UNIVERSIDADE FEDERAL DE MATO GROSSO DO SUL CURSO DE DIREITO - CPTL

ANDERSON MAIRLON CALDAS ALVES

A EVOLUÇÃO DOS CRIMES DIGITAIS E OS DESAFIOS PARA SUA CONTENÇÃO NO CENÁRIO ATUAL

TRÊS LAGOAS,

MS 2025

ANDERSON MAIRLON CALDAS ALVES

A EVOLUÇÃO DOS CRIMES DIGITAIS E OS DESAFIOS PARA SUA CONTENÇÃO NO CENÁRIO ATUAL

Trabalho de Conclusão de Curso apresentado ao Curso de Graduação em Direito do Campus de Três Lagoas da Universidade Federal de Mato Grosso do Sul, como requisito parcial para obtenção do grau de Bacharel em Direito, sob a orientação da Professora Doutora Heloisa Helena de Almeida Portugal.

TRÊS LAGOAS,

MS 2025

ANDERSON MAIRLON CALDAS ALVES

A EVOLUÇÃO DOS CRIMES DIGITAIS E OS DESAFIOS PARA SUA CONTENÇÃO NO CENÁRIO ATUAL

Este Trabalho de Conclusão de Curso foi avaliado e julgado aprovado em sua forma final, como requisito parcial para obtenção do grau de Bacharel em Direito, perante Banca Examinadora constituída pelo Colegiado do Curso de Graduação em Direito do Campus de Três Lagoas da Universidade Federal de Mato Grosso do Sul, composta pelos seguintes membros:

Professora Doutora Heloisa Helena de Almeida Portugal

UFMS/CPTL - Orientadora

Professora Doutora Josilene Hernandes Ortolan Di Pietro

UFMS/CPTL - Membro

Professor Doutor Carolina Ellwanger

UFMS/CPTL - Membro

RESUMO

O presente artigo analisa o impacto do avanço tecnológico e da expansão da internet, ressaltando que, embora essa evolução tenha proporcionado grandes benefícios à sociedade, também originou novos desafios, como o aumento dos crimes digitais. O estudo aborda o conceito e a classificação dos crimes virtuais, identificando seus sujeitos ativo e passivo, bem como os principais delitos praticados no ambiente digital. Além disso, discute as dificuldades enfrentadas pelo legislador diante da rápida transformação tecnológica e a importância da atualização constante das normas jurídicas. Por fim, analisa o papel da Inteligência Artificial (IA) tanto como ferramenta utilizada na prática criminosa quanto como instrumento de prevenção e combate aos crimes virtuais, destacando a necessidade de equilíbrio entre inovação tecnológica e segurança jurídica.

Palavras-chave: Crimes digitais. Internet. Inteligência Artificial. Legislação.

ABSTRACT

This article analyzes the impact of technological advancement and the expansion of the internet, emphasizing that although this evolution has brought great benefits to society, it has also generated new challenges, such as the increase in digital crimes. The study addresses the concept and classification of cybercrimes, identifying their active and passive subjects, as well as the main offenses committed in the digital environment. Furthermore, it discusses the difficulties faced by legislators due to the rapid pace of technological change and the importance of constantly updating legal norms. Finally, it examines the role of Artificial Intelligence (AI) both as a tool used in criminal activities and as an instrument for preventing and combating cybercrimes, highlighting the need to balance technological innovation and legal security.

Keywords: Cybercrimes. Internet. Artificial Intelligence. Legislation.

SUMÁRIO

1. **INTRODUÇÃO**

É notório que o surgimento da internet representou um avanço significativo para a humanidade. Graças a essa tecnologia, hoje desfrutamos de recursos e possibilidades que seriam inimagináveis há cinquenta anos, transformando profundamente a forma como nos comunicamos, trabalhamos e acessamos informações. No entanto, junto com esses benefícios, surgiram também novos desafios, entre eles o aumento e a diversidade dos crimes digitais, que se tornaram uma preocupação constante para a sociedade contemporânea.

O presente artigo aborda temas relevantes relacionados aos desafios e às formas de combate aos crimes virtuais, fenômeno que vem crescendo de maneira acelerada em razão do avanço tecnológico e da expansão da internet. A era digital trouxe inúmeros benefícios para a sociedade, mas também possibilitou o surgimento de novas modalidades de condutas ilícitas, exigindo do Estado e da legislação respostas rápidas e eficazes para a proteção de direitos e garantias fundamentais.

Serão discutidos ao longo deste trabalho o conceito de crime digital, suas principais classificações, bem como a identificação dos sujeitos ativo e passivo dessas práticas criminosas. Também serão analisados os delitos mais recorrentes no ambiente virtual, a forma como estão tipificados na legislação brasileira e os desafios enfrentados pelo legislador diante da constante evolução tecnológica, que frequentemente antecipa a criação de novas leis.

Por fim, será examinado o papel da Inteligência Artificial (IA) nesse contexto, tanto como ferramenta utilizada na prática de crimes digitais quanto como instrumento de prevenção e combate a essas infrações. O objetivo é promover uma reflexão crítica sobre a importância da atualização das normas penais e do desenvolvimento de políticas públicas voltadas à segurança digital, buscando equilibrar inovação tecnológica e proteção jurídica no ambiente virtual.

