

CRIMES CIBERNÉTICOS: ANÁLISE DA LEGISLAÇÃO ATUAL E A ADAPTAÇÃO DO SISTEMA PENAL ÀS NOVAS TECNOLOGIAS

CYBERCRIMES: ANALYSIS OF CURRENT LEGISLATION AND THE ADAPTATION OF THE CRIMINAL JUSTICE SYSTEM TO NEW TECHNOLOGIES

Laurah Zuíla Verçosa de Lima ¹
Williane Tibúrcio Facundes²

LIMA, Laurah Zuíla Verçosa de; FACUNDES, Williane Tibúrcio. **Crimes cibernéticos: análise da legislação atual e a adaptação do sistema penal às novas tecnologias.** 19 páginas. Trabalho de Conclusão de Curso de Graduação em Direito – Centro Universitário UNINORTE, Rio Branco. 2026.

RESUMO

O presente estudo analisa os crimes cibernéticos e a adaptação do sistema penal brasileiro frente às transformações tecnológicas contemporâneas, examinando os principais desafios jurídicos relacionados à criminalidade digital. Inicialmente, aborda-se o conceito e a tipologia dos crimes cibernéticos, destacando modalidades como invasão de dispositivos informáticos, fraudes eletrônicas, crimes contra a honra, cyberbullying e assédio virtual. Em seguida, o trabalho examina a evolução da legislação brasileira voltada ao combate desses delitos, com ênfase no Marco Civil da Internet (Lei nº 12.965/2014), na Lei Carolina Dieckmann (Lei nº 12.737/2012), na Lei Geral de Proteção de Dados (Lei nº 13.709/2018) e na Convenção de Budapeste sobre o Cibercrime. A pesquisa evidencia que, embora existam avanços normativos significativos, persistem lacunas legislativas, dificuldades de tipificação penal, limitações investigativas e desafios relacionados à cooperação internacional e à jurisdição em ambiente digital globalizado. O estudo também discute a necessidade de constante atualização do ordenamento jurídico diante do avanço de tecnologias como inteligência artificial e *deepfakes*, bem como a importância da capacitação técnica de profissionais do sistema de justiça e do fortalecimento de mecanismos de investigação digital. Conclui-se que o enfrentamento eficaz dos crimes cibernéticos exige atuação integrada entre legislação atualizada, investimentos tecnológicos, educação digital, especialização institucional e cooperação internacional, visando assegurar maior proteção aos direitos fundamentais no ambiente virtual e efetividade na persecução penal dos delitos digitais.

¹ Discente do 9º período do curso de bacharelado em Direito pelo Centro Universitário Uninorte.

² Docente do Centro Universitário Uninorte. Graduada em Direito pela U: VERSE. Especialista em Psicopedagogia pela Universidade Varzeagrandense e Direito Digital e Educação Especial e Inclusiva pela Faculdade Metropolitana. Graduada em Letras Vernáculas pela Universidade Federal do Acre-UFAC. Coordenadora do Núcleo de Acessibilidade e Apoio à Inclusão da UNINORTE.

Palavras-chave: crimes cibernéticos; direito digital; legislação penal; segurança da informação; tecnologia.

ABSTRACT

This study analyzes cybercrimes and the adaptation of the Brazilian criminal justice system to contemporary technological transformations, examining the main legal challenges related to digital criminality. Initially, it addresses the concept and typology of cybercrimes, highlighting modalities such as device invasion, electronic fraud, crimes against honor, cyberbullying, and virtual harassment. Subsequently, the paper examines the evolution of Brazilian legislation aimed at combating these offenses, with emphasis on the Brazilian Civil Rights Framework for the Internet (Marco Civil da Internet), the Carolina Dieckmann Law, the General Data Protection Law (LGPD), and the Budapest Convention on Cybercrime. The research demonstrates that, despite significant legislative advances, there are still legal gaps, difficulties in criminal classification, investigative limitations, and challenges related to international cooperation and jurisdiction in a globalized digital environment. The study also discusses the need for constant updating of the legal system in light of the advancement of technologies such as artificial intelligence and deepfakes, as well as the importance of technical training for justice system professionals and the strengthening of digital investigation mechanisms. It concludes that the effective fight against cybercrime requires integrated action involving updated legislation, technological investments, digital education, institutional specialization, and international cooperation in order to ensure greater protection of fundamental rights in the virtual environment and effectiveness in the criminal prosecution of digital offenses.

Keywords: cybercrime; digital law; criminal legislation; information security; technology.

INTRODUÇÃO

A crescente expansão das tecnologias digitais e o intenso avanço da internet transformaram significativamente as relações sociais, econômicas e jurídicas contemporâneas. A conectividade global, embora tenha proporcionado inúmeros benefícios à sociedade, também ampliou a incidência de práticas ilícitas realizadas no ambiente virtual, dando origem aos chamados crimes cibernéticos. Essas condutas abrangem diversas modalidades criminosas, como invasão de dispositivos informáticos, fraudes eletrônicas, crimes contra a honra, cyberbullying, vazamento de dados e ataques a sistemas digitais, atingindo diretamente direitos fundamentais relacionados à privacidade, segurança, honra e dignidade da pessoa humana.

Os crimes cibernéticos apresentam características próprias que dificultam sua repressão pelo Estado, especialmente em razão da rapidez das inovações

tecnológicas, da facilidade de anonimato proporcionada pela internet e da natureza transnacional dessas infrações. Nesse contexto, o sistema penal brasileiro passou a enfrentar importantes desafios quanto à adequação normativa, à produção de provas digitais e à efetividade da persecução penal diante de delitos cada vez mais sofisticados e complexos.

Com o objetivo de enfrentar essa nova realidade, o ordenamento jurídico brasileiro passou por relevantes transformações legislativas, destacando-se a promulgação da Lei nº 12.737/2012 (Lei Carolina Dieckmann), do Marco Civil da Internet (Lei nº 12.965/2014), da Lei Geral de Proteção de Dados Pessoais – LGPD (Lei nº 13.709/2018) e da adesão à Convenção de Budapeste sobre o Cibercrime. Tais instrumentos representam avanços importantes na proteção dos usuários e na responsabilização de agentes que praticam ilícitos no ambiente digital.

Diante desse cenário, o presente trabalho tem como objetivo analisar os crimes cibernéticos, examinando a legislação brasileira vigente e os principais desafios relacionados à adaptação do sistema penal às novas tecnologias. Busca-se compreender as limitações normativas existentes, as dificuldades investigativas e probatórias, bem como a necessidade de atualização constante das normas jurídicas, da capacitação dos profissionais do sistema de justiça e do fortalecimento da cooperação internacional no combate aos delitos digitais.

1 CONCEITO E TIPOLOGIA DE CRIMES CIBERNÉTICOS

1.1 DEFINIÇÃO DE CRIMES CIBERNÉTICOS

Crimes cibernéticos referem-se a atividades ilícitas cometidas no ambiente virtual, que abrangem uma vasta variedade de ações criminosas no meio digital, utilizando a internet e dispositivos eletrônicos.

