REVISTA DE DIREITO DO TRABALHO, PROCESSO DO TRABALHO E DIREITO DA SEGURIDADE SOCIAL

Julho - Dezembro
v.14, n.2, 2025
ISSN: 2674-6913
DOI: 10.35987

ARTIGO

CRIMINALINDADE DIGITAL E VULNERABILIDADE SOCIAL: O PAPEL DO DIREITO PENAL NA EFETIVAÇÃO DOS DIREITOS HUMANOS E FUNDAMENTAIS DAS VÍTIMAS DE FRAUDES ONLINE

Julia Leal Brito[1]

Marcos Marcílio Eça Santos[2]

RESUMO

O presente artigo tem como objetivo analisar a eficácia do Direito Penal brasileiro na proteção dos direitos humanos de vítimas hipervulneráveis de fraudes digitais, considerando o contexto de exclusão digital e desigualdade social no país. A pesquisa parte da constatação de que a criminalidade virtual vem crescendo de forma alarmante, afetando desproporcionalmente segmentos sociais em situação de vulnerabilidade estrutural, como aqueles marcados pela exclusão informacional, renda limitada e baixo grau de letramento digital. Por meio de uma abordagem qualitativa e exploratória, o estudo revisita conceitos como hipervulnerabilidade, exclusão digital e princípios constitucionais de proteção à vítima. Além disso, examina os instrumentos penais existentes, os desafios enfrentados pelo sistema de justiça e propõe uma atuação penal mais sensível às demandas sociais contemporâneas. A conclusão aponta para a necessidade de uma resposta estatal mais integrada, humanizada e efetiva, que articule repressão qualificada e ações preventivas no combate às fraudes online.

Palavras-chave: fraudes digitais; direitos humanos; direito penal; vulnerabilidade social; exclusão digital.

ABSTRACT

This article aims to analyze the effectiveness of Brazilian criminal law in protecting the human rights of hypervulnerable victims of digital fraud, considering the country's context of digital exclusion and social

[1] Bacharel em Direito e Pós-Graduando em Direitos Humanos e Sociais pela UNEB, Campus XIX – Camaçari – BA. E-mail: lealjulia_@outlook.com
[2] Professor orientador deste trabalho. E-mail: mmarcilio@uneb.br

Julho - Dezembro
v.14, n.2, 2025
ISSN: 2674-6913
DOI: 10.35987

inequality. The research begins with the observation that cybercrime has grown alarmingly, disproportionately impacting socially disadvantaged groups, particularly those affected by low digital literacy, limited financial resources, and restricted access to digital infrastructure. Using a qualitative and exploratory approach, the study revisits concepts such as hypervulnerability, digital exclusion, and constitutional principles related to victim protection. It also examines existing criminal law instruments, the challenges faced by the justice system, and proposes a more socially sensitive penal approach. The conclusion highlights the need for a more integrated, humanized, and effective state response that combines qualified repression with preventive measures in addressing online fraud.

Keywords: digital fraud; human rights; criminal law; social vulnerability; digital exclusion.

1. INTRODUÇÃO

Nas últimas décadas, a revolução digital transformou de maneira radical os modos de interação social, econômica e institucional, integrando a internet como parte essencial da vida cotidiana. Com isso, novas formas de criminalidade surgiram e ganharam proporções alarmantes, sobretudo no espaço cibernético. As fraudes digitais, como golpes por aplicativos de mensagens, e-mails falsos, phishing, engenharia social, e estelionatos online, passaram a fazer parte do cenário contemporâneo de insegurança, atingindo milhares de pessoas, especialmente aquelas em situação de hipervulnerabilidade.

A vulnerabilidade digital não decorre apenas do desconhecimento técnico. Ela está diretamente relacionada às desigualdades socioeconômicas, à exclusão digital e à baixa escolarização de grande parte da população brasileira. Pessoas idosas, pobres, com pouco acesso a tecnologias, com baixo grau de instrução e que residem em áreas periféricas ou rurais estão entre as mais afetadas. Nesses contextos, a hipervulnerabilidade das vítimas de fraudes digitais é não apenas tecnológica, mas estrutural e histórica, em função de um modelo de sociedade desigual e excludente.

Diante desse cenário, o presente trabalho tem como objetivo geral analisar o papel do Direito Penal na proteção dos direitos humanos e fundamentais das vítimas hipervulneráveis de fraudes digitais, avaliando se o sistema penal brasileiro tem cumprido uma função garantista, protetiva e eficaz diante das novas dinâmicas de criminalidade cibernética.

Julho - Dezembro
v.14, n.2, 2025
ISSN: 2674-6913
DOI: 10.35987

A escolha do tema se justifica não apenas por sua atualidade e relevância social, mas também pela necessidade de se repensar a função do Direito Penal à luz do contexto digital e de suas novas vítimas, frequentemente invisibilizadas pela ausência de políticas públicas que integrem tecnologia, justiça e cidadania.

Para alcançar esse objetivo, a estrutura da pesquisa foi dividida em quatro capítulos principais. O primeiro capítulo aborda a exclusão digital como um reflexo das desigualdades sociais e examina o conceito de hipervulnerabilidade no contexto da era digital, destacando como a falta de acesso e domínio das tecnologias contribui para a marginalização de certos grupos. O segundo capítulo investiga a criminalidade digital e os direitos humanos, traçando a dinâmica das fraudes online e o perfil socioeconômico das vítimas, com base em dados e estudos recentes. Já o terceiro capítulo se debruça sobre o Direito Penal como mecanismo de proteção, analisando os limites da atuação estatal, os desafios probatórios, as reformas legislativas e as perspectivas de uma abordagem mais humanizada na proteção às vítimas. Por fim, o quarto capítulo (considerações finais) sistematiza as análises desenvolvidas, apontando os caminhos para uma resposta penal mais efetiva, inclusiva e comprometida com os direitos fundamentais.

A metodologia adotada é de cunho qualitativo, com base em pesquisa bibliográfica e documental, envolvendo legislações pertinentes, artigos científicos, livros e publicações acadêmicas que tratam da temática da criminalidade digital, da exclusão social e dos direitos humanos.

Dessa forma, este trabalho propõe uma reflexão crítica sobre os limites e possibilidades do Direito Penal diante de um novo cenário de vitimização, marcado por desigualdades estruturais e pela fragilidade digital de amplas parcelas da população. Mais do que propor respostas punitivas, busca-se ressaltar a urgência de um sistema penal que, em um Estado Democrático de Direito, seja também instrumento de acolhimento, proteção e efetivação de direitos, sobretudo daqueles que historicamente têm sido deixados à margem.