2. **DESENVOLVIMENTO**

2.1 SURGIMENTO DA INTERNET

O surgimento da Internet constitui um dos maiores marcos tecnológicos da história moderna, transformando a maneira como a sociedade se comunica, trabalha e compartilha informações. Segundo Castells (2016, p. 42), “a Internet não é apenas uma tecnologia, mas uma estrutura social de comunicação que redefine os processos de produção, poder e experiência”.

Costa (1997) aponta que a necessidade de registro e comunicação remonta às origens da humanidade: "Desde a época primitiva, o homem tenta de algum modo comunicar-se ou transmitir informações de sua existência para gerações futuras, através de hieróglifos gravados em tábuas de pedras e mapas de batalhas."

A origem da Internet remonta à década de 1960, durante o período da Guerra Fria, quando o Departamento de Defesa dos Estados Unidos criou a ARPANET (*Advanced Research Projects Agency Network*), com o objetivo de garantir a comunicação entre centros de pesquisa, mesmo em situações de conflito (UNITED STATES DEPARTMENT OF DEFENSE, 1983). Essa rede inicial permitia o envio de informações entre computadores distantes e serviu de base para o desenvolvimento da rede global que conhecemos atualmente.

De acordo com Lévy (1999, p. 17), “a cibercultura emergiu como o novo espaço de comunicação, sociabilidade e inteligência coletiva”. Assim, o avanço tecnológico proporcionado pela Internet não apenas revolucionou o acesso ao conhecimento, mas também criou uma nova forma de interação social, em que o tempo e o espaço foram significativamente reduzidos.

A popularização da Internet ocorreu a partir dos anos 1990, com o surgimento da World Wide Web, criada por Tim Berners-Lee, o que permitiu a criação de páginas virtuais e o acesso público à rede (LÉVY, 1999). No Brasil, esse processo de expansão foi impulsionado por instituições acadêmicas e governamentais, consolidando-se por meio do Comitê Gestor da Internet no Brasil (CGI.br), que até hoje coordena as políticas de governança da rede no país (CGI.br, 2025).

Entretanto, como observa Castells (2016), a mesma tecnologia que trouxe inovação e conectividade também abriu espaço para novos tipos de ameaças, como o aumento de crimes digitais, exigindo do Estado e das instituições jurídicas uma adaptação constante às novas formas de criminalidade virtual.

2.2 CONCEITO DE CRIMES DIGITAIS

Segundo Costa (1997), o avanço da tecnologia é notável, pois "Abstraindo-se tal ilação, devemos nos render a realidade: estamos nos informatizando em velocidade acima do que até se pode notar, ou seja, muito rapidamente."

Os crimes digitais, também conhecidos como crimes cibernéticos ou cibercrimes, correspondem às atividades ilícitas praticadas por indivíduos ou grupos que utilizam a Internet e dispositivos eletrônicos como meio para cometer infrações penais. De acordo com Costa

(2021, p. 47), “os crimes digitais são condutas criminosas que se valem das tecnologias de informação e comunicação para violar direitos, causar danos ou obter vantagens ilícitas”. Essas práticas ocorrem no ambiente virtual, denominado ciberespaço, um espaço imaterial onde circulam informações, dados pessoais e comunicações de todo o mundo.

Os criminosos digitais utilizam equipamentos como computadores, celulares, tablets e redes de comunicação para executar diversas ações ilícitas, que vão desde fraudes financeiros e invasão de sistemas até a disseminação de conteúdos falsos e ataques a instituições públicas. Como observa Silva (2020, p. 83), “a facilidade de acesso à internet e o anonimato proporcionado pelas redes ampliaram o alcance e a complexidade das práticas criminosas virtuais”.

Esses delitos representam um grande desafio para o Direito e para os órgãos de segurança pública, pois ultrapassam fronteiras geográficas e exigem constante atualização legislativa e tecnológica para garantir a efetiva punição dos responsáveis.

Atividades criminosas virtuais (ou cibercrime) são aquelas executadas por meio de tecnologias de informação e comunicação. Elas representam um espectro amplo de delitos que se manifestam no espaço cibernético, variando de ataques diretos à infraestrutura de sistemas e invasão de dados confidenciais a esquemas de fraude eletrônica, distribuição de vírus (*malware*) e outras táticas, como o *phishing*.

2.2.1 CLASSIFICAÇÃO DOS CRIMES DIGITAIS

A compreensão das diferentes formas de crimes virtuais é essencial para o estudo da criminalidade contemporânea, já que a tecnologia alterou profundamente o modo como as infrações são cometidas. Conforme Ferreira Filho e Torres (2024), a classificação dos crimes digitais é necessária para delimitar o alcance da legislação penal diante das novas modalidades de condutas ilícitas que surgiram com o avanço da Internet. Esses autores destacam que a doutrina jurídica tem buscado diferenciar as diversas naturezas dos delitos cibernéticos, considerando o papel desempenhado pelos meios tecnológicos na prática criminosa.

