

CYBERCRIMES AND CIVIL LIABILITY: CHALLENGES AND LEGAL IMPACTS IN THE DIGITAL AGE

CIBERCRIMES E RESPONSABILIDADE CIVIL: DESAFIOS E IMPACTOS JURÍDICOS NA ERA DIGITAL

Eduardo Fardim Soares

Graduando em Direito, Faculdade de Ensino Superior de Linhares, Brasil

E-mail: eduardofasu45@gmail.com

Jakeline Martins Silva Rocha

Graduada em Direito pela UFMA - Universidade Federal do Maranhão. Especialista em Direito Empresarial pela FVC - Faculdade Vale do Cricaré. Especialista em Educação e Supervisão pela FVC. Mestra em Gestão Social, Educação e Desenvolvimento Regional pela FVC. Advogada. No Centro Universitário Vale do Cricaré é professora da Graduação em Direito e Coordenadora e orientadora do NPJ/UNIVC. Na FACELI - Faculdade de Ensino Superior de Linhares/ES/ bloco de Direito Privado. É Membro da CPA - Comissão Permanente de Avaliação/ Faceli.

Membro titular do CONSUP - Conselho Superior/Faceli e membro suplente do CONCUR - Conselho Curador da Fundação Faceli. É profa pesquisadora do grupo " Temas Avançados de Direito Privado". Conselheira da 12 Subseção, OAB/ES (2022-2024). Vice-diretora administrativa da ESA (norte do ES)-Escola Superior da Advocacia/ES (2019 a 2021). Secretária-Geral Adjunta da 12 Subseção/OAB-ES. 2025-2027). Procuradora-Geral da Fundação Faceli (2024-atual.) email :

jakeline.rocha@faceli.edu e jakeline.rocha@ivc.br

Recebido: 01/10/2025 – Aceito: 10/10/2025

Resumo

O artigo analisa os impactos da prática de crimes virtuais no âmbito da responsabilidade civil, evidenciando a crescente incidência de cibercrimes e seus reflexos nas relações interpessoais em ambientes digitais. A problemática central deste estudo é compreender até que ponto o direito

brasileiro é capaz de oferecer ferramentas eficazes de punição e prevenção diante dos desafios de anonimato e transnacionalidade imposta pela era digital. A pesquisa, de natureza bibliográfica e documental, fundamentou-se no Código Civil de 2002 e legislações específicas — como o Marco Civil da Internet e a Lei Geral de Proteção de Dados — e também a análise de doutrinas e jurisprudências. A metodologia utilizada conseguiu demonstrar lacunas normativas, a dificuldade de se utilizar os meios tradicionais para aplicação das normas e a necessidade da harmonização entre o Código Civil e a Legislação Especial. O estudo demonstra a importância e urgência da discussão sobre a proteção de direitos em ambientes virtuais, frente ao crescimento dos cibercrimes, que impactam tanto indivíduos como toda a coletividade. Com a análise crítica e comparativa com o ordenamento jurídico brasileiro tradicional e a legislação especial, apresentou resultados que demonstram um avanço perante a problemática, entretanto, evidência também a necessidade de atualizações normativas e jurisprudenciais para conseguir efetivar um ambiente virtual seguro e adequado para todos.

Palavras-chave: Responsabilidade civil; ambiente digital; cibercrimes; danos; proteção jurídica.

Abstract

This article analyzes the impacts of cybercrime on civil liability, highlighting the growing incidence of cybercrimes and their impact on interpersonal relationships in digital environments. The central issue of this study is understanding the extent to which Brazilian law offers effective punishment and prevention tools in the face of the challenges of anonymity and transnationality imposed by the digital age. The research, of a bibliographical and documentary nature, was based on the 2002 Civil Code and specific legislation—such as the Internet Civil Framework and the General Data Protection Law—as well as an analysis of doctrines and case law. The methodology used demonstrated regulatory gaps, the difficulty of using traditional means to enforce the rules, and the need for harmonization between the Civil Code and Special Legislation. The study demonstrates the importance and urgency of discussing the protection of rights in virtual environments, given the growth of cybercrimes, which impact both individuals and the community as a whole. Through critical and comparative analysis of the traditional Brazilian legal system and special legislation, results were presented that demonstrate progress in addressing the problem. However, they also highlight the need for regulatory and jurisprudential updates to create a safe and suitable virtual environment for everyone.

Keywords: Civil liability; digital environment; cybercrimes; damages; legal protection.

1 INTRODUÇÃO

Com o avanço das tecnologias da informação e comunicação, intensificou-se a interação entre indivíduos em ambientes digitais. Esse cenário trouxe novos desafios aos institutos clássicos do Direito Civil, especialmente no que se refere à responsabilidade civil por danos decorrentes de atos ilícitos praticados no espaço virtual. Os chamados cibercrimes, caracterizados por condutas lesivas em meio digital, afetam diretamente a convivência interpessoal e demandam respostas jurídicas adequadas.