2. EXCLUSÃO DIGITAL, DESIGUALDADE SOCIAL E HIPERVULNERABILIDADE: NOVOS DESAFIOS NA ERA DIGITAL

Vivemos em um mundo globalizado onde a tecnologia redefine não apenas a economia, mas também as relações sociais, o acesso à informação e as próprias noções de cidadania. Nesse cenário, a exclusão digital deixa de ser um problema técnico para se tornar uma das faces mais críticas da desigualdade contemporânea.

Julho - Dezembro
v.14, n.2, 2025
ISSN: 2674-6913
DOI: 10.35987

Se, por um lado, a revolução digital prometeu democratizar oportunidades, por outro, ela também aprofundou abismos sociais, criando novas formas de marginalização. É nesse contexto que se insere a discussão sobre exclusão digital, desigualdade social e hipervulnerabilidade, desafios urgentes em uma era que exige conectividade não como privilégio, mas como condição básica de inclusão.

A exclusão digital é um fato que deve ser compreendido como um fenômeno multifacetado onde se ultrapassa o simplório entendimento limitado que o restringe a falta de acesso à internet. Em verdade, esse conceito também abrange aspectos como uso limitado e falta de habilidades para o manuseio da tecnologia, bem como a ausência de infraestrutura adequada para utilização.

Esta realidade é inserida no contexto daquilo que Manuel Castells (2000) denominou de sociedade informacional, marcada por uma economia que gira em torno do conhecimento e da tecnologia. Nesse contexto, a produtividade se amplia quando há domínio e disseminação das informações, exigindo também condições mínimas para que essas ferramentas sejam acessíveis a todos.

Quando parte da população fica à margem desse processo, a exclusão digital vai além da simples falta de equipamentos, ela se torna um obstáculo concreto à integração no mercado de trabalho e na vida social como um todo. Essa é uma questão urgente, que afeta diretamente a capacidade de indivíduos e comunidades de se inserirem no mundo atual.

Este tipo de exclusão materializa-se através das barreiras e disparidades que afetam parcela considerável da população no que se refere ao acesso às tecnologias da informação e comunicação. Desta forma, verifica-se que mesmo quando há disponibilidade de equipamentos, a ausência de compreensão e domínio tecnológico gera novos obstáculos excludentes.

Neste contexto, Pierre Lévy (1999) nos lembra que toda revolução na comunicação cria suas próprias formas de exclusão. Antes da escrita, não existiam analfabetos; com a imprensa e a televisão, surgiu a divisão entre quem tinha voz e quem ficava à margem.

Essa reflexão histórica mostra que a exclusão digital não é um problema contemporâneo, sim mais um capítulo em um processo contínuo: cada salto tecnológico reforça desigualdades já existentes. Entender isso é essencial, visto que não se trata apenas de falta de acesso à internet, mas de um padrão que se repete, exigindo respostas que vão além da simples distribuição de dispositivos.

No Brasil, essa problemática é carreada de contornos alarmantes, especialmente quando levadas em consideração as discrepâncias socioeconômicas históricas e a persistente concentração de renda e oportunidades. Conforme destaca Picazio et al. (2023), refletir sobre a exclusão digital é, antes, refletir sobre

Julho - Dezembro
v.14, n.2, 2025
ISSN: 2674-6913
DOI: 10.35987

todas as exclusões que as antecedem, visto que as exclusões, as faltas, as falhas, as ausências estão vinculadas à esta desigualdade, que, como sabemos, atinge a maior parte da população no Brasil.

Neste contexto, Gomes (2023) ressalta que numa sociedade progressivamente digitalizada, indivíduos desprovidos de acesso à internet enfrentam obstáculos para a efetivação de direitos fundamentais, particularmente no que tange ao acesso à informação e às possibilidades de participação no âmbito político. Assim, a hipervulnerabilidade na era digital não é um acaso, mas o resultado de um sistema que reproduz e intensifica exclusões já enraizadas.

Diante desse cenário, compreende-se a supramencionada exclusão digital como um problema estrutural que está diretamente ligado as modalidades convencionais de vulnerabilidade social, as quais abrangem fatores de ordem social, econômica e educacional.

Sobre a complexidade da questão nos alerta Lévy (1999, p.238):

> (...) o problema do 'acesso para todos' não pode ser reduzido às dimensões tecnológicas e financeiras geralmente apresentadas. Não basta estar na frente de uma tela, munido de todas as interfaces amigáveis que se possa pensar, para superar uma situação de inferioridade. É preciso antes de mais nada estar em condições de participar ativamente dos processos de inteligência coletiva que representam o principal interesse do ciberespaço. [...] Em outras palavras, na perspectiva da cibercultura assim como das abordagens mais clássicas, as políticas voluntaristas de luta contra as desigualdades e a exclusão devem visar o ganho em autonomia das pessoas e grupos envolvidos. Devem, em contrapartida, evitar o surgimento de novas dependências provocadas pelo consumo de informações ou de serviços de comunicação concebidos e produzidos em uma ótica puramente comercial ou imperial e que têm efeito, muitas vezes, desqualificar os saberes e as competências tradicionais dos grupos sociais e das regiões desfavorecidas.

A gravidade desse quadro reside no fato de que a exclusão digital se soma a outros fatores de vulnerabilidade social, como baixa renda, baixa escolaridade e distância dos centros urbanos, ampliando o risco de violação de direitos no ambiente online. Conforme aponta Castel (2013, p. 100), "a sociedade em rede tende a recriar hierarquias, pois os excluídos do acesso informacional ficam ainda mais distanciados dos processos de desenvolvimento".

Neste sentido, o acesso formal à internet, sem o desenvolvimento das capacidades para utilizá-la de forma crítica e segura, não assegura o exercício pleno da cidadania digital. Sen (2010, p. 33) complementa essa visão ao afirmar que "ter mais liberdade para fazer as coisas que são justamente valorizadas é (1)

Julho - Dezembro
v.14, n.2, 2025
ISSN: 2674-6913
DOI: 10.35987

importante por si mesmo para a liberdade global da pessoa e (2) importante porque favorece a oportunidade da pessoa ter resultados valiosos". Esta compreensão teórica evidencia que a inclusão digital transcende a mera conectividade, exigindo o desenvolvimento de competências específicas que permitam aos indivíduos navegarem de forma autônoma e crítica no ambiente digital.

Nesta perspectiva, Cavalli et al. (2021) destacam que é necessário, para existir uma verdadeira democracia no mundo cibernético, que haja não apenas o acesso à informação, mas a sua efetiva democratização e uso sem influências que possam manipular a vontade dos usuários, pois sem isto, não se está diante de uma democracia verdadeira, ainda que no âmbito da internet. Esta reflexão revela a dimensão política da exclusão digital, demonstrando como a ausência de competências críticas no ambiente virtual pode comprometer não apenas a participação individual, mas a própria qualidade democrática da sociedade.