De acordo com Almeida e Oliveira (2022), os crimes virtuais podem ser classificados em crimes próprios (ou puros) e crimes impróprios (ou impuros). Os crimes próprios são aqueles cuja prática só é possível por meio de dispositivos tecnológicos ou sistemas informáticos, como invasão de dados e disseminação de vírus. Já os crimes impróprios são infrações tradicionais — como estelionato, calúnia e difamação — que passaram a ser cometidas também no ambiente digital. Os autores destacam que, embora existam leis específicas, como a Lei nº 12.737/2012 (Lei Carolina Dieckmann), ainda há lacunas na legislação, o que dificulta a aplicação penal diante da complexidade do ciberespaço.

Além dessa divisão, a doutrina também propõe classificações mais amplas. Para Fiorillo (2013), os crimes cibernéticos podem ser classificados em exclusivamente virtuais, mistos e comuns. Os crimes exclusivamente virtuais ocorrem apenas no meio digital, como o ataque a sistemas e a manipulação de dados eletrônicos. Os crimes mistos são aqueles em que o uso da tecnologia é um meio essencial para atingir o resultado ilícito, ainda que o bem jurídico violado não seja de natureza informática. Já os crimes virtuais comuns referem-se às condutas tradicionais, nas quais a Internet é utilizada apenas como ferramenta auxiliar, e não como elemento indispensável do crime.

> *Os crimes cibernéticos englobam todas as ações ilícitas praticadas por meio de sistemas digitais ou direcionadas contra eles, podendo ser classificados em três grandes grupos: (a) crimes contra a confidencialidade, integridade e disponibilidade de sistemas e dados informáticos, como invasões e disseminação de vírus; (b) crimes cometidos através da internet, em que o meio digital é utilizado para viabilizar práticas já conhecidas, como fraudes, extorsões e ofensas; e (c) crimes cujo objeto é o próprio conteúdo ilícito difundido em redes digitais, a exemplo da pornografia infantil, do discurso de ódio e da violação de direitos autorais. Essa classificação busca harmonizar as definições internacionais e facilitar a cooperação entre países no combate ao cibercrime." (NAÇÕES UNIDAS, 2020, p. 12).*

2.2.2 SUJEITO ATIVO

De acordo com Zacarias e Freire (2023), o sujeito ativo dos crimes virtuais é aquele que pratica a conduta ilícita utilizando-se de recursos tecnológicos e conhecimento especializado em informática. Em geral, esses agentes possuem habilidades técnicas que lhes permitem manipular sistemas, invadir redes e obter informações de forma indevida. No entanto, os autores destacam que o perfil do criminoso digital é diversificado, abrangendo desde indivíduos com alta qualificação técnica até usuários comuns que utilizam a internet para cometer fraudes, ofensas ou disseminar conteúdo ilícito.

Os criminosos virtuais atuam explorando as fragilidades dos sistemas tecnológicos e o anonimato proporcionado pelo ambiente digital, o que torna sua identificação um grande desafio para as autoridades. Conforme informações da Rádio Câmara (2015), esses agentes utilizam técnicas sofisticadas para invadir redes, obter dados pessoais e financeiros, disseminar programas maliciosos e praticar fraudes de diversas naturezas. Diferentemente da criminalidade

tradicional, o cibercrime não exige a presença física do infrator, permitindo que ele atue de qualquer parte do mundo, o que dificulta a delimitação da jurisdição e a efetividade da punição. Além disso, os criminosos virtuais costumam empregar mecanismos de ocultação de identidade e de criptografia, tornando a rastreabilidade das ações extremamente complexa. Esse cenário evidencia a necessidade de cooperação internacional, de aprimoramento das políticas de segurança digital e de constante atualização tecnológica por parte do Estado.

2.2.3 SUJEITO PASSIVO

Um dos principais fatores que contribuem para o sucesso das ações criminosas no ambiente digital é o desconhecimento dos usuários sobre os riscos aos quais estão expostos ao navegar na internet. Muitos internautas, em busca de entretenimento gratuito, acabam acessando sites piratas para assistir a filmes ou baixar conteúdo diversos, sem perceber o perigo envolvido nessa prática. Ao clicar em links suspeitos ou realizar downloads ilegais, o usuário pode instalar vírus, malwares ou programas espiões em seu dispositivo, comprometendo seus dados pessoais, senhas e até informações bancárias. Essas atitudes aparentemente inofensivas podem resultar em grandes prejuízos financeiros e de privacidade, evidenciando a importância da conscientização e da adoção de medidas básicas de segurança digital.

Conforme Zacarias e Freire (2023), o sujeito passivo dos crimes virtuais é aquele que sofre os efeitos da ação ilícita praticada no ambiente digital, sendo o titular do bem jurídico lesado. A vítima pode ser tanto uma pessoa física quanto uma pessoa jurídica, dependendo da natureza do delito. Em muitos casos, trata-se de indivíduos que têm seus dados pessoais, informações financeiras ou identidade digital violados. Os autores ressaltam ainda que, no contexto das redes sociais, o sujeito passivo pode ser alvo de ataques à honra, à imagem e à privacidade, o que amplia o alcance e a gravidade do dano causado pelos crimes cibernéticos.

Existem diversas formas de defesa contra os crimes virtuais, que podem ser classificadas em defesa técnica, preventiva, comportamental e educativa.