No que tange à conceituação de crimes cibernéticos, pode-se citar Rosa (2002, p.53):

A conduta atenta contra o estado natural dos dados e recursos oferecidos por um sistema de processamento de dados, seja pela compilação, armazenamento ou transmissão de dados, na sua forma, compreendida pelos elementos que compõem um sistema de tratamento, transmissão ou armazenagem de dados, ou seja, ainda, na forma mais rudimentar; 2. O “Crime de Informática” é todo aquele procedimento que atenta contra os

dados, que faz na forma em que estejam armazenados, compilados, transmissíveis ou em transmissão; 3. Assim, o “Crime de Informática” pressupõe dois elementos indissolúveis: contra os dados que estejam preparados às operações do computador e, também, através do computador, utilizando-se software e hardware, para perpetrá-los; 4. A expressão crimes de informática, entendida como tal, é toda a ação típica, antijurídica e culpável, contra ou pela utilização de processamento automático e/ou eletrônico de dados ou sua transmissão; 5. Nos crimes de informática, a ação típica se realiza contra ou pela utilização de processamento automático de dados ou a sua transmissão. Ou seja, a utilização de um sistema de informática para atentar contra um bem ou interesse juridicamente protegido, pertence à ordem econômica, à integridade corporal, à liberdade individual, à privacidade, à honra, ao patrimônio público ou privado, à Administração Pública, etc.

Diferentemente dos crimes habituais, os cibercrimes transcendem fronteiras geográficas, podendo ser cometidos de forma praticamente anônima e causando grande impacto na sociedade, seja de forma financeira, psicológica, moral, ou relacionada à reputação e à privacidade dos indivíduos.

Segundo a Organização das Nações Unidas, os crimes cibernéticos configuram uma modalidade de crime transnacional em expansão, marcado por sua complexidade, ausência de fronteiras e crescente participação de organizações criminosas (UNODC, 2013).

Em todo o mundo, a legislação vem se aprimorando para combater os crimes cibernéticos. Como esses crimes estão em constante evolução, eles se tornam um desafio contínuo para a legislação e as práticas jurídicas.

No Brasil, a adaptação à realidade desses crimes se dá através da criação de leis específicas que tipificam condutas antes não previstas. Conforme a vasta evolução e o aprimoramento desses crimes, as leis também devem acompanhar a complexidade deles, para definir estratégias e combater essas infrações, a fim de garantir a segurança e proteger os direitos dos usuários das redes tecnológicas. A legislação não aborda somente a execução dos crimes, mas também as dificuldades investigativas e probatórias, como rastreamento, a coleta de provas e a necessidade de cooperação internacional para a persecução penal.

É imprescindível compreender que os crimes cibernéticos não se limitam apenas a ataques diretos a sistemas de computadores, abrangem vastas atividades ligadas ao uso da tecnologia, de várias formas, desde fraudes online até difamação nas redes sociais, golpes e crimes contra a honra e a dignidade do indivíduo.

Existe ainda uma classificação que divide os crimes cibernéticos em dois tipos: os Crimes Cibernéticos Próprios e os Crimes Cibernéticos Impróprios.

Nos Crimes Cibernéticos Próprios, a execução do crime acontece no meio virtual ou da informática, conforme esclarece Marco Túlio Viana (2003) em seu livro Fundamentos de direito Penal Informático, onde diz que “são aqueles em que o bem jurídico protegido pela norma penal é a inviolabilidade das informações automatizadas (dados).”

Já nos Crimes Cibernéticos Impróprios, são praticados por meio virtual, mas não dependem somente desse meio para a efetivação dos delitos.

1.2 PRINCIPAIS TIPOS DE CRIMES CIBERNÉTICOS

Os crimes cibernéticos, por abrangerem uma ampla variedade de ações ilegais que acontecem no mundo digital, resultam em uma diversidade de tipologias delitivas, cada qual com suas particularidades. Tal circunstâncias que impõe desafios substanciais à aplicação da lei e à persecução penal dessas atividades ilícitas praticadas no ambiente virtual. Compreender essas tipologias e suas particularidades é essencial para o desenvolvimento de estratégias de combate e prevenção. Neste trabalho, serão detalhados os principais tipos de crimes cibernéticos, em conformidade com a estrutura proposta.

1.2.1 *Hacking* e invasão de sistemas

Os termos *hacking* e invasão de sistemas referem-se à conduta de acessar, sem o devido conhecimento e autorização, sistemas computacionais, redes de dados e dispositivos eletrônicos. Entretanto, nem toda invasão de sistemas possui intenção maliciosa. Em muitos casos, o acesso é realizado por hackers éticos – profissionais que utilizam suas habilidades para identificar e corrigir vulnerabilidades, atuando preventivamente, em vez de explorá-las.

Podem ser motivados por diversas finalidades, sendo que as principais delas são a finalidade experimental ou demonstrativa, o que será caracterizado como *hacking* ético, este é realizado através do conhecimento e da autorização. E atos com intenção delituosa para a obtenção de informações sigilosas, manipulação de dados, interrupção de serviços ou a inserção de códigos maliciosos, como os denominados

ataques de *scareware*, que consistem em coagir a vítima para que ela faça o que o hacker desejar.

Em 2021, o Brasil foi alvo de um vazamento de dados que atingiu 223 milhões de indivíduos. Tal incidente gerou grande impacto social e jurídico significativo, pois a exposição dessas informações pode desencadear uma série de condutas ilícitas subsequentes.

1.2.2 Fraude on-line

A fraude on-line, também conhecida como fraude eletrônica, constitui uma das modalidades de cibercrime mais notórias, pois tem como finalidade primordial induzir vítimas a erro para a obtenção de vantagens ilícitas, geralmente de natureza financeira. Com o avanço tecnológico e a proliferação do comércio eletrônico e dos serviços bancários digitais, a incidência desse delito tem se expandido significativamente.

Visando coibir essa prática, a Lei nº 14.155, de 2021, promoveu alterações no Código Penal, inserindo a figura da Fraude Eletrônica, tipificada nos §§ 2º-A, 2º-B e 3º do artigo 171. Essa modalidade, também conhecida como Estelionato Digital, configura uma forma qualificada do crime de estelionato, o que justifica a aplicação de uma pena mais severa.

Dentre as formas mais comuns, destacam-se as fraudes em compras online. Com o crescimento do comércio digital, o índice dessa modalidade aumentou expressivamente, onde os golpistas criam lojas virtuais falsas ou oferecem produtos inexistentes ou fraudulentos. As vítimas, muitas vezes por falta de conhecimento técnico, acreditam estar comprando em sites confiáveis e, ao realizar o pagamento, consomem o golpe.

