

CRIMINALIDADE CIBERNÉTICA E OS DESAFIOS DA EFETIVIDADE DA LEGISLAÇÃO BRASILEIRA FRENTE À EXPANSÃO DAS TECNOLOGIAS DIGITAIS

CYBERCRIME AND THE CHALLENGES REGARDING THE EFFECTIVENESS OF BRAZILIAN LEGISLATION IN LIGHT OF THE EXPANSION OF DIGITAL TECHNOLOGIES

LA CIBERDELINCUENCIA Y LOS DESAFÍOS A LA EFICACIA DE LA LEGISLACIÓN BRASILEÑA ANTE LA EXPANSIÓN DE LAS TECNOLOGÍAS DIGITALES

Maria Eduarda Pereira Rios¹

Marco Antônio Alves Bezerra²

RESUMO: A expansão das tecnologias digitais transformou as relações sociais, econômicas e institucionais, mas também favoreceu o surgimento e a ampliação dos crimes cibernéticos, criando novos desafios para o Direito e para os órgãos responsáveis pela segurança e investigação. Com base nisso, esse estudo teve como objetivo analisar a efetividade da legislação brasileira frente à expansão das tecnologias digitais e ao crescimento dos crimes cibernéticos, com destaque para a Lei nº 14.155/2021 e a Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais). Na metodologia, realizou-se pesquisa bibliográfica e documental, de abordagem qualitativa e caráter descritivo, fundamentada em legislação brasileira, doutrina jurídica, artigos científicos e jurisprudência publicados ou atualizados entre 2022 e 2026. Nos resultados, verificou-se que o ordenamento jurídico brasileiro apresentou avanços relevantes na proteção do ambiente digital, especialmente com a criminalização e o agravamento de determinadas condutas praticadas por meios eletrônicos, a proteção de dados pessoais e a definição de mecanismos processuais específicos. A jurisprudência também tem contribuído para adaptar a aplicação das normas às particularidades dos delitos digitais. Entretanto, persistem dificuldades relacionadas à identificação da autoria, preservação da prova digital, transnacionalidade dos delitos, capacitação dos agentes públicos e rápida evolução tecnológica. Conclui-se que a legislação brasileira apresenta avanços importantes, mas sua efetividade depende de atualização contínua, investimentos em tecnologia e perícia digital, capacitação profissional, cooperação institucional e internacional e fortalecimento das ações preventivas e educativas voltadas à segurança digital.

Palavras-chave: Crimes cibernéticos. Legislação brasileira. Proteção de dados. Tecnologias digitais.

¹Acadêmica do curso de Direito Universidade de Gurupi (UNIRG).

²Professor Orientador.

ABSTRACT: The expansion of digital technologies has transformed social, economic, and institutional relations, but it has also fostered the emergence and proliferation of cybercrimes, creating new challenges for the legal system and for agencies responsible for security and investigation. Against this backdrop, this study aimed to analyze the effectiveness of Brazilian legislation in the face of the expansion of digital technologies and the rise of cybercrimes, focusing specifically on Law nº. 14.155/2021 and Law nº. 13.709/2018 (the General Personal Data Protection Law). The methodology involved bibliographic and documentary research—qualitative in approach and descriptive in nature—grounded in Brazilian legislation, legal doctrine, scientific articles, and case law published or updated between 2022 and 2026. The results indicate that the Brazilian legal system has made significant strides in protecting the digital environment, particularly through the criminalization and increased penalties for certain acts committed via electronic means, the protection of personal data, and the establishment of specific procedural mechanisms. Case law has also contributed to adapting the application of legal norms to the unique characteristics of digital offenses. However, challenges persist regarding the identification of perpetrators, the preservation of digital evidence, the transnational nature of the crimes, the training of public officials, and the rapid pace of technological evolution. The study concludes that while Brazilian legislation shows important progress, its effectiveness depends on continuous updating, investment in technology and digital forensics, professional training, institutional and international cooperation, and the strengthening of preventive and educational measures focused on digital security.

Keywords: Cybercrimes. Brazilian legislation. Data protection. Digital technologies.

RESUMEN: La expansión de las tecnologías digitales ha transformado las relaciones sociales, económicas e institucionales, pero también ha favorecido la aparición y expansión de los ciberdelitos, creando nuevos desafíos para el derecho y para los organismos responsables de la seguridad y la investigación. En este contexto, el presente estudio tuvo como objetivo analizar la efectividad de la legislación brasileña frente a la expansión de las tecnologías digitales y el crecimiento de los ciberdelitos, con énfasis en la Ley N° 14.155/2021 y la Ley N° 13.709/2018 (Ley General de Protección de Datos Personales). La metodología incluyó investigación bibliográfica y documental, con un enfoque cualitativo y descriptivo, basada en la legislación brasileña, la doctrina jurídica, artículos científicos y jurisprudencia publicados o actualizados entre 2022 y 2026. Los resultados mostraron que el ordenamiento jurídico brasileño ha logrado avances significativos en la protección del entorno digital, especialmente en la criminalización y agravamiento de ciertas conductas realizadas por medios electrónicos, la protección de datos personales y la definición de mecanismos procesales específicos. La jurisprudencia también ha contribuido a adaptar la aplicación de las normas a las particularidades de los delitos digitales. Sin embargo, persisten dificultades relacionadas con la identificación de la autoría, la preservación de la evidencia digital, la naturaleza transnacional de los delitos, la capacitación de los funcionarios públicos y la rápida evolución tecnológica. Se concluye que la legislación brasileña muestra avances importantes, pero su eficacia depende de la actualización continua, las inversiones en tecnología y análisis forense digital, la capacitación profesional, la cooperación institucional e internacional y el fortalecimiento de las acciones preventivas y educativas centradas en la seguridad digital.

Palabras clave: Delitos cibernéticos. Legislación brasileña. Protección de datos. Tecnologías digitales.

I. INTRODUÇÃO

A criminalidade cibernética tem se consolidado como um dos principais desafios contemporâneos no âmbito do Direito Penal, especialmente diante da rápida expansão das tecnologias digitais e do uso massivo da internet. No Brasil, o aumento de práticas ilícitas no ambiente virtual — como fraudes eletrônicas, invasões de dispositivos e vazamento de dados — evidencia a necessidade de um aparato jurídico eficaz e atualizado.

Nesse contexto, Masseno (2025) cita que normas como a Lei nº 12.737/2012 e a Lei nº 13.709/2018 surgem como importantes instrumentos legais para o enfrentamento desses crimes, embora ainda enfrentem limitações diante da constante evolução tecnológica.

Diante desse cenário, surge o seguinte problema de pesquisa: como a legislação brasileira tem atuado frente ao crescimento da criminalidade cibernética e quais são os principais desafios para sua efetiva aplicação no combate aos crimes digitais? Dessa forma, questionou-se se as normas vigentes são suficientes para acompanhar a dinamicidade das tecnologias digitais, bem como se os mecanismos de investigação e responsabilização são adequados diante da complexidade e, muitas vezes, da natureza transnacional dessas infrações, o que pode comprometer a efetividade da justiça penal.

O presente estudo teve como objetivo geral analisar a efetividade da legislação brasileira no enfrentamento da criminalidade cibernética diante da expansão das tecnologias digitais. Como objetivos específicos, pretendeu-se: identificar as principais formas de crimes cibernéticos praticados no Brasil; avaliar a adequação das normas jurídicas existentes frente às novas demandas tecnológicas; e pesquisar jurisprudência dos tribunais brasileiros relacionada à aplicação das leis em casos concretos de crimes digitais, a fim de compreender como o Poder Judiciário tem interpretado e aplicado tais normas.