O Código Civil de 2002 (arts. 186, 187 e 927) estabelece fundamentos para a reparação de danos, os quais foram complementados por legislações específicas, como o Marco Civil da Internet (Lei n. 12.965/2014) e a Lei Geral de Proteção de Dados (Lei n. 13.709/2018). Ainda assim, permanecem lacunas normativas e dificuldades na responsabilização de agentes e provedores de serviços digitais, apresentando a seguinte problemática, o ordenamento jurídico brasileiro está preparado e munido de mecanismos eficazes de responsabilização civil diante dos crescentes cometimentos de cibercrimes?

Diante de tal cenário, o objetivo deste estudo é analisar como a responsabilidade civil está sendo utilizada em relação ao cometimento dos cibercrimes, buscando como o ordenamento jurídico brasileiro vem se moldando ao ambiente digital. Assim, foi utilizada uma abordagem bibliográfica e documental para investigar a fundo o assunto, examinando jurisprudência, doutrina, dados jornalísticos e principalmente a legislação vigente. A metodologia utilizada permitiu compreender as fragilidades e avanços do direito brasileiro diante dos desafios contemporâneos impostos pela era digital.

A relevância desta pesquisa fica aparente ao demonstrar a urgência do debate a cerca da proteção dos direitos civis no ambiente digital e pela necessita de incrementação na legislação vigente aplicável à prática dos cibercrimes, demonstrando uma lacuna jurídica frente ao crescimento de práticas ilícitas virtuais. O aumento constante do cometimento de cibercrimes como fraudes digitais, *cyberbullying* e crimes contra honra em redes sociais, evidencia os impactos negativos causados a toda população exigindo uma resposta jurídica eficaz.

Dessa forma, esse estudo busca apresentar uma reflexão crítica perante a responsabilização civil a cerca do cometimento de atos ilícitos causados em

ambientes digitais, destacando seu papel como ferramenta de reparação e prevenção, direcionando para a harmonização do direito civil tradicional em relação as novas demandas da sociedade moderna.

2 RESPONSABILIDADE CIVIL EM AMBIENTES DIGITAIS

2.1 RESPONSABILIDADE CIVIL

Responsabilidade Civil trata-se de uma obrigação de reparar outrem por dano causado por ato ilícito, onde o Código Civil Brasileiro de 2002 arts. (186 e 187), prevê como ato ilícito, a relação de antagonismo entre a conduta humana voluntária e o ordenamento jurídico, onde causa uma obrigação de indenização (art. 927, CC). Nessa seara, Carlos Roberto Gonçalves (2024), a responsabilidade civil representa a restauração do equilíbrio, contraprestação e reparação do dano, evidenciando-se como uma forma jurídica de reparação por uma ação prejudicial decorrente de ato ilícito. Esse conceito é fundamental ao discutir questões legais relacionadas à conduta humana e suas consequências sobre terceiros.

Compreender a responsabilidade civil como um mecanismo de reparação, evidencia a relevância de análise de questões relevantes e contemporâneas, como os desafios legais decorrentes do avanço tecnológicos e em consonância com a prática de crimes em ambientes virtuais. Nesse sentido, Pablo Stolze Gagliano e Rodolfo Pamplona Filho(2020), enfatizam a importância da responsabilização pelos danos causados nesses ambientes à luz dos princípios do direito civil.

Para que haja o direito de indenizar, o entendimento doutrinário majoritário define quatro elementos essenciais a serem observados: a conduta, o dano, o nexo de causalidade e nos casos de responsabilidade subjetiva, a culpa. Para Cavalieri Filho, conduta é “o comportamento humano voluntário que se exterioriza através de uma ação ou omissão, produzindo consequências jurídicas” (2012, p. 25).

O segundo elemento essencial para configuração de indenização é o dano, que é a conduta de um ato ilícito artigos 186 e 187 CC (BRASIL, 2002), sendo de ordem patrimonial ou extrapatrimonial. As indenizações ligadas aos danos

causados em ambientes digitais, são em sua grande maioria de natureza extrapatrimonial, como nas hipóteses de difamação online, invasão da privacidade, *cyberbullying*. Não se excluindo a de natureza patrimonial como vazamento de dados e fraudes. Dano é a lesão a um interesse jurídico, que pode ser de natureza patrimonial ou moral (Gonçalves, 2019).

Nexo de causalidade constitui um elemento essencial para se delimitar a imputação da conduta lesiva cometida pelo agente, para que a obrigação de indenizar seja consequência direta e imediata do ato ilícito cometido.

O vínculo entre o prejuízo e a ação designa-se 'nexo causal', de modo que o fato lesivo deverá ser oriundo da ação, diretamente ou como sua consequência previsível. Tal nexos representa, portanto, uma relação necessária entre o evento danoso e a ação que o produziu, de tal sorte que esta é considerada como sua causa. — Maria Helena Diniz (2012, p. 129).

O último elemento essencial para se caracterizar a obrigação de indenizar por dano ou ato ilícito, levando ao agente o dever de se responsabilizar civilmente é a culpa, caracterizada por negligência, imprudência ou imperícia (culpa stricto sensu) e podendo se caracterizar como dolo – quando há a intenção de prejudicar – Rui Stoco (2007, p. 133). Na responsabilidade subjetiva, torna-se indispensável sua comprovação, por outro lado na responsabilidade objetiva basta que haja nexos de causalidade entre a conduta e o dano.