(Santos, 2018), ao abordar as epistemologias do Sul, destaca que a exclusão digital entrelaça-se com outras formas de exclusão, como a social, a econômica e a cultural, especialmente nos países periféricos, onde o acesso desigual à informação e ao conhecimento reforça as hierarquias sociais. Assim, a exclusão digital não deve ser analisada isoladamente, mas integrada no contexto das desigualdades sociais mais amplas.

Nesta perspectiva, Sorj (apud BARRETO JÚNIOR; RODRIGUES, 2012, p.172) adverte que:

> Como toda inovação social, o impacto da telemática aumenta potencialmente a desigualdade social, já que dela se apropriam inicialmente os setores mais ricos da população, tornando a luta contra a exclusão digital não tanto uma luta para diminuir a desigualdade social, mas um esforço para não permitir que a desigualdade cresça ainda mais com as vantagens que os grupos da população com mais recursos e educação podem obter pelo acesso exclusivo a este instrumento.

Esta análise revela que a tecnologia, longe de ser neutra, tende a reproduzir e amplificar as estruturas de poder existentes, exigindo intervenções deliberadas para evitar o aprofundamento das disparidades sociais.

O panorama brasileiro revela um cenário de desafios persistentes, onde a exclusão digital é mesclada com a desigualdade social, criando um contexto propício para a hipervulnerabilidade das vítimas, especialmente diante da crescente criminalidade digital.

Barreto Júnior e Rodrigues (2012) chamam atenção para um paradoxo da era digital: ao mesmo tempo em que as tecnologias revolucionaram nossa comunicação e interações sociais, criando possibilidades inéditas de conexão, elas também deram origem a novas formas de segregação. Essa transformação não

Julho - Dezembro
v.14, n.2, 2025
ISSN: 2674-6913
DOI: 10.35987

se limitou aos meios técnicos, reconfigurou comportamentos, expectativas e até mesmo nossa percepção de pertencimento social na contemporaneidade.

O aprofundamento da exclusão e da vulnerabilidade digital pode ser compreendido à luz das teorias críticas da exclusão social, como as propostas por Castel (2013), que argumenta que a sociedade em rede pode tanto promover a inclusão quanto aprofundar a marginalização dos excluídos tecnológicos.

Estas perspectivas reforçam a necessidade de políticas públicas integradas que articulem inclusão digital, proteção jurídica e fortalecimento dos direitos humanos, reconhecendo que os desafios da era digital exigem respostas complexas e multidisciplinares.

3. CRIMINALIDADE DIGITAL E DIREITOS HUMANOS: A DINÂMICA DAS FRAUDES E O PERFIL DAS VÍTIMAS

A criminalidade digital emerge como um dos fenômenos mais complexos da sociedade contemporânea, ultrapassando barreiras geográficas e sociais, com impactos desiguais sobre diferentes estratos populacionais. No Brasil, esse cenário assume contornos particularmente alarmantes, revelando não apenas fragilidades tecnológicas, mas também desigualdades estruturais que amplificam a exposição a riscos no ambiente virtual. A compreensão desse fenômeno exige uma análise crítica sobre como as disparidades socioeconômicas se reproduzem no ciberespaço, gerando novos padrões de vitimização que demandam respostas jurídicas e políticas públicas especializadas.

3.1 PRINCIPAIS TIPOS DE FRAUDES ONLINE: TAXONOMIA E MECANISMOS DE OPERAÇÃO

A diversificação das modalidades fraudulentas no ambiente digital reflete a sofisticação crescente dos agentes criminosos e a ampliação das vulnerabilidades decorrentes da digitalização acelerada de serviços e transações.

Rosa (2002, p. 53-54) conceitua o crime cibernético como "conduta atente 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

Julho - Dezembro
v.14, n.2, 2025
ISSN: 2674-6913
DOI: 10.35987

sistema de tratamento rudimentar". Esta conceituação evidencia a amplitude dos fenômenos criminosos no ambiente digital, que transcendem as modalidades tradicionais de delito.

O phishing, modalidade criminosa que consiste na obtenção fraudulenta de informações confidenciais mediante simulação de comunicações legítimas, representa uma das técnicas mais difundidas no cenário nacional. Silva (2021, p. 8) destaca que o "phishing realizado pelo envio de disparos de SMS para celulares, são geralmente são mensagens com informações de que a vítima está endividada ou ganhou um sorteio inesperado, fazendo com que a vítima tome decisões imediatas". Esta modalidade evidencia como os criminosos exploram a urgência e a ansiedade das vítimas para induzi-las a comportamentos comprometedores de sua segurança digital.

A engenharia social, técnica que explora falhas humanas ao invés de vulnerabilidades tecnológicas, constitui outro pilar fundamental da criminalidade digital contemporânea. Johnstone e Psaroulis (2024, p. 1) observam que "os golpistas usam técnicas psicológica sofisticadas, eles exploram nossas vulnerabilidades humanas mais profundas e ignoram o pensamento racional para explorar nossas respostas emocionais". Esta "guerra psicológica" mencionada pelos autores coage as vítimas a tomarem decisões impulsivas, demonstrando como a manipulação psicológica se tornou ferramenta central na criminalidade contemporânea.

Os golpes bancários digitais constituem categoria específica que merece atenção particular devido aos impactos econômicos diretos sobre as vítimas. Estas modalidades fraudulentas incluem desde a clonagem de cartões de crédito e débito até invasões de contas bancárias e transferências não autorizadas via PIX, modalidade que se tornou particularmente visada devido à sua praticidade e rapidez nas transações. A implementação do sistema PIX, embora represente avanço significativo na democratização do acesso ao sistema financeiro, paradoxalmente criou novas oportunidades para a ação criminosa, especialmente entre usuários com menor conhecimento sobre segurança digital.

O fenômeno do romance scam, modalidade que explora relacionamentos afetivos falsificados para aplicação de golpes financeiros, representa tendência crescente que atinge particularmente pessoas em situação de isolamento social ou vulnerabilidade emocional. Santos e Lima (2019) alertam que "os crimes de natureza emocional e financeira são muitas vezes difíceis de provar em tribunal", destacando que "a legislação brasileira ainda precisa avançar neste aspecto". Os autores enfatizam que "é crucial que a legislação seja atualizada para refletir a realidade do estelionato sentimental e fornecer proteção adequada às vítimas".

Silva (2021, p. 6) contextualiza a amplitude do problema ao observar que "a internet é um campo extremamente abastecido de informações valiosíssimas e de imensurável valor, o que se torna altamente

Julho - Dezembro
v.14, n.2, 2025
ISSN: 2674-6913
DOI: 10.35987

atraente a ataques e por ser um ambiente de fácil acesso, de inúmeras possibilidades e com muitos usuários que diariamente, utilizam a internet". Esta observação evidencia como a democratização do acesso digital, embora benéfica, cria simultaneamente novos vetores de vulnerabilidade.