A Lei nº 14.155/2021 introduziu importantes inovações no Código Penal, notadamente ao agravar as penas para crimes de estelionato cometidos por meio eletrônico (art. 171, § 2º-A, CP). No âmbito jurisprudencial, tribunais têm consolidado o entendimento de que o estelionato digital não se distingue do estelionato tradicional em sua essência, mas revela um maior potencial lesivo devido ao alcance massivo da internet (STJ, HC 712.781/SP, 2022). De acordo com Nucci (2022), a fraude cibernética desafia os mecanismos tradicionais de persecução penal, exigindo o desenvolvimento de técnicas de investigação adaptadas às dinâmicas digitais.

1.2.3 Crimes contra a honra e a imagem

Com o avanço da tecnologia, o ambiente digital se consolidou como um campo fértil para o aumento dos crimes contra a honra e a imagem, um cenário intensificado pelo fácil e rápido alcance na disseminação das informações pela internet.

A proteção desses bens jurídicos é garantida no mais alto nível legal, conforme estabelece a Constituição Federal em seu Artigo 5º, onde diz que “são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;”. (Brasil, 1988)

Os crimes contra a honra, calúnia, difamação e injúria tornam-se ainda mais graves quando cometidos no meio digital. Essa majoração decorre da facilidade de acesso às redes sociais, que potencializa o impacto na vida da vítima devido ao elevado alcance e ao período duradouro em que a informação permanece online, além da inerente dificuldade na remoção do conteúdo.

Diferentemente da percepção popular, a internet não é terra sem lei. Embora a Constituição Federal garanta o direito de liberdade de expressão, os delitos cometidos nas redes podem acarretar responsabilização civil e criminal, configurando-se como mecanismos essenciais no combate aos crimes que atentam contra a honra e a imagem.

Um grande exemplo desse tipo de crime é o caso da atriz Carolina Dieckmann, ocorrido em 2012, quando um hacker invadiu seu e-mail e divulgou imagens íntimas na Internet, gerando-lhe danos significativos. Em resposta direta a esse evento, foi sancionada a Lei nº 12.737/2012, popularmente conhecida como Lei Carolina Dieckmann, que tipificou delitos informáticos no Código Penal.

Nesse sentido, a proteção e o combate eficazes aos crimes contra a honra e a imagem no ambiente digital exigem a conscientização ativa dos usuários das redes, bem como a rigorosa aplicação da legislação penal, a qual prevê o aumento das penas para esses delitos.

1.2.4 Cyberbullying e assédio virtual

O *cyberbullying* e o Assédio Virtual consistem em toda conduta de ofensa, hostilização ou ameaça dirigida a um indivíduo no ambiente digital. Embora apresente

mera semelhança com o *bullying* tradicional, o assédio on-line tende a ser mais danoso e maléfico para a vítima, uma vez que abrange diversos aspectos que potencializam o prejuízo moral e psicológico.

Nesse sentido, Pradas (2006) argumenta que, embora o *bullying* e o *cyberbullying* sejam substancialmente análogos, os danos infligidos às vítimas de assédio virtual são frequentemente mais graves. Isso ocorre porque a Internet assegura o anonimato do agressor, dificultando os mecanismos de resposta e proteção contra a humilhação. Além disso, o meio digital confere uma amplitude temporal e espacial acentuada ao ato discriminatório.

O assédio virtual e o *cyberbullying* manifestam-se de diversas maneiras e são, em sua maioria, praticados por jovens com fácil acesso às redes sociais. O sentimento de "conforto" ou impunidade para a prática desses atos reside, em parte, nas dificuldades investigativas e probatórias, o que contribui para a crescente incidência dessas condutas. Causando assim, consequências gravíssimas para as vítimas, as quais sofrem danos emocionais, físicos e moral, e, em casos extremos podem levar ao suicídio.

2 LEGISLAÇÃO BRASILEIRA SOBRE CRIMES CIBERNÉTICOS

2.1 MARCO CIVIL DA INTERNET (LEI Nº 12.965/2014)

Criada em 2014, o Marco Civil da Internet (MCI) estabeleceu os princípios, garantias, direitos e deveres essenciais para o uso da rede no país. Essa lei, considerada a "Constituição da Internet" brasileira, representa um marco na regulamentação digital, pois não existia legislação específica anterior para tratar do tema. Com isso, antes de 2014, a regulamentação do uso da internet era dependente apenas da aplicação e interpretação do artigo 5º da Constituição Federal.

Entre os pilares fundamentais do MCI, destacam-se a Neutralidade da Rede, que, conforme o artigo 3º, inciso IV, e detalhada no artigo 9º da Lei n.º 12.965/2014, obriga os provedores de conexão e de aplicação tratarem de forma igualitária quaisquer pacotes de dados que trafegam na rede. Isso significa que é vedada a discriminação ou o privilégio de qualquer conteúdo, aplicação ou serviço, garantindo aos usuários que o acesso à Internet será livre de bloqueios, filtragens ou limitações

arbitrárias impostas pelos provedores. O principal objetivo é garantir que as informações possam circular de forma livre e justa.

Outro pilar é a Responsabilidade dos Provedores, que estabelece um regime civil específico para provedores de aplicações de internet (como redes sociais, blogs e plataformas de vídeo). Conforme o MCI, o provedor não é responsável pelo conteúdo gerado por terceiros (usuários) em sua plataforma, visando proteger a liberdade de expressão. Contudo, essa irresponsabilidade cessa em casos específicos. O provedor só será responsabilizado se, após notificação judicial que determine a remoção do conteúdo ilícito, ele não tomar as providências necessárias. O objetivo desse mecanismo é, simultaneamente, garantir a liberdade de expressão e o direito à informação, e assegurar que o usuário que violar a lei seja o responsável primário pelo seu ato, evitando que as plataformas façam uma censura antecipada.

Por fim, a Guarda de Registros de Acesso é um dever fundamental estabelecido pelo MCI, sendo crucial para a identificação de usuários e a investigação de ilícitos na rede. Em que o artigo 13 do MCI impõe aos provedores de conexão à internet o dever de guardar e manter os registros de conexão sob sigilo, em ambiente controlado e seguro, pelo prazo de um ano.

Já o artigo 15, determina que os provedores de aplicação de Internet (como redes sociais e e-mails) também devem armazenar os respectivos registros de acesso, observando as mesmas exigências de sigilo e segurança, contudo, no prazo de seis meses.

Posto isso, a Lei n.º 12.965/2014 possui limitações e lacunas no que se refere à tipificação penal de crimes virtuais, atuando predominantemente em caráter regulatório e de proteção de direitos, em vez de punitivo. Desse modo, o Marco Civil da Internet atua como um instrumento complementar à legislação penal vigente, fornecendo os dados e o devido respaldo para a responsabilização dos agentes.

