

INTELIGÊNCIA ARTIFICIAL E CRIMES CIBERNÉTICOS: A APLICAÇÃO DE GOLPES CONTRA MULHERES EM AMBIENTES VIRTUAIS

ARTIFICIAL INTELLIGENCE AND CYBERCRIME: ONLINE SCAMS TARGETING
WOMEN

Ciências Humanas, Ciências Sociais Aplicadas • 28/08/2026

REGISTRO DOI: [10.70773/revistatopicos/787848580](https://doi.org/10.70773/revistatopicos/787848580)

Isabelle Cristinne Alves Azevedo¹

Aile Brandão Cardoso²

Victor Lucas Queiroz Braga³

Guilherme Saldanha Santana⁴

Diogo de Almeida Viana dos Santos⁵

RESUMO

O presente artigo analisa a relação entre cidadania, direitos humanos e a vulnerabilidade das mulheres diante de golpes praticados com Inteligência Artificial (IA), considerando os impactos da revolução digital na proteção da dignidade humana. O avanço da IA potencializa fraudes, ampliando riscos relacionados à manipulação de informações, à violação da privacidade e ao uso indevido da imagem, afetando direitos fundamentais. A insuficiência do Direito contemporâneo para enfrentar essas ameaças evidencia a necessidade de respostas que ultrapassem a atuação estatal. A maior exposição das mulheres a golpes digitais revela desigualdades estruturais de gênero. Por meio de revisão bibliográfica de artigos, documentos normativos e estudos interdisciplinares, o trabalho busca contribuir para o fortalecimento da proteção jurídica e para a formulação de políticas públicas voltadas ao enfrentamento da violência digital.

Palavras-chave: Tecnocracia; Segurança Digital; Direitos Humanos; Vulnerabilidade; Inteligência Artificial.

ABSTRACT

This article examines the relationship between citizenship, human rights, and women's vulnerability to scams enabled by Artificial Intelligence (AI), considering the impacts of the digital revolution on the protection of human dignity. AI advances have intensified fraudulent practices, increasing risks related to information manipulation, privacy violations, and image misuse, thereby affecting fundamental rights. The limitations of contemporary legal frameworks in addressing these threats highlight the need for responses that extend beyond State action. Women's greater exposure to digital scams reflects persistent structural gender inequalities. Using a bibliographic review of scientific articles, legal

documents, and interdisciplinary studies, this research contributes to discussions on strengthening legal protection and developing public policies to address emerging forms of AI-enabled digital violence against women.

Keywords: Technocracy; Digital Security; Human Rights; Vulnerability; Artificial Intelligence.

1. INTRODUÇÃO

A análise da relação entre cidadania, direitos humanos e a vulnerabilidade das mulheres, relacionada a golpes praticados com o uso de Inteligência Artificial (IA), a partir da compreensão de que os direitos humanos constituem um processo histórico e dinâmico, mostra-se fundamental no cenário hodierno. Nesse sentido, observa-se que o avanço tecnológico, especialmente no contexto da revolução digital, tem produzido novas formas de poder capazes de gerar ameaças inéditas à dignidade humana.

Diante disso, a evolução dos direitos humanos evidencia a passagem de uma concepção abstrata de sujeito para o reconhecimento de grupos específicos, como as mulheres, o que demanda a criação de mecanismos de proteção diferenciados diante de vulnerabilidades particulares no ambiente digital.

Além disso, o desenvolvimento da IA potencializa práticas fraudulentas, ampliando riscos relacionados à manipulação de informações, violação da privacidade, uso indevido da imagem, entre outras formas de violação, o que impacta diretamente direitos fundamentais. Nesse cenário, a cidadania contemporânea revela-se insuficiente para garantir proteção efetiva contra o poder tecnocrático, uma vez que as ameaças à liberdade não se

restringem mais à atuação estatal, mas também decorrem do uso indevido da tecnologia.

Dessa forma, a maior exposição das mulheres a golpes digitais evidencia desigualdades estruturais de gênero, reforçando a necessidade de uma abordagem jurídica e social que considere tais especificidades. Conclui-se que a garantia da cidadania plena no ambiente digital depende da formulação de novos direitos e da atuação positiva do Estado, a fim de assegurar a proteção contra os riscos provocados pelo mau uso das inovações tecnológicas e promover a efetivação dos direitos humanos na era digital.

O presente artigo tem o objetivo de analisar o crescente fenômeno do uso da IA com o propósito da aplicação de golpes, a partir da identificação dos principais impactos e da avaliação dos riscos para usuários e sistemas, relacionando gênero, tecnologia e violência digital, cuja metodologia utilizada trata-se de uma revisão bibliográfica, por meio da análise de artigos científicos, documentos normativos e estudos interdisciplinares sobre direitos humanos, cidadania digital, Inteligência Artificial e violência de gênero no ambiente virtual.

2. FUNDAMENTAÇÃO TEÓRICA OU REVISÃO DA LITERATURA

O marco teórico desta pesquisa fundamenta-se em quatro eixos complementares: a teoria da evolução dos direitos humanos e da cidadania de Norberto Bobbio (2004, p. 55); a concepção de violência estrutural de Baratta (1993, p. 56); a crítica ao capitalismo de vigilância e ao poder tecnocrático, desenvolvida por Zuboff (2019, p. 20); e a análise da concentração do poder tecnológico e da necessidade de governança democrática, proposta por Acemoglu e

Johnson (2024, p. 404). A articulação desses referenciais permite compreender a vulnerabilidade feminina no ambiente digital como resultado da interação entre desigualdades estruturais de gênero, novas formas de poder tecnológico e a insuficiência dos mecanismos jurídicos tradicionais de proteção dos direitos humanos na era da Inteligência Artificial.