2.2 DANOS DIGITAIS: DEFINIÇÃO E TIPOLOGIA

Danos digitais se configura como uma categoria de lesão a direitos, que surge a partir da crescente digitalização das relações sociais entre indivíduos, gerando afronta aos direitos constitucionais previsto no art. 5º, X CF/88, “são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação” (BRASIL, 1988).

Para o sociólogo Polonês Zygmunt Bauman, vivemos em tempos voláteis e que estão em constante mudanças.

As instituições e estruturas sociais já não são sólidas e duráveis, mas fluidas e maleáveis, as formas de vida, as relações e as identidades se tornaram

provisórias e descartáveis, exigindo de cada indivíduo uma constante adaptação.

Nesse sentido, o pensamento do sociólogo apresenta uma realidade que a sociedade está tendo que se adaptar, a interação de indivíduos em ambientes digitais, que se tornou cada vez mais instável causado pela falta de respaldo jurídico que esses novos modos de interação ocasionam.

Ao abordar o tema, podemos visualizar diversos tipos de danos que são frequentemente sofridos pelos usuários em ambientes virtuais: os danos materiais, ligados a vazamentos de dados, clonagem de cartões, fraudes eletrônicas e uso indevido de informações de usuários, ocasionando prejuízo financeiro. Danos morais, ocasionado pelo uso indevido de imagem, violação da privacidade, propagação de informações falsas (*fake news*), afetando a relação direta de seus usuários, e os danos coletivos ou difusos, que ocorre com o vazamento de dados em grande proporção de usuários, “Cerca de 290 mil clientes da concessionária de energia Enel em Osasco, na Grande São Paulo, tiveram informações sensíveis vazadas após falha de segurança”. (Aragão, 2022).

2.3 RESPONSABILIDADE CIVIL DIGITAL

Com o advento da Internet o modo de comunicação ficou muito mais rápido e fácil, diminuindo a distância entre os usuários de ambientes virtuais, ocasionando em uma das maiores vertentes do ordenamento jurídico contemporâneo. Nesse viés, surgem desafios à proteção e prevenção de danos materiais, morais, coletivos e difusos praticados por meio eletrônico.

Para Carlos Roberto Gonçalves (2021), a responsabilidade civil possui um caráter dinâmico, e necessita se adaptar as novas realidades da interação de indivíduos em ambientes digitais. Nessa seara, Guilherme Magalhães Martins (2020), explica que as relações virtuais privadas que não são de natureza consumerista, podem ser causadoras de danos a terceiros, onde os responsáveis necessitam ser responsabilizados. Esse cenário guarda semelhança com o modelo de responsabilização pelos danos imposto aos prestadores de serviços, tal como previsto no Código de Defesa do Consumidor (CDC). Maria Helena Diniz (2019),

ênfatiou que a reparaç o dessas novas rela  es sociais, devem ser evoluir de acordo com os novos riscos sociais, abrangendo assim, os novos danos causados pela evolu  o da intera  o entre esses indiv duos.

Um dos aspectos mais importantes a serem analisados no regime de responsabilidade civil digital,   a prote  o da privacidade e dos dados dos usu rios. Nesse sentido, o ordenamento jur dico brasileiro implementou leis espec ficas como o Marco Civil da Internet (2014) e a Lei Geral de Prote  o de Dados Pessoais (2018), para tentar coibir esses danos e punir os causadores, este que podem ser cidad os ou provedores.

Nesse sentido, podemos analisar no seguinte julgado s  STJ:

Ao oferecer um servi o por meio do qual se possibilita que os usu rios divulguem livremente suas opini es, deve o provedor de conte do ter o cuidado de propiciar meios para que se possa identificar cada um desses usu rios, coibindo o anonimato e atribuindo a cada imagem uma autoria certa e determinada. Sob a  tica da dilig ncia m dia que se espera do provedor, do dever de informa o e do princ pio da transpar ncia, deve este adotar as provid ncias que, conforme as circunst ncias espec ficas de cada caso, estiverem ao seu alcance para a individualiza o dos usu rios do site, sob pena de responsabiliza o subjetiva por culpa in omittendo. Precedentes. Uma vez ciente do ajuizamento da a o e da pretens o nela contida – de obten o dos dados de um determinado usu rio – estando a quest o subjudice, o m nimo de bom senso e prud ncia sugerem a iniciativa do provedor de conte do no sentido de evitar que essas informa es se percam. Essa provid ncia   condizente com a boa-f  que se espera n o apenas dos fornecedores e contratantes em geral, mas tamb m da parte de um processo judicial, nos termos dos arts.4. ,III,do CDC,422doCC/02e14doCPC.As informa es necess rias   identifica o do usu rio devem ser armazenadas pelo provedor de conte do por um prazo m nimo de 03 anos, a contar do dia em que o usu rio cancela o servi o. (STJ, REsp 1.417.641/RJ, 3.  Turma, Rel. Min. Nancy Andrighi, j. 25.02.2014, DJe 10.03.2014).