3.2 PERFIL SOCIOECONÔMICO DAS VÍTIMAS E IMPACTOS SOCIAIS DAS FRAUDES

A análise do perfil das vítimas de crimes digitais revela padrões que corroboram as teorias sobre exclusão digital e vulnerabilidade social apresentadas nos capítulos anteriores.

Uma esquisa publicada em abril de 2025 pelo instituto DataSenado indica que os golpes digitais vitimaram 24% dos brasileiros com mais de 16 anos nos últimos 12 meses, representando mais de 40,85 milhões de pessoas que perderam dinheiro em função de algum crime cibernético.

Esta proporção alarmante evidencia a generalização da vulnerabilidade digital na sociedade brasileira, transcendendo barreiras socioeconômicas tradicionais, embora mantendo padrões diferenciados de impacto conforme as características demográficas das vítimas.

Os dados revelam que, contrariando expectativas comuns, os mais afetados são jovens entre 16 e 29 anos, que correspondem a 27% das vítimas, enquanto a faixa com mais de 60 anos, tradicionalmente considerada mais vulnerável, representa proporção menor do total de vitimizados. Esta constatação sugere que a vulnerabilidade digital não se limita à familiaridade tecnológica, mas relaciona-se com padrões comportamentais específicos e maior exposição ao ambiente digital.

Tocantins (2023, p. 1) observa que "a rápida evolução tecnológica trouxe consigo a conveniência e a eficiência, mas também abriu portas para novas formas de criminalidade". O autor destaca que "os criminosos cibernéticos se aproveitam de brechas na segurança digital e ingenuidade dos usuários para cometer crimes que podem causar prejuízos financeiros, emocionais e psicológicos significativos".

Os idosos, embora representem proporção menor do total de vítimas, emergem como grupo que sofre impactos desproporcionalmente severos quando vitimizado. A menor familiaridade com as dinâmicas comunicacionais do ambiente digital, combinada com maior disponibilidade de tempo para interações online e, frequentemente, maior disponibilidade financeira, cria um contexto de risco específico.

Johnstone e Psaroulis (2024, p. 1) explicam que "às vezes os golpistas espalham seus métodos entre muitas vítimas em potencial para ver quem é vulnerável. Outras vezes, os criminosos se concentram em uma pessoa específica", demonstrando a sofisticação das estratégias de seleção de vítimas.

Julho - Dezembro
v.14, n.2, 2025
ISSN: 2674-6913
DOI: 10.35987

A população de baixa renda, paradoxalmente, representa outro segmento de alta vulnerabilidade, mesmo possuindo menor capacidade financeira. Esta aparente contradição se explica pelo fato de que indivíduos com menores recursos educacionais e digitais apresentam maior dificuldade em identificar tentativas fraudulentas, sendo mais suscetíveis a golpes que prometem ganhos financeiros rápidos ou benefícios sociais extraordinários.

Para estas populações, mesmo prejuízos de valores relativamente baixos podem representar impactos desproporcionais em suas condições de vida, gerando consequências que se estendem muito além da esfera financeira.

3.3 INTERSEÇÃO ENTRE VULNERABILIDADE DIGITAL E VIOLAÇÃO DE DIREITOS HUMANOS

A criminalidade digital transcende a esfera meramente patrimonial, configurando-se como fenômeno que atenta contra múltiplos direitos fundamentais consagrados na Constituição Federal e nos tratados internacionais de direitos humanos.

A violação da privacidade, através do acesso não autorizado a dados pessoais e comunicações privadas, representa uma das dimensões mais evidentes desta problemática. Contudo, os impactos são estendidos para além desta esfera, atingindo direitos como a dignidade humana, a segurança, a propriedade e, em casos extremos, a própria integridade física e psicológica das vítimas.

O direito à privacidade, reconhecido tanto no âmbito constitucional quanto na Lei Geral de Proteção de Dados Pessoais (LGPD), sofre violações sistemáticas através das práticas criminosas digitais. O vazamento e comercialização de dados pessoais, práticas comuns no ecossistema da criminalidade cibernética, criam um ambiente de constante insegurança jurídica onde os indivíduos perdem o controle sobre suas informações pessoais.

Esta situação é particularmente grave considerando que muitas vítimas sequer têm conhecimento de que seus dados foram comprometidos, permanecendo expostas a riscos futuros sem possibilidade de adoção de medidas preventivas.

Nesse sentido, a dignidade humana, princípio fundamental do Estado Democrático de Direito, é sistematicamente violada através de práticas criminosas que exploram vulnerabilidades pessoais, familiares e socioeconômicas das vítimas. Os golpes baseados em engenharia social frequentemente utilizam informações íntimas sobre as vítimas, obtidas através de vasculhamento de redes sociais ou vazamentos

Julho - Dezembro
v.14, n.2, 2025
ISSN: 2674-6913
DOI: 10.35987

de dados, para construir narrativas convincentes que exploram medos, esperanças e necessidades pessoais.

Johnstone e Psaroulis (2024, p. 1) destacam que esta "guerra psicológica" representa uma forma particularmente perversa de violação da dignidade, reduzindo as pessoas a meros objetos de exploração econômica através da manipulação de suas "vulnerabilidades humanas mais profundas".

O direito de acesso à justiça, garantia fundamental para a efetivação dos demais direitos, encontra-se severamente comprometido no contexto da criminalidade digital. Os crimes de natureza emocional e financeira são muitas vezes difíceis de provar, evidenciando como as características específicas destes crimes, como a transnacionalidade, o anonimato dos agentes, a complexidade técnica das evidências e a rapidez na consumação dos delitos, criam barreiras substanciais para a persecução penal efetiva.

A questão da reparação dos danos assume contornos particulares na criminalidade digital, especialmente considerando que muitas vítimas pertencem a grupos socioeconomicamente vulneráveis para os quais mesmo prejuízos financeiros relativamente pequenos podem representar impactos desproporcionais.

Tocantins (2023, p. 1) observa que os crimes digitais "podem causar prejuízos financeiros, emocionais e psicológicos significativos", demonstrando como a dificuldade em localizar e responsabilizar os agentes criminosos, combinada com a complexidade dos mecanismos de ressarcimento, frequentemente deixa as vítimas em situação de desamparo prolongado.

O direito à educação, compreendido em sua dimensão contemporânea como incluindo a alfabetização digital, emerge como elemento fundamental para a prevenção da vitimização.

