CURSO DE DIREITO

THAYNARA GABRIELA DA SILVA SOARES

CRIMES CIBERNÉTICOS NAS PLATAFORMAS DIGITAIS: DIFAMAÇÃO

Cuiabá/MT

2025

CURSO DE DIREITO

THAYNARA GABRIELA DA SILVA SOARES

CRIMES CIBERNÉTICOS NAS PLATAFORMAS DIGITAIS: DIFAMAÇÃO

Projeto de monografia apresentado à Banca Avaliadora do Departamento de Direito, da Faculdade Fasipe Cuiabá, como requisito para a obtenção do título de Bacharel em Direito.

Orientador(a): Prof. Sonny Jacyntho Taborelli da Silva

Cuiabá/MT
2025

THAYNARA GABRIELA DA SILVA SOARES

CRIMES CIBERNÉTICOS NAS PLATAFORMAS DIGITAIS: DIFAMAÇÃO

Projeto de monografia apresentado à Banca Avaliadora do Curso de Direito – da Faculdade Fasipe Cuiabá como requisito para a obtenção do título de Bacharel em Direito.

Aprovado em ____/____/_____

Sonny Jacyntho Taborelli da Silva
Professor(a) Orientador(a):
Departamento de Direito – FASIPE

Professor(a) Avaliador(a):
Departamento de Direito – FASIPE

Professor(a) Avaliador(a):
Departamento de Direito – FASIPE

Olmir Bampi Junior
Coordenador do Curso de Direito

Cuiabá/MT
2025

SOARES, Thaynara Gabriela da Silva. Crimes cibernéticos nas plataformas digitais: Difamação. 2025. 40 folhas. Trabalho de Conclusão de Curso – Faculdade Fasipe Cuiabá.

RESUMO

O presente trabalho aborda os crimes cibernéticos nas plataformas digitais, com enfoque no delito de difamação. A crescente digitalização das relações humanas e a expansão da internet impulsionaram a prática de ilícitos virtuais, especialmente os que atingem a honra das pessoas. A difamação digital, amplamente disseminada em redes sociais, caracteriza-se pela imputação de fato ofensivo à reputação de outrem, mesmo que verdadeiro. O estudo destaca a falsa sensação de anonimato como incentivadora da impunidade, dificultando a responsabilização dos ofensores. A pesquisa adota metodologia bibliográfica, com base em obras recentes e legislação atual, como o Marco Civil da Internet, a Lei Geral de Proteção de Dados (LGPD) e a Lei Carolina Dieckmann. Além da análise jurídica, o trabalho examina os métodos de fiscalização utilizados pelas autoridades, o papel das plataformas digitais e a importância da educação digital como ferramenta de prevenção. Conclui-se que o combate à difamação digital exige uma atuação integrada entre o Judiciário, os provedores de internet e a sociedade, aliando repressão penal, conscientização dos usuários e atualização legislativa. O respeito à dignidade humana deve prevalecer no ambiente virtual, assegurando-se o equilíbrio entre liberdade de expressão e proteção da reputação.

Palavras-chave: Crimes cibernéticos; Difamação digital; Liberdade de expressão.

SOARES, Thaynara Gabriela da Silva. Cybercrimes on digital platforms: Defamation. 2025. 40 pages. Trabalho de Conclusão de Curso – Faculdade Fasipe Cuiabá.

ABSTRACT

This paper addresses cybercrimes on digital platforms, with a focus on the crime of defamation. The increasing digitalization of human relations and the expansion of the Internet have driven the practice of virtual crimes, especially those that affect people's honor. Digital defamation, widely disseminated on social networks, is characterized by the imputation of an offensive fact to the reputation of another, even if true. The study highlights the false sense of anonymity as an incentive for impunity, making it difficult to hold offenders accountable. The research adopts a bibliographic methodology, based on recent works and current legislation, such as the Internet Civil Rights Framework, the General Data Protection Law (LGPD) and the Carolina Dieckmann Law. In addition to the legal analysis, the paper examines the monitoring methods used by the authorities, the role of digital platforms and the importance of digital education as a prevention tool. It is concluded that combating digital defamation requires integrated action between the Judiciary, Internet providers and society, combining criminal repression, user awareness and legislative updating. Respect for human dignity must prevail in the virtual environment, ensuring a balance between freedom of expression and protection of reputation.