Na defesa técnica, de acordo com a Kaspersky (2025), uma das principais maneiras de o sujeito passivo se proteger é manter os sistemas e softwares de segurança constantemente atualizados, incluindo antivírus, firewalls e programas de detecção de ameaças. A atualização frequente impede que invasores explorem falhas conhecidas e reduz significativamente as chances de infecção por malwares ou ataques de ransomware.

Já na defesa preventiva, a Kaspersky (2025) enfatiza que a prevenção é o meio mais eficaz de proteção digital, recomendando o uso de senhas fortes e únicas, a autenticação em dois fatores e a verificação criteriosa de links e anexos recebidos por e-mail ou redes sociais. Essas práticas ajudam a evitar o roubo de credenciais e o acesso indevido a contas pessoais ou corporativas.

Por fim, segundo orienta a Kaspersky (2025), a educação digital e o comportamento consciente dos usuários são essenciais para reduzir o risco de se tornar vítima de crimes virtuais. É fundamental desconfiar de ofertas falsas, verificar a autenticidade de sites antes de fornecer informações pessoais e realizar cópias de segurança periódicas (backups), a fim de minimizar possíveis prejuízos em caso de ataques cibernéticos

2.2.4 PRINCIPAIS CRIMES VIRTUAIS E SUAS DIFICULDADES EM COMBATÊ-LOS

Os crimes virtuais têm crescido de forma expressiva nas últimas décadas, acompanhando a expansão da internet e o avanço das tecnologias digitais. Entre os delitos mais comuns estão o estelionato eletrônico, o furto de dados bancários, a invasão de dispositivos informáticos, o sequestro de informações (ransomware), a difamação e calúnia em redes sociais, além da disseminação de conteúdos ilícitos, como a pornografia infantil e os chamados *deepfakes*.

2.2.4.1 PEDOFILIA

A pedofilia é um dos crimes mais abomináveis e repudiados pela sociedade, por colocar em risco a integridade física, psicológica e emocional de crianças e adolescentes, podendo causar traumas que perduram por toda a vida. No ambiente virtual, esse tipo de delito adquire proporções ainda mais preocupantes, uma vez que as imagens e vídeos compartilhados na internet podem nunca ser completamente apagados, perpetuando o sofrimento das vítimas e dificultando o controle estatal sobre o conteúdo ilícito.

De acordo com Almeida (2021), a pedofilia virtual representa uma das formas mais graves de crimes cibernéticos, pois explora a vulnerabilidade de menores em espaços digitais. O autor destaca que a facilidade de acesso à internet e o anonimato oferecido pelas plataformas online favorecem o aliciamento, a exploração sexual e a disseminação de material pornográfico envolvendo crianças e adolescentes, o que exige uma atuação firme e coordenada do Estado, bem como a constante atualização das leis de proteção à infância e à juventude.

A Constituição Federal de 1988, em seu artigo 227, determina que é dever da família, da sociedade e do Estado assegurar, com absoluta prioridade, os direitos da criança e do adolescente, garantindo-lhes proteção contra qualquer forma de negligência, discriminação, exploração, violência e opressão. O Estatuto da Criança e do Adolescente (Lei nº 8.069/1990) reforça essa proteção ao tipificar, em seu artigo 241-A, como crime a produção, reprodução, direção, transmissão ou armazenamento de material pornográfico envolvendo menores de idade. Dessa forma, a legislação brasileira busca assegurar que o avanço tecnológico não se torne instrumento de violação dos direitos fundamentais das crianças e adolescentes, mas sim um meio de fortalecimento da proteção e da dignidade humana.

Segundo a Câmara dos Deputados (2025), o uso indevido de imagens de crianças e adolescentes nas redes sociais e em conteúdos gerados por inteligência artificial tem motivado a criação de diversos projetos de lei voltados à proteção da infância no ambiente digital, evidenciando a preocupação do legislativo com os riscos da exposição infantil e a necessidade de mecanismos mais eficazes de controle e responsabilização.

"Ao todo, 32 projetos de lei em análise na Câmara dos Deputados tratam da proteção de crianças e adolescentes contra o uso indevido de suas imagens em ambientes digitais, especialmente em conteúdos criados com inteligência artificial." (CÂMARA DOS DEPUTADOS, 2025).

Ainda em relação à dificuldade do legislador em acompanhar o ritmo acelerado das transformações tecnológicas e sociais, observa-se que a adultização de crianças em ambientes digitais já era uma realidade há bastante tempo, mas somente ganhou destaque após a denúncia pública feita pelo influenciador digital Felca. O episódio expôs a vulnerabilidade de crianças e adolescentes diante da exposição precoce e inadequada nas redes sociais, revelando a morosidade do processo legislativo em responder a problemas urgentes da era digital.

De acordo com o Senado Federal (2025), a denúncia serviu de impulso para a tramitação e aprovação do Projeto de Lei nº 2.628/2022, que busca proteger crianças e adolescentes contra a exploração de sua imagem e comportamento em plataformas digitais. Essa situação demonstra que, muitas vezes, o poder legislativo apenas reage após a ocorrência de fatos de grande repercussão, evidenciando os desafios enfrentados pelo Estado em criar normas preventivas que acompanhem a velocidade da evolução tecnológica e os impactos sociais decorrentes da cultura digital.