Quanto à metodologia, a pesquisa foi de natureza qualitativa, com abordagem descritiva e exploratória, baseada em revisão bibliográfica e documental. Foram analisadas legislações pertinentes, doutrinas jurídicas, artigos científicos e decisões judiciais, com destaque para julgados dos tribunais superiores.

2. DOS CRIMES CIBERNÉTICOS: ASPECTOS GERAIS

A evolução dos crimes cibernéticos está diretamente relacionada ao desenvolvimento das tecnologias da informação, da expansão da internet e da crescente digitalização das relações sociais, econômicas e institucionais. Inicialmente, as condutas ilícitas praticadas por meio de

computadores estavam mais associadas à invasão de sistemas, manipulação de dados e obtenção indevida de informações (ALMEIDA; OLIVEIRA, 2022).

Com a popularização da internet, entretanto, o fenômeno tornou-se mais complexo, passando a envolver fraudes eletrônicas, furtos de dados, ataques a sistemas, disseminação de conteúdos ilícitos, crimes contra a honra, perseguições virtuais e outras práticas realizadas ou potencializadas pelo ambiente digital (ALMEIDA; OLIVEIRA, 2022). Arruda e Lima (2023) destacam que o cibercrime deixou de ser um fenômeno restrito ao universo tecnológico e passou a constituir importante questão jurídica, criminológica e social.

Os crimes cibernéticos podem ser compreendidos como:

[...] condutas criminosas praticadas mediante utilização de computadores, dispositivos móveis, redes, sistemas informáticos ou internet, podendo a tecnologia constituir o próprio objeto do delito ou apenas servir como instrumento para a execução de uma infração tradicional. Essa diferenciação é importante porque existem crimes cibernéticos próprios, nos quais o sistema ou dispositivo informático constitui elemento essencial da prática delitiva, e crimes cibernéticos impróprios ou ciberdependentes/ciberfacilitados, nos quais a tecnologia é utilizada para potencializar ou viabilizar uma conduta criminosa (CAVALCANTI NETO, 2023, p. 02).

Do ponto de vista jurídico, Groskreutz (2022) pontua que o conceito de crime cibernético se relaciona à necessidade de identificar uma conduta típica, ilícita e culpável praticada em contexto tecnológico. Entre os exemplos encontram-se a invasão de dispositivos, o acesso não autorizado a sistemas, o furto ou obtenção ilícita de dados, fraudes eletrônicas, estelionato digital, ataques contra sistemas, disseminação de códigos maliciosos e determinadas formas de violência praticadas por intermédio da internet.

Em uma perspectiva criminológica, o cibercrime também deve ser compreendido como “um fenômeno que ultrapassa fronteiras territoriais e pode envolver indivíduos, empresas, organizações criminosas e até instituições públicas” (MACHADO; DUARTE, 2021, p.05). A vítima pode sofrer prejuízos patrimoniais, violação de privacidade, exposição indevida de informações, danos à reputação ou comprometimento de sistemas e serviços essenciais.

No que tange às suas características, apresenta-se o quadro abaixo:

Quadro 1 – Principais características dos crimes cibernéticos

CARACTERÍSTICA	DESCRIÇÃO
Utilização de tecnologia	Envolve computadores, smartphones, servidores, redes sociais, aplicativos, sistemas ou internet.
Transnacionalidade	O autor, a vítima, os servidores e os dados podem estar localizados em diferentes países.
Dificuldade de identificação	Técnicas de anonimização, falsificação de identidade e utilização de diferentes infraestruturas dificultam a identificação do responsável.

Rapidez de execução	Uma ação criminosa pode atingir grande quantidade de vítimas em curto espaço de tempo.
Volatilidade da prova	Evidências digitais podem ser apagadas, modificadas ou perder-se rapidamente, exigindo procedimentos adequados de preservação.
Escalabilidade	Uma única ferramenta ou estratégia criminosa pode ser utilizada contra milhares de vítimas.
Diversidade de modalidades	Abrange fraudes, invasões, furtos de dados, ataques a sistemas, perseguição virtual, crimes contra a honra e outras condutas.
Potencial econômico	Pode gerar prejuízos financeiros expressivos para indivíduos, empresas e instituições.
Evolução constante	Os métodos utilizados pelos criminosos acompanham o desenvolvimento de novas tecnologias.
Necessidade de cooperação	A investigação frequentemente depende da atuação conjunta entre polícia, empresas de tecnologia, provedores e autoridades de diferentes países.

Fonte: Adaptado de Arruda e Lima (2023).

Essas características tornam os crimes cibernéticos particularmente complexos para os sistemas tradicionais de investigação e persecução penal. Castells (2022) ressalta especialmente a volatilidade dos vestígios, a dificuldade de atribuição de autoria e a necessidade de mecanismos de cooperação internacional.

Conforme explana Barreto, Kufa e Silva (2022), o enfrentamento dos crimes cibernéticos tem como principal objetivo proteger bens jurídicos fundamentais no ambiente digital, incluindo patrimônio, privacidade, intimidade, honra, segurança de dados, integridade de sistemas e confiabilidade das relações realizadas por meios eletrônicos.

Santos (2024) por sua vez, explica que a finalidade da tutela jurídica é impedir ou reduzir a ocorrência de comportamentos que causem danos aos usuários e às instituições, estabelecendo mecanismos de prevenção, investigação e responsabilização dos autores. Nesse sentido, a legislação brasileira busca adaptar instrumentos tradicionais de proteção penal às características específicas do ambiente virtual.

Outro objetivo consiste em aprimorar a capacidade do Estado de investigar e responsabilizar os agentes envolvidos em delitos digitais. Para isso, Tavares (2023) aduz que são fundamentais a preservação e análise de evidências eletrônicas, a capacitação de investigadores e peritos, a cooperação entre instituições e o intercâmbio internacional de informações. Nesse sentido, o autor cita a Convenção de Budapeste, que representa importante instrumento nesse contexto, especialmente por estabelecer mecanismos de cooperação e procedimentos relacionados à investigação e à produção de provas eletrônicas.

Entre as principais espécies de crimes cibernéticos identificadas pela literatura jurídica e criminológica destacam-se as seguintes:

Quadro 2 – Espécies de crimes cibernéticos

ESPÉCIE DE CRIME CIBERNÉTICO	CARACTERIZAÇÃO
Invasão de dispositivos informáticos	Acesso não autorizado a computadores, celulares ou sistemas digitais para obter, alterar ou destruir dados.
Fraudes eletrônicas	Golpes virtuais envolvendo transferências bancárias, clonagem de cartões ou estelionato digital.
<i>Phishing</i>	Técnica de engenharia social utilizada para enganar usuários e obter informações pessoais ou financeiras.
Disseminação de <i>malware</i>	Propagação de vírus ou softwares maliciosos destinados a causar danos ou roubar informações.
<i>Ransomware</i>	Sequestro de dados ou sistemas mediante exigência de pagamento para restabelecer o acesso.
Crimes contra a honra na internet	Prática de calúnia, injúria ou difamação por meio de redes sociais e plataformas digitais.
Violação de direitos autorais	Distribuição ilegal de conteúdos protegidos por direitos de propriedade intelectual.
Exploração sexual e pornografia infantil online	Compartilhamento ou produção de material ilícito envolvendo menores na internet.