Keywords: Cybercrimes; Digital defamation; Freedom of expression.

SUMÁRIO

1. INTRODUÇÃO

Com o crescimento acelerado da internet e a digitalização de praticamente todos os aspectos da vida moderna, as plataformas digitais e os provedores de internet desempenham um papel fundamental na intermediação das interações humanas e na disponibilização de informações.

Esse cenário, porém, trouxe também novos desafios no campo jurídico, especialmente no que diz respeito à prática de crimes cibernéticos, como fraudes, difamações, vazamentos de dados e outros delitos cometidos no ambiente online.

É estritamente necessário deliberar sobre a punibilidade dos crimes virtuais, já tal aspecto possui suma importância para a regularização social no meio da internet no Brasil. Com isso, este projeto possui relevância não apenas dirigida ao âmbito jurídico, embora esteja dotado de cunho científico. A importância deste assunto se volta para a sociedade conscientizar-se da necessidade e das regras que regem o meio virtual em que é utilizado no Brasil e no mundo.

Com isso, em razão do vasto uso da internet, cria-se a sensação nos usuários de serem totalmente anônimo ou de estarem completamente impunes. Deste modo, urge a necessidade de regulamentar as diretrizes virtuais, afim de penalizar aqueles que transgridam a legislação penal pátria, sendo uma dessas legislações, a lei Carolina Dieckmann, que trata sobre a tipificação de delitos no âmbito virtual.

Indubitavelmente, a internet é uma ferramenta indispensável para a rotina de qualquer cidadão que esteja inserido no meio virtual. Em razão da dinâmica de informações e vasta velocidade de transmissão de dados, a utilização das redes virtuais só tende a crescer cada dia mais.

Como desdobramento deste uso inadequado da internet, não é difícil que muitos dos utilizadores brasileiros incorrem em cometer crimes no ambiente cibernético, entretanto, muitos tem a falsa sensação de impunibilidade em face de suposta impossibilidade de rastreamento, situação que não reflete a realidade investigativa, já que é possível acompanhar e investigar crimes cibernéticos.

Ademais, quantos aos métodos metodológicos, ferramentas e processos a aplicados para o desenvolvimento da pesquisa realizada são a revisão da bibliografia por meio de pesquisa bibliográfica; os dados disponibilizados aqui tem como base os últimos 05 anos, visando manter a atualidade do assunto em questão, literaturas estas que retratam a possibilidade da aplicação do tema em questão.

2. OS CRIMES CIBERNÉTICOS

Os crimes cibernéticos, também conhecidos como crimes digitais ou crimes informáticos, são definidos como delitos cometidos utilizando computadores, redes de comunicação ou a internet como ferramentas para a prática criminosa. De acordo com a Organização para a Cooperação e Desenvolvimento Econômico (OCDE), os crimes cibernéticos são ações ilícitas que envolvem o uso de sistemas informatizados ou a internet, seja como meio ou alvo do delito (GOMINHO, 2022). Esses crimes têm se tornado cada vez mais comuns à medida que a sociedade se digitaliza e as interações humanas migram para o ambiente virtual.

No Brasil, a definição de crimes cibernéticos é abordada pela Lei n.º 12.737/2012, conhecida como Lei Carolina Dieckmann, que dispõe sobre a tipificação criminal de invasão de dispositivos informáticos (GOMINHO, 2022).

A legislação brasileira, consoante Gominho (2022) também inclui no Código Penal, após a Lei n.º 12.965/2014 (Marco Civil da Internet), definições específicas para delitos cometidos no ambiente digital. Nesse sentido, os crimes cibernéticos englobam tanto ações direcionadas a dispositivos eletrônicos quanto aquelas que se utilizam de meios digitais para cometer infrações, como difamação, fraudes e ataques a sistemas de informação.