A ausência de políticas públicas efetivas de educação para a segurança digital representa, em si mesma, uma forma de violação do direito à informação e à educação, na medida em que deixa parcelas significativas da população expostas a riscos evitáveis.

A dimensão coletiva dos direitos violados pela criminalidade digital merece atenção especial. Para além dos impactos individuais, estes crimes afetam a confiança social nas tecnologias digitais, potencialmente comprometendo processos mais amplos de inclusão digital e desenvolvimento tecnológico. A erosão da confiança no ambiente digital pode resultar em exclusão voluntária de grupos vulneráveis, perpetuando ciclos de marginalização e aprofundando desigualdades existentes.

Silva (2021, p. 6) contextualiza esta problemática ao destacar que a internet, embora seja "um campo extremamente abastecido de informações valiosíssimas", torna-se simultaneamente "altamente atraente a ataques" devido às suas características de acessibilidade e amplitude de usuários.

Julho - Dezembro
v.14, n.2, 2025
ISSN: 2674-6913
DOI: 10.35987

A interseccionalidade das vulnerabilidades evidencia-se de forma particular na análise dos impactos diferenciados sobre distintos grupos populacionais. Mulheres idosas de baixa renda, por exemplo, enfrentam múltiplas camadas de vulnerabilidade que se potencializam mutuamente: menor familiaridade tecnológica, maior isolamento social, frequente dependência financeira e, muitas vezes, menor acesso a redes de apoio para enfrentamento das consequências da vitimização.

Esta sobreposição de fatores de risco demanda abordagens específicas que considerem as particularidades de cada grupo, superando visões homogeneizadoras que não capturam adequadamente a complexidade das vulnerabilidades contemporâneas.

Somente através de políticas públicas abrangentes que considerem as dimensões educativa, tecnológica, jurídica e social será possível construir um ambiente digital verdadeiramente inclusivo e seguro, onde o exercício dos direitos fundamentais seja garantido a todos os cidadãos, independentemente de suas características socioeconômicas ou grau de familiaridade tecnológica.

4. O DIREITO PENAL COMO MECANISMO DE PROTEÇÃO: LIMITES, DESAFIOS E PESPECTIVAS HUMANIZADAS

A análise da criminalidade digital contemporânea exige uma reflexão profunda sobre o papel do direito penal como instrumento de proteção social. Conforme observa Zaffaroni (2018), o sistema penal não pode ser compreendido apenas como mecanismo repressivo, mas deve ser repensado sob uma perspectiva garantista que prime pela proteção efetiva dos direitos fundamentais. Nesse contexto, a proteção das vítimas de crimes digitais demanda uma abordagem multidisciplinar que transcenda os limites tradicionais da dogmática penal.

A evolução legislativa brasileira demonstra essa preocupação crescente: a Lei nº 12.737/2012 (Lei Carolina Dieckmann) introduziu os primeiros tipos penais específicos para crimes informáticos no Código Penal, seguida pela Lei nº 12.965/2014 (Marco Civil da Internet), que estabeleceu princípios fundamentais para o uso da rede mundial de computadores. Mais recentemente, a Lei nº 14.155/2021 agravou as penas para fraudes eletrônicas e tipificou o crime de invasão de dispositivo informático, evidenciando a evolução do tratamento penal da criminalidade digital.

Nesse sentido, é inegável que a transformação digital da sociedade brasileira trouxe consigo novos desafios para o sistema de justiça criminal. Conforme dados do Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação (2023), o Brasil registrou um crescimento de 185% nos

Julho - Dezembro
v.14, n.2, 2025
ISSN: 2674-6913
DOI: 10.35987

crimes digitais entre 2020 e 2023, evidenciando a urgência de uma resposta estatal adequada e humanizada. Este cenário demanda uma análise crítica dos mecanismos existentes e a proposição de alternativas que conciliem efetividade punitiva com proteção integral das vítimas.

4.1 AVALIAÇÃO CRÍTICA DA ATUAÇÃO DO ESTADO E DO SISTEMA DE JUSTIÇA PENAL

A atuação estatal no combate à criminalidade digital revela um conjunto de contradições e limitações estruturais que comprometem a efetividade da proteção às vítimas. Conforme análise de Greco (2020), o sistema de justiça penal brasileiro ainda opera com uma lógica fragmentária, caracterizada pela desarticulação entre os órgãos de persecução penal e pela ausência de protocolos específicos para o atendimento de vítimas de crimes cibernéticos.

A primeira limitação identificada reside na formação deficitária dos operadores do direito. Conforme observa Crespo (2011, p. 72-73):

> "aquele que causa dano a dados informáticos de outrem, ainda que dolosamente e ainda que cause verdadeira perda econômica, não está sujeito às penas do Código Penal, mas apenas ao que dispõe a legislação quanto à Responsabilidade Civil."

Esta lacuna normativa, parcialmente corrigida pelas Leis nº 12.737/2012 e 14.155/2021, demonstra como o direito penal brasileiro demorou a se adaptar à realidade digital, resultando em aplicação inadequada das normas existentes pelos operadores jurídicos.

O segundo aspecto problemático relaciona-se à morosidade processual. Esta dilação temporal agrava o sofrimento das vítimas e compromete a efetividade da resposta penal, criando um ambiente de impunidade que estimula a prática delitiva. A demora processual assume contornos ainda mais graves nos crimes digitais, considerando que as evidências eletrônicas podem ser facilmente destruídas ou alteradas, e o dano à vítima frequentemente se perpetua durante toda a tramitação do processo.

A desarticulação institucional constitui outro elemento crítico. Esta fragmentação é particularmente prejudicial nos crimes digitais, que demandam cooperação interinstitucional ampla e célere troca de informações. A falta de protocolos unificados de investigação e a inexistência de um sistema integrado de compartilhamento de dados comprometem gravemente a capacidade estatal de resposta à criminalidade cibernética.

Julho - Dezembro
v.14, n.2, 2025
ISSN: 2674-6913
DOI: 10.35987

A infraestrutura tecnológica inadequada representa um obstáculo significativo. Pesquisa do Instituto de Segurança Pública (2023) revela que apenas 45% das delegacias de polícia possuem equipamentos adequados para investigação de crimes digitais, enquanto somente 30% dispõem de peritos especializados em tecnologia da informação. Esta precariedade estrutural compromete gravemente a capacidade investigativa estatal, resultando em baixos índices de elucidação e responsabilização criminal.

Ademais, a análise da legislação vigente revela disparidades significativas na valoração penal dos crimes digitais. Conforme apontam Diniz, Cardoso e Puglia (2022, p. 15), "é mais negócio para o criminoso praticar ilícitos por meio da internet (via anonimato) do que ir para as ruas e cometer assaltos", pois "para o criminoso é mais seguro e lucrativo cometer o delito de estelionato do que o de roubo." Esta distorção no sistema punitivo evidencia a necessidade de reformulação das penas cominadas aos crimes digitais, considerando sua gravidade e impacto social.