Ao analisar a decis o do Tribunal, podemos visualizar a import ncia da responsabiliza o dos provedores, para que haja a individualiza o e quebra de sigilo de seus usu rios, ponde assim, serem responsabilizados pelo seus atos danosos em intera  es online. Podemos ver isso na pr tica com a pris o de um indiv duo que ame o o influenciador Felca, ap s a quebra do sigilo de seus dados por determina o judicial (Tavares,2025).Nessa  tica,a responsabilidade civil digital se mostra como um regime jur dico do direito civil brasileiro de extrema import ncia nos tempos atuais, mostrando a necessidade de an lise cautelosa e

imperiosa para que haja uma harmonização entre os princípios do direito civil tradicional e a demanda das novas relações entre indivíduos em ambientes online.

3 CRIMES VIRTUAIS (CIBERCRIMES)

3.1 O SURGIMENTO DO AMBIENTE VIRTUAL

Na década de 1960 Tim Berners-Lee abordou a ideia “Rede das Redes”, para denominar a nova era da tecnologia que culminou com o surgimento da Internet. A nova rede de comunicação teve seu surgimento no auge da Guerra Fria, onde o Departamento de Defesa dos EUA criou a *ARPANET*, com o objetivo de interligar bases militares e de pesquisa durante o conflito.

No Brasil, foi nos anos 1980 que se iniciou o período de implementação e estruturação da nova era digital no país. Um marco que simbolizou essa implementação foi o primeiro ponto de acesso oficial à Internet no Brasil, que ocorreu no ano de 1991.

Contudo, com o surgimento desses novos “espaços digitais”, trouxe consigo novos desafios para os princípios clássicos do sistema jurídico. Com essas novas interações entre os indivíduos, surgiram os chamados cibercrimes, onde são condutas ilícitas praticadas por meio da internet (Costa, 2019, p. 45). Nesse sentido, o sistema jurídico deve se moldar para responsabilizar os autores desses atos ilícitos.

3.2 PRINCIPAIS CIBERCRIMES

Esses crimes que são cometidos em ambiente virtual, englobam uma gama de atividades ilícitas, onde se utiliza a internet e produtos eletrônicos para o cometimento desses atos. Esses crimes podem ser divididos em crimes cibernéticos próprios, onde o alvo de invasão é o dispositivo eletrônico (Código Penal, art. 154-A), e em crimes cibernético impróprios, que de acordo com Patrícia Peck (2020), “[...]quando a informática constitui apenas o meio para a prática do delito, como nos casos de estelionato, pedofilia ou crimes contra a honra praticados em ambiente digital.”

3.1.1 Phishing e fraude online

Constitui como uma das modalidades mais utilizadas para a prática de fraudes digitais, onde o indivíduo induz a vítima a fornecer dados pessoais, senhas e informações bancárias, através de mensagens que induzem a vítima a fornecer esses dados, aplicativos e sites falsos que simulam instituições legítimas. Ocasionalmente ao dano tanto de indivíduos, como de empresas.

Somente em 2024 foram registrados mais de 2,1 milhões de estelionatos digitais no Brasil, de acordo com o 19º Anuário Brasileiro de Segurança Pública (2025). Ficando evidente que a fraude online desrespeita o art. 171 do Código Penal (1940) tipificado como crime de estelionato e atualizado pela Lei 14.155/2021, em seus § 2º-A e §2º-B, que aumentou a pena deste crime praticado em ambiente digital. A prática de Phishing e fraude online leva a responsabilização também em âmbito civil, envolvendo a reparação aos danos causados às vítimas. Nesse sentido, Guilherme Magalhães Martins (2020), enfatiza que os provedores também podem ser responsabilizados civilmente por não terem fornecido a segurança necessária para proteção de dados de seus usuários. Segundo Salgado (2024), entre 2022 e 2023, os estelionatos subiram 13,6% no meio virtual.

3.2.1 Cyberbullying

Caracteriza-se a intimidação sistemática(*bullying*) quando há violência física ou psicológica em atos de intimidação, humilhação ou discriminação Lei nº13.1855/2015, se enquadrando também na modalidade online.

Diferente da forma tradicional, o *cyberbullying* possui um alcance muito mais abrangente, onde o anonimato contribui para a disseminação do ato lesivo e dificulta a responsabilização dos indivíduos que os cometem.

Para Patrícia Peck Pinheiro (2020, p.135), “o *cyberbullying* é uma das faces mais cruéis da violência digital, pois expõe a vítima a um linchamento público que não encontra barreiras geográficas e temporais”.

Os impactos sofridos pelas vítimas são expressivos e afetam a saúde mental e física das vítimas, contribuindo para problemas sociais e emocionais graves que prejudicam a interação social de quem sofre essa conduta lesiva.

As vítimas de cyberbullying apresentam maior propensão ao desenvolvimento de sintomas de ansiedade, depressão, ideação suicida e isolamento social, sendo os impactos emocionais e psicológicos frequentemente duradouros e prejudiciais à qualidade de vida. (RONDINA et al., 2016, p. 89).