3. METODOLOGIA

Trata-se de uma revisão bibliográfica, por meio da análise de artigos científicos, documentos normativos e estudos interdisciplinares sobre direitos humanos, cidadania digital, Inteligência Artificial e violência de gênero no ambiente virtual.

4. RESULTADOS E DISCUSSÕES OU ANÁLISE DOS DADOS

4.1. A Inteligência Artificial e Suas Repercussões Quanto à Revolução Digital

Historicamente, a criação e o uso de ferramentas que facilitam a existência humana, seja para colheitas mais eficazes, transporte mais rápido e seguro ou para melhorar a saúde, costumam ser divisores de águas para a humanidade, tendo consequências tanto positivas quanto negativas. A expansão do uso da Inteligência Artificial (IA) tem provocado transformações na dinâmica digital e social, pervadindo diferentes esferas da vida humana desde a sua concepção, embora não haja consenso quanto à sua definição (Acemoglu; Johnson, 2024, p. 404).

De acordo com Mo e Oyoung (2025, p. 512), IA generativa é o aprendizado de máquina levado a outro patamar, em que as respostas se assemelham à interação humana, sendo geradas a

partir de um *prompt*, ou seja, um comando verbal específico, baseadas em informações contidas na internet e/ou fornecidas pelo *user*, não havendo, contudo, qualquer raciocínio real por trás da interação com o programa.

Nesse contexto, os debates quanto ao impacto da IA e à forma responsável de utilizá-la, bem como normas, leis e outras formas de regulação, têm permeado diversas áreas do conhecimento, desde ciências da computação até direito internacional. O crescimento exponencial do uso da IA ultrapassa as estruturas regulatórias atuais, trazendo questionamentos éticos e quanto a como estabelecer mecanismos de governança e transparência, bem como questões relacionadas à cooperação internacional, considerando seu caráter transnacional e transfronteiriço (Abdussalam; Auladi, 2024, p. 2).

O Departamento de Comércio dos Estados Unidos publicou o AI RMF 1.0, *Artificial Intelligence Risk Management Framework* ou Estrutura de Gestão de Riscos em Inteligência Artificial, um documento cujo objetivo é oferecer estratégias que ampliem a confiabilidade dos sistemas de Inteligência Artificial, além de estimular o desenvolvimento, a aplicação de medidas e o uso responsáveis desses sistemas ao longo do tempo às organizações e aos indivíduos (National Institute of Standards and Technology, 2023, p. 4).

No Brasil, o Ministério da Ciência, Tecnologia e da Inovação (2025) estabeleceu a Estratégia Brasileira de Inteligência Artificial (EBIA), que, diferentemente da AI RMF 1.0, tem uma abordagem institucional, baseada nas diretrizes previamente estabelecidas pela Organização para a Cooperação e Desenvolvimento Econômico (OCDE), visando o desenvolvimento para o uso responsável,

equitativo e transparente, estimulando a inovação e cooperação interna e externa.

A OCDE (2026, p. 3), em seu *due diligence framework*, ou estrutura de devida diligência, apresenta medidas que os governos se comprometem a implementar, por exemplo, a integração de práticas de responsabilidade empresarial às políticas institucionais e aos sistemas de gestão das organizações, bem como a identificação e análise de riscos e impactos negativos, reais ou potenciais, relacionados às suas atividades, produtos e serviços. Além disso, estabelecem a necessidade de interromper, prevenir e mitigar efeitos adversos, acompanhar a implementação das medidas adotadas e seus resultados, garantir transparência na forma como os impactos são tratados e promover ou cooperar com mecanismos de reparação quando necessário.

Figura 1. Representação gráfica do framework de due diligence para IA responsável

Representação gráfica do *framework* de due diligence de RBC



Fonte: Adaptado de Organization for Economic Co-operation and Development (2026, p. 14).

No âmbito do direito internacional, a Convenção de Budapeste sobre Cibercrimes (2024), em seu artigo 4º, estabelece que os Estados Partes devem assegurar que infrações penais já previstas em outras convenções e protocolos internacionais também sejam reconhecidas como crimes no âmbito do direito interno quando praticadas por meio de sistemas de tecnologias da informação e comunicação (TICs). Ou seja, ainda que determinada conduta criminosa já seja regulada por instrumentos internacionais anteriores, caso ela seja cometida ou facilitada por recursos tecnológicos e ambientes digitais, os países signatários devem prever essa modalidade específica em sua legislação nacional (Freitas; Gonçalves; Torres, 2023, p. 301).

Dessa forma, é perceptível que a inovação tecnológica traz consigo a necessidade de estabelecer uma ordem através da qual é possível utilizá-la sem comprometer os direitos humanos, as leis e a sociedade, visando a proteção dos direitos já estabelecidos, sem que

estes sejam utilizados em detrimento de outrem, cujos principais obstáculos são tanto a novidade tecnológica quanto a expressiva coleta de dados, ferramentas monopolizadas por elites tecnológicas, além da falta de participação da sociedade em discussões pertinentes a todos (Acemoglu; Johnson, 2024, p. 453; Lima; Rego, 2024, p. 64).