Conforme a doutrina, a natureza abrangente do MCI é destacada:

A lei do Marco Civil foi criada para suprir as lacunas no sistema jurídico em relação aos crimes virtuais, num primeiro momento tratando dos fundamentos, conceitos para sua interpretação e objetivos que o norteiam, além de enumerar os direitos dos usuários, tratar de assuntos polêmicos como por exemplo a solicitação de histórico de registros, a atuação do poder público perante os crimes virtuais e por último garante o exercício do direito do cidadão de usufruir da internet de modo individual e coletivo estando devidamente protegido. (Siqueira *et al.*, 2017, p. 126)

Maia (2017) afirma que o Marco Civil se assenta em três pilares essenciais, a garantia da neutralidade da rede, proteção à privacidade do usuário da Internet e a Garantia da liberdade de expressão.

2.2 LEI CAROLINA DIECKMANN (LEI Nº 12.737/2012)

A Lei n.º 12.737/2012 foi a pioneira no Direito Penal brasileiro ao promover a tipificação das condutas relativas a crimes cibernéticos. Popularmente conhecida como Lei Carolina Dieckmann, em decorrência do caso emblemático ocorrido em 2012, no qual a atriz Carolina Dieckmann teve seu dispositivo informático ilicitamente invadido por hackers que, após o acesso indevido, chantagearam mediante a exigência da quantia de R\$ 10.000,00 (dez mil reais) para que não fossem divulgadas suas imagens de íntimas. Tal evento gerou uma grande repercussão nacional e inegáveis danos à sua vida pessoal.

Portanto, a Lei n.º 12.737/2012 promoveu substanciais alterações no Código Penal (Decreto-Lei n.º 2.848/40), visando à inclusão e à modificação de dispositivos relevantes aos crimes cibernéticos. Dentre os dispositivos incluídos, destaca-se o artigo 154-A, que introduziu a tipificação penal da Invasão de dispositivo informático:

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 3 (três) meses a 1 (um) ano, e multa. (Brasil, 1940)

Assim, os novos dispositivos inseridos, criminalizou especificamente a conduta de invasão de dispositivos informáticos, conferindo tutela penal a bens jurídicos que, até então, careciam de proteção adequada no ordenamento.

Portanto, a promulgação da Lei n.º 12.737/2012 representou um avanço fundamental no âmbito jurídico, ao criminalizar condutas digitais ilícitas que, precedentemente, careciam de tipificação penal específica. A norma estabeleceu um alicerce legal para a repressão dos delitos cibernéticos, promovendo o reforço da tutela da privacidade e intimidade dos usuários no ambiente digital. Consequentemente, a lei conferiu maior eficácia ao combate e à repressão da

disseminação não autorizada de dados e informações confidenciais, atuando nas áreas de prevenção e punição.

Não obstante a inclusão das novas tipificações penais, o ordenamento jurídico ainda padece de lacunas e enfrenta desafios inerentes à matéria. O Direito Penal Digital, por sua natureza dinâmica, é constantemente desafiado a enfrentar o vertiginoso ritmo de avanço tecnológico e o surgimento contínuo de novas modalidades de crimes cibernéticos.

Tal contexto impõe a necessidade premente de revisão e atualização legislativa regular. Nesse diapasão, a Lei n.º 12.737/2012 tornou-se um alicerce indispensável à compreensão do tema que possibilitou a edição de futuras e importantes normativas sobre a temática.

2.3 LEI GERAL DE PROTEÇÃO DE DADOS (LGPD) E SUAS IMPLICAÇÕES

A Lei Geral de Proteção de Dados Pessoais (LGPD) foi instituída a fim de assegurar a privacidade e a proteção dos dados pessoais dos cidadãos brasileiros, estabelecendo diretrizes e parâmetros para empresas e órgãos públicos quanto à forma de coletar, armazenar, processar e compartilhar tais informações.

De acordo com o artigo 1º da Lei nº 13.709, de 14 de agosto de 2018, a norma é aplicável a toda e qualquer atividade de tratamento de dados pessoais, realizada por pessoa natural ou jurídica, de direito público ou privado, independentemente do meio utilizado. O referido dispositivo legal dispõe que:

Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. (Brasil, 2018)

A abrangência prevista no artigo 1º da LGPD é de extrema relevância, pois demonstra o caráter universal e transversal da norma, alcançando tanto o setor público quanto o privado, e incidindo sobre quaisquer operações que envolvam dados pessoais. Essa amplitude é essencial diante do crescente cenário de intensa digitalização e o aumento da incidência de crimes cibernéticos, nos quais o tratamento indevido de informações pessoais figura como um dos principais vetores de violação de direitos.

Conforme explica Doneda (2021), a LGPD representa um avanço fundamental

na consolidação de uma cultura de proteção de dados no Brasil, uma vez que “integra a privacidade à noção de dignidade da pessoa humana e ao núcleo dos direitos fundamentais”. Assim, o tratamento de dados pessoais passa a ser condicionado a princípios éticos e jurídicos que visam garantir a transparência, a segurança e a responsabilidade dos agentes que os manipulam.

Nesse sentido, a LGPD se firmou como um marco normativo essencial no ordenamento jurídico brasileiro, estabelecendo bases legais para a responsabilização de agentes que manipulam dados de forma irregular. A legislação atua não apenas como um mecanismo regulatório, mas também como instrumento de prevenção e repressão de condutas ilícitas relacionadas aos crimes cibernéticos, especialmente aquelas que envolvem o uso indevido de informações pessoais.

Dessa forma, a LGPD contribui diretamente para o enfrentamento dos crimes cibernéticos, ao promover maior segurança jurídica e transparência nas relações digitais, além de fortalecer a cultura de proteção de dados e o respeito à privacidade como expressão dos direitos fundamentais do cidadão na era digital.

2.4 OUTRAS LEGISLAÇÕES PERTINENTES

A Convenção de Budapeste sobre o Cibercrime, promulgada no Brasil por meio do Decreto nº 11.491, de 2023, representa um marco histórico na luta contra os crimes cibernéticos. Seu principal objetivo é promover a cooperação internacional na prevenção, investigação e repressão de delitos praticados no ambiente virtual, assegurando que os responsáveis por tais infrações sejam identificados e punidos, mesmo quando as condutas são cometidas a partir de diferentes países.

A relevância da Convenção de Budapeste reside no fato de que os crimes cibernéticos, por sua própria natureza transnacional, transcendem as fronteiras territoriais, o que dificulta a atuação isolada dos Estados. Assim, a cooperação jurídica internacional torna-se essencial para viabilizar o rastreamento de provas digitais, a identificação de autores e a responsabilização penal efetiva.

Nesse sentido, André Furquim destaca a importância da adesão do Brasil à Convenção:

Considerando que as investigações operadas no Brasil demandam, cada vez mais, provas eletrônicas que se encontram em outros países, esta Convenção irá facilitar e, portanto, encorajar os investigadores brasileiros a

utilizar tal estratégia. (Furquim, 2023).

A recente Lei nº 15.211, de 17 de setembro de 2025, popularmente conhecida como Estatuto Digital da Criança e do Adolescente (ECA Digital), representa um importante avanço normativo na proteção de menores em ambientes digitais. A norma foi elaborada com o escopo de assegurar que crianças e adolescentes tenham seus direitos fundamentais preservados no uso de tecnologias e plataformas on-line, complementando o Estatuto da Criança e do Adolescente (Lei nº 8.069/1990) e a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018).