2.2.4.2 INVASÃO DE PRIVACIDADE

De acordo com Cavalheiro (2023), a invasão de privacidade digital caracteriza-se pelo acesso, divulgação ou compartilhamento de dados pessoais, imagens, vídeos e outras informações privadas sem o consentimento do titular, violando direitos fundamentais assegurados pela Constituição Federal, como a intimidade e a vida privada. O autor explica que esse tipo de crime ocorre de diversas formas, desde o acesso indevido a dispositivos eletrônicos e contas em redes sociais até a divulgação não autorizada de conteúdos pessoais. Em muitos casos, as vítimas sofrem graves consequências emocionais, sociais e financeiras, especialmente porque o material exposto na internet pode se perpetuar indefinidamente. Cavalheiro (2023) ressalta ainda que o combate à invasão de privacidade requer tanto o aprimoramento das medidas de segurança digital quanto o fortalecimento da legislação penal e civil, a fim de responsabilizar os infratores e garantir a proteção da dignidade humana no ambiente virtual.

2.2.4.3 CRIME CONTRA A HONRA

Atualmente, os crimes contra a honra estão cada vez mais em evidência, especialmente em razão da ampla expansão das redes sociais e da facilidade de disseminação de informações no ambiente digital. Muitos usuários utilizam esses espaços para propagar ofensas, calúnias, difamações e notícias falsas (*fake news*), o que atinge diretamente a reputação e a dignidade das vítimas. Diante dessa realidade, o Poder Público tem buscado mecanismos legais e regulatórios para responsabilizar as plataformas digitais pela circulação de conteúdos ilícitos, com o objetivo de conter a propagação de discursos de ódio e proteger os direitos da personalidade no ambiente virtual.

Contudo, essa tentativa de regulação suscita um relevante debate jurídico e ético, pois envolve um possível conflito entre princípios constitucionais fundamentais, como o direito à honra, à imagem e à dignidade da pessoa humana, e a liberdade de expressão e de comunicação. De acordo com a Constituição Federal de 1988, em seu artigo 5º, incisos IV, IX e X, é assegurado a todos o direito de livre manifestação do pensamento e de expressão, ao mesmo tempo em que se garante a inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas (BRASIL, 1988). Assim, o grande desafio contemporâneo consiste em equilibrar a proteção da honra e da reputação com a preservação da liberdade de expressão, evitando que o combate aos crimes virtuais se converta em censura e garantindo um ambiente digital mais ético e responsável.

Além disso, Soares (2016) destaca que a anonimidade proporcionada pelas redes sociais e o uso de perfis falsos dificultam a identificação e responsabilização dos agressores, criando um ambiente de impunidade que incentiva a repetição dessas condutas ilícitas. O autor defende que o ordenamento jurídico brasileiro deve evoluir para garantir uma aplicação mais efetiva das normas penais e maior cooperação entre plataformas digitais e autoridades públicas, de forma a proteger a honra e a dignidade das pessoas também no espaço virtual, em conformidade com os princípios previstos na Constituição Federal.

2.2.4.4 ESTELIONATO

Diferentemente de outros delitos cibernéticos, o estelionato digital possui finalidade estritamente patrimonial, ou seja, busca a obtenção de vantagem econômica ilícita mediante fraude virtual. O número de ocorrências relacionadas a esse tipo de crime é incalculável, uma vez que novas modalidades surgem constantemente, acompanhando a evolução das tecnologias e das formas de interação on-line. O ambiente virtual, pela sua amplitude e anonimato, favorece a atuação de golpistas e dificulta a identificação dos autores, o que exige métodos de investigação mais eficazes e políticas públicas voltadas ao fortalecimento da segurança digital e da educação cibernética.

De acordo com o Senado Federal (2025), os casos de estelionato por meio eletrônico cresceram cerca de 17% em 2024, totalizando aproximadamente 281 mil registros, o que evidencia o aumento da vulnerabilidade dos consumidores diante das fraudes digitais e a necessidade de medidas legislativas mais enérgicas para o setor.

Um dos principais fatores que contribuem para o êxito dos crimes virtuais é a falsa ilusão de ganho fácil difundida nas redes sociais e em plataformas digitais. Muitos usuários são atraídos por promessas de lucros rápidos e rendimentos elevados, sem perceber que estão sendo vítimas de golpes estruturados e fraudes disfarçadas de investimentos. Nesse contexto, os chamados “jogos de azar virtuais” e aplicativos de apostas, como o popularmente conhecido “Tigrinho”, podem ser analisados sob a ótica do estelionato digital, uma vez que exploram a vulnerabilidade e a ganância dos usuários para obter vantagens ilícitas.

Entretanto, o legislador ainda enfrenta dificuldades em regulamentar esse tipo de prática, especialmente por envolver grandes empresas e plataformas internacionais que operam fora do território nacional. A ausência de legislação específica e de mecanismos eficazes de fiscalização favorece a continuidade dessas atividades, que geram prejuízos significativos a milhares de pessoas. Assim, torna-se urgente o aperfeiçoamento das leis e o fortalecimento das

ações de prevenção e educação digital, a fim de proteger os consumidores e coibir a exploração financeira no ambiente virtual.