Fonte: Adaptado de Oliveira; Calvet (2022, p. 09).

De acordo com Pinheiro (2022), essas modalidades demonstram a diversidade e complexidade das práticas criminosas no ambiente digital, que se ampliam à medida que novas tecnologias são incorporadas ao cotidiano da sociedade.

Os impactos dos crimes cibernéticos são amplos e podem atingir tanto indivíduos quanto empresas e órgãos públicos. No âmbito individual, Pinheiro (2022) afirma que as vítimas podem sofrer perdas financeiras, roubo de identidade, exposição de informações pessoais, violação de privacidade, danos à reputação e consequências psicológicas e sociais. No âmbito empresarial, ataques podem provocar interrupção das atividades, perda de informações, despesas extraordinárias, redução da confiança dos consumidores e prejuízos à imagem institucional.

No âmbito estatal e social, Climaco (2022) destaca que a expansão dos crimes cibernéticos impõe desafios relacionados à segurança pública, à proteção de infraestruturas críticas, à capacidade investigativa e à atualização permanente da legislação. A dificuldade de identificação da autoria, a natureza transnacional dos delitos e a rápida transformação das ferramentas tecnológicas podem produzir lacunas entre a prática criminosa e a capacidade de resposta institucional.

No Brasil, estudos recentes identificam avanços legislativos importantes, mas também apontam a necessidade de investimentos em perícia, capacitação, cooperação internacional e

atualização normativa diante de recursos como inteligência artificial, deepfakes e técnicas sofisticadas de anonimização.

A esse respeito, apresenta-se o tópico seguinte.

3. LEGISLAÇÃO BRASILEIRA FRENTE AOS CRIMES CIBERNÉTICOS

A legislação brasileira voltada ao enfrentamento dos crimes cibernéticos evoluiu gradualmente nas últimas décadas, acompanhando o avanço das tecnologias digitais e a ampliação do uso da internet pela sociedade. Segundo explica Montel e Paiva (2024), inicialmente, o ordenamento jurídico nacional não possuía normas específicas para lidar com delitos praticados no ambiente virtual, sendo necessário aplicar dispositivos tradicionais do Direito Penal para enquadrar condutas ilícitas realizadas por meio de computadores ou redes digitais.

Com o crescimento dos ataques cibernéticos, fraudes eletrônicas e invasões de sistemas, tornou-se evidente a necessidade de criar normas jurídicas específicas capazes de regular o ambiente digital e responsabilizar os autores dessas infrações (MONTEL; PAIVA, 2024).

Um dos primeiros marcos legislativos importantes nesse contexto foi a Lei nº 12.737/2012, que passou a tipificar crimes relacionados à invasão de dispositivos informáticos. Essa lei alterou o Código Penal brasileiro, acrescentando os artigos 154-A e 154-B, que tratam da invasão de computadores, celulares ou outros dispositivos eletrônicos com o objetivo de obter, adulterar ou destruir dados sem autorização do titular. No texto do art. 154-A aduz:

Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita.
Pena - detenção, de 03 (três) meses a 01 (um) ano, e multa.
(BRASIL, 2012)

Para Rocha et al. (2024), a criação dessa norma representou um avanço significativo na proteção da privacidade e da segurança da informação, pois passou a reconhecer juridicamente condutas criminosas que antes não possuíam tipificação penal específica no ordenamento brasileiro.

Outro instrumento normativo fundamental para a regulação do ambiente digital no Brasil é o Lei nº 12.965/2014. Essa legislação estabeleceu princípios, direitos e deveres para o uso da internet no país, garantindo a liberdade de expressão, a proteção da privacidade e a preservação dos dados pessoais dos usuários (BRASIL, 2014).

Além disso, o Marco Civil definiu regras sobre a responsabilidade dos provedores de serviços digitais e sobre a guarda de registros de acesso, elementos importantes para a investigação de crimes praticados no ambiente virtual. Assim, a lei passou a funcionar como uma espécie de “constituição da internet” no Brasil, estruturando juridicamente o funcionamento das relações digitais (ROCHA et al., 2024).

3.1 DA LEI Nº 13.709/2018

A expansão das tecnologias digitais e a crescente utilização da internet para atividades pessoais, comerciais e institucionais ampliaram também a exposição da sociedade a práticas ilícitas envolvendo dados e sistemas informáticos. Nesse contexto, a Lei nº 13.709, de 14 de agosto de 2018 – Lei Geral de Proteção de Dados Pessoais (LGPD), representa importante marco normativo brasileiro, embora não seja uma lei penal especificamente destinada à criminalização dos crimes cibernéticos.

De acordo com Silva et al. (2026), sua finalidade principal consiste em disciplinar o tratamento de dados pessoais e proteger direitos fundamentais relacionados à liberdade, à privacidade e ao livre desenvolvimento da personalidade. O próprio art. 1º estabelece que a Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, com o objetivo de proteger esses direitos (BRASIL, 2018).

No entendimento de Hernandez e Toledo (2021), a LGPD apresenta especial relevância para o enfrentamento dos crimes cibernéticos porque estabelece obrigações de segurança e governança para aqueles que realizam operações de tratamento de dados pessoais. Dessa maneira, embora a lei não estabeleça, em regra, tipos penais específicos para cada modalidade de ataque cibernético, cria um sistema preventivo destinado a reduzir vulnerabilidades e proteger informações contra acessos não autorizados e outras formas de utilização ilícita.

Essa função preventiva torna-se especialmente importante diante de situações como vazamentos de bancos de dados, invasões de sistemas, obtenção indevida de informações pessoais, fraudes eletrônicas e utilização abusiva de dados (HERNANDEZ; TOLEDO, 2021).

Entre os fundamentos da proteção de dados, a LGPD estabelece, em seu art. 2º, valores diretamente relacionados à proteção do indivíduo no ambiente digital. A norma contempla, entre outros, o respeito à privacidade, a autodeterminação informativa, a liberdade de expressão, de informação e de comunicação, a inviolabilidade da intimidade, da honra e da imagem, além do desenvolvimento econômico e tecnológico (BRASIL, 2018).

Para Silva et al. (2026), esses fundamentos são particularmente relevantes para os crimes cibernéticos porque os ataques digitais frequentemente envolvem a violação simultânea de diferentes direitos. Assim, um vazamento de dados, por exemplo, pode ultrapassar o mero prejuízo patrimonial e atingir a privacidade, a imagem, a segurança e a dignidade da vítima.

Outro aspecto fundamental está previsto no art. 6º da LGPD, que determina que as atividades de tratamento devem observar princípios como finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação e responsabilização e prestação de contas (BRASIL, 2018).

O princípio da segurança possui especial importância no contexto dos crimes cibernéticos, pois exige a adoção de medidas capazes de proteger os dados pessoais. A obra de Maldonado, Blum e Borelli (2022) destaca justamente a amplitude da LGPD e sua aplicação articulada com diferentes áreas do Direito, oferecendo interpretação sistematizada de seus dispositivos.

A proteção contra incidentes de segurança é tratada de maneira mais específica no art. 46 da LGPD, segundo o qual os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito (BRASIL, 2018). Segundo Lopes et al. (2024), esse dispositivo demonstra que a legislação não se limita a estabelecer direitos abstratos aos titulares, mas também impõe uma obrigação de prevenção aos agentes que controlam ou operam dados pessoais.

