruna Marques. **A importância da Lei Geral de Proteção de Dados em combates aos crimes cibernéticos.** São Paulo, 2022.

DAMIÃO, Alisson Santana; NOVAIS, Thyara Gonçalves. **Consequências jurídicas da LGPD para os crimes virtuais.** Revista Ibero-Americana de Humanidades, Ciências e Educação – REASE, São Paulo, v. 10, n. 11, 2024.

LOPES, Marciano Pereira; LOPES, José Augusto Bezerra. **Crimes virtuais no ordenamento jurídico brasileiro.** Revista Ibero-Americana de Humanidades, Ciências e Educação – REASE, São Paulo, v. 9, n. 8, 2023.

QUEIROZ, Liv Ferreira Augusto Severo. **Os crimes cibernéticos no ordenamento jurídico brasileiro: investigação criminal e desafios**. Revista do CNMP, 12. ed., 2024.

SILVA, Ronaldo Couto da; NOVAIS, Thyara Gonçalves. **A Lei Geral de Proteção de Dados e sua aplicação no combate aos crimes cibernéticos: desafios e perspectivas.** Revista Ibero-Americana de Humanidades, Ciências e Educação – REASE, São Paulo, v. 9, n. 10, 2023.