Um estudo realizado por pesquisadores da Universidade Federal de Minas Gerais (UFMG) e do Instituto Brasileiro de Geografia e Estatística (IBGE), revelou que 13,2% dos jovens afirmaram já ter sofrido *cyberbullying*, onde foram ouvidos 159.245 entre 13 e 17 anos do ensino fundamental e médio de escolas públicas e privadas. Outrossim, um levantamento realizado pelo Colégio Notarial do Brasil (CNB) e divulgado pelo jornal folha de São Paulo, em 2024 foram solicitadas 145,3 mil atas notariais para comprovar *cyberbullying*, 14% a mais do que em 2023.

Nesse viés, é de extrema importância responsabilizar os autores de tal infração penal, tanto na esfera criminal como também na esfera civil. Isso somente será possível com a aplicação de políticas públicas eficazes, a educação digital adequada e a responsabilização de indivíduos e provedores que contribuem para a disseminação do *cyberbullying*.

3.2.2 Crimes Contra Honra

A honra, instituto jurídico resguardado pela CF/88 em seu art. 5º, X, garante a dignidade e como o indivíduo é visto perante a sociedade, refletindo-se diretamente a autoestima destes. Assim, é um bem jurídico que deve ser resguardado, onde ofendê-la, trará malefícios diretos para as vítimas perante a sociedade.

De acordo com Bitencourt (2017):

A honra, independentemente do conceito que se lhe atribua, tem sido através dos tempos um direito ou interesse penalmente protegido. [...] A proteção da honra, como bem jurídico autônomo, não constitui interesse exclusivo do indivíduo, mas da própria coletividade, que tem interesse na preservação da honra, da incolumidade moral e da intimidade, além de

outros bens jurídicos indispensáveis para a harmonia social. Quando determinadas ofensas ultrapassam esses limites toleráveis justifica-se a sua punição, que, na disciplina do Código Penal vigente, pode assumir a forma de calúnia, difamação e injúria. (BITENCOURT, 2017, p.314).

Os crimes contra a honra, calúnia, difamação e injúria estão tipificados no Código Penal Brasileiro (1940), entre os arts. 138 e 140. Calúnia e difamação, a honra tutelada é a objetiva, que diz respeito a reputação do indivíduo perante a sociedade. Enquanto na injúria, a honra tutelada é a subjetiva, que representa a proteção a dignidade que cada pessoa tem a si mesmo.

“A calúnia consiste em atribuir falsamente a alguém a prática de fato definido como crime, atentando contra sua honra objetiva e sujeitando o agente à responsabilização penal e civil.” Capaz (2021). Nesse sentido, o autor de tal delito deverá ser responsabilizado criminal e civilmente, se praticado em ambiente físico ou virtual.

Difamação, de acordo com o Código Penal (1940), trata-se de um delito onde o indivíduo imputa a outrem informações inverídicas perante a sociedade, que diferente da calúnia, não são falácias sobre atos criminosos da vítima.

De acordo com Nucci (2017), a injúria tem o mesmo objetivo de ofensa e insulta, porém, ela atinge diretamente a pessoa da vítima, desrespeitando sua dignidade ou moral. Ela está prevista no art. 140 do Código Penal.

Nesse viés, os crimes contra a honra são passíveis de serem praticados em ambientes virtuais, onde o anonimato dos autores e facilidade de disseminação de acusações e informações falsas, corroboram para causar danos significativos para a moral e saúde mental das vítimas.

Podemos verificar um entendimento do TJSP sobre o tema:

APELAÇÃO. Ação de obrigação de fazer c/c indenização por danos materiais e morais. Golpe pelo aplicativo Whatsapp. Clonagem do perfil do filho da autora. Terceiros que se passaram pelo filho da autora, solicitando transferência bancária, o que foi feito pela requerente. Sentença de improcedência. Apelação manejada pela autora. EXAME: preliminar de ilegitimidade passiva afastada. Facebook e Whatsapp que integram o mesmo grupo econômico. Precedentes. Falha na prestação de serviços não vislumbrada. Perfil que não utilizava fotografia ou número de telefone do filho da autora. Transferência bancária de valor considerável realizada pela requerente em benefício de terceiros, sem contatar seu filho previamente.

Ausência de provas de tentativa de contato com a ré para solução do problema ou bloqueio do perfil. Morosidade e desídia não vislumbradas. Culpa exclusiva da vítima, nos termos do art. 14, § 3, II do Código de Defesa do Consumidor. Sentença mantida. Honorários sucumbenciais majorados. RECURSO IMPROVIDO

Dessa forma, podemos analisar que a jurisprudência vem se moldando para punir os indivíduos que praticam tais atos que prejudicam a sociedade como um todo.

4 IMPACTOS NO ÂMBITO CIVIL REFERENTE AS PRÁTICAS DOS CIBERCRIMES E A REPERCUSSÃO JURÍDICA

4.1 COMPROVAÇÃO DE DANO E A RESPONSABILIDADE CIVIL

O dano, é com toda certeza o ponto central para o sujeito ser responsabilizado civilmente. Nesse sentido, os impactos ocasionados pela prática de atos lesivos em ambientes digitais afetam desde o indivíduo até a coletividade, pois a revolução tecnológica promoveu uma mudança no mundo das relações interpessoais e jurídicas. Tais condutas lesivas têm a possibilidade de o autor ser responsabilizado a indenizar a vítima por danos morais e materiais.