Nesse sentido, o conceito de cidadania adotado por Bobbio (2004, p. 55), que está intrinsicamente ligada à proteção dos direitos fundamentais e sustenta que o individualismo é a base filosófica da democracia, em que cada indivíduo é uma pessoa moral com igual dignidade, e o poder do governo deriva do reconhecimento de direitos fundamentais inalienáveis, é primordial para compreender as necessidades específicas de determinados grupos que são mais vulneráveis no ambiente virtual, como mulheres e crianças.

É perceptível que o ambiente digital é uma extensão do meio físico e, por conseguinte, seria lógico que os direitos digitais deveriam se estabelecer como extensão dos direitos humanos previamente estabelecidos. Considerando que as leis internacionais são pautadas em contextos geográficos, culturais e sociais, passando por um período de adaptabilidade, é natural que, com a revolução digital, somando-se a isso uma transformação normativa, esse processo se prove ainda mais complexo (Shany, 2023, p. 3).

Nesse escopo, assim como prévias revoluções tecnológicas, a revolução digital provoca mudanças socioculturais, econômicas e políticas, exigindo um suporte jurídico equivalente, capaz de atender às demandas legais, uma vez que diversos crimes são facilitados pelas Tecnologias da Informação e Comunicação, exigindo ainda

coordenação internacional, considerando o caráter transfronteiriço da IA e suas repercussões (Shany, 2023, p. 12).

4.2. O Emprego da Inteligência Artificial na Aplicação de Golpes

Desde a polarização do uso da internet, surgiram diferentes modalidades de crimes que a utilizam como meio. Silva *et al.* (2025, p. 9), a partir de uma revisão integrativa, demonstraram o crescimento e a diversificação dos cibercrimes em âmbito nacional e internacional, especialmente práticas como *phishing*, roubo de credenciais, estelionato e fraude eletrônica. O estudo também identificou mulheres entre os grupos mais vulneráveis, em razão da maior exposição ao meio digital e de fatores sociotecnológicos. Ademais, a adaptabilidade demonstrada pelos cibercriminosos em suas estratégias baseadas no perfil das vítimas, na localidade e nos recursos tecnológicos disponíveis.

Nesse contexto, é necessário compreender que existem duas modalidades de crimes: *cyber-enabled crimes*, ou crimes facilitados pelas tecnologias digitais, e *cyber-dependent crimes*, ou crimes dependentes das tecnologias digitais. Ambas culminam no “uso malicioso da IA”, em que atores, sejam pessoas ou instituições, utilizam técnicas de manipulação mais sofisticadas para fins fraudulentos (Blauth; Gstrein; Zwitter, 2022, p. 77114; Brundage *et al.*, 2018; Europol, 2020, p. 17).

No que concerne à governança relacionada ao uso da IA, Roberts *et al.* (2024, p. 1277) afirmam que as iniciativas internacionais provam-se limitadas no enfrentamento aos diversos riscos e impactos associados ao uso da IA, especialmente porque os princípios internacionais que fundamentam seu desenvolvimento são

formulados de maneira abrangente, cuja especificidade depende dos valores e interesses de cada Estado. Ademais, a ausência de mecanismos obrigatórios de cumprimento limita a efetividade desses instrumentos, uma vez que não têm força vinculante e o descumprimento não culmina em sanções.

Segundo Anastácio, Muniz e Teodoro (2026, p.10), as *deepfakes* e a clonagem de voz transformaram o estelionato de uma infração artesanal baseada na mentira verbal em uma indústria tecnológica lucrativa baseada na manipulação algorítmica e na simulação de identidades digitais, uma vez que recursos como *chatbots*, sintetizadores de voz e modelos multimodais permitem a criação de conteúdos sofisticados, incluindo textos persuasivos, assinaturas eletrônicas falsificadas, reproduções vocais fidedignas e vídeos sintéticos de alta verossimilhança, potencializando práticas de manipulação.

Nesse contexto, esses recursos são utilizados, por exemplo, tanto para o estelionato comum quanto para o estelionato sentimental, caracterizado pela exploração de um vínculo afetivo ou amoroso estabelecido com a vítima, por meio do qual o agente obtém vantagens indevidas. Nessa modalidade, a confiança decorrente da relação emocional é utilizada como instrumento para induzir a vítima a realizar transferências patrimoniais ou assumir obrigações que lhe causem prejuízo, sendo o crime de estelionato consumado quando o agente obtém a vantagem indevida pretendida e provoca efetivo prejuízo patrimonial à vítima (Nóbrega e Silva, 2026, p.7).

Figura 2. Crimes facilitados pelo uso da Inteligência Artificial

Classe taxonômica	Exemplo de crime com uso de IA
-------------------	--------------------------------

Perturbações adversariais	Ataques adversariais a sistemas de reconhecimento facial para burlar a segurança
Veículos autônomos	Uso de veículos autônomos para ataques terroristas ou como meio de fuga após roubos
Conteúdo falso	Disseminação de notícias falsas ou propaganda usando conteúdo gerado por IA
Escuta automatizada	Uso de vigilância com IA para espiar indivíduos ou organizações
Robótica	Uso de robôs com IA para atividades criminais, como furtos ou vandalismo
Biometria	Uso de dados biométricos roubados para roubo de identidade ou acesso não autorizado
Reconhecimento prévio	Uso de sistemas de IA para prever atividades criminosas ou explorar vulnerabilidades em sistemas de segurança
Detecção de anomalias	Uso de IA para detectar padrões incomuns de comportamento e identificar alvos potenciais para furtos ou outros crimes
Ciência da Computação, não IA	Exploração de vulnerabilidades em sistemas de computador usando técnicas tradicionais de invasão
Software malicioso automatizado	Uso de malware com IA para infectar e controlar sistemas de computador
Criptografia	Uso de IA para quebrar códigos de criptografia e acessar dados sensíveis
Efeitos colaterais da IA	Consequências não intencionais de sistemas de IA que levam a violações de segurança ou outros crimes

Fonte: Adaptado de Abbas *et al.*, 2024, p.144.