4.2 DIREITOS E GARANTIAS CONSTITUCIONAIS E TRATADOS INTERNACIONAIS DE PROTEÇÃO ÀS VÍTIMAS

A proteção das vítimas de crimes digitais encontra fundamento sólido no ordenamento jurídico brasileiro e nos tratados internacionais dos quais o país é signatário. A Constituição Federal de 1988, em seu artigo 5º, estabelece um amplo catálogo de direitos fundamentais que deve nortear a atuação estatal na prevenção e repressão da criminalidade cibernética (BRASIL, 1988).

A evolução legislativa infraconstitucional demonstra o reconhecimento crescente da necessidade de proteção específica no ambiente digital, materializada na Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018) e nas sucessivas alterações do Código Penal para incluir tipos penais relacionados à criminalidade informática.

O princípio da dignidade humana, previsto no artigo 1º, inciso III, da Constituição, constitui o fundamento axiológico central da proteção às vítimas. Conforme leciona Sarlet (2015), este princípio impõe ao Estado o dever de criar condições materiais e jurídicas que assegurem uma existência digna a todos os cidadãos, incluindo a proteção contra violações decorrentes de crimes digitais.

No contexto da criminalidade cibernética, a dignidade humana manifesta-se na necessidade de proteger a integridade psíquica, a privacidade e a honra das vítimas contra ataques virtuais. Este princípio exige uma abordagem holística que considere não apenas a punição do agressor, mas também a reparação integral dos danos causados e a prevenção de novas vitimizações.

Julho - Dezembro
v.14, n.2, 2025
ISSN: 2674-6913
DOI: 10.35987

O direito à intimidade e à vida privada, assegurado pelo artigo 5º, inciso X, assume particular relevância nos crimes digitais. A Lei Geral de Proteção de Dados Pessoais (LGPD) complementa esta proteção constitucional, estabelecendo princípios específicos para o tratamento de dados pessoais e criando mecanismos de responsabilização para violações. No ambiente digital, esta proteção materializa se não apenas na punição dos crimes contra a privacidade, mas também na criação de obrigações preventivas para controladores e operadores de dados.

A inviolabilidade das comunicações, prevista no artigo 5º, inciso XII, estabelece limites claros à atuação estatal investigativa, exigindo equilíbrio entre eficiência da persecução penal e respeito aos direitos fundamentais.

A Lei nº 13.964/2019 (Pacote Anticrime) introduziu importantes alterações no processo penal, incluindo regras específicas para investigação de crimes praticados através de meios eletrônicos, reforçando a necessidade de observância dos requisitos constitucionais de necessidade, adequação e proporcionalidade.

O princípio da isonomia, consagrado no caput do artigo 5º, exige que a proteção estatal seja universal e não discriminatória. No contexto dos crimes digitais, isto significa que grupos vulneráveis, devem receber proteção especial e diferenciada, considerando sua maior suscetibilidade à vitimização cibernética.

No plano internacional, o Brasil ratificou diversos tratados que estabelecem parâmetros para a proteção de vítimas de crimes. A Convenção Americana sobre Direitos Humanos (Pacto de São José da Costa Rica), promulgada pelo Decreto nº 678/1992, estabelece em seu artigo 25 o direito à proteção judicial efetiva, que implica o dever estatal de proporcionar recursos jurídicos adequados e eficazes para a proteção de direitos fundamentais. No contexto digital, este dispositivo fundamenta a exigência de procedimentos judiciais especializados e céleres para o tratamento de crimes cibernéticos.

A Convenção sobre o Cibercrime (Convenção de Budapeste), embora ainda não ratificada pelo Brasil, constitui referência internacional fundamental para o tratamento da criminalidade digital. A convenção enfatiza a necessidade de equilibrar medidas eficazes de aplicação da lei com a proteção dos direitos humanos e liberdades fundamentais.

A Declaração Universal dos Direitos Humanos, incorporada ao ordenamento brasileiro, estabelece em seu artigo 12 a proteção contra interferências arbitrárias na vida privada e na correspondência. No contexto digital, este dispositivo fundamenta a proteção contra invasões de privacidade, vazamento de dados pessoais e outras formas de violação da esfera íntima através de meios eletrônicos.

Julho - Dezembro
v.14, n.2, 2025
ISSN: 2674-6913
DOI: 10.35987

4.3 SÍNTESE INTEGRATIVA: DIREITO PENAL HUMANIZADO E A CONSTRUÇÃO DE UM PARADIGMA DE PROTEÇÃO EFETIVA ÀS VÍTIMAS DE FRAUDES ONLINE

A análise pormenorizada da criminalidade digital e sua intersecção com a vulnerabilidade social revela a necessidade premente de reconstrução paradigmática do direito penal brasileiro.

As deficiências identificadas na atuação do Estado e do sistema de Justiça Penal demonstram que a mera tipificação criminal não assegura proteção efetiva aos direitos humanos e fundamentais das vítimas de fraudes digitais.

Esta problemática se intensifica quando se observa que "não basta a elaboração da norma propriamente dita", uma vez que "já existem diversas Leis sem apresentações reais de resultados eficazes" (CAMPOS, 2018, p. 20). O autor ainda adverte que "o Direito e, consequentemente, a legislação devem evoluir para acompanhar de perto a dinâmica social, sob pena de se tornar letra morta, sem aplicabilidade aos casos concretos e sem força coercitiva" (CAMPOS, 2018, p. 20). Esta constatação encontra particular relevância no contexto das fraudes online, onde a evolução tecnológica supera constantemente a capacidade normativa estatal.

A incorporação dos princípios constitucionais e tratados internacionais de proteção às vítimas estabelece parâmetros normativos que exigem reformulação das práticas de combate à criminalidade digital.

A dignidade humana, como fundamento axiológico central, impõe ao Estado o dever de criar mecanismos eficazes que transcendam a perspectiva meramente punitiva, contemplando prevenção, proteção e reparação integral às vítimas. Esta necessidade de adequação normativa torna-se ainda mais evidente quando se constata que "o Brasil sofre inúmeras críticas no que se refere à sua legislação, de modo geral", especialmente por "não haver uma legislação específica à respeito de crimes virtuais ou cibernéticos" (BARBOSA, 2020, p. 18), demonstrando que as lacunas legislativas comprometem sistematicamente a proteção das vítimas mais vulneráveis.

O paradigma de proteção efetiva às vítimas de fraudes online demanda, portanto, a superação da dicotomia entre eficiência punitiva e garantismo processual. A experiência demonstra que sistemas penais exclusivamente focados na repressão não apenas falham em prevenir novos delitos, como também negligenciam as necessidades específicas das vítimas de crimes digitais, particularmente aquelas em situação de vulnerabilidade social.