O art. 927 do Código Civil, é claro ao afirmar que “aquele que, por ato ilícito, causar dano a outrem, fica obrigado a repará-lo”. Danos esses que são de ordem material ou imaterial. Entretanto, para que haja a responsabilização civil, necessita além da comprovação do dano, como também comprovação dos demais pressupostos já apresentados, a conduta ilícita e o nexo de causalidade.

No ambiente digital, a comprovação do dano se torna uma tarefa mais complexa, pois a materialização do dano se dá na maioria das vezes de forma intangível, atingindo o emocional, a reputação e ocasionando a perda de oportunidades da vítima.

Para (CAVALIERI FILHO, 2012, p. 52), quando se trata de nexo de causalidade, o ordenamento jurídico brasileiro adota a teoria da causalidade adequada, onde só considera causa a ocorrência, que de forma concreta e direta deu origem ao dano. Nesse sentido, só será responsabilizado o agente que comete a conduta ilícita, sendo essencial o cometimento do ato para sua

responsabilização.

Em suma, a comprovação dos danos cometidos em ambientes digitais é indispensável para se responsabilizar o agente, para isso é importante que a vítima apresente provas consistentes como prints de tela, registros eletrônicos e até o rastreamento do endereço de IP se possível, para que demonstre o nexo entre o ato lesivo e o dano sofrido.

4.2 DA RESPONSABILIZAÇÃO DOS PROVEDORES

O Marco Civil da Internet (BRASIL, 2014), estabelece que a responsabilidade civil das plataformas digitais se manifesta de maneira limitada, onde será responsabilizada após prévia ordem judicial, dificultando a comprovação dos pressupostos necessários para responsabilização dos indivíduos e consequentemente atordoando os direitos das vítimas.

Assim versa o art. 19:

O provedor de aplicações de internet somente poderá ser responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros se, após ordem judicial específica, não tomar as providências para [...] tornar indisponível o conteúdo apontado como infringente (BRASIL, 2014).

Dessa forma, o dispositivo jurídico vem sofrendo com uma série de críticas e acusações de inconstitucionalidade, uma vez que, limita a proteção dos direitos da personalidade. Nesse sentido, o STF julgou os temas 987 e 533 de repercussão geral, onde a corte suprema reconheceu que a regra do art. 19 do Marco Civil da Internet é parcialmente inconstitucional, uma vez que nada impede que as plataformas retirem conteúdos considerados ofensivos que já foram matéria de decisões judiciais condenatórias, devendo assim remover após notificação judicial ou extrajudicial.

Portando, podemos analisar que o ordenamento jurídico vem se moldando para que haja a devida prevenção e responsabilização aos autores das condutas lesivas cometidas em ambientes digitais.

4.3 LEGISLAÇÃO APLICÁVEL

O direito brasileiro vem tentando acompanhar a evolução das relações interpessoais acometidas pelo avanço da tecnologia. Nesse sentido, ROMÃO e MATOS destacam:

Dada a grande variação de situações e tipos de crimes cometidos no âmbito virtual/Cibernético, o combate aos crimes virtuais continua sendo um grande desafio para o Direito Brasileiro, não havendo até o momento um consenso da melhor definição para crimes relacionados à tecnologia, tendo em vista que os danos causados trazem inúmeros impactos psicológicos, econômicos e financeiros. (2023, online)

A Lei nº 12.737, conhecida como “Lei Carolina Dieckmann” e a Lei nº 13.709, conhecida como Lei Geral de Proteção de Dados (LGPD) e o Marco Civil da Internet (2014), são os principais dispositivos que protegem a sociedade em face do cometimento dos cibercrimes. Resguardando direitos como a invasão de dispositivos eletrônicos, a distribuição de informações e conteúdos sem o consentimento das vítimas e da privacidade e proteção de dados.

Legislações clássicas do ordenamento jurídico brasileiro como a Constituição Federal (1988), o Código Civil (2002) e o Código de Defesa do Consumidor (1990), fornecem uma proteção mais ampla aos direitos individuais e coletivos. Entretanto, como o cometimento dos crimes cibernéticos digitais transcendem as fronteiras transnacionais e o anonimato dificulta a identificação dos indivíduos, têm-se a necessidade de criação de leis específicas para que os impactos causados por danos em ambientes digitais diminuam.

4.4 PREVENÇÃO E MITIGAÇÃO DOS CIBERCRIMES

A responsabilidade civil nesse sentido deve buscar instrumentos jurídicos e sociais para que os autores das condutas ilícitas em meios digitais sejam responsabilizados, como também exerce um papel crucial para a sociedade que é a diminuição desses atos infracionais. Nesse viés, Gonçalves (2022) disserta “A responsabilidade civil cumpre, portanto, não apenas uma função reparatória, mas igualmente preventiva, constituindo instrumento de inibição de condutas danosas.”