Abbas *et al.* (2024, p. 141) relatam também as dificuldades relacionadas à responsabilização e ao processamento de crimes facilitados por sistemas de Inteligência Artificial, ressaltando a necessidade de um arcabouço normativo adequado para lidar com essas condutas emergentes. Observando a necessidade de compreender as repercussões jurídicas dos crimes habilitados por IA, enfatizando a relevância de estratégias integradas e multidimensionais para sua prevenção e enfrentamento.

Ademais, o aumento da incidência de práticas abusivas no ambiente digital, como os ciberataques de natureza criminosa, o ciberterrorismo e as ofensivas cibernéticas de caráter militar, tem impulsionado a elaboração de declarações voltadas aos direitos humanos digitais, destacando a importância da cibersegurança e da construção de um espaço virtual seguro. Esse cenário evidencia a crescente integração entre o Direito Internacional dos Direitos Humanos e outros instrumentos normativos relacionados ao ciberespaço, a exemplo da Convenção de Budapeste sobre o Cibercrime e do Regulamento Geral sobre a Proteção de Dados da União Europeia (GDPR), além de aproximá-lo dos processos internacionais de regulação da esfera digital (Shany, 2023, p. 17).

Entretanto, há a questão da preservação das provas digitais, o que constitui um dos principais desafios da perícia computacional, uma vez que qualquer falha ao longo da cadeia de custódia pode comprometer sua admissibilidade em juízo. Entre os principais obstáculos destacam-se: a volatilidade de determinados dados, que podem ser perdidos rapidamente caso não sejam coletados de forma adequada, a utilização de mecanismos de criptografia e o grande volume de informações armazenadas em dispositivos e serviços em nuvem. Além disso, há riscos relacionados à

manipulação e ao processamento das evidências, visto que alterações, ainda que involuntárias, podem afetar sua confiabilidade (Narasimhan e Kala, 2024, p. 2444).

Nesse escopo, os conflitos de soberania exercem um impacto profundo e complexo na coleta de provas digitais transfronteiriças, criando obstáculos que variam desde atrasos processuais até tensões diplomáticas. Questões sobre a territorialidade, conflitos de soberania que podem obstruir o acesso a provas, divergências entre modelos jurisdicionais, consenso quanto ao armazenamento de evidências, além da ineficiência do sistema de Tratados de Assistência Jurídica Mútua (MLAT), criticado por sua lentidão extrema. Por exemplo, pedidos entre a União Europeia e os EUA podem levar até dez meses para serem processados, tempo suficiente para que os dados voláteis desapareçam ou se tornem inúteis (Guan, 2025, p. 12).

4.3. A Vulnerabilidade Feminina Frente aos Golpes no Ambiente Digital

A violência não se constitui apenas de práticas cometidas contra um indivíduo, mas de tudo o que permite que seus direitos sejam violados. Nesse sentido, o conceito de violência estrutural adotado por Baratta (1993, p. 56) se estabelece como norteador para a análise de crimes cometidos no ambiente digital, uma vez que este é uma extensão da sociedade. As mesmas estruturas sociais se repetem no ambiente virtual, de modo que as violências vividas em sociedade são replicadas e até intensificadas, tornando as vulnerabilidades já existentes ainda mais evidentes.

Ademais, soma-se a vulnerabilidade social humana à vulnerabilidade sistêmica da IA, uma vez que o uso malicioso da IA se estabelece nas “brechas” que o sistema apresenta. A partir de técnicas os criminosos criam formas mais elegantes de cometer fraudes, utilizando não apenas recursos, mas também a permissibilidade da IA, do próprio algoritmo das redes sociais, para aumentar sua probabilidade de sucesso e se aproximar das vítimas, utilizando-se ainda das *deepfakes* em tempo real (Blauth, Gstrein e Zwitter, 2022, p. 77115; Zuboff, 2019, p. 20; Westerlund, 2019, p. 39).

Silva *et al.* (2025, p. 8), em sua análise integrativa, observaram que mulheres se encontram entre os grupos mais vulneráveis, representando mais da metade das ocorrências registradas, enfatizando que mulheres são vítimas desses crimes com maior frequência, demonstrando ainda que o Brasil tem seguido as tendências mundiais de progressão, em que apenas em São Paulo houve um crescimento de 256% referente a estelionato digital.