2.3 LEIS EM USO

A Lei nº 12.965/2014, conhecida como Marco Civil da Internet, é o principal marco regulatório do uso da rede no Brasil e estabelece os princípios, garantias, direitos e deveres para o uso da internet. Essa norma consagra o acesso à internet como um direito fundamental, essencial ao exercício da cidadania e à liberdade de expressão, conforme previsto na Constituição Federal de 1988, que assegura, em seu artigo 5º, o direito à comunicação, à privacidade e à informação (BRASIL, 1988). O artigo 1º da referida lei dispõe que:

"Esta Lei estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil e determina as diretrizes para atuação da União, dos Estados, do Distrito Federal e dos Municípios em relação à matéria." (BRASIL, 2014).

Desse modo, o Marco Civil da Internet consolida a liberdade de expressão, a proteção da privacidade e a preservação da neutralidade da rede como fundamentos essenciais para o uso democrático da internet no país, garantindo a todos os brasileiros o direito de acesso e de comunicação em ambiente digital seguro e livre.

2.4 DIFICULDADE EM LEGISLAR NOVOS CRIMES

Vale ressaltar que os crimes digitais evoluem com grande rapidez, acompanhando o avanço das tecnologias da informação e da comunicação. Essa constante transformação faz com que o legislador encontre dificuldades em prever as novas condutas ilícitas que podem surgir, o que torna mais complexa a criação de leis preventivas capazes de combater tais práticas antes mesmo de sua ocorrência. Um exemplo emblemático dessa situação foi o caso da atriz Carolina Dieckmann, cuja invasão de dados pessoais e divulgação de imagens privadas motivou a criação da Lei nº 12.737/2012, conhecida como Lei Carolina Dieckmann. Essa legislação alterou o Código Penal para incluir o artigo 154-A, que dispõe:

"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." (BRASIL, 2012).

Essa norma representou um marco jurídico na tipificação dos crimes informáticos, estabelecendo punições para invasões de dispositivos e fortalecendo a proteção dos dados pessoais no ambiente digital.

2.5 USO DAS IAS EM CRIMES DIGITAIS

O desenvolvimento da Inteligência Artificial (IA) teve início na década de 1950, quando pesquisadores como Alan Turing propuseram a ideia de que máquinas poderiam simular o raciocínio humano. Desde então, a área evoluiu significativamente, passando por períodos de estagnação e grandes avanços com o surgimento do aprendizado de máquina e das redes neurais. Atualmente, a IA está presente em diversos setores, impactando a economia, a educação e a segurança digital (RUSSELL; NORVIG, 2022).

Como visto na notícia publicada pela Câmara dos Deputados (2025), foi aprovada uma campanha nacional de conscientização e prevenção voltada ao combate dos crimes digitais cometidos com o uso de inteligência artificial. A proposta busca envolver escolas, órgãos públicos e a sociedade civil em ações educativas, com o objetivo de orientar principalmente crianças, adolescentes e pessoas com deficiência sobre os riscos do ambiente virtual e o uso ético das novas tecnologias. Além disso, a iniciativa pretende fortalecer a cooperação entre o governo e as instituições de ensino, promovendo uma cultura de segurança digital e de combate à desinformação.

A recente atualização legislativa reforça o combate à violência de gênero no ambiente digital. De acordo com a Câmara dos Deputados (2025), foi sancionada a lei que agrava as penas para casos de violência psicológica contra a mulher praticados com o uso de inteligência artificial. A norma “prevê aumento de pena quando o agressor utilizar recursos tecnológicos que alterem imagem, voz ou criem conteúdo falso com o objetivo de causar danos emocionais ou morais à vítima” (BRASIL, 2025). Essa medida representa um avanço na proteção da dignidade feminina diante dos novos riscos trazidos pela era digital.

De acordo com notícia divulgada pela Câmara dos Deputados (2025), a Comissão de Defesa do Consumidor aprovou um projeto que agrava as penas para crimes contra a honra — como calúnia, difamação e injúria — quando cometidos com o uso de inteligência artificial. A proposta altera o Decreto-Lei nº 2.848/1940 (Código Penal), acrescentando aumento de pena nos casos em que a tecnologia seja utilizada para criar, manipular ou divulgar conteúdos falsos com a intenção de ofender a reputação de alguém. A medida busca adequar a legislação à

realidade digital, reconhecendo que o uso da IA amplia o alcance e o impacto das ofensas, tornando-as mais graves e de difícil reparação (BRASIL, 2025).

Conforme a reportagem publicada pela BBC News Brasil (2024), o avanço da inteligência artificial generativa tem possibilitado que criminosos utilizem ferramentas tecnológicas para clonar rostos, vozes e comportamentos humanos, criando vídeos e áudios falsos extremamente realistas. Essa prática, conhecida como deepfake, vem sendo empregada em golpes virtuais e fraudes de identidade, nos quais as vítimas acreditam estar se comunicando com familiares, colegas de trabalho ou representantes de instituições financeiras. A matéria destaca que esses conteúdos falsificados são produzidos com base em amostras disponíveis na internet, como vídeos, áudios e postagens em redes sociais, o que amplia a vulnerabilidade das pessoas expostas digitalmente. Esse tipo de crime evidencia os riscos da falta de regulamentação e da necessidade urgente de políticas públicas voltadas à proteção de dados, à segurança digital e ao uso ético da inteligência artificial, uma vez que o impacto emocional e financeiro sobre as vítimas pode ser devastador.