Outrossim, medidas como a implementação de educação infantojuvenil digital, o incentivo a denúncia de condutas ilícitas em ambientes digitais e o fácil acesso ao judiciário contribuem para que o Estado, a sociedade civil e o setor privado combatam a disseminação dos cibercrimes. A lei Geral de Proteção de Dados (Brasil, 2018) é um exemplo de instrumento jurídico que previne e pune o cometimento de crimes virtuais.

Nessa seara, o comprometimento entre o setor público e privado torna se uma importante arma contra a propagação desses crimes, onde o desenvolvimento de sistemas de proteção virtual como antivírus, *firewalls* e programas que facilitam a coleta de dados dos usuários facilitariam a prevenção e mitigação do problema.

Portanto, o equilíbrio da prevenção e da mitigação dos atos lesivos cometidos em ambientes virtuais em concomitante com políticas públicas e legislativas eficazes, educação digital, conscientização da população e investimento privado, fará com que grande parte dos danos acometido pela prática de cibercrimes sejam prevenidos e os autores devidamente responsabilizados.

5 CONSIDERAÇÕES FINAIS

O estudo evidenciou que os cibercrimes constituem um dos maiores desafios contemporâneos para o Direito Civil, em razão de sua natureza transnacional, do anonimato de seus agentes e da rapidez com que os danos se propagam no ambiente digital. Embora o Brasil disponha de instrumentos relevantes — como o Marco Civil da Internet, a LGPD e a Lei Carolina Dieckmann —, a responsabilização civil ainda enfrenta entraves relacionados à comprovação do dano, ao nexo de causalidade e à limitação da responsabilidade dos provedores.

Os dados analisados demonstram o aumento expressivo de crimes como estelionato digital, *cyberbullying* e delitos contra a honra, evidenciando a urgência de medidas preventivas e reparatórias mais eficazes. Constatou-se, ainda, a necessidade de políticas públicas integradas, educação digital e maior cooperação entre Estado, sociedade civil e setor privado.

Conclui-se que o fortalecimento da responsabilidade civil digital é essencial para garantir a proteção dos direitos da personalidade, assegurar a reparação de danos e promover um ambiente virtual seguro e confiável. O tema permanece aberto a novos estudos, sobretudo quanto à harmonização entre direito interno e normas internacionais, indispensável em um contexto de crescente interconexão global.

REFERÊNCIAS

ARAGÃO, Alexandre. **5 grandes vazamentos de dados no Brasil – e suas consequências**. JOTA, São Paulo, 28 jan. 2022. Disponível em: <https://www.jota.info/tributos-e-empresas/mercado/vazamentos-de-dados-no-brasil>. Acesso em: (25/08/2025).

BAUMAN, Zygmunt. **Modernidade Líquida**. Tradução de Plínio de P. Martins. Rio de Janeiro: Zahar, 2001.

BITENCOURT, Cezar Roberto. **Tratado de Direito Penal: parte especial 2, dos crimes contra a pessoa**. 17. ed. São Paulo: Saraiva, 2017.

BRASIL. CC. **Código Civil**. Lei 10.406, de 10 de janeiro de 2002.

BRASIL. CDC. **Código de Defesa do Consumidor**. Lei 8.078, de 8 de setembro de 1990.

BRASIL. CF. **Constituição Federal**. 1988

BRASIL. Decreto-Lei nº 2.848, de 07 de dezembro de 1940. **Código Penal**. Diário Oficial da União, Rio de Janeiro, 31 dez. 1940.

BRASIL. Lei n. 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de**

Dados Pessoais (LGPD). Diário Oficial da União: seção 1, Brasília, DF, n. 159, p. 59-64, 15 ago. 2018.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. **Estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil.** Diário Oficial da União, Brasília, DF, 24 abr. 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011_2014/2014/lei/l12965.htm. Acesso em: 31 ago. 2025.

BRASIL. Lei nº 13.185, de 6 de novembro de 2015. **Institui o Programa de Combate à Intimidação Sistemática(bullying).** Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/l13185.htm. Acesso em: 27 ago. 2025.

BRASIL. Ministério das Comunicações. **Plano Nacional de Banda Larga (PNBL).** Brasília: Ministério das Comunicações, 2010. Disponível em: <https://www.gov.br/mcom/pt-br/assuntos/plano-nacional-de-banda-larga>. Acesso em: 27 ago. 2025.

BRASIL. STJ, **REsp 1.417.641/RJ**, 3.^a Turma, Rel. Min. Nancy Andrighi, j. 25.02.2014, DJe 10.03.2014.

CAPEZ, Fernando. **Curso de direito penal: parte especial**, arts. 121 a 212. 18. ed. São Paulo: Saraiva, 2021. v. 2.

CASTELLS, Manuel. **A sociedade em rede.** 8. ed. São Paulo: Paz e Terra, 2003.

CGI.BR – **Comitê Gestor da Internet no Brasil. História da Internet no Brasil.** São Paulo: CGI.br, 2019. Disponível em: <https://www.cgi.br>. Acesso em: 27ago.2025.

COSTA, Marco Aurélio Rodrigues da. **Crimes cibernéticos e proteção de dados pessoais**. Belo Horizonte: Fórum, 2019.