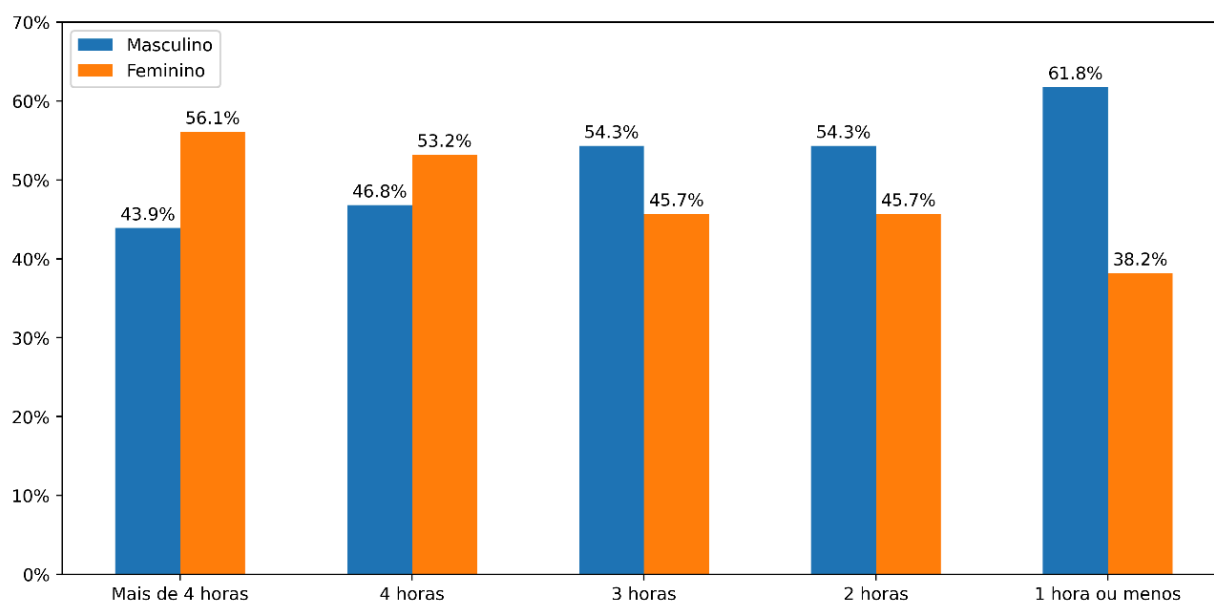
Nesse sentido, por representarem mais da metade da população que utiliza a internet, as mulheres se tornam mais afetadas, ainda mais quando também se encontram num segundo grupo, de idosos, que são particularmente vulneráveis por questões de maior dificuldade de compreensão do funcionamento das tecnologias, sendo principalmente alvos de estelionato eletrônico (Silva *et al.*, 2025, p. 9). Mulheres idosas também são alvo do estelionato sentimental, em que os criminosos se utilizam ainda de conexões emocionais para subtrair da vítima.

Nóbrega e Silva (2026, p. 2) afirmam que o período de transformações vividas pela humanidade quanto ao crescimento das tecnologias propicia relacionamentos que se desenvolvem

rapidamente no ambiente virtual, em que há dificuldade de determinar o caráter de uma pessoa baseado apenas nas interações ocorridas nas plataformas, facilitando a manipulação emocional, utilizando-se de um ciclo contínuo de manipulação emocional, baseado na criação de confiança, reconhecimento afetivo e laços de dependência, a vítima tem sua autonomia psíquica gradativamente reduzida, tornando-se mais vulnerável ao engano e à exploração.

Carcelén-García, Narros-González e Galmes-Cerezo (2024, p. 812) conceituam a vulnerabilidade digital como a possibilidade de sofrer danos psicológicos, de reputação ou físicos devido ao envolvimento em atividades online. Dessa maneira, a interação entre criminosos virtuais e suas vítimas se encaixa nesse perfil, pois além dos danos citados acrescenta-se também o dano financeiro. As autoras também identificaram um fator de risco maior para mulheres, principalmente relacionado ao fato de que mulheres têm maior participação online do que homens, como disposto na imagem a seguir:

Figura 3. Tempo de uso das redes sociais discriminado por gênero.



Fonte: Adaptado de Carcelén-García, Narros-González e Galmes-Cerezo (2024, p. 818).

Ademais, conforme notado por Silva *et al.* (2025, p. 8), mulheres são mais frequentemente alvos de crimes cibernéticos, o que é também associado ao tempo de exposição às redes sociais e à maneira de exploração personalizada das vulnerabilidades por parte de criminosos digitais, que se aproveitam de informações compartilhadas pelas próprias vítimas.

Segundo Berlimi (2023, p. 43), o estelionato sentimental é compreendido, no ordenamento jurídico brasileiro, como uma modalidade de fraude em que o agente se vale de um relacionamento afetivo para induzir ou manter a vítima em erro, com a finalidade de obter vantagem econômica ilícita. Embora a expressão não esteja prevista de forma expressa no Código Penal, sua configuração encontra fundamento no artigo 171, que tipifica o crime de estelionato mediante artifício, ardil ou fraude. Nesse contexto, a jurisprudência tem reconhecido que o próprio vínculo amoroso pode funcionar como o meio fraudulento utilizado para a obtenção da vantagem indevida.

Entretanto, nem toda transferência de recursos entre parceiros caracteriza estelionato sentimental. A distinção fundamental reside na comprovação da manipulação fraudulenta e do nexo causal entre a conduta do agente e o prejuízo econômico sofrido pela vítima. Auxílios financeiros prestados espontaneamente no contexto de um relacionamento, assim como o mero término da relação afetiva, não configuram ilícito por si sós. Quando demonstrado o dolo, contudo, podem surgir diversas consequências jurídicas, incluindo a anulação de negócios jurídicos praticados sob erro induzido, a restituição dos valores indevidamente obtidos e a reparação por danos materiais e morais (Berlimi, 2023, p. 41).