Julho - Dezembro
v.14, n.2, 2025
ISSN: 2674-6913
DOI: 10.35987

A construção deste novo paradigma exige transformações estruturais que perpassem desde a especialização dos operadores do direito até a criação de mecanismos diferenciados de atendimento às vítimas vulneráveis. A humanização do direito penal no contexto digital pressupõe o reconhecimento de que vítimas, autores e comunidade possuem dignidade inalienável que deve ser respeitada em todas as fases do processo.

Neste contexto, torna-se evidente a necessidade de superar a "ausência de força coercitiva das sanções", reconhecendo que "uma pena de detenção de três meses a um ano jamais seria suficiente para inibir e reprimir delitos", pois "a sanção branda ou inexistente não se mostra como uma solução viável, eficaz e suficiente à repressão" (SÁ; SILVA, 2020, p. 34). Esta crítica assume particular relevância nas fraudes digitais, onde a desproporcionalidade entre dano causado e sanção aplicada estimula a perpetuação delitiva.

As perspectivas futuras para um direito penal humanizado no combate às fraudes online apontam para a necessidade de integração entre justiça restaurativa, políticas públicas preventivas e mecanismos efetivos de reparação às vítimas. Esta abordagem multidimensional reconhece que a proteção efetiva não se esgota na resposta penal, mas requer articulação com políticas de inclusão digital, educação financeira e fortalecimento das redes de proteção social. A vulnerabilidade social que facilita a vitimização por fraudes online deve ser enfrentada através de políticas públicas integradas que atuem sobre suas causas estruturais.

Ademais, a utilização de tecnologias emergentes oferece oportunidades inéditas para aprimoramento da proteção às vítimas, desde sistemas de alerta precoce até mecanismos automatizados de bloqueio de transações suspeitas. Contudo, estas inovações devem ser implementadas com rigorosa observância aos princípios da transparência, proporcionalidade e proteção de dados pessoais, evitando que medidas protetivas se transformem em instrumentos de vigilância excessiva.

A consolidação de um Direito Penal humanizado e eficaz na proteção às vítimas de fraudes online representa, em última análise, um imperativo constitucional e civilizatório. A superação dos paradigmas exclusivamente punitivos em favor de abordagens integradas que considerem a vulnerabilidade social das vítimas não constitui apenas uma opção política, mas uma exigência decorrente dos compromissos assumidos pelo Estado brasileiro na efetivação dos direitos humanos e fundamentais. Somente através desta transformação paradigmática será possível construir um sistema de justiça penal verdadeiramente democrático, inclusivo e respeitoso da dignidade humana em todas as suas dimensões, especialmente no ambiente digital contemporâneo.

Julho - Dezembro
v.14, n.2, 2025
ISSN: 2674-6913
DOI: 10.35987

5. CONSIDERAÇÕES FINAIS

A presente pesquisa teve como propósito examinar criticamente o papel do Direito Penal na proteção dos direitos fundamentais das vítimas hipervulneráveis de fraudes digitais, em um contexto brasileiro marcado por desigualdade social, exclusão digital e crescimento exponencial da criminalidade cibernética. Partiu-se da constatação de que, embora a tecnologia tenha proporcionado avanços inegáveis em diversas esferas da vida cotidiana, ela também deu origem a novas formas de violação de direitos que afetam, de modo mais intenso, grupos já marginalizados ou com acesso limitado à informação e à proteção institucional.

A análise demonstrou que as fraudes digitais não são apenas um problema de segurança tecnológica, mas sobretudo uma questão social e de direitos humanos. Os dados colhidos em pesquisas oficiais e acadêmicas apontam que idosos, pessoas com baixa escolaridade, moradores de regiões periféricas e indivíduos com limitado acesso à internet estão entre os principais alvos de práticas criminosas como o phishing, os golpes bancários e os ataques de engenharia social. Tais práticas, muitas vezes, resultam não apenas em prejuízos econômicos significativos, mas também em abalos emocionais, constrangimento e perda de confiança nos sistemas digitais e nas instituições públicas.

Nesse cenário, verifica-se que o Direito Penal brasileiro, embora disponha de instrumentos normativos específicos — como a Lei nº 12.737/2012 (Lei Carolina Dieckmann), a Lei nº 14.155/2021 e disposições do Código Penal , ainda se mostra limitado quanto à sua capacidade de oferecer respostas céleres, eficazes e acessíveis às vítimas desses delitos. Soma-se a isso a carência de estrutura das polícias civis para lidar com crimes tecnológicos, a morosidade do Judiciário e a baixa taxa de elucidação e responsabilização dos agressores.

Além disso, a presente investigação evidenciou que a lógica tradicional do Direito Penal, centrada na repressão e na punição, precisa ser revisitada à luz de uma abordagem garantista, inclusiva e comprometida com os direitos fundamentais das vítimas. A efetividade penal, nesse contexto, não deve se limitar à imposição de sanções, mas deve também garantir o acesso à justiça, o acolhimento das vítimas e a reparação dos danos sofridos. Tal perspectiva encontra amparo tanto nos princípios constitucionais brasileiros quanto em tratados internacionais de direitos humanos, como a Convenção Americana sobre Direitos Humanos (Pacto de San José da Costa Rica) e a Convenção de Budapeste sobre Cibercrime.

A pesquisa também evidenciou que a hipervulnerabilidade das vítimas de crimes cibernéticos não é um fator apenas individual, mas estrutural. A desigualdade digital reflete a desigualdade social mais ampla do

Julho - Dezembro
v.14, n.2, 2025
ISSN: 2674-6913
DOI: 10.35987

país, tornando necessário repensar a proteção penal sob a ótica da interseccionalidade e da justiça social. A ausência de educação digital básica e o déficit informacional imposto às populações de baixa renda configuram um terreno fértil para a vitimização reiterada e a impunidade. Portanto, a efetivação de políticas públicas que promovam inclusão tecnológica é essencial para mitigar os danos causados pela criminalidade virtual.

Por fim, o enfrentamento das fraudes digitais deve ser concebido como um esforço coletivo e interinstitucional. O sistema de justiça penal, isoladamente, não possui os instrumentos adequados para lidar com a complexidade dos crimes digitais modernos. A resposta precisa envolver o fortalecimento das instituições, a promoção de direitos humanos, a educação da população e o aprimoramento da legislação penal. Somente assim será possível construir um arcabouço normativo e institucional verdadeiramente comprometido com a defesa da dignidade humana na era digital. Conclui-se, portanto, que o Direito Penal, para ser compatível com sua função protetiva em um Estado Democrático de Direito, deve caminhar de forma articulada com políticas de prevenção, inclusão e educação, garantindo que nenhuma vítima seja deixada para trás no avanço da sociedade da informação.