O art. 47 amplia essa preocupação ao determinar que os agentes de tratamento ou qualquer outra pessoa que intervenha em uma das fases do tratamento se obrigam a garantir a segurança da informação em relação aos dados pessoais, mesmo depois de seu término (BRASIL, 2018). Nogueira e Nolasco (2022) pontuam que tal disposição é importante diante da dinâmica dos crimes cibernéticos, nos quais informações obtidas em determinado momento podem continuar sendo utilizadas posteriormente para fraudes, extorsões, criação de identidades falsas ou outras práticas ilícitas. Dessa forma, a proteção jurídica não se encerra necessariamente quando termina a atividade inicialmente realizada com os dados, permanecendo a preocupação com sua segurança e integridade.

Outro dispositivo diretamente relacionado aos incidentes cibernéticos é o art. 48 da LGPD, que determina que o controlador deve comunicar à Autoridade Nacional de Proteção

de Dados (ANPD) e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares (BRASIL, 2018). A comunicação constitui importante mecanismo de transparência e resposta, permitindo que sejam adotadas medidas para reduzir os possíveis prejuízos.

A LGPD também criou a Autoridade Nacional de Proteção de Dados (ANPD), responsável por exercer funções de fiscalização, regulamentação e aplicação de sanções administrativas previstas na legislação (BRASIL, 2018). Dias e Azevedo (2026) mencionam que a existência de uma autoridade especializada representa importante avanço institucional, pois permite estabelecer orientações, regulamentações e mecanismos de fiscalização relacionados ao tratamento de dados pessoais. Entretanto, é necessário diferenciar a atuação administrativa da LGPD da persecução penal: a ocorrência de um incidente de segurança pode desencadear consequências administrativas no âmbito da proteção de dados, mas, dependendo da conduta praticada, também poderá caracterizar crime previsto em outras normas penais brasileiras. Essa articulação entre diferentes instrumentos jurídicos é fundamental para o enfrentamento dos crimes cibernéticos.

Nesse sentido, a LGPD deve ser interpretada conjuntamente com outras normas que compõem o sistema brasileiro de proteção no ambiente digital. A Lei nº 12.965/2014 (Marco Civil da Internet) estabelece princípios, garantias, direitos e deveres para o uso da internet; a Lei nº 12.737/2012, conhecida como Lei Carolina Dieckmann, introduziu importantes disposições penais relacionadas à invasão de dispositivos informáticos; e a Lei nº 14.155/2021 agravou o tratamento penal de determinadas condutas praticadas por meios eletrônicos, incluindo modalidades de fraude e invasão de dispositivo informático. Assim, a LGPD não substitui a legislação penal, mas integra um conjunto normativo destinado à proteção do cidadão no ambiente digital.

A relação entre LGPD e crimes cibernéticos torna-se ainda mais evidente quando se considera que os dados pessoais constituem um dos principais alvos e instrumentos das práticas criminosas contemporâneas. Informações como nome, CPF, endereço, dados financeiros, credenciais de acesso e informações sensíveis podem ser utilizadas para obtenção de vantagens econômicas, falsificação de identidade e execução de fraudes (BRASIL, 2018). Por isso, a proteção estabelecida pela LGPD possui caráter preventivo e contribui para reduzir a exposição das pessoas e organizações a determinados riscos.

3.2 DA LEI Nº 14.155/2021

A Lei nº 14.155, de 27 de maio de 2021, constitui importante marco no processo de atualização da legislação penal brasileira diante do crescimento dos crimes praticados por meio eletrônico ou pela internet. A norma alterou o Código Penal e o Código de Processo Penal com o propósito de tornar mais graves determinadas condutas relacionadas à invasão de dispositivos informáticos, ao furto mediante fraude e ao estelionato eletrônico, além de estabelecer regras específicas de competência para determinadas modalidades de estelionato. A própria ementa da lei estabelece que seu objetivo foi “tornar mais graves os crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela internet” (BRASIL, 2021).

Uma das principais alterações promovidas pela Lei nº 14.155/2021 ocorreu no art. 154-A do Código Penal, que trata da invasão de dispositivo informático. A legislação passou a estabelecer que constitui crime “invadir dispositivo informático de uso alheio”, conectado ou não à rede de computadores, com a finalidade de obter, adulterar ou destruir dados ou informações sem autorização, ou instalar vulnerabilidades para obter vantagem ilícita. A pena prevista para a forma básica passou a ser de reclusão de 1 a 4 anos e multa. Além disso, o § 2º passou a prever aumento de pena de um terço a dois terços quando da invasão resultar prejuízo econômico (BRASIL, 2021).

A alteração do art. 154-A demonstra uma preocupação específica do legislador com a proteção da integridade dos dispositivos e das informações armazenadas em ambientes digitais. A mudança ampliou a resposta penal diante de práticas que podem envolver invasões de computadores, celulares e outros dispositivos utilizados para armazenamento ou processamento de informações. Lai e Mourão (2021) observam que a evolução tecnológica e a migração de diversas práticas ilícitas para o ambiente virtual exigiram atualização legislativa, especialmente diante do aumento da utilização da internet durante a pandemia da COVID-19.

A presente lei também promoveu mudanças importantes no crime de furto, acrescentando o § 4º-B ao art. 155 do Código Penal. Conforme a norma, a pena passou a ser de reclusão de 4 a 8 anos e multa quando o furto mediante fraude for cometido por meio de dispositivo eletrônico ou informático, conectado ou não à rede de computadores, com ou sem violação de mecanismo de segurança, utilização de programa malicioso ou outro meio fraudulento análogo. O legislador ainda estabeleceu causas de aumento de pena quando o crime for praticado mediante servidor mantido fora do território nacional ou contra pessoa idosa ou vulnerável (BRASIL, 2021).

Outra inovação de grande relevância foi a criação da denominada fraude eletrônica, prevista no § 2º-A do art. 171 do Código Penal. O dispositivo estabelece pena de reclusão de 4 a 8 anos e multa quando a fraude for praticada mediante utilização de informações fornecidas pela vítima ou por terceiro induzido a erro por meio de redes sociais, contatos telefônicos, envio de correio eletrônico fraudulento ou outro meio fraudulento análogo (BRASIL, 2021). Dessa maneira, a legislação passou a conferir tratamento penal específico a modalidades de estelionato que utilizam recursos tecnológicos para induzir a vítima em erro.

A previsão da fraude eletrônica representa uma importante adaptação do Direito Penal às novas formas de obtenção ilícita de vantagem patrimonial. Golpes praticados por meio de redes sociais, mensagens, ligações telefônicas, e-mails fraudulentos e outras ferramentas digitais podem atingir grande número de pessoas e dificultar a identificação do responsável. Gomes e Medrado (2023), ao analisarem a Lei em comento, destacam que a alteração conferiu maior responsabilidade penal aos autores do estelionato virtual, embora permaneçam necessários investimentos em segurança, capacitação dos usuários, tecnologia e políticas públicas de prevenção.

A legislação também estabeleceu mecanismos de agravamento das penas em determinadas circunstâncias. No caso do furto mediante fraude praticado por meio eletrônico, o art. 155, § 4º-C, prevê aumento de um terço a dois terços quando houver utilização de servidor mantido fora do território nacional e aumento de um terço ao dobro quando a vítima for idosa ou vulnerável. No estelionato, o § 2º-B do art. 171 prevê aumento de um terço a dois terços quando a fraude eletrônica for praticada mediante utilização de servidor mantido fora do território nacional (BRASIL, 2021).