O ECA Digital estabelece obrigações específicas para provedores, plataformas, redes sociais, jogos eletrônicos e demais serviços digitais, exigindo a implementação de mecanismos de verificação de idade, supervisão familiar ou parental, bem como medidas preventivas contra conteúdos nocivos e práticas que possam comprometer o desenvolvimento físico, emocional e psicológico de crianças e adolescentes.

A legislação também impõe restrições à publicidade e à monetização de conteúdos direcionados a menores de idade, além de determinar que as empresas adotem padrões elevados de segurança e proteção de dados, em conformidade com os princípios da privacidade desde a concepção (*privacy by design*).

Outro ponto de destaque é que a lei amplia o conceito de “acesso provável por crianças e adolescentes”, alcançando qualquer serviço digital que possa ser utilizado por esse público, ainda que não seja voltado especificamente a ele. Assim, o ECA Digital reforça a responsabilidade das plataformas em adotar medidas que reduzam riscos de exposição e assegurem o uso ético e seguro do ambiente virtual.

Por fim, o Decreto nº 11.491/2023 atribui à Autoridade Nacional de Proteção de Dados (ANPD) a função de regulamentar e fiscalizar a aplicação dessa lei, promovendo a integração entre as políticas de proteção de dados e os direitos da infância e juventude.

Dessa forma, o ECA Digital consolida-se como um instrumento jurídico essencial para a promoção de um ambiente digital mais seguro, ético e responsável, reafirmando o compromisso do Estado brasileiro com a proteção integral da criança e do adolescente na era da informação.

3 DESAFIOS DA LEGISLAÇÃO ATUAL

3.1 LACUNAS E AMBIGUIDADES NA LEGISLAÇÃO

Com o grande avanço da tecnologia e o aumento do uso das redes digitais, as condutas criminosas nesse ambiente também evoluíram, sendo necessário que o Código Penal brasileiro passe por constantes atualizações, de modo a contemplar os novos tipos penais relacionados a essas inovações tecnológicas. Como destacam Lopes e Lopes (2023), as normativas vigentes ainda não conseguem abarcar toda a gama de crimes que podem ser praticados no ambiente virtual, resultando em lacunas significativas no ordenamento jurídico brasileiro.

Entretanto, ainda existem diversas dificuldades quanto à aplicação da legislação em crimes cibernéticos. Por se tratar de delitos que podem ser praticados de qualquer lugar do mundo simultaneamente, surge um desafio quanto à efetividade da lei brasileira na punição dos autores. Mesmo com a adesão à Convenção de Budapeste, a cooperação internacional continua a enfrentar barreiras comunicacionais, burocráticas e jurisdicionais, dificultando a investigação e a responsabilização penal desses crimes.

Outra questão que apresenta grandes desafios é o anonimato que a internet pode proporcionar aos criminosos, por meio do uso de VPNs, rede TOR e outros recursos que dificultam a rastreabilidade. Portanto, tais condutas exigem que as autoridades desenvolvam ferramentas e técnicas digitais avançadas, capazes de identificar, localizar e responsabilizar os infratores, garantindo maior efetividade na aplicação da lei em ambientes virtuais.

3.2 DIFICULDADES NA TIPIIFICAÇÃO PENAL DE CRIMES CIBERNÉTICOS

É notório que ainda há grande dificuldade na tipificação penal dos crimes cibernéticos. Apesar das importantes leis recentemente criadas, a legislação ainda carece de dispositivos específicos capazes de abarcar a totalidade das condutas ilícitas praticadas no ambiente virtual. A complexidade na aplicação das normas em casos cibernéticos transcende as barreiras tradicionais do Direito Penal, uma vez que o crescimento exponencial da Internet e das tecnologias digitais tem desafiado continuamente o ordenamento jurídico brasileiro a adaptar-se a novos paradigmas (Lopes e Lopes, 2023).

No que tange às dificuldades práticas, uma das maiores inquietações reside na

efetivação da instrução probatória em ações penais relacionadas a crimes virtuais. A natureza intangível e volátil dos dados digitais, aliada à falta de capacitação técnica, frequentemente limita a atuação do Judiciário. Não raro, evidências cruciais se perdem ou tornam-se inacessíveis antes que possam ser adequadamente coletadas e analisadas (Santana, 2021).

As “deepfakes” representam um exemplo claro dessa problemática, pois, diante da ausência clara de tipificação penal específica para as deepfakes, o ordenamento jurídico brasileiro recorre à aplicação de normas já existentes, especialmente voltadas à proteção da honra, da imagem e da dignidade sexual. No que tange à essas tipificações, Siqueira (2019) aponta que:

A legislação brasileira não criminaliza especificamente o “deep fake”. Contudo, os intérpretes têm buscado amparo em tipos penais abertos descritos na Lei n.º 12.735/2012 (Lei Azeredo), Lei n.º 12.737/2012 (Lei Carolina Dieckmann), Lei n.º 12.965/2014 (Marco Civil da Internet), Lei n.º 13.718/2018, Lei n.º 13.709/2018 (Lei Geral de Proteção de Dados Pessoais) e Lei n.º 13.853/2019. Além disso, aplicam-se dispositivos previstos na Lei de Crimes Financeiros (Lei n.º 7.492/1986), Lei de Falências (Lei n.º 11.101/2005), Código Eleitoral (Lei n.º 4.737/1965) e, principalmente, nos crimes contra a honra (arts. 138 a 145 do Código Penal) e contra a dignidade sexual (arts. 213 a 235 do Código Penal).

Esta tecnologia de inteligência artificial simula de maneira extremamente realista a voz e a imagem de outras pessoas. O uso criminoso dessas ferramentas, como a imitação de voz para cometer fraudes financeiras ou a manipulação de vídeos íntimos com a substituição sem autorização, sublinha a dificuldade de aplicar as leis penais existentes. O sistema legal é, assim, desafiado a desenvolver soluções para lidar com as ações criminosas que se tornam progressivamente mais complexas e tecnologicamente avançadas.

Outro desafio significativo refere-se ao Princípio da Legalidade, que estabelece que não há crime sem lei anterior que o defina, nem pena sem prévia cominação legal. Tal princípio implica que toda conduta criminosa deve estar expressamente prevista em lei. Entretanto, sua aplicação aos crimes cibernéticos gera um dilema considerável para os legisladores, devido à constante e rápida evolução da tecnologia. Surge, então, a questão: como criar normas capazes de abranger condutas futuras e imprevisíveis? Trata-se de um desafio crítico, que exige conciliar a necessidade de tipificação clara e precisa com o velocíssimo avanço tecnológico, sem comprometer os direitos e garantias fundamentais.