DE SANTANA, Katiene Gouveia; DOS SANTOS, Keila Oliveira. **CRIMES CONTRA A HONRA NO AMBIENTE VIRTUAL**. Dataveni@, v. 11, n. 1, p. 34-34, 2023. (TJ-SP - AC: 10002037020228260390 Nova Granada, Relator.: Celina Dietrich Trigueiros, Data de Julgamento: 27/06/2023, 10ª Câmara de Direito Público, Data de Publicação: 27/06/2023).

DINIZ, Maria Helena. **Curso de Direito Civil Brasileiro: responsabilidade civil**. 26. ed. São Paulo: Saraiva, 2012. v. 7.

DINIZ, Maria Helena. **Curso de direito civil brasileiro: responsabilidade civil**. 33. ed. São Paulo: Saraiva Educação, 2019.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais: elementos da formação da autoridade, de proteção de dados**. Rio de Janeiro: Renovar, 2006.

FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA. **19º Anuário Brasileiro de Segurança Pública. São Paulo: FBSP, 2025**. Disponível em: <https://forumseguranca.org.br/publicacoes/anuariobrasileiro-de-seguranca-publica/>. Acesso em: 27 ago. 2025.

GAGLIANO, Pablo Stolze; PAMPLONA FILHO, Rodolfo. **Novo Curso de Direito Civil: Responsabilidade Civil**. 18. ed. São Paulo: Saraiva Educação, 2020.

GLOBO. **Polícia de SP prende homem acusado de fazer ameaças ao youtuber Felca**. G1: São Paulo, 25 ago. 2025. Disponível em: <https://g1.globo.com/sp/sao-paulo/noticia/2025/08/25/policiade-sp-prende-homem-acusado-de-fazer-ameacas-ao-youtuber-felca.ghtml>. Acesso em: 26 ago 2025.

GONÇALVES, Carlos Roberto. **Direito Civil Brasileiro. 17. ed.** São Paulo: Saraiva Educação, 2019. v. 4: Responsabilidade Civil.

GONÇALVES, Carlos Roberto. **Direito civil brasileiro: Responsabilidade civil.** 119. ed. São Paulo: SaraivaJur, 2024. v. 4.

GONÇALVES, Carlos Roberto. **Responsabilidade civil. 18. ed.** São Paulo: Saraiva Educação, 2021.

GONÇALVES, Carlos Roberto. **Responsabilidade civil. 19. ed.** São Paulo: Saraiva, 2022.

INSTITUTO BRASILEIRO DE DIREITO DE FAMÍLIA (IBDFAM). **Registros de cyberbullying aumentam um ano após inclusão no Código Penal.** IBDFAM, 07 abr. 2025. Disponível em: <https://ibdfam.org.br/noticias/12780/Registros+de+cyberbullying+aumentam+um+ano+ap%C3%B3s+inclus%C3%A3o+no+C%C3%B3digo+Penal>. Acesso em: 31 ago. 2025.

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

MEDEIROS, Alex Cristhian Rodrigues de. **Deepfakes e responsabilidade civil: análise jurídica sobre a reparação por atos ilícitos no ambiente digital.** 2025.

NUCCI, Guilherme de Souza. **Manual de Direito Penal.17.ed.** Rio de Janeiro: Forense, 2017.

PINHEIRO, Patrícia Peck. **Direito digital. 7. ed.** São Paulo: Saraiva Educação, 2020.

ROMÃO, Erick Ferreira; MATOS, Manoel Alfredo Barbosa de. **Avanços e retrocessos na responsabilização dos crimes virtuais**. 2023. Trabalho de Conclusão de Curso. Acesso em: 31 ago. 2025.

RONDINA, J. M. ; MOURA, J. L. ; CARVALHO, M. D. de. **Cyberbullying: o complexo bullying da era digital**. R. Saúd. Digi. Tec. Edu., Fortaleza, v. 1, n. 1, p. 20-41, jan./jul. 2016.

SALGADO, Felipe. **Golpes virtuais crescem no país, enquanto crimes de rua caem**. Poder360, 21 jul. 2024. Disponível em: https://www.poder360.com.br/seguranca-publica/golpes-virtuais-crescem-no-pais-enquanto-crimes-de-rua-caem/?utm_source=chatgpt.com. Acesso em: 28 ago. 2025.

SILVA, Hellen Eduarda Rodrigues et al. **RESPONSABILIDADE CIVIL NA ERA DIGITAL: Desafios e perspectivas**. Revista Acadêmica Online, v. 10, n. 50, p. 1-18, 2024.

STOCO, Rui. **Tratado de responsabilidade civil: doutrina e jurisprudência**. 7. ed. São Paulo: Revista dos Tribunais, 2007.

SUPREMO TRIBUNAL FEDERAL. **Informação à sociedade: questões pendentes no julgamento do Marco Civil da Internet**. Brasília, DF, 2025. Disponível em: https://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/Informac807a7710a768SociidadeArt19MCI_vRev.pdf. Acesso em: 31 ago. 2025.

VICENTE, Isabella Cerqueira. **A responsabilidade civil nos crimes virtuais**. 2024.