3. **CONSIDERAÇÕES FINAIS**

Diante da análise apresentada, é possível afirmar que o avanço tecnológico, embora tenha proporcionado inúmeros benefícios à humanidade, também trouxe consigo desafios complexos relacionados à segurança digital e à prática de crimes virtuais. O crescimento

exponencial da internet e das novas ferramentas tecnológicas criou um ambiente fértil para o surgimento de condutas ilícitas que exigem respostas rápidas e eficazes do Estado e da sociedade.

Constatou-se que os crimes digitais assumem diversas formas — desde fraudes financeiras até invasões de sistemas e violações de dados pessoais —, afetando diretamente a vida cotidiana dos cidadãos e a estabilidade das instituições. O estudo evidenciou ainda que a legislação brasileira, embora tenha evoluído com leis como a Lei Carolina Dieckmann, o Marco Civil da Internet e a Lei Geral de Proteção de Dados (LGPD), ainda enfrenta o desafio de acompanhar a velocidade das transformações tecnológicas. Essa defasagem normativa dificulta a responsabilização dos criminosos e a proteção efetiva dos direitos fundamentais no ambiente virtual.

Por fim, conclui-se que o combate aos crimes virtuais requer uma abordagem multidisciplinar, envolvendo não apenas a atualização constante das normas jurídicas, mas

também investimentos em educação digital, cooperação internacional e uso ético da Inteligência Artificial. A IA, quando utilizada de forma responsável, pode ser uma poderosa aliada na prevenção, detecção e investigação de delitos cibernéticos, contribuindo para um espaço digital mais seguro e equilibrado. Assim, o grande desafio do século XXI consiste em harmonizar inovação tecnológica e segurança jurídica, garantindo que o progresso digital continue servindo ao desenvolvimento humano e à preservação da dignidade e da liberdade individual.

REFERÊNCIAS FINAIS

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, São Paulo, v. 8, n. 11, p. 277–294, nov. 2022. ISSN 2675-3375. DOI: 10.51891/rease.v8i11.7554.

BBC NEWS BRASIL. 'Eram meu rosto e minha voz, mas era golpe': como criminosos 'clonam pessoas' com inteligência artificial. São José do Rio Preto (SP), 28 fev. 2024. Disponível em: https://www.bbc.com/portuguese/articles/cd1jv45dq3go. Acesso em: 26 out. 2025.

BRASIL. Câmara dos Deputados. Comissão aprova campanha contra crimes digitais com uso de inteligência artificial. Brasília, DF: Agência Câmara de Notícias, 16 out. 2025. Disponível em: https://www.camara.leg.br/noticias/1203930-comissao-aprova-campanha-contra-crimes-digitais-com-uso-de-inteligencia-artificial/. Acesso em: 19 out. 2025.

BRASIL. Câmara dos Deputados. Comissão aprova penas maiores para crimes contra a honra cometidos com uso de IA. Brasília, DF: Agência Câmara de Notícias, 23 jul. 2025. Disponível em: https://www.camara.leg.br/noticias/1179250-comissao-aprova-penas-maiores-para-crimes-contra-a-honra-cometidos-com-uso-de-ia/. Acesso em: 20 out. 2025.

BRASIL. Câmara dos Deputados. Rádio Câmara. Cibercrime: como agem os bandidos virtuais. Brasília, DF: Câmara dos Deputados, 29 jun. 2015. Disponível em: https://www.camara.leg.br/radio/programas/365667-cibercrime-como-agem-os-bandidos-virtuais/. Acesso em: 20 out. 2025.

BRASIL. Câmara dos Deputados. Sancionada lei que agrava pena em crime de violência contra a mulher com uso de IA. Brasília, DF: Agência Câmara de Notícias, 25 abr. 2025. Disponível em: https://www.camara.leg.br/noticias/1153179-sancionada-lei-que-agrava-pena-em-crime-de-violencia-contra-a-mulher-com-uso-de-ia/. Acesso em: 20 out. 2025.

BRASIL. Lei nº 8.069, de 13 de julho de 1990. Dispõe sobre o Estatuto da Criança e do Adolescente. Diário Oficial da União, Brasília, DF, 16 jul. 1990. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8069.htm. Acesso em: 26 out. 2025.

BRASIL. Lei nº 12.737, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos. Diário Oficial da União, Brasília, DF, 3 dez. 2012. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 19 out. 2025.

CÂMARA DOS DEPUTADOS. Denúncia sobre uso indevido de imagens de crianças motiva 32 projetos na Câmara dos Deputados. Brasília, DF: Agência Câmara de Notícias, 15 ago. 2025. Disponível em: https://www.camara.leg.br/noticias/1187375-denuncia-sobre-uso-indevido-de-imagens-de-criancas-motiva-32-projetos-na-camara-dos-deputados/. Acesso em: 26 out. 2025.

CASTELLS, Manuel. *A sociedade em rede*. 11. ed. São Paulo: Paz e Terra, 2016.