Entre os principais tipos de crimes cibernéticos, destacam-se as fraudes digitais. As fraudes consistem em enganar pessoas ou instituições para obter vantagens financeiras ilícitas por meio da internet ou de dispositivos eletrônicos (Wanderley, Costa e Ribeiro, 2022). Com o crescimento do comércio eletrônico e das transações bancárias digitais, esse tipo de crime se tornou um dos mais frequentes. De acordo com dados da Federação Brasileira de Bancos (FEBRABAN), o número de fraudes envolvendo cartões de crédito e transferências eletrônicas cresceu substancialmente nos últimos anos (FEBRABAN, 2022).

Outro crime cibernético amplamente praticado é a difamação online, que ocorre quando uma pessoa utiliza a internet para espalhar informações falsas ou ofensivas sobre outra pessoa com o intuito de prejudicar sua reputação (GOMINHO, 2022). Esse tipo de crime tem ganhado relevância nas redes sociais, onde a disseminação de conteúdo é rápida e

muitas vezes incontrolável. O Marco Civil da Internet estabelece que provedores de conteúdo podem ser responsabilizados por não removerem, após notificação, conteúdos difamatórios (BRASIL, 2014).

O *hacking*, ou invasão de sistemas, também é um dos crimes cibernéticos mais discutidos. *Hackers* exploram vulnerabilidades de sistemas de informação com o objetivo de roubar dados, prejudicar operações ou obter informações sigilosas (GOMINHO, 2022). Embora o hacking possa ser realizado com intenções variadas, incluindo ativismo digital (hacktivismo), a maior parte dessas atividades é considerada criminosa por comprometer a segurança digital de empresas e indivíduos.

> Com a grande disseminação dos computadores e do acesso à internet, acabaram surgindo crimes e criminosos com especialização na linguagem da informática, com proliferação por todo o mundo. Esses crimes são denominados crimes virtuais, digitais, informáticos, telemáticos, dentre outro (RODRIGUES, 2021, p. 09).

O vazamento de dados é outro problema que afeta tanto empresas quanto indivíduos no contexto digital. Esse crime ocorre quando informações sensíveis, como dados pessoais ou financeiros, são divulgadas sem autorização (WANDERLEY; COSTA; RIBEIRO, 2022). Com a promulgação da Lei Geral de Proteção de Dados, o Brasil deu um passo importante na regulamentação da proteção de dados, impondo sanções para o uso indevido dessas informações (BRASIL, 2018). Entretanto, os vazamentos de dados continuam sendo uma preocupação crescente, especialmente devido à dificuldade de rastrear os autores desses crimes no ambiente digital.

Hoje, a internet é uma ferramenta indispensável para o dia a dia de qualquer cidadão inserido no ambiente virtual. Devido à dinâmica das informações e à vasta velocidade de transmissão de dados, o uso de redes virtuais tende a crescer cada vez mais.

Crimes cibernéticos são aqueles que utilizam computadores, redes de computadores ou dispositivos eletrônicos conectados para praticar ações criminosas, que geram danos a indivíduos ou patrimônios, por meio de extorsão de recursos financeiros, estresse emocional ou danos à reputação de vítimas expostas na Internet.

No entanto, a internet cria em seus usuários uma falsa sensação de anonimato, dando-lhes a impressão de que tudo o que podem e querem, eles fazem. Assim, Cruz (2018), aponta que em decorrência dessa ideia, o roubo de dados e identidade, calúnia, difamação, bullying, crimes financeiros, pornografia infantil, chantagem e diversos outros crimes que podem ser vistos na rede virtual dão frutos.

Diante do exposto, passa-se a uma análise do paradigma de confronto para aplicação do princípio da dignidade da pessoa humana, pois, este preceito que é fundamento da República Federativa do Brasil segundo o art. 1.º, inciso III da Carta da República deverá servir como pilar tanto da proteção da pessoa do acautelado provisoriamente nas unidades prisionais quanto da sociedade pela preservação da segurança pública e da manutenção do devido processo legal (SOUSA, S., 2010).

Como a população em geral tem amplo acesso à conexão de internet no dia a dia, pode-se afirmar com clareza que o mundo está virtualmente interconectado e com acesso imediato aos dados e transmissão de informações, sendo essas informações a transmissão de mensagens de e-mail, telefonemas e, a exemplo de Rodrigues (2018), até por videoconferências instantâneas.

Assim, como explica Vidal (2015), com esse acesso a uma área tecnológica, é natural que surjam pessoas com más intenções, prontas para cometer o que ele chama de crimes cibernéticos ou crimes virtuais.