Outro aspecto relevante da Lei nº 14.155/2021 foi a alteração do Código de Processo Penal, especialmente do art. 70, com a inclusão do § 4º. Nas hipóteses de estelionato praticado mediante depósito, emissão de cheque sem fundos ou com pagamento frustrado, ou transferência de valores, a competência passou a ser determinada pelo domicílio da vítima; havendo pluralidade de vítimas, aplica-se a prevenção (BRASIL, 2021). Para Silva et al. (2026), a alteração possui importância prática porque os crimes virtuais frequentemente envolvem autores, vítimas, contas bancárias e dispositivos localizados em diferentes municípios ou até mesmo países.

Apesar de representar avanço significativo, a Lei nº 14.155/2021 não solucionou integralmente os desafios relacionados aos crimes cibernéticos. A evolução acelerada das

tecnologias possibilita o surgimento constante de novas estratégias criminosas, enquanto a investigação desses delitos depende de conhecimento técnico, preservação de evidências digitais, cooperação entre instituições e, em muitos casos, colaboração internacional. Montel e Paiva (2024) ressaltam que o panorama legislativo brasileiro demonstra avanços na tipificação e repressão dos crimes cibernéticos, mas ainda existem desafios para garantir uma resposta suficientemente eficaz às novas modalidades de delitos digitais.

Sobre essa questão, apresenta-se o tópico seguinte.

4. DA EFETIVIDADE DA LEGISLAÇÃO BRASILEIRA FRENTE À EXPANSÃO DAS TECNOLOGIAS DIGITAIS

A expansão das tecnologias digitais modificou profundamente as relações sociais, econômicas e institucionais, proporcionando benefícios relacionados à comunicação, ao acesso à informação e à realização de atividades comerciais e financeiras. Paralelamente, esse processo também criou novas oportunidades para a prática de condutas ilícitas, aumentando a necessidade de adaptação do sistema jurídico. No Brasil, a resposta legislativa vem sendo construída por meio de diferentes diplomas, entre os quais, as já citadas anteriormente, o Marco Civil da Internet, a Lei Geral de Proteção de Dados Pessoais (LGPD), a Lei nº 14.155/2021 e, mais recentemente, normas voltadas à proteção de crianças e adolescentes no ambiente digital.

13

Para Barreto, Kufa e Silva (2022), a expansão do ciberespaço produz desafios específicos para o Direito Penal, especialmente em razão da transnacionalidade, da velocidade de execução dos delitos e das dificuldades relacionadas à identificação de autoria e produção probatória.

A efetividade da legislação brasileira, portanto, não pode ser analisada apenas pela quantidade de leis criadas nos últimos anos. É necessário verificar se as normas são capazes de produzir mecanismos concretos de prevenção, investigação, responsabilização e proteção das vítimas. Nesse sentido, Stroppa e Rothenburg (2023) pontuam que a legislação brasileira apresentou avanços significativos ao reconhecer determinadas modalidades de criminalidade digital e estabelecer instrumentos jurídicos para enfrentá-las. A Lei nº 14.155/2021, por exemplo, tornou mais graves os crimes de invasão de dispositivo informático, furto mediante fraude e estelionato praticados de forma eletrônica ou pela internet.

Entretanto, a simples existência de tipos penais específicos não garante, por si só, a efetividade da tutela jurídica. Conforme salienta Marques (2024), os crimes cibernéticos apresentam características que dificultam a aplicação tradicional do Direito Penal, especialmente porque o autor pode estar fisicamente distante da vítima, utilizar recursos de

anonimização e explorar infraestruturas tecnológicas situadas em diferentes localidades. Montel e Paiva (2024) observam que o ordenamento jurídico brasileiro avançou na construção de um panorama legislativo voltado aos crimes cibernéticos, mas destacam a necessidade de medidas mais assertivas para que a legislação produza resultados concretos na prevenção e interrupção dessas práticas.

Outro elemento essencial para avaliar a efetividade da legislação é a capacidade de investigação e produção da prova digital. Diferentemente da prova tradicional, os vestígios eletrônicos podem ser facilmente alterados, apagados ou deslocados entre diferentes servidores e dispositivos. Por isso, a investigação exige conhecimentos técnicos especializados e procedimentos capazes de preservar a autenticidade e a integridade das evidências. Pereira França (2024) explica que a obtenção de provas digitais possui características próprias e que o processo penal brasileiro demanda disciplina jurídica específica para orientar medidas como busca e apreensão de dispositivos e obtenção de dados digitais.

A doutrina jurídica também ressalta que a efetividade do combate aos crimes cibernéticos depende da cooperação entre diferentes instituições. Casotti (2024) enfatiza que a Polícia Judiciária, Ministério Público, Poder Judiciário, provedores de aplicação, instituições financeiras e órgãos especializados precisam atuar de maneira coordenada para possibilitar a identificação dos responsáveis e a preservação dos vestígios. Barreto, Kufa e Silva (2022) destacam, entre os principais desafios do combate aos cibercrimes, a investigação em ambientes digitais, a produção de provas no ciberespaço e a necessidade de cooperação internacional, considerando que a criminalidade digital frequentemente ultrapassa as fronteiras nacionais.

A questão da competência jurisdicional constitui outro exemplo de adaptação legislativa às características dos delitos digitais. A Lei nº 14.155/2021 acrescentou o § 4º ao art. 70 do Código de Processo Penal, estabelecendo que, em determinadas hipóteses de estelionato praticado mediante depósito, transferência de valores ou determinadas modalidades de cheque, a competência será definida pelo domicílio da vítima (BRASIL, 2021). Essa alteração, de acordo com Rodrigues e Freire (2026), possui especial relevância porque os crimes praticados pela internet podem envolver vítima, autor, conta bancária e servidores localizados em diferentes cidades ou países. Assim, a modificação legislativa procurou aproximar o processo penal do local em que os efeitos do crime atingem diretamente a vítima.

Nesse contexto, destaca-se o entendimento firmado pelo Superior Tribunal de Justiça (STJ) no Conflito de Competência nº 181.726/PR, julgado pela Terceira Seção, sob relatoria da

Ministra Laurita Vaz. O Tribunal reconheceu a aplicação imediata da alteração promovida pela Lei nº 14.155/2021 e estabeleceu que, nas hipóteses abrangidas pelo § 4º do art. 70 do CPP, a competência para o julgamento do estelionato é do juízo do domicílio da vítima:

CONFLITO NEGATIVO DE COMPETÊNCIA. PROCESSUAL PENAL. ESTELIONATO. CRIME QUE SE UTILIZOU DE IMAGENS DE DOCUMENTOS FEDERAIS PARA INDUZIR A VÍTIMA EM ERRO. INEXISTÊNCIA DE PREJUÍZO A INTERESSES, SERVIÇOS OU BENS DA UNIÃO. CONFLITO CONHECIDO PARA DECLARAR A COMPETÊNCIA DA JUSTIÇA ESTADUAL. CRIME PRATICADO MEDIANTE DEPÓSITO BANCÁRIO. SUPERVENIÊNCIA DA LEI N. 14.155/2021. PERSECUÇÃO PENAL EM FASE DE INQUÉRITO POLICIAL. NORMA PROCESSUAL. APLICAÇÃO IMEDIATA. CONFLITO CONHECIDO PARA DECLARAR COMPETENTE O JUÍZO DO DOMICÍLIO DA VÍTIMA. 1. No caso, a Vítima direta do estelionato foi pessoa jurídica sediada na República Popular da China e a obtenção da vantagem ilícita se deu nos Estados Unidos da América. Para a prática do delito, os criminosos se fizeram passar por agentes de empresa brasileira sediada no Estado do Paraná. Não há notícia sobre a autoria delitiva ou mesmo a nacionalidade dos eventuais autores, tampouco onde teriam sido praticados os atos executórios, todos realizados por meios eletrônicos, a exceção de contato com telefone da cidade de São Paulo - SP. 2. **Embora o estelionatário tenha se utilizado de imagens digitais adulteradas de passaporte válido de terceiro e documentos emitidos por órgão públicos federais para, induzindo a vítima em erro, receber depósito de valores em conta corrente no exterior, inexistente evidência de prejuízo a interesses, bens ou serviços da União, pois não houve falsificação de passaporte, como informou a própria Polícia Federal, mas sim a remessa, por meio eletrônico, de uma imagem de adulterada de documento válido, com a finalidade de enganar o destinatário.** 3. Do mesmo modo, a falsificação de selo ou sinal público (art. 296 do Código Penal) teria sido utilizada para dar falsa aparência de regularidade ao negócio fraudulento, em prejuízo da empresa vítima, o que não implica em lesão aos interesses do Ministério da Agricultura, consoante precedentes desta Corte Superior. Logo, **por via de consequência, falece competência à Justiça Federal para processar o julgar o feito.** 4. **Afastada a competência da Justiça Federal, urge fixar o Juízo Estadual competente para processar o feito. Nos termos do art. 70, § 4º, do Código de Processo Penal, com a redação atribuída pela Lei n. 14.155/2021, a competência será definida pelo local do domicílio da vítima no caso de crime de estelionato praticado mediante depósito, transferência de valores ou cheque sem provisão de fundos em poder do sacado ou com o pagamento frustrado.** 5. Conflito conhecido para declarar competente o Juízo Estadual da Comarca de Guararapes - PE, onde se situa a representação da Empresa Vítima no Brasil. (SUPERIOR TRIBUNAL DE JUSTIÇA. Conflito de Competência nº 181.726/PR. Relatora: Ministra Laurita Vaz. Terceira Seção. Julgado em 8 set. 2021. Informativo de Jurisprudência, Brasília, DF, edição extraordinária n. 4, 31 jan. 2022). (grifo da autora).

A decisão demonstra que a jurisprudência tem desempenhado papel importante na adaptação do ordenamento às novas formas de criminalidade. O STJ esclareceu que a alteração legislativa possui natureza processual e aplicação imediata, embora a competência territorial seja relativa e possa incidir a regra da *perpetuatio jurisdictionis* quando já oferecida a denúncia (CAVALCANTI NETO, 2023). A jurisprudência evidencia, portanto, que a efetividade da legislação depende também da interpretação judicial capaz de solucionar situações novas decorrentes da utilização das tecnologias digitais.

A proteção de dados pessoais constitui outra dimensão indispensável da efetividade jurídica no ambiente digital. A LGPD não é uma lei penal de combate aos crimes cibernéticos, mas estabelece obrigações preventivas para agentes de tratamento e mecanismos destinados a proteger dados pessoais contra acessos não autorizados, perda, destruição, alteração ou tratamento ilícito. Nesse sentido, a legislação atua antes mesmo da ocorrência de determinadas práticas criminosas, estabelecendo padrões de segurança e governança (CASOTTI, 2024). Pinheiro (2023) ressalta que a proteção preventiva é particularmente importante porque os dados pessoais podem ser utilizados como instrumentos para fraudes, falsificação de identidade, extorsões e outras modalidades de criminalidade digital.

A efetividade do sistema jurídico também depende da capacidade de acompanhar novas formas de comunicação e de circulação de conteúdos ilícitos. O ambiente digital possibilitou que informações fossem produzidas e disseminadas em velocidade e escala incomparavelmente superiores às existentes nos meios tradicionais. No estudo de Groskreutz (2022), demonstrou que o regime brasileiro de responsabilização de provedores de redes sociais constitui questão complexa, envolvendo a necessidade de equilibrar proteção contra conteúdos ilícitos, liberdade de expressão e segurança jurídica. A pesquisa apontou que o sistema brasileiro pode aprimorar mecanismos de formalização e transparência sem abandonar os parâmetros jurídicos existentes.

16

A expansão tecnológica também exige que o Direito considere a cibersegurança como questão de interesse público. A criação da Política Nacional de Cibersegurança, instituída pelo Decreto nº 11.856/2023, demonstra que o enfrentamento dos riscos digitais ultrapassa a esfera exclusivamente penal. Na visão de Arruda e Lima (2023), a proteção de infraestruturas críticas, serviços públicos, sistemas financeiros e bases de dados exige políticas preventivas e mecanismos permanentes de gestão de riscos.

Outro aspecto que interfere diretamente na efetividade da legislação é a necessidade de atualização constante. A tecnologia evolui em ritmo muito mais acelerado do que o processo legislativo, fazendo com que determinadas condutas possam surgir antes da existência de uma previsão normativa específica. Inteligência artificial generativa, deepfakes, automação de golpes, engenharia social sofisticada e novas formas de manipulação de dados são exemplos de tecnologias que podem ser utilizadas tanto de maneira legítima quanto criminosa (RODRIGUES; FREIRE, 2026).

Nesse cenário, Lai e Mourão (2021, p. 238) destaca que “a interpretação jurídica, a produção doutrinária e a jurisprudência assumem importância complementar à atividade legislativa, permitindo que o ordenamento responda às transformações sem abandonar os princípios constitucionais e as garantias fundamentais”.

A efetividade da legislação também está relacionada à capacidade do Estado de proteger grupos mais vulneráveis. A própria Lei nº 14.155/2021 estabeleceu causas específicas de aumento de pena para determinadas situações envolvendo vítimas idosas ou vulneráveis, reconhecendo que determinados grupos podem apresentar maior exposição a fraudes eletrônicas. Além disso, a Lei nº 14.811/2024 ampliou a tutela penal de crianças e adolescentes ao incluir o cyberbullying no Código Penal, demonstrando que o legislador vem respondendo a modalidades de violência que se desenvolvem ou são potencializadas pelos ambientes virtuais (BRASIL, 2024). A legislação recente, assim, revela movimento de ampliação da proteção jurídica diante das diferentes formas de violência digital.

Apesar desses avanços, persistem obstáculos relevantes para a efetiva responsabilização dos autores. A identificação do agente criminoso pode depender de registros mantidos por provedores, dados de conexão, informações bancárias e outros elementos que nem sempre estão imediatamente disponíveis às autoridades. Além disso, quando os dados estão armazenados no exterior, a investigação pode depender de mecanismos de cooperação internacional. Nesse ponto, a doutrina de Barreto, Kufa e Silva (2022) destaca que o caráter transnacional dos cibercrimes constitui um dos principais desafios para sua repressão, exigindo articulação internacional e mecanismos eficientes de obtenção de informações.

Dessa maneira, pode-se afirmar que a legislação brasileira apresenta efetividade parcial e progressiva diante da expansão das tecnologias digitais. Houve avanços importantes na tipificação de condutas, na proteção de dados, na definição de competências, na responsabilização de agentes e na criação de políticas de cibersegurança (RODRIGUES; FREIRE, 2026).