CAVALHEIRO, Renan. *O que é invasão de privacidade?* São Paulo: Academia de Forense Digital, 2023. Disponível em: https://academiadeforensedigital.com.br/o-que-e-invasao-de-privacidade/. Acesso em: 27 out. 2025.

CGI.br – COMITÊ GESTOR DA INTERNET NO BRASIL. Histórico da Internet no Brasil. Disponível em: https://www.cgi.br. Acesso em: 12 out. 2025.

COSTA, Fernando de Almeida. *Crimes cibernéticos e segurança digital*. São Paulo: Atlas, 2021.

COSTA, Marco Aurélio Rodrigues. Crimes de informática. Revista Jus Navigandi, Teresina, ano 2, n. 2249, 5 maio 1997. Disponível em: https://jus.com.br/artigos/1826/crimes-de-informatica. Acesso em: 17 out. 2025.

FERREIRA FILHO, Agnaldo Adriano; TORRES, Leonardo Guimarães. Estudo sobre crimes virtuais e suas implicações legais na sociedade moderna. Revista Ibero-Americana de Humanidades, Ciências e Educação, São Paulo, v. 10, n. 5, p. 2942–2955, maio 2024. DOI: 10.51891/rease.v10i5.14073.

KASPERSKY. What is cybercrime? How to protect yourself. Disponível em: https://www.kaspersky.com.br/resource-center/threats/what-is-cybercrime. Acesso em: 26 out. 2025.

LÉVY, Pierre. *Cibercultura*. São Paulo: Editora 34, 1999.

NAÇÕES UNIDAS. *Relatório Global sobre Crimes Cibernéticos*. Viena: ONU, 2020. Disponível em: https://brasil.un.org/pt-br/80468-cibercrime-movimenta-us15-trilhão-por-ano-diz-onu. Acesso em: 19 out. 2025.

RUSSELL, Stuart; NORVIG, Peter. *Inteligência Artificial*. 4. ed. Rio de Janeiro: LTC, 2022.

SANTOS, Andressa Martins dos; NASCIMENTO, Deivid Jose dos Santos. O enfrentamento dos cibercrimes pelo direito brasileiro na era da internet. Revista Jus Navigandi, Teresina, ano 28, n. 16, 29 nov. 2023. Disponível em: https://jus.com.br/artigos/107431/o-enfrentamento-dos-cibercrimes-pelo-direito-brasileiro-na-era-da-internet. Acesso em: 17 out. 2025.

SENADO FEDERAL. Adultização: Senado aprova projeto para proteger crianças em ambientes digitais. Brasília, DF: Agência Senado, 27 ago. 2025. Disponível em: https://www12.senado.leg.br/noticias/materias/2025/08/27/adultizacao-senado-aprova-projeto-para-proteger-criancas-em-ambientes-digitais. Acesso em: 27 out. 2025.

SILVA, Ricardo dos Santos. *Direito Digital e os desafios da cibercriminalidade*. Rio de Janeiro: Forense, 2020.

SOARES, Samuel Silva Basílio. Os crimes contra a honra na perspectiva do ambiente virtual. Revista Científica Semana Acadêmica, Fortaleza, 26 dez. 2016. Disponível em: https://semanaacademica.org.br/artigo/os-crimes-contra-honra-nas-perspectiva-do-ambiente-virtual. Acesso em: 27 out. 2025.

UNITED STATES DEPARTMENT OF DEFENSE. *History of the ARPANET*. Washington, D.C., 1983.

ZACARIAS, Fabiana; FREIRE, Lucas Zacharias. Crimes virtuais: análise das dificuldades e limitações ao combate. Revista JurES, v. 16, n. 29, p. 29–61, jun. 2023.

República Federativa do Brasil
Ministério da Educação
Fundação Universidade Federal de Mato Grosso do Sul

Termo de Autenticidade

Eu, **ANDERSON MAIRLON CALDAS ALVES**, acadêmico(a) regularmente apto(a) a proceder ao depósito do Trabalho de Conclusão de Curso intitulado **"A EVOLUÇÃO DOS CRIMES DIGITAIS E OS DESAFIOS PARA SUA CONTENÇÃO NO CENÁRIO ATUAL"**, declaro, sob as penas da lei e das normas acadêmicas da UFMS, que o Trabalho de Conclusão de Curso ora depositado é de minha autoria e que fui instruído pela minha orientadora acerca da ilegalidade do plágio, de como não o cometer e das consequências advindas de tal prática, sendo, portanto, de minha inteira e exclusiva responsabilidade, qualquer ato que possa configurar plágio.

Três Lagoas/MS, 07 novembro de 2025.

gov.br
Documento assinado digitalmente
ANDERSON MAIRLON CALDAS ALVES
Data: 07/11/2025 20:59:40-0300
Verifique em https://validar.iti.gov.br

ANDERSON MAIRLON CALDAS ALVES

Orientações: O acadêmico ou acadêmica deverá preencher e assinar este documento e, após, uni-lo ao TCC e ao Termo de Depósito e Composição da Banca Examinadora em um único arquivo PDF. O acadêmico ou acadêmica deverá, então, proceder ao depósito desse arquivo PDF único, observando a data limite estipulada pelo Colegiado de Curso.