3.3 JURISDIÇÃO E APLICAÇÃO DA LEI EM UM AMBIENTE GLOBALIZADO

No contexto da globalização digital, as compras online em plataformas internacionais, como a *Shein*, exemplificam os desafios jurídicos relacionados à jurisdição e à aplicação da lei. Essas transações frequentemente envolvem consumidores em um país e fornecedores em outro, gerando questões sobre qual legislação deve ser aplicada em caso de litígios.

Ainda que o direito brasileiro adote a teoria da ubiquidade (art. 6º do Código Penal) para determinar o lugar do crime, permitindo a persecução penal no local da ação ou do resultado, a execução da sanção e a obtenção de provas eletrônicas dependem de mecanismos de cooperação jurídica internacional.

Consequentemente, a Convenção de Budapeste, internalizada pelo Decreto n.º 11.491/2023, emerge como instrumento jurídico essencial para mitigar a disparidade entre a territorialidade da lei e a transnacionalidade da conduta delitiva. O avanço da tecnologia exige, portanto, que a soberania nacional se adapte a uma realidade em que a aplicação da lei depende da efetivação de cartas rogatórias e de um intercâmbio probatório célere entre os Estados.

4 ADAPTAÇÃO DO SISTEMA PENAL ÀS NOVAS TECNOLOGIAS

4.1 CAPACITAÇÃO DE PROFISSIONAIS DO SISTEMA DE JUSTIÇA

A capacitação do Judiciário é essencial para garantir decisões jurídicas fundamentadas, precisas e eficazes, assegurando julgamentos com pleno conhecimento técnico sobre as matérias analisadas. Jêior (2019) destaca a importância da educação e da conscientização como medidas preventivas contra o crime cibernético, argumentando que as leis, por si só, são insuficientes para lidar com a complexidade do problema.

Nesse sentido, Pinheiro (2021), em sua obra *Direito Digital*, enfatiza a relevância da capacitação contínua de agentes públicos e privados, bem como do desenvolvimento de estruturas organizacionais adequadas, capazes de lidar com a complexidade e o volume crescente de delitos digitais. A ausência de conhecimento técnico e de recursos especializados pode comprometer significativamente a eficácia

da atuação das autoridades e a resolução dos casos.

Diante disso, torna-se fundamental a criação de programas de capacitação, bem como de varas, promotorias e delegacias especializadas em crimes cibernéticos, dotadas de profissionais treinados e capacitados para enfrentar a alta complexidade dos casos e o rápido aumento e evolução dos delitos digitais.

4.2 FERRAMENTAS TECNOLÓGICAS E INVESTIGAÇÕES CIBERNÉTICAS

Para garantir decisões justas e coerentes, é fundamental o investimento em perícia forense digital, munida de recursos tecnológicos avançados, como análise de malwares e outras técnicas especializadas. Esses recursos visam assegurar a integralidade, coleta e análise de provas digitais, garantindo sua aceitabilidade e respaldo em juízo.

As ferramentas forenses digitais são essenciais para rastrear atividades maliciosas, recuperar dados perdidos ou ocultos e identificar os autores de condutas ilícitas no ambiente digital. Nesse contexto, a capacitação técnica dos profissionais da área, aliada à disponibilidade de recursos adequados, desempenha um papel crucial na investigação, permitindo analisar, preservar e coletar provas eletrônicas de forma que sua validade jurídica seja plenamente reconhecida.

4.3 COLABORAÇÃO INTERNACIONAL NO COMBATE AOS CRIMES CIBERNÉTICOS

Com a crescente globalização e a natureza transnacional dos crimes cibernéticos, impõe-se a necessidade clara de cooperação internacional. Não existem fronteiras para essas condutas, permitindo que os criminosos atuem de qualquer lugar do mundo, atingindo diversas vítimas em diferentes países, o que torna essencial o apoio internacional para a efetividade jurídica.

Nesse sentido, é fundamental estabelecer acordos e tratados internacionais que visem combater e prevenir os crimes cibernéticos entre as nações. Sem esses instrumentos, seria praticamente impossível conduzir investigações que permitam localizar, identificar e coletar provas contra os autores de delitos digitais.

A Convenção de Budapeste, promulgada pelo Decreto nº 11.491/2023, representa um marco na cooperação internacional no enfrentamento dos crimes

cibernéticos. Ela busca harmonizar as legislações nacionais sobre crimes digitais, aprimorar técnicas de investigação e ampliar a colaboração entre os Estados-membros.

Apesar da importância dessa colaboração, a soberania de cada Estado representa um desafio relevante. As diferenças nas legislações e nas jurisdições podem gerar conflitos significativos, sendo necessário criar mecanismos que permitam a cooperação internacional sem infringir a autonomia jurídica dos Estados envolvidos.

4.4 DECISÕES JUDICIAIS RELEVANTES E SUAS REPERCUSSÕES

A constante evolução dos crimes cibernéticos tem desafiado o Judiciário no que tange à interpretação e aplicação da legislação, bem como na adaptação dos entendimentos a esse novo ambiente digital. O enfrentamento dessas condutas exige da jurisprudência brasileira um constante exercício de atualização e adaptação do Código Penal, do Código de Processo Penal e das leis específicas sobre crimes digitais à realidade virtual contemporânea.

Nesse contexto, os Tribunais Superiores, como o STJ e o STF, têm proferido decisões emblemáticas que orientam e moldam a interpretação e a aplicação das normas relativas aos crimes digitais, contribuindo para a construção de precedentes consistentes e para o fortalecimento da segurança jurídica nesse campo.

Uma decisão relevante do STJ é o julgamento do Agravo Regimental no Recurso em *Habeas Corpus* nº 92.801, em que a Quinta Turma considerou ilícita a prova obtida diretamente dos dados armazenados no celular do acusado, sem prévia autorização judicial. No caso, policiais acessaram mensagens de texto e conversas por meio de aplicativos como o *WhatsApp* durante a prisão em flagrante, sem autorização judicial. A decisão reafirma a necessidade de respeitar os direitos fundamentais e a inviolabilidade das comunicações, conforme previsto no artigo 5º, inciso XII, da Constituição Federal.

Outra decisão relevante é o Recurso Especial nº 1.125.661/DF, em que a Primeira Turma do STJ aplicou a Lei nº 12.737/2012 (Lei Carolina Dieckmann) para tipificar a invasão de dispositivo informático alheio, mesmo sem a comprovação de prejuízo material. No caso, o réu acessou o computador da vítima sem autorização para obter informações pessoais. A decisão destaca que a tipificação penal independe da demonstração de dano efetivo, bastando a violação do dispositivo e a obtenção de

dados sem consentimento, conforme previsto no artigo 154-A do Código Penal, introduzido pela referida lei.

4.5 TENDÊNCIAS NA APLICAÇÃO DA LEGISLAÇÃO

Diante da alta complexidade e da constante evolução dos crimes cibernéticos, a mera aplicação da legislação existente, ainda que adequada, não é suficiente para garantir segurança e justiça no ambiente digital. Torna-se, portanto, essencial que o conjunto normativo seja continuamente atualizado, incorporando inovações tecnológicas e contemplando novas modalidades de ataques e condutas ilícitas.