Nesse contexto, as mulheres figuram entre os principais grupos vulneráveis ao estelionato sentimental em razão da convergência entre fatores sociais, emocionais e tecnológicos que potencializam sua exposição a esse tipo de fraude. Estudos apontam que criminosos exploram expectativas afetivas, necessidades de pertencimento e relações de confiança construídas gradualmente em ambientes digitais, utilizando estratégias de manipulação emocional para obter vantagens econômicas indevidas. Além disso, desigualdades de gênero historicamente presentes na sociedade também se reproduzem no espaço virtual, favorecendo situações de vulnerabilidade que podem ser agravadas por fatores como idade avançada, isolamento social e intensa participação em plataformas digitais (Nóbrega; Silva, 2026, p. 6).

Dessarte, o estelionato sentimental ultrapassa a dimensão patrimonial, produzindo impactos psicológicos significativos, uma vez que a vítima não apenas sofre prejuízos financeiros, mas também enfrenta a quebra da confiança, o abalo emocional e a violação de sua dignidade, tornando necessária uma abordagem jurídica e social que considere as especificidades de gênero na prevenção e no enfrentamento dessa modalidade criminosa (Carcelén-García, Narros-González e Galmes-Cerezo, 2024, p. 12).

A partir disso, é necessário compreender que a vulnerabilidade feminina insere-se de forma significativa nesse contexto, uma vez que a expansão das práticas abusivas no ambiente digital intensifica desigualdades de gênero já existentes na sociedade. As mulheres encontram-se particularmente expostas a diferentes modalidades de violência e fraudes mediadas por tecnologias, como golpes financeiros, disseminação não consentida de imagens, falsificação

de identidade por meio de Inteligência Artificial, assédio virtual e manipulação de dados pessoais (Silva *et al.*, 2025, p. 8).

Diante desse cenário, a preocupação com a cibersegurança e a construção de um ambiente digital seguro transcende a proteção genérica dos usuários e passa a exigir uma abordagem sensível às questões de gênero. Assim, a articulação entre o Direito Internacional dos Direitos Humanos e os instrumentos normativos voltados à regulação do ciberespaço torna-se fundamental para a criação de mecanismos de prevenção, responsabilização e proteção capazes de enfrentar as novas formas de violência digital, promovendo a efetivação da dignidade humana, da igualdade e da cidadania digital (Shany, 2023, p. 12).

5. CONCLUSÃO/CONSIDERAÇÕES FINAIS

A expansão da Inteligência Artificial representa uma das mais significativas transformações da revolução digital contemporânea, trazendo benefícios expressivos para diversos setores da sociedade, mas também novos desafios relacionados à proteção dos direitos humanos e à segurança no ambiente virtual. Conforme demonstrado, a utilização maliciosa dessas tecnologias tem potencializado práticas criminosas já existentes, tornando fraudes, estelionatos e golpes digitais mais sofisticados, persuasivos e difíceis de identificar e combater.

Nesse contexto, verificou-se que a vulnerabilidade das mulheres diante desses crimes não decorre exclusivamente das ferramentas tecnológicas empregadas, mas também de desigualdades estruturais que se reproduzem no espaço digital. A combinação entre vulnerabilidades sociais pré-existentes e os recursos

proporcionados pela IA, como *deepfakes*, clonagem de voz e manipulação algorítmica, amplia os riscos de exploração financeira, emocional e reputacional, especialmente em modalidades como o estelionato sentimental (Westerlund, 2019, p. 41).

Observou-se ainda que os mecanismos normativos e institucionais atualmente existentes, embora representem avanços importantes, ainda se mostram insuficientes para enfrentar de forma efetiva os desafios impostos pela velocidade da inovação tecnológica e pela natureza transnacional dos cibercrimes. As dificuldades relacionadas à responsabilização dos agentes, à cooperação internacional e à preservação das provas digitais evidenciam a necessidade de aperfeiçoamento dos instrumentos jurídicos e dos modelos de governança da Inteligência Artificial.

Diante disso, é perceptível que a proteção das mulheres no ambiente digital exige uma abordagem multidimensional, capaz de articular regulação tecnológica, cooperação internacional, fortalecimento das capacidades investigativas, educação digital e políticas públicas voltadas à redução das desigualdades de gênero. Somente por meio da atuação conjunta do Estado, das organizações internacionais, das empresas de tecnologia e da sociedade civil será possível assegurar uma cidadania digital efetiva, promovendo o desenvolvimento responsável da Inteligência Artificial e garantindo a proteção da dignidade humana frente às novas formas de violência e exploração no ciberespaço.

Conclui-se que o uso malicioso da Inteligência Artificial tem ampliado significativamente os riscos associados aos golpes praticados no ambiente digital, especialmente aqueles que exploram vínculos afetivos como instrumento de fraude. Nesse

cenário, as mulheres figuram entre os grupos mais vulneráveis, em razão da combinação entre desigualdades estruturais de gênero, maior exposição a determinadas formas de violência digital e estratégias sofisticadas de manipulação emocional empregadas pelos criminosos. O estelionato sentimental evidencia como a tecnologia potencializa práticas fraudulentas pré-existentes, permitindo a construção de identidades falsas, a simulação de relacionamentos e a exploração da confiança das vítimas em escala cada vez maior.

Dessa forma, o enfrentamento desse fenômeno exige não apenas o aperfeiçoamento dos mecanismos jurídicos de responsabilização e proteção das vítimas, mas também o fortalecimento da educação digital, da conscientização social e das políticas públicas voltadas à redução das vulnerabilidades de gênero. Somente por meio de uma abordagem integrada será possível garantir a efetiva proteção dos direitos humanos e da cidadania no contexto das transformações promovidas pela era digital.