Teixeira (2014) traz em seu trabalho uma definição simples de crime virtual, que, embora curta, representa perfeitamente o seu significado.

Conforme ensina Gomes (2007), diversamente das regras que normatizam determinada situação fática e vale a lógica do tudo ou nada, os princípios não conflitam, "colidem" e quando se colidem, não se excluem. Como expressam critérios e razões para uma determinada decisão, os princípios podem ter incidência em casos concretos (por vezes, concomitantemente). Assim, há que se promover investigação minuciosa e ponderar, à luz da razoabilidade, em que momento deverá um prevalecer em face do outro.

> Todos os dias,tem-se acesso a notícias praticamente em tempo reale o mesmo acontece com conversas on-line, seja através somente de textos como também com o auxílio da webcam. Na internet,temos acesso a praticamente tudo: informação imediata, você tem a liberdade de percorrer caminhos diferenciados na internet;a princípio,com segurançarealizam-sepesquisas, exploram-seconteúdos, acessam-sesites de relacionamentos a trabalho, entre outras tantas atividades que a internet oferece. Oaumento de uso da internet e de suas facilidades pelas empresasé uma prática constante que traz benefícios para o desempenho de suas atividades diárias, em quese destacam o acesso imediato a informaçãoe a rapidez na comunicação e umas dessas facilidades que se destacaé a utilização do e-mail e navegação da internet, mais coma utilização inadequadadessas facilidades pode-se deixar as organizações vulneráveis (RODRIGUES, 2021, p. 07).

Ademais, há de se falar de uma legislação recente, conforme pontuado por Rodrigues (2018), sendo ela a Lei Carolina Dieckmann (Lei n° 12.737/2012), que acrescentou no Código

Penal dispositivos legais que tipificam mais alguns delitos cibernéticos, sendo eles, por exemplo a invasão de dispositivo informático, que aparece no Código Penal no artigo 154-A. Além desse, há também a instrução do tipo de ação penal a ser diligenciada processualmente no caso da aplicação da lei em questão.

A Lei n° 12.737/2012 leva este nome porque, consoante exposto por Rodrigues (2018), a atriz Carolina Dieckmann sofreu uma invasão em sua rede de computadores, ocasião na qual passou a ser chantageada para não ter informações e fotos divulgadas na internet.

Deste modo, Cruz (2018), aponta que decorrente dessa ideia, frutificam roubo de dados e de identidade, calúnia, difamação, bullying, crimes financeiros, pornografia infantil, chantagem e diversos outros crimes que podem ser vistos na rede virtual.

Já que diariamente a população em geral possua amplo acesso à conexão de internet, pode se afirmar claramente que o mundo está virtualmente interligado e com acesso imediato de dados e transmissão de informações, sendo essas informações transmissões de mensagens de e-mails, chamadas telefônicas e, como exemplificado por Rodrigues (2018), até mesmo por videoconferências instantâneas.

> Focalizando-se a Internet, há dois pontos de vista a considerar: crimes ou ações que merecem incriminação praticados por meio da internet e crimes ou ações que merecem incriminação praticados contra a Internet, enquanto bem jurídico autônomo. Quanto ao primeiro, cabe observar que os tipos penais, no que concerne à sua estrutura, podem ser crimes de resultado de conduta livre, crimes de resultado de conduta vinculada, crimes de mera conduta ou formais (sem querer discutir se existe distinção entre estes) e crimes de conduta com fim específico, sem prejuízo da inclusão eventual de elementos normativos. Nos crimes de resultado de conduta livre, à lei importa apenas o evento modificador da natureza, com, por exemplo, o homicídio. O crime, no caso, é provocador o resultado morte, qualquer que tenha sido o meio ou a ação que o causou (RODRIGUES, 2021, p. 09).

O acesso a uma área tecnológica, é natural que se despontem pessoas com intenções maliciosas, prontas para cometer os denominados por ele como crimes cibernéticos ou crimes virtuais.