A tendência observada é a adaptação dinâmica das normas, aliada ao aperfeiçoamento da jurisprudência, de modo a proporcionar respostas mais rápidas, eficazes e coerentes frente às mudanças constantes do ciberespaço. Nesse contexto, o combate eficiente aos crimes digitais exige a integração entre legislação atualizada, capacitação profissional, ferramentas tecnológicas e cooperação internacional.

4.6 SUGESTÕES PARA A ATUALIZAÇÃO E FORTALECIMENTO DA LEGISLAÇÃO

Diante da crescente sofisticação dos crimes cibernéticos e da rápida evolução tecnológica, é imperativo que o ordenamento jurídico brasileiro se adapte para garantir a eficácia na prevenção, investigação e punição dessas infrações. A seguir, apresentam-se propostas para a atualização e fortalecimento da legislação vigente.

A Criação de uma Lei Geral de Crimes Cibernéticos, embora a Lei nº 12.737/2012 (Lei Carolina Dieckmann) tenha sido um marco na tipificação de crimes informáticos, ela não abrange todas as condutas ilícitas no ambiente digital. A elaboração de uma legislação específica e abrangente permitiria a tipificação clara de diversas práticas criminosas, como ataques a sistemas críticos, fraudes digitais e crimes envolvendo inteligência artificial. A proposta do Projeto de Lei nº 4.658/2024, que visa aumentar as penas para crimes cometidos com o uso da internet, é um exemplo de iniciativa nesse sentido.

Ademais, o aprimoramento da Lei de Proteção de Dados Pessoais (LGPD) (Lei nº 13.709/2018) estabelece diretrizes para o tratamento de dados pessoais, mas sua aplicação enfrenta desafios, especialmente em relação à fiscalização e à punição de infrações. É essencial fortalecer os mecanismos de fiscalização e estabelecer sanções

mais rigorosas para empresas que não cumprirem as normas de proteção de dados, garantindo maior segurança para os cidadãos no ambiente digital.

Além disso, o fortalecimento da Cooperação Internacional, seria uma sugestão, visto que os crimes cibernéticos frequentemente transcendem fronteiras nacionais, dificultando a investigação e a punição dos responsáveis. O Brasil já é signatário da Convenção de Budapeste sobre Cibercrime, mas é necessário intensificar a cooperação internacional por meio de acordos bilaterais e multilaterais, facilitando a troca de informações e a execução de investigações conjuntas.

A implementação de Mecanismos de Responsabilização para Plataformas Digitais, pois as plataformas digitais desempenham um papel central na disseminação de conteúdos ilícitos. É necessário estabelecer normas que responsabilizem essas plataformas por conteúdos prejudiciais, como notícias falsas e discursos de ódio, incentivando-as a adotar medidas eficazes de moderação e prevenção.

A Promoção da Educação Digital e Conscientização Pública, pois a prevenção de crimes cibernéticos também passa pela educação da população. Campanhas de conscientização sobre segurança digital, privacidade e direitos no ambiente online são essenciais para reduzir a vulnerabilidade dos cidadãos e promover uma cultura de responsabilidade digital.

CONSIDERAÇÕES FINAIS

O avanço das tecnologias digitais e a crescente utilização da internet transformaram profundamente as relações sociais, econômicas e jurídicas, criando novas possibilidades de interação, mas também ampliando significativamente a incidência de crimes praticados no ambiente virtual. Os crimes cibernéticos, em razão de sua natureza dinâmica, transnacional e tecnológica, representam um dos maiores desafios contemporâneos para o Direito Penal e para o sistema de justiça brasileiro.

Ao longo deste estudo, verificou-se que o ordenamento jurídico brasileiro passou por importantes avanços legislativos voltados ao enfrentamento dessas condutas, destacando-se a Lei Carolina Dieckmann, o Marco Civil da Internet, a Lei Geral de Proteção de Dados e a adesão à Convenção de Budapeste. Tais instrumentos contribuíram para o fortalecimento da proteção jurídica no ambiente digital, ampliando mecanismos de responsabilização e assegurando maior proteção

aos direitos fundamentais dos usuários da internet.

Entretanto, constatou-se que a legislação ainda apresenta lacunas significativas diante da rápida evolução tecnológica e do surgimento constante de novas modalidades criminosas, como fraudes digitais sofisticadas e o uso indevido de inteligência artificial e *deepfakes*. Além disso, permanecem desafios relacionados à tipificação penal adequada, à obtenção e preservação de provas digitais, à limitação técnica das autoridades responsáveis pelas investigações e às dificuldades de cooperação internacional.

Dessa forma, conclui-se que o enfrentamento eficaz dos crimes cibernéticos exige uma atuação integrada entre atualização legislativa, fortalecimento institucional, investimentos em tecnologia forense, capacitação contínua dos profissionais do sistema de justiça e ampliação da cooperação jurídica internacional. Também se mostra indispensável a promoção da educação digital e da conscientização social, visando prevenir práticas ilícitas e garantir maior segurança no ambiente virtual. Assim, somente por meio de medidas conjuntas e permanentemente atualizadas será possível assegurar a efetividade do sistema penal diante das constantes transformações tecnológicas da sociedade contemporânea.

REFERÊNCIAS

ALEXANDRE, Brenda Cristina; ARAÚJO, Julianna Martins; RABELO, Cesar Leandro de Almeida. A evolução dos crimes cibernéticos e os desafios da legislação brasileira. **Revista FT** Ciências Humanas, v. 27, ed. 128, nov. 2023. DOI: 10.5281/zenodo.10223548. Disponível em: <https://revistaft.com.br/a-evolucao-dos-crimes-ciberneticos-e-os-desafios-da-legislacao-brasileira/>. Acesso em: 26 set. 2025.

AGÊNCIA NACIONAL DE PROTEÇÃO DE DADOS (ANPD). **ECA Digital e as competências da ANPD**. Brasília, 2025. Disponível em: <https://www.gov.br/anpd>. Acesso em: 6 out. 2025.

AURUM. **O que é Marco Civil da Internet? Conheça os princípios**. Disponível em: <https://www.aurum.com.br/blog/marco-civil-da-internet/>. Acesso em: 25 set. 2025.

BRASIL. Constituição (1988). Constituição da República Federativa do Brasil de 1988. Brasília, DF: Presidência da República, 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 18 set. 2025.

BRASIL. Decreto nº 11.491, de 20 de junho de 2023. Promulga a Convenção sobre o Cibercrime, celebrada em Budapeste, em 23 de novembro de 2001. Diário Oficial da

União, Brasília, DF, 21 jun. 2023.

BRASIL. Decreto-Lei nº 2.848, de 7 de dezembro de 1940. Código Penal. Rio de Janeiro, RJ: Presidência da República, 1940. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 18 set. 2025.