REFERÊNCIAS BIBLIOGRÁFICAS

ABBAS, Thamer Najm Abdullah; KADHIM, Ali Akram; HAMEED, Raed; QASIM, Nameer Hashim. Artificial Intelligence and Criminal Liability: Exploring the Legal Implications of AI-Enabled Crimes. **Revista de Ciencias Humanas, Teoría Social y Pensamiento Crítico: Encuentros**, n. 22, p. 140–159, set./dez. 2024. DOI: 10.5281/zenodo.13386675. Disponível em: <https://dialnet.unirioja.es/servlet/articulo?codigo=9812678>. Acesso em: 5 jun. 2026.

ABDUSSALAM, Achmad Varis; AULADI, Ghifari Alif. Pushing Boundaries: AI and Computer Science in the Era of Technological Revolution. TechComp Innovations: **Journal of Computer Science and Technology**, v. 1, n. 1, p. 1–9, 2024. DOI: 10.70063/techcompinnovations.v1i1.22. Disponível em: <https://mabadiiqtishada.org/index.php/TechCompInnovations/article/view/22>. Acesso em: 5 jun. 2026.

ACEMOGLU, Daron; JOHNSON, Simon. **Poder e progresso**: uma luta de mil anos entre a tecnologia e a prosperidade. 1ª Edição. Objetiva, 2024. 512 p

ANASTÁCIO, Gabriel Carlos de Brito; MUNIZ, Aline de Assis Rodrigues do Amaral; TEODORO, Marina. **O uso indevido de inteligências artificiais generativas nos crimes de estelionato no Brasil**: desafios de tipificação e responsabilidade penal. RevistaFT, v. 30, n. 157, 2026. DOI: 10.69849/b37szm95.

ANDRADE, Vera Regina Pereira de. **Cidadania**: do direito aos direitos humanos. São Paulo: Acadêmica, 1993.

BARATTA, Alessandro. Direitos humanos: entre a violência estrutural e a violência penal. Tradução de Ana Lucia Sabadell. **Revista da Faculdade de Direito da UFRGS**, Porto Alegre, v. 6, n. 2, p. 44–61, abr./maio/jun. 1993.

BERLINI, Luciana Fernandes. **Responsabilidade civil por estelionato sentimental**. In: Desafios da responsabilidade civil contemporânea. São Paulo: Escola Superior de Advocacia da OAB/SP, 2023. (Revista Científica Virtual da ESA/OAB-SP, ed. 43). Disponível em: <https://www.esaoabsp.edu.br/Revistas>. Acesso em: 9 jun. 2026.

BLAUTH, Taís Fernanda; GSTREIN, Oskar Josef; ZWITTER, Andrej. **Artificial Intelligence Crime: An Overview of Malicious Use and Abuse of AI.** *IEEE Access*, v. 10, p. 77110–77122, 2022. DOI: 10.1109/ACCESS.2022.3191790. Disponível em: <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9831441>. Acesso em: 26 de maio de 2026.

BOBBIO, Norberto. **A era dos direitos.** Tradução de Carlos Nelson Coutinho. 7. tiragem. Rio de Janeiro: Elsevier, 2004.

BRUNDAGE, Miles et al. The malicious use of artificial intelligence: forecasting, prevention, and mitigation. **Oxford: Future of Humanity Institute**, arXiv, 2018. Rev. 2024. Disponível em: <https://arxiv.org/abs/1802.07228>. Acesso em: 26 de maio de 2026.

CARCELÉN-GARCÍA, Sonia; NARROS-GONZÁLEZ, María José; GALMES-CEREZO, María. Digital vulnerability in young people: gender, age and online participation patterns. **Journal of Youth Studies**, v. 27, n. 6, p. 811–829, 2024. DOI: 10.1080/02673843.2023.2287115. Disponível em: <https://www.tandfonline.com/doi/full/10.1080/02673843.2023.2287115#abstract>. Acesso em: 9 jun. 2026.

EUROPOL. **Internet organised crime threat assessment (IOCTA) 2020.** The Hague: European Union Agency for Law Enforcement Cooperation, 2020. Disponível em: https://www.europol.europa.eu/cms/sites/default/files/documents/internet_organised_crime_threat_assessment_iocta_2020.pdf. Acesso em: 20 ago. 2026.

FREITAS, Camila Cristina Gonzaga de; GONÇALVES, Jonas Rodrigo; TORRES, Mateus Guimarães. A evolução do direito penal brasileiro

relacionado aos crimes cibernéticos. **Revista JRG de Estudos Acadêmicos**, v. 6, n. 12, p. 296-311, 2023. DOI: 10.5281/zenodo.7760710. Disponível em: <https://revistajrg.com/index.php/jrg/article/view/520>

GUAN, Chang. Cross-Border Cybercrime Digital Evidence: Current Research and Fundamental Categories. **Modern Law Research**, v. 6, n. 4, out. 2025. DOI: 10.37420/j.mlr.2025.027.

LIMA, Mario Jorge Philocreon de Castro; REGO, Hiolanda Silva. O “eu digital”: complexidades e desafios dos direitos humanos na sociedade tecnológica. **Direito.UnB - Revista de Direito da Universidade de Brasília**, Brasília, v. 8, n. 1, p. 61-85, 2024. DOI: <https://doi.org/10.26512/2357-80092024e47389>. Disponível em: <https://periodicos.unb.br/index.php/revistadedireitounb/article/view/47389>. Acesso em: 26 maio 2026.