Contudo, a eficácia concreta das normas ainda depende de investimentos em investigação cibernética, perícia digital, capacitação de profissionais, cooperação internacional, segurança da informação e educação digital. A legislação, isoladamente, não é capaz de acompanhar todas as transformações tecnológicas, sendo necessária uma abordagem integrada entre Direito, tecnologia, segurança pública e sociedade.

Por fim, a efetividade da legislação brasileira frente às tecnologias digitais deve ser compreendida como um processo permanente de adaptação. A evolução tecnológica cria novas possibilidades de interação e desenvolvimento econômico, mas também amplia a superfície de ataque para práticas criminosas (PINHEIRO, 2023). Nesse cenário, o Direito precisa combinar repressão e prevenção, garantindo simultaneamente a segurança dos usuários e a preservação dos direitos fundamentais.

A experiência brasileira demonstra que leis como a Lei nº 14.155/2021, a LGPD, o Marco Civil da Internet e a legislação mais recente constituem importantes instrumentos de proteção, mas sua efetividade dependerá da capacidade institucional de aplicá-las adequadamente e de atualizar continuamente os mecanismos de enfrentamento da criminalidade digital.

5. CONSIDERAÇÕES FINAIS

A análise desenvolvida ao longo deste estudo permitiu compreender que os crimes cibernéticos constituem um dos principais desafios contemporâneos para o Direito, especialmente diante da rápida expansão das tecnologias digitais e da crescente dependência da sociedade em relação à internet.

A utilização de dispositivos eletrônicos, redes sociais, sistemas bancários e plataformas digitais ampliou as possibilidades de interação, mas também criou novos espaços para a prática de condutas ilícitas. Nesse cenário, tornou-se indispensável a construção de mecanismos jurídicos capazes de proteger os usuários e responsabilizar aqueles que utilizam os recursos tecnológicos para fins criminosos.

No Brasil, observa-se uma evolução gradual da legislação destinada ao enfrentamento dessas práticas. A Lei nº 14.155/2021 representou importante avanço ao modificar o Código Penal e o Código de Processo Penal, agravando as consequências jurídicas de determinados crimes praticados por meios eletrônicos e estabelecendo regras específicas de competência para algumas modalidades de estelionato. A norma passou a conferir tratamento mais rigoroso à invasão de dispositivos informáticos, ao furto mediante fraude praticado por meio eletrônico e à fraude eletrônica, demonstrando uma tentativa do legislador de aproximar o Direito Penal das transformações ocorridas no ambiente digital.

Também se verificou que a proteção jurídica não se limita à repressão penal. A Lei Geral de Proteção de Dados Pessoais, o Marco Civil da Internet e outras normas relacionadas à segurança digital complementam o sistema de proteção, estabelecendo direitos, deveres e

mecanismos preventivos. Dessa forma, o enfrentamento dos crimes cibernéticos exige uma atuação integrada entre prevenção, proteção de dados, investigação criminal, responsabilização dos autores e preservação dos direitos fundamentais dos usuários.

Apesar dos avanços legislativos, conclui-se que a efetividade da legislação brasileira ainda encontra limitações decorrentes da própria dinâmica das tecnologias digitais. Os criminosos conseguem utilizar recursos tecnológicos cada vez mais sofisticados, enquanto a identificação da autoria, a preservação das evidências digitais e a localização de dados armazenados em diferentes territórios podem dificultar a investigação. Assim, a existência de normas específicas representa apenas uma etapa do processo de enfrentamento dos crimes cibernéticos, sendo igualmente necessários investimentos em perícia digital, capacitação dos agentes públicos, infraestrutura tecnológica e cooperação nacional e internacional.

Portanto, a legislação brasileira apresenta evolução significativa, mas precisa permanecer em constante aperfeiçoamento para acompanhar a transformação do ambiente digital. A efetividade das normas dependerá não somente da criação de novos instrumentos jurídicos, mas também da capacidade das instituições públicas e privadas de aplicá-los de maneira eficiente.

Nesse sentido, o combate aos crimes cibernéticos deve ser compreendido como uma responsabilidade compartilhada, envolvendo Poder Legislativo, Poder Judiciário, Ministério Público, órgãos policiais, empresas de tecnologia e sociedade civil, de modo a garantir maior segurança digital sem comprometer as liberdades e garantias fundamentais.

REFERÊNCIAS

ALMEIDA, Haian de Assis Lopes de; OLIVEIRA, Tamar Ramos de. Crimes virtuais: o avanço dos crimes eletrônicos e a evolução das leis específicas no Brasil. **Revista Ibero-Americana de Humanidades, Ciências e Educação**, v. 8, n. 11, 2022. Disponível em: <https://doi.org/10.51891/rease.v8i11.7554>. Acesso em: 18 ago. 2026.

ARRUDA, Vanessa Cristina Dias; LIMA, Marília Freitas. Crimes cibernéticos: análise da legislação civil e penal vigente no Brasil. **RECIMA21 – Revista Científica Multidisciplinar**, v. 4, n. 12, 2023. Disponível em: <https://doi.org/10.47820/recima21.v4i12.4578>. Acesso em: 10 ago. 2026.

BARRETO, Alesandro Gonçalves; KUFA, Karina; SILVA, Marcelo Mesquita. **Ciber Crimes e seus reflexos no direito brasileiro**. 3. ed. Salvador: JusPodivm, 2022.

BRASIL. **Lei nº 12.737, de 30 de novembro de 2012**. Dispõe sobre a tipificação criminal de delitos informáticos e dá outras providências. Brasília, DF: Presidência da República, 2012. Disponível

em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 15 ago. 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: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 15 ago. 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: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709compilado.htm. Acesso em: 15 ago. 2026.

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 violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela internet; e o Decreto-Lei nº 3.689, de 3 de outubro de 1941 (Código de Processo Penal), para definir a competência em modalidades de estelionato. Brasília, DF: Presidência da República, 2021. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14155.htm. Acesso em: 15 ago. 2026.

BRASIL. SUPERIOR TRIBUNAL DE JUSTIÇA (STJ). **Conflito de Competência nº 178.697/PR**. Relatora: Ministra Laurita Vaz. Terceira Seção. Julgado em 22 jun. 2022. Disponível em: <https://www.stj.jus.br/websecstj/cgi/revista/REJ.cgi/ITA?dt=20220627&formato=HTML&nreg=202101037573&salvar=false&seq=2190122&tipo=o&utm>. Acesso em: 20 ago. 2026.

CASOTTI, Igor José et al. Garantindo a segurança da informação na era digital: riscos e soluções. **Revista Delos**, 2024. Disponível em: <https://ojs.revistadelos.com/ojs/index.php/delos/article/view/2193>. Acesso em: 16 ago. 2026.

CASTELLS, Manuel. **A sociedade em rede**. 6. ed. São Paulo: Paz e Terra, 2022.

CAVALCANTI NETO, Gabriel de Oliveira. Direito penal cibernético: da evolução legislativa à necessidade de tipificação de crimes cibernéticos próprios. **Revista Foco**, v. 16, n. 6, 2023. Disponível em: <https://doi.org/10.54751/revistafoco.v16n6-028>. Acesso em: 10 ago. 2026.