BRASIL. Lei nº 12.737, de 30 de novembro de 2012. Dispõe sobre a tipificação de crimes informáticos e dá outras providências. Diário Oficial da União, Brasília, DF, 1 dez. 2012. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 6 out. 2025.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Marco Civil da Internet. **Diário Oficial da União**, Brasília, DF, 24 abr. 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 29 set. 2025.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). **Diário Oficial da União**, Brasília, DF, 15 ago. 2018.

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. Diário Oficial da União, Brasília, DF, 28 maio 2021.

BRASIL. Lei nº 14.811, de 12 de janeiro de 2024. Dispõe sobre a proteção de crianças e adolescentes em ambientes digitais. **Diário Oficial da União**, Brasília, DF, 15 jan. 2024. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2024/lei/l14811.htm. Acesso em: 29 set. 2025.

BRASIL. Lei nº 15.211, de 17 de setembro de 2025. Dispõe sobre a proteção de crianças e adolescentes em ambientes digitais e altera a Lei nº 8.069, de 13 de julho de 1990 (Estatuto da Criança e do Adolescente). **Diário Oficial da União**, Brasília, DF, 18 set. 2025.

BRASIL. Ministério da Justiça e Segurança Pública. Convenção de Budapeste é promulgada no Brasil. Brasília, 17 abr. 2023. Disponível em: <https://www.gov.br/mj/pt-br/assuntos/noticias/convencao-de-budapeste-e-promulgada-no-brasil>. Acesso em: 14 out. 2025.

BRASIL. Superior Tribunal de Justiça. **Agravo Regimental no Recurso em Habeas Corpus nº 92.801**. Relatora: Min. Maria Thereza de Assis Moura. Julgamento em: 17 jun. 2018. Disponível em: https://www.stj.jus.br/sites/portaltsp/Paginas/Comunicacao/Noticias-antigas/2018/2018-06-17_06-57_Crimes-pela-internet-novos-desafios-para-a-jurisprudencia.aspx. Acesso em: 6 out. 2025.

BRASIL. Superior Tribunal de Justiça. **Recurso Especial nº 1.125.661/DF**. Relatora: Min. Maria Thereza de Assis Moura. Julgamento em: 27 mar. 2012. Disponível em: https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias-antigas/2012/2012-03-27_06-57_Crimes-informaticos-e-a-jurisprudencia-do-STJ.aspx. Acesso em: 6 out. 2025.

CÂMARA DOS DEPUTADOS. **Projeto de Lei nº 4.658/2024**. Disponível em: <https://www.camara.leg.br/propostas-legislativas/4658/2024>. Acesso em: 6 out. 2025.

DONEDA, Danilo. **Lei Geral de Proteção de Dados Pessoais**: comentada. 2. ed. São Paulo: Thomson Reuters Brasil, 2021.

FURQUIM, André. **Convenção de Budapeste e a cooperação internacional no combate ao cibercrime**. Brasília: Ministério da Justiça e Segurança Pública, 2023. Disponível em: <https://www.gov.br/mj/pt-br/assuntos/noticias/convencao-de-budapeste-e-promulgada-no-brasil>. Acesso em: 6 out. 2025.

GROPKSREUTZ, H. R. Os crimes cibernéticos e o princípio da legalidade. **Revista Brasileira de Ciências Criminais**, 2024. Disponível em: <https://publicacoes.ibccrim.org.br/index.php/RBCCRIM/article/view/86>. Acesso em: 29 set. 2025.

JÚNIOR, Júlio César Alexandre. Cibercrime: um estudo acerca do conceito de crimes informáticos. **Revista Eletrônica da Faculdade de Direito de Franca**, Franca, v. 14, n. 1, jul. 2019. Disponível em: <https://revista.direitofranca.br/index.php/refdf/article/view/602>. Acesso em: 14 out. 2025.

LOPES, Marciano Pereira; LOPES, José Augusto Bezerra. Crimes virtuais no ordenamento jurídico brasileiro. **Revista Ibero-Americana de Humanidades, Ciências e Educação**, São Paulo, v. 9, n. 8, p. 462-472, ago. 2023. Disponível em: <https://periodicorease.pro.br/rease/article/view/10850>. Acesso em: 14 out. 2025.

MAIA, Maurício Reis. O Marco Civil da Internet: fundamentos, princípios e desafios à sua efetivação. **Revista de Direito, Governança e Novas Tecnologias**, v. 3, n. 1, p. 45-63, 2017.

NUCCI, Guilherme de Souza. **Crimes cibernéticos**: comentários à Lei 12.737/2012 e à Lei 12.965/2014 (Marco Civil da Internet). 2. ed. Rio de Janeiro: Forense, 2022.

PINHEIRO, Patrícia Peck. **Direito digital**. 7. ed. São Paulo: Saraiva Educação, 2021.

PRADAS, Pedro. **Cyberbullying**: o assédio moral virtual e suas consequências jurídicas e sociais. São Paulo: Atlas, 2006.

ROSA, José de Faria Costa. **Crimes de informática**. Curitiba: Juruá, 2002.

SANTANA, Roque Felipe da Silva. **Crimes cibernéticos**: análise evolutiva da

legislação penal brasileira e seus desafios. 2021. 24 f. Trabalho de Conclusão de Curso (Graduação em Direito) — Universidade Católica do Salvador, Salvador, 2021. Disponível em: <https://ri.ucsal.br/items/eacce13d-1953-456e-af9a-28ae647dd351>. Acesso em: 25 set. 2025.

SIQUEIRA, Dirceu Pereira; SILVA, Fernanda Caroline da; SANTOS, Andreza Cristina dos. **Marco Civil da Internet**: uma análise sob a ótica dos direitos fundamentais. In: SIQUEIRA, Dirceu Pereira (org.). *Direito, tecnologia e sociedade: reflexões interdisciplinares*. Birigui: Boreal, 2017. p. 117-132.

SIQUEIRA, P. A. R. de. **O “deep fake” e a legislação brasileira**: utilização de instrumentos legais para a proteção à imagem. *Conteúdo Jurídico*, 2019. Disponível em: <https://www.conteudojuridico.com.br/consulta/artigo/53256/o-deep-fake-e-a-legislao-brasileira-utilizao-de-instrumentos-legais-para-a-proteo-imagem>. Acesso em: 6 maio 2026.

UNITED NATIONS OFFICE ON DRUGS AND CRIME (UNODC). **Comprehensive Study on Cybercrime**. Viena: United Nations, 2013. Disponível em: https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf. Acesso em: 25 set. 2025.

VIANA, Marco Túlio. **Fundamentos de Direito Penal Informático**. Belo Horizonte: Mandamentos, 2003.

ARTIGO 07

CRIMES CONTRA DIGNIDADE SEXUAL DE MENORES: ANÁLISE DO CRIME DE PORNOGRAFIA INFANTIL NO CASO DO RECURSO ESPECIAL N.º 1.899.266/SC

Mariana Ferreira Miranda

Arthur Braga de Souza