Os crimes cibernéticos englobam um conjunto amplo de condutas ilícitas praticadas por meio de tecnologias digitais e vêm crescendo em ritmo alarmante. A internet, ao oferecer anonimato, agilidade e alcance global, tornou-se um ambiente propício para fraudes, ataques à honra, invasões de sistemas e outros delitos. Conforme diz Lima (2019), o avanço tecnológico, embora tenha gerado benefícios à comunicação e ao comércio, também criou novas formas de criminalidade que desafiam os métodos tradicionais de investigação.

Esses crimes podem afetar tanto pessoas físicas quanto jurídicas, causando prejuízos

financeiros, danos morais e violações de privacidade. A facilidade de acesso a ferramentas de disseminação de dados falsos, de engenharia social e de ataques hacker contribui para o crescimento desse tipo de delito. Ferreira (2019) aponta que a falta de consciência digital da população é um fator que aumenta a vulnerabilidade das vítimas no ambiente virtual.

A categorização dos crimes cibernéticos varia entre os que usam o computador como meio e os que o têm como fim. Exemplos do primeiro tipo são a difamação online e o estelionato praticado por redes sociais, enquanto no segundo estão os crimes como invasão de dispositivos e ataques a servidores. Traz a análise de Lima (2019) que essa distinção é importante para fins de investigação e enquadramento legal, pois determina as estratégias a serem adotadas pelas autoridades.

O anonimato, que é um dos grandes atrativos da internet, também é um obstáculo na responsabilização dos criminosos. Muitos usuários criam perfis falsos, utilizam redes privadas virtuais ou atuam em ambientes da chamada “deep web”, dificultando sua identificação. Ferreira (2019) destaca que os métodos de ocultação usados por criminosos digitais exigem da perícia uma atualização constante de ferramentas e técnicas investigativas.

A atuação das delegacias especializadas é essencial para o combate a esses crimes. Esses órgãos contam com profissionais capacitados e recursos tecnológicos voltados à investigação de delitos informáticos. Conforme diz Lima (2019), a especialização das polícias civis e federais no Brasil tem evoluído, mas ainda encontra limitações diante da complexidade das infrações virtuais e da velocidade com que ocorrem.

Os crimes cibernéticos não conhecem fronteiras geográficas, o que representa outro grande desafio. Um ataque pode ser cometido por um autor localizado em outro país, com vítimas espalhadas por diversos continentes. Ferreira (2019) afirma que a transnacionalidade dessas infrações impõe a necessidade de acordos de cooperação internacional para que as investigações sejam eficazes.

Entre os crimes mais comuns estão o estelionato eletrônico, a falsidade ideológica digital, a divulgação não autorizada de imagens íntimas, a extorsão por meio de vazamentos de dados e os crimes contra a honra. Traz a análise de Lima (2019) que, embora diversos desses crimes já existissem antes da era digital, o meio virtual os potencializou de forma significativa, exigindo novos olhares jurídicos.

As redes sociais, em particular, têm sido palco frequente de condutas ilícitas, como ameaças, perseguições e disseminação de discurso de ódio. Muitos desses comportamentos se escondem sob a ideia de liberdade de expressão, confundindo crítica com ofensa. Conforme diz Ferreira (2019), o direito à livre manifestação não pode se sobrepor ao direito à dignidade,

sendo necessária uma atuação firme contra os abusos cometidos nas plataformas digitais.

A legislação brasileira tem se adaptado à realidade digital, com leis específicas como o Marco Civil da Internet e a Lei Carolina Dieckmann, que criminaliza a invasão de dispositivos eletrônicos. No entanto, ainda há lacunas jurídicas e desafios na aplicação dessas normas. Traz a análise de Lima (2019) que o dinamismo do ciberespaço exige constante atualização legislativa, de modo a acompanhar a criatividade dos agentes infratores.

Além da esfera penal, os crimes cibernéticos geram consequências civis e administrativas. Empresas e pessoas prejudicadas por ataques virtuais muitas vezes recorrem ao Judiciário para obter indenizações ou para que os conteúdos ilícitos sejam removidos. Ferreira (2019) ressalta que a atuação judicial deve ser célere e técnica, garantindo ao mesmo tempo a liberdade na rede e a proteção contra abusos.