Ministério da Ciência, Tecnologia e Inovação. **Estratégia Brasileira de Inteligência Artificial**. Brasília, DF, 2025. Disponível em: [Portal Gov.br – EBIA](#). Acesso em: 26 maio 2026.

MO, Hongwei; OUYANG, Shumiao. (Generative) AI in financial economics. **Journal of Chinese Economic and Business Studies**, v. 23, n. 4, p. 509–587, 2025. DOI: 10.1080/14765284.2025.2569006. Disponível em: <https://doi.org/10.1080/14765284.2025.2569006>. Acesso em: 12 jun. 2026.

NARASIMHAN, Premanand; KALA, N. Ensuring the Integrity of Digital Evidence: The Role of the Chain of Custody in Digital Forensics. **International Journal of Scientific Research in Computer Science, Engineering and Information Technology**, 2024. DOI: 10.32628/CSEIT2410612443.

National Institute of Standards and Technology. **Artificial Intelligence Risk Management Framework (AI RMF 1.0)**. NIST AI 100-1. Washington, DC: U.S. Department of Commerce, jan. 2023. DOI: 10.6028/NIST.AI.100-1.

NÓBREGA, Sabrina Picanço; SILVA, Rosana Reis de Melo. Estelionato sentimental: desafios da tipificação penal e a efetiva proteção da vítima. **Revista Ibero-Americana de Humanidades, Ciências e Educação (REASE)**, v. 12, n. 5, 2026. DOI: 10.51891/rease.v12i5.27292. Disponível em: <https://periodicorease.pro.br/rease/article/view/27292>. Acesso em: 26 maio 2026.

Organisation for Economic Co-operation and Development. **OECD Due Diligence Guidance for Responsible AI**. Paris: OECD Publishing, 2026. DOI: 10.1787/41671712-en. Disponível em: [OECD Due Diligence Guidance for Responsible AI \(PDF\)](#). Acesso em: 26 maio 2026.

ROBERTS, Huw; HINE, Emmie; TADDEO, Mariarosaria; FLORIDI, Luciano. Global AI governance: barriers and pathways forward. **International Affairs**, v. 100, n. 3, p. 1275-1286, 2024. DOI: <https://doi.org/10.1093/ia/iiae073>. Disponível em: <https://academic.oup.com/ia/article/100/3/1275/7641064>. Acesso em: 26 maio 2026.

SHANY, Yuval. Digital Rights and the Outer Limits of International Human Rights Law. **German Law Journal**, Cambridge, v. 24, n. esp. 3, p. 461–472, abr. 2023. DOI: 10.1017/glj.2023.35. Disponível em: [Cambridge University Press – Digital Rights and the Outer Limits of International Human Rights Law](#). Acesso em: 26 maio 2026.

SILVA, Daniel Braga da et al. Cibercrimes sob a perspectiva científica: revisão integrativa da produção nacional e internacional. **Revista Aracê**, São José dos Pinhais, v. 7, n. 8, p. 1-11, 2025. DOI: 10.56238/arev7n8-257. Disponível em:

<https://periodicos.newsciencepubl.com/arace/article/view/7643>.

Acesso em: 26 maio 2026.

UNITED NATIONS. **United Nations Convention against Cybercrime: Strengthening International Cooperation for Combating Certain Crimes Committed by Means of Information and Communications Technology Systems and for the Sharing of Evidence in Electronic Form of Serious Crimes**. New York: United Nations, 2024. Disponível em: [United Nations Convention against Cybercrime – Full Text](#). Acesso em: 26 maio 2026.

WESTERLUND, Mika. The emergence of deepfake technology: a review. **Technology Innovation Management Review**, v. 9, n. 11, p. 40-53, nov. 2019. DOI: <https://doi.org/10.22215/timreview/1282>

ZUBOFF, Shoshana. **The age of surveillance capitalism: the fight for a human future at the new frontier of power**. New York: PublicAffairs, 2019.

¹ Mestrado em Direito e Afirmação de Vulneráveis (CEUMA). E-mail: [acesse o artigo original para visualizar o e-mail](#). ORCID: <https://orcid.org/0009-0003-2115-3030>. LATTES: <http://lattes.cnpq.br/2069579944428784>.

² Mestrado em Direito e Afirmação de Vulneráveis (CEUMA). E-mail: [acesse o artigo original para visualizar o e-mail](#). ORCID:

<https://orcid.org/0009-0001-4217-4258>. LATTES:

<https://lattes.cnpq.br/7577086793371097>.

³ Mestrado em Direito e Afirmação de Vulneráveis (CEUMA). E-mail:

[acesse o artigo original para visualizar o e-mail](#). ORCID:

<https://orcid.org/0000-0003-2635-2031>. LATTES:

<http://lattes.cnpq.br/5112546446975117>.

⁴ Mestre em Direito, Universidade Ceuma (CEUMA). E-mail: [acesse o artigo original para visualizar o e-mail](#). ORCID: <https://orcid.org/0000-0001-6962-8646>. LATTES: <http://lattes.cnpq.br/2326377637283885>.

⁵ Doutor Phd em International Cooperation, Instituição: Universidade Ceuma (CEUMA). E-mail: [acesse o artigo original para visualizar o e-mail](#). ORCID: <https://orcid.org/0000-0001-9392-7689>.

LATTES: <http://lattes.cnpq.br/1432752484802169>.