6. REFERÊNCIAS BIBLIOGRÁFICAS

BARRETO JÚNIOR, I. F.; RODRIGUES, C. B. Exclusão e inclusão digitais e seus reflexos no exercício de direitos fundamentais. Revista Direitos Emergentes na Sociedade Global, v. 1, n.1, jan.-jun., 2012. Disponível em: https://periodicos.ufsm.br/REDESG/article/view/5958/pdf. Acesso em 23 de julho de 2025.

BARBOSA, M. I. A. C. Crimes virtuais a evolução dos crimes cibernéticos e os desafios no combate. 2020. 24 f. Artigo Científico (Bacharelado em Direito) – Escola de Direito e Relações Internacionais, Curso de Direito, Pontifícia Universidade Católica de Goiás, Goiânia, 2020.

BRASIL. Constituição da República Federativa do Brasil de 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acessado em: 18/07/2025.

BRASIL. Decreto-Lei nº 2.848, de 7 de dezembro de 1940. Código Penal. Diário Oficial da União: seção 1, Rio de Janeiro, p. 1, 31 dez. 1940. Disponível em: https://www2.camara.leg.br/legin/fed/declei/1940-1949/decreto-lei-2848-7-dezembro 1940-412868-norma-pe.html. Acesso em: 20 julho 2025. BRASIL. Lei nº 12.737, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 – Código Penal; e dá outras providências. Diário Oficial

Julho - Dezembro
v.14, n.2, 2025
ISSN: 2674-6913
DOI: 10.35987

da União: seção 1, Brasília, DF, p. 1, 03 dez. 2012. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 20 julho 2025.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil – Marco Civil da Internet. Diário Oficial da União: seção 1, Brasília, DF, p. 1, 24 abr. 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 20 julho 2025.

BRASIL. Lei nº 13.431, de 4 de abril de 2017. Estabelece o sistema de garantia de direitos da criança e do adolescente vítima ou testemunha de violência. Diário Oficial da União, Brasília, DF, 5 abr. 2017. Disponível em:http://www.planalto.gov.br/ccivil_03/_ato2 Acesso em: 20 julho 2025.

CAMPOS, Y. de V. A evolução do Direito Penal frente às novas tecnologias: um estudo sobre os crimes virtuais de natureza sexual. 2018. 21 f. Artigo (Graduação em Direito) – Centro de Ciências Humanas e Sociais Aplicadas do Centro Universitário de Maringá, Maringá, 2018.

CASTEL, Robert. As metamorfoses da questão social: uma crônica do salário. 10. ed. Petrópolis: Vozes, 2013.

CASTELLS, M. A sociedade em rede, v. 1, 8ed. rev. amp., trad. Roneide Venâncio Majer, São Paulo: Paz e Terra, 2000.

DATASENADO. Pesquisa Nacional sobre Golpes Digitais. Brasília: Instituto DataSenado, 2024. Disponível em: https://www12.senado.leg.br/noticias/materias/2024/10/01/golpes-digitais-atingem 24-da-populacao-brasileira-revela-datasenado. Acesso em: 24 jul. 2025.

GOMES, Camila P. B. A exclusão digital como forma de violação dos direitos humanos. Revista Sapiência, v. 12, n. 4, p. 337–350, 2023.

JOHNSTONE Mike; PSAROULIS Geórgia. As armas Psicológicas que os golpistas usam, como se proteger delas. Disponível em: https://www.bbc.com/portuguese/articles/cn4nv22p6rlo Artigo Publicado na BBC. de Mike Johnstone e Geórgia Psaroulis, da Edith Cowan University, 2024. Acessado em: 18/08/2024.

LÉVY, P. . Cibercultura. São Paulo: Editora 34, 1999

PICAZIO, J. R. A.; SANCHES, S. H. D. F. N.; BARRETO JÚNIOR, I. F. A exclusão digital na sociedade da informação e o exercício da cidadania. Revista Direito & Paz, v. 1, n. 46, 2022. Disponível em: https://revista.unisal.br/lo/index.php/direitoepaz/article/view/1648. Acesso em 21 de julho de 2025.

ROSA, Fabrízio. Crimes de Informática. Campinas: Ed. Bokseller. 2002.

Julho - Dezembro
v.14, n.2, 2025
ISSN: 2674-6913
DOI: 10.35987

SÁ, D. S. O. Li. de; SILVA, P. P. Da ineficácia da lei Carolina Dieckmann na ocorrência de crimes virtuais. 2021. 28 f. Trabalho de Conclusão de Curso (Graduação em Direito) - Centro Universitário Una, Bom Despacho, 2021.

SANTOS, Boaventura de Sousa. Construindo as Epistemologias do Sul: para um pensamento alternativo de alternativas. Buenos Aires: CLACSO, 2018. v. 1. Disponível em: https://estudogeral.uc.pt/bitstream/10316/81474/1/Construindo%20as%20Epistemologias%20do%20Sul_Vol%201.pdf. Acesso em: 20 de julho de 2025

SARLET, Ingo Wolfgang. Dignidade da pessoa humana e direitos fundamentais na Constituição Federal de 1988. 10. ed. Porto Alegre: Livraria do Advogado, 2015.

SEN, Amartya. Desenvolvimento como liberdade. Tradução de Laura Teixeira Motta. São Companhia das Letras, 2010. Disponível em: https://www.companhiadasletras.com.br/trechos/80156.pdf

SILVA. Gilsimar Pinheiro da. Crimes Digitais: Evolução dos crimes e a aplicação do direito. Universidade 2021. Potiguar: Artigo científico. Disponível em: 46 https://repositorio.animaeducacao.com.br/bitstreams/65597262-4fec-4790-8267- 65d7f57bb5ed/download Acessado em: 20 de julho de 2025.

SORJ, B.; GUEDES, L. E. Exclusão digital: problemas conceituais, evidências empíricas e políticas públicas. Novos Estudos, 72, julho, 2005. Disponível em: https://www.scielo.br/j/nec/a/vZ6fSRKr6SDKBHP6vdxbGTP/?format=pdf&lang=pt. Acesso em 23 de julho de 2025.

TOCANTINS, Hortência Matos. Crimes Cibernéticos na atualidade: Desafios e impactos na sociedade moderna. Disponível em: https://www.jusbrasil.com.br/artigos/crimes-ciberneticos-na-atualidade-desafios eimpactos-na-sociedade-moderna/2104354886. Acessado em: 21 de julho de 2025.

Artigo recebido: 01.07.2025
Artigo publicado em: 30.12.2025