CLIMACO, Caroline. Crimes cibernéticos: impunidades. **Revista Real – Repositório Institucional ICESP**, 32(12) 1-14; 2022. Disponível em: <https://revistas.icesp.br/index.php/Real/article/view/3939>. Acesso em: 17 ago. 2026.

DIAS, Antônio Jorge; AZEVEDO, Delner do Carmo. Crimes cibernéticos e a proteção de dados: a legislação brasileira em relação aos crimes cibernéticos com base na proteção de dados pessoais. **Cognitio Juris**, v. 16, n. 59, 2026. Disponível em: <https://cognitiojuris.com.br/crimes-ciberneticos-e-a-protecao-de-dados-a-legislacao-brasileira-em-relacao-aos-crimes-ciberneticos-com-base-na-protecao-de-dados-pessoais/>. Acesso em: 20 ago. 2026.

GOMES, Walyson Milhomem de Sousa; MEDRADO, Lucas Cavalcante. Crimes cibernéticos: uma ponderação sobre a Lei 14.155 de 2021 aplicável ao crime de estelionato virtual. **Revista Ibero-Americana de Humanidades, Ciências e Educação**, v. 9, n. 9, p. 1870-1894, 2023.

Disponível em: <https://periodicorease.pro.br/rease/article/view/11321>. Acesso em: 16 ago. 2026.

GROSKREUTZ, Hugo Rogério. Os crimes cibernéticos e o princípio da legalidade: os tipos penais abertos, em branco e a indefinição de dispositivos informáticos. **Revista Brasileira de Ciências Criminais**, São Paulo, v. 188, p. 105-137, 2022. Disponível em: <https://publicacoes.ibccrim.org.br/index.php/RBCCRIM/article/view/86>. Acesso em: 24 ago. 2026.

HERNANDEZ, Erika Fernanda Tangerino; TOLEDO, Nathália Karina Abucci de. Crimes cibernéticos: seus efeitos revolucionários diante de uma legislação em constante evolução. **Revista Jurídica da UniFil**, v. 17, n. 17, 2021.

LAI, Sauvei; MOURÃO, Pedro Borges. Lei nº 14.155/2021 dos crimes cibernéticos. **Revista do Ministério Público do Estado do Rio de Janeiro**, n. 82, p. 233-241, out./dez. 2021. Disponível em: <https://www.mprj.mp.br/servicos/revista-do-mp/revista-82/artigo-das-pags-233-241>. Acesso em: 18 ago. 2026.

LOPES, Líliam dos Reis et al. Crimes cibernéticos e direito penal: a regulação e a resposta jurídica ao crime no ambiente digital. **IOSR Journal of Business and Management (IOSR-JBM)**, v. 26, n. 11, ser. 8, 2024.

MACHADO, Rafael Lopes Kassem; DUARTE, Neuziane Lima. Crimes cibernéticos, invasão de privacidade e a efetividade da resposta estatal: os impactos da Lei 12.737/2012 – Lei Carolina Dieckmann e da Lei Geral de Proteção de Dados no combate aos crimes cibernéticos de invasão de privacidade. **Projeção, Direito e Sociedade**, v. 12, n. 2, p. 1-16, 2021. Disponível em: <https://projecaociencia.com.br/index.php/Projecao2/article/view/1798>. Acesso em: 10 ago. 2026.

MALDONADO, Viviane Nóbrega; BLUM, Renato Opice; BORELLI, Alessandra. **LGPD: Lei Geral de Proteção de Dados Pessoais: comentada**. 4. ed. São Paulo: Revista dos Tribunais, 2022.

MARQUES, Thalya Aparecida Silva. Crime de estelionato na contemporaneidade frente à tecnologia virtual. **RECIMA21 – Revista Científica Multidisciplinar**, v. 5, n. 5, 2024. Disponível em: <file:///C:/Users/WIN10/Downloads/submissao-5244-arquivo-31916%20.pdf>. Acesso em: 20 ago. 2026.

MONTEL, Izadora Fonseca; PAIVA, Jaqueline de Kassia Ribeiro de. **Crimes cibernéticos: panorama legislativo**. 2024. Disponível em: <https://www.researchgate.net/publication/385990912>. Acesso em: 16 ago. 2026.

NOGUEIRA, Flavio Mirã de Souza; NOLASCO, Loreci Gottschalk. Crimes cibernéticos - desafios para o direito. **Revista Jurídica Direito, Sociedade e Justiça**, v. 9, n. 13, 2022.

OLIVEIRA, Elaine; CALVET, Marcelo. Os crimes virtuais e as implicações jurídicas de natureza penal. **Revista Real – ICESP**, v. 1, n. 1, 1-10; 2022. Disponível em: <https://revistas.icesp.br/index.php/Real/article/view/4237>. Acesso em: 17 ago. 2026.

PEREIRA FRANÇA, Beatricia dos Santos Carvalho. Crimes cibernéticos e a legislação brasileira. **Revista FT, Ciências Sociais Aplicadas**, v. 28, n. 138, 2024. Disponível em: https://revistaft.com.br/crimes-ciberneticoealeislacaobrasileira/?utm_source=chatgpt.com. Acesso em: 18 ago. 2026.

PINHEIRO, Patrícia Peck. **Direito digital aplicado**. 7. ed. São Paulo: Thomson Reuters Brasil, 2022.

_____. **Proteção de dados pessoais: comentários à Lei nº 13.709/2018 (LGPD)**. 4. ed. São Paulo: SaraivaJur, 2023.

ROCHA, Veronica Alkmim et al. The (in)efficiencies of evidence in Brazilian legislation and the challenges of criminal prosecution in crimes of invasion of computer devices. **Lumen et Virtus**, v. 16, n. 51, p. e7041, 2024. Disponível em: <https://periodicos.newsciencepubl.com/LEV/article/view/7041>. Acesso em: 17 ago. 2026.

RODRIGUES, Thainara de Jesus; FREIRE, Antônio Carlos Pantoja. A eficácia da Lei Geral de Proteção de Dados Pessoais (LGPD) no combate aos crimes cibernéticos e na proteção da privacidade dos usuários. **Lumen et Virtus**, v. 17, n. 58, 2026. Disponível em: <https://periodicos.newsciencepubl.com/LEV/article/view/12726>. Acesso em: 20 ago. 2026.

SANTOS, Isabella Abrahão Rodrigues dos. Crimes cibernéticos: desafios e impactos na sociedade. **Aurum Revista Multidisciplinar**, 1(7), 129-138; 2024. Disponível em: <https://aurumpublicacoes.com/index.php/MA/article/view/446>. Acesso em: 17 ago. 2026.

SILVA, Adriano Fábio Cordeiro da et al. Crimes cibernéticos: limites e possibilidades do Direito Penal Digital. **Revista DCS**, v. 23, n. 86, 2026. Disponível em: Revista DCS – artigo completo. Acesso em: 17 ago. 2026.

22

STROPPIA, Tatiana; ROTHENBURG, Walter Claudius. A regulação de conteúdo nas redes sociais: uma breve análise comparativa entre o NetzDG e a solução brasileira. **Revista Direito GV**, São Paulo, v. 19, 2023. Disponível em: https://www.scielo.br/j/rdgv/a/qwwzmCyw5FmFQmTpRw3HCQh/?format=html&lang=pt&ilang=pt_BR. Acesso em: 20 ago. 2026.

TAVARES, André Ramos. **Direito digital e proteção de dados**. São Paulo: Saraiva, 2023.