O papel das empresas de tecnologia também é fundamental no combate aos crimes digitais. Plataformas de redes sociais, provedores de internet e empresas de armazenamento em nuvem devem colaborar com a Justiça para fornecer dados essenciais à investigação. Conforme diz Lima (2019), essa cooperação é um dever ético e jurídico, diante do impacto social causado pelas condutas criminosas na internet.

A educação digital da população é uma medida preventiva essencial. Ao instruir crianças, jovens e adultos sobre os riscos da internet e os limites legais de conduta, cria-se uma cultura de responsabilidade no uso das tecnologias. Ferreira (2019) enfatiza que a prevenção é mais eficaz quando acompanhada de informação clara e acessível sobre as consequências de comportamentos ilícitos no mundo virtual.

As vítimas de crimes cibernéticos muitas vezes se sentem desamparadas, pois o impacto emocional e social dos ataques é grande e nem sempre há solução imediata. A sensação de impotência diante da impunidade pode agravar o sofrimento psicológico. Traz a análise de Lima (2019) que o acolhimento jurídico e psicológico às vítimas deve ser parte integrante da política de combate ao cibercrime.

A atuação de grupos organizados, como quadrilhas especializadas em golpes bancários e invasões de sistemas, tem preocupado autoridades em todo o mundo. Esses grupos operam de forma estruturada e utilizam tecnologias avançadas para cometer delitos em larga escala. Ferreira (2019) aponta que o enfrentamento desses grupos depende de inteligência policial, cooperação internacional e investimentos em cibersegurança pública.

A utilização da inteligência artificial e da análise de dados vem sendo adotada como estratégia de fiscalização. Essas ferramentas permitem identificar padrões suspeitos de comportamento, automatizar a triagem de denúncias e antecipar movimentos de grupos

cibercriminosos. Conforme diz Lima (2019), a tecnologia pode ser uma aliada poderosa da Justiça, desde que seu uso respeite direitos fundamentais e a privacidade dos cidadãos.

A responsabilização criminal de menores em crimes virtuais também é um tema sensível e recorrente. Muitos adolescentes, por falta de orientação, se envolvem em práticas como cyberbullying, difamação ou compartilhamento de conteúdos íntimos. Ferreira (2019) alerta que a responsabilização deve ser educativa e não meramente punitiva, com enfoque na recuperação e conscientização do jovem.

Muitos crimes cibernéticos têm motivações econômicas, como os golpes financeiros praticados por meio de links falsos ou engenharia social. Outros, porém, têm natureza emocional, como as vinganças amorosas ou a perseguição digital. Traz a análise de Lima (2019) que a motivação do crime influencia na forma de investigação e na dosimetria da pena, sendo um elemento relevante para o processo penal.

A criação de ambientes digitais mais seguros passa pela combinação de tecnologia, educação e responsabilidade social. A adoção de senhas fortes, autenticação de dois fatores e cuidados com o compartilhamento de dados são medidas simples que podem prevenir muitos crimes. Ferreira (2019) defende que a proteção digital começa com o comportamento individual consciente.

A imprensa também tem papel importante na divulgação de informações seguras e na conscientização sobre os crimes digitais. Campanhas públicas e matérias jornalísticas bem fundamentadas ajudam a combater a desinformação e a estimular o uso seguro da tecnologia. Conforme diz Lima (2019), o jornalismo ético é parte essencial da resposta social ao cibercrime.

Teixeira (2014) traz em sua obra uma simples e singela definição de crime virtual, que, embora curta, representa perfeitamente seu significado:

O crime virtual, numa breve definição, é aquele praticado no ambiente virtual, a internet pode ser tanto ambiente propício para a consumação de crimes, quanto para a realização de seus atos preparatórios. (TEIXEIRA, 2014, p. 18).

Com um raciocínio mais extenso, Cruz (2018) expõe em sua pesquisa que existem dois tipos de crimes virtuais: o próprio, o impróprio e o misto. Deste modo, o mesmo faz a definição com suas próprias palavras:

Delitos informáticos impróprios são aqueles nos quais o computador é usado como instrumento para a execução do crime, mas não há ofensa ao bem jurídico da informatização automatizada, podendo neste caso utilizar como exemplo o crime de ameaça. Delitos Informáticos Próprios são aqueles em que o bem jurídico protegido pela norma penal é a

inviolabilidade das informações automatizadas (dados), ou seja, se tem a ofensa dos dados, a exemplo invasão de dispositivo de informática. Já os crimes informáticos mistos em que, além da proteção da inviolabilidade dos dados, a norma visa a tutelar bem jurídico de natureza diversa, assim se tem a título de exemplo os praticados em âmbito eleitoral.

Com um raciocínio mais extenso, Cruz (2018) expõe em sua pesquisa que existem dois tipos de crimes virtuais: o próprio, o impróprio e o misto dentro da análise formal de cada aspecto.

3 MÉTODOS DE FISCALIZAÇÃO DE CRIMES CIBERNÉTICOS

O papel das plataformas digitais e provedores de internet, portanto, é multifacetado, abrangendo desde a oferta de infraestrutura até a moderação de conteúdo e a proteção dos usuários. Conforme ressalta Ferreira (2019), essas empresas enfrentam um delicado equilíbrio entre a facilitação da comunicação livre e a prevenção de abusos e crimes cibernéticos, sendo constantemente pressionadas a desenvolver políticas e tecnologias que aumentem a segurança sem comprometer os direitos fundamentais.

A capacitação contínua dos profissionais que atuam na investigação e no julgamento de crimes cibernéticos é uma necessidade urgente. Juízes, promotores, defensores e policiais precisam compreender as dinâmicas do ambiente virtual para tomar decisões técnicas e eficientes. Traz a análise de Lima (2019) que o conhecimento jurídico, sem a compreensão das ferramentas tecnológicas envolvidas, pode tornar ineficaz a repressão a esses delitos.

Outro ponto de atenção está na lentidão com que, muitas vezes, se concretizam os pedidos judiciais de quebra de sigilo e fornecimento de dados por parte de empresas de tecnologia. Em casos de crimes virtuais, o fator tempo é determinante para a obtenção de provas. Ferreira (2019) observa que a demora pode resultar na perda de dados, dificultando ou até inviabilizando a identificação do autor do crime.

A impunidade em crimes cibernéticos é um dos maiores estímulos à reincidência. Muitos infratores acreditam que, pela complexidade das investigações e pela dificuldade de rastreamento, jamais serão descobertos ou punidos. Conforme diz Lima (2019), a sensação de impunidade alimenta um ciclo contínuo de infrações, o que demanda respostas mais efetivas por parte do sistema de justiça.

A questão da responsabilidade das plataformas digitais é cada vez mais debatida. Embora não sejam obrigadas a monitorar conteúdos de forma prévia, essas empresas devem agir com rapidez quando notificadas sobre conteúdos ilícitos. Traz a análise de Ferreira (2019) que a omissão dessas plataformas pode configurar conivência e até responsabilidade

subsidiária, principalmente em casos de reincidência e inércia.

O ambiente escolar, muitas vezes, também é afetado pelos crimes cibernéticos, especialmente com a prática do cyberbullying. Alunos são expostos, ridicularizados e atacados por meio de mensagens, vídeos ou perfis falsos. Conforme diz Lima (2019), esse tipo de conduta tem impactos diretos no desenvolvimento emocional e educacional das vítimas, exigindo ações conjuntas entre escola, família e poder público.

Outro tipo recorrente de crime digital é o vazamento de dados sensíveis, que pode atingir desde pessoas comuns até grandes corporações. Esses vazamentos expõem informações bancárias, prontuários médicos, conversas privadas e outros conteúdos sigilosos. Ferreira (2019) ressalta que esses ataques não apenas violam a intimidade, como também abrem margem para outros delitos, como fraudes e chantagens.

A discussão sobre a responsabilidade contratual e legal desses intermediários no Brasil e no exterior destaca a necessidade de um marco regulatório que proteja tanto os usuários quanto as empresas. Segundo Viana (2015), a busca por um equilíbrio entre liberdade e segurança deve ser o foco das futuras reformas legislativas, considerando o impacto das decisões jurídicas e políticas públicas no desenvolvimento da economia digital e na proteção dos direitos dos cidadãos.

Por fim, o estudo da função e natureza dos provedores de internet e plataformas digitais mostra que, à medida que a sociedade avança na digitalização, a responsabilidade desses intermediários torna-se cada vez mais central. Como aponta Ferreira (2019), o futuro da internet dependerá da capacidade de esses atores se adaptarem às novas demandas por segurança e privacidade, ao mesmo tempo em que garantem um ambiente digital livre e acessível para todos.

O Marco Civil da Internet (Lei n.º 12.965/2014) é considerado o principal marco regulatório do uso da internet no Brasil, estabelecendo direitos e deveres para usuários, provedores de serviços e o governo no ambiente digital. Um dos aspectos centrais do Marco Civil é a definição da responsabilidade dos provedores de conexão e aplicação de internet em relação a conteúdos ilícitos, como difamação, vazamentos de dados e outros crimes cibernéticos.

De acordo com o artigo 18 da referida lei, os provedores de conexão não são responsabilizados por danos decorrentes de conteúdo gerado por terceiros, uma vez que sua função se restringe ao fornecimento de acesso à rede, porém sua responsabilização se limita ao âmbito civil.

A responsabilização dos provedores de aplicação de internet (plataformas digitais que

oferecem serviços específicos, como redes sociais) segue regras específicas. Essa disposição foi importante para preservar a liberdade de expressão no ambiente online, evitando a censura prévia, mas ao mesmo tempo garantindo que as vítimas de crimes cibernéticos possam buscar reparação judicial quando necessário (SILVA, 2023).

Outro ponto de destaque do Marco Civil da Internet é a garantia da neutralidade da rede, prevista no artigo 9º. A neutralidade da rede assegura que os provedores de conexão tratem de forma igualitária todos os dados trafegados, sem discriminar por tipo, origem ou destino. No entanto, esse princípio também pode gerar discussões em casos de crimes cibernéticos, visto que os provedores podem argumentar que, por não interferirem no tráfego de dados, não têm responsabilidade sobre conteúdos ilícitos veiculados por meio de suas redes (Silva, 2023).

Além do Marco Civil, outra legislação fundamental no tratamento de crimes cibernéticos no Brasil é a Lei Geral de Proteção de Dados (LGPD), Lei n.º 13.709/2018. A LGPD estabelece diretrizes para a coleta, armazenamento e tratamento de dados pessoais, impondo aos provedores de internet e plataformas digitais a responsabilidade de proteger a privacidade dos usuários (VIANA, 2015).

A legislação prevê sanções administrativas para o descumprimento de suas normas, o que pode incluir multas e, em casos mais graves, a suspensão ou proibição de tratamento de dados. De acordo com Viana (2015), a LGPD foi um passo significativo para reforçar a proteção dos direitos dos cidadãos no ambiente digital, especialmente em um cenário de crescente coleta de dados pessoais por plataformas digitais.

Os crimes virtuais representam uma nova era de desafios para o Direito Penal, exigindo uma reformulação constante das estratégias de combate e prevenção. Com a popularização da internet, novas modalidades criminosas surgiram, atingindo desde sistemas financeiros até a intimidade de cidadãos comuns. Conforme destaca Silva (2023), o ambiente digital oferece aos infratores um território sem fronteiras, onde o anonimato e a velocidade da informação dificultam a ação imediata das autoridades.

Uma das principais características dos crimes virtuais é sua transversalidade: eles podem afetar qualquer pessoa, independentemente de idade, classe social ou localização geográfica. Estelionatos digitais, difamações, invasões de dispositivos e vazamentos de dados são apenas alguns exemplos do vasto leque de delitos praticados no meio eletrônico. Silva (2023) observa que a natureza horizontal da internet amplia o alcance dos ataques e torna o controle mais complexo.

A ausência de barreiras territoriais é um fator que intensifica os desafios das investigações. Muitos dos autores estão fora do país ou utilizam servidores estrangeiros para dificultar a localização e a responsabilização penal. Traz a análise de Silva (2023) que, nesse cenário, a cooperação jurídica internacional torna-se essencial, embora ainda enfrente barreiras burocráticas e políticas significativas.

As vítimas, em muitos casos, demoram a perceber que foram alvo de um crime digital. Seja por desconhecimento, vergonha ou pela natureza silenciosa de algumas fraudes, a notificação às autoridades costuma ser tardia, prejudicando a apuração. Conforme relata Silva (2023), essa demora contribui para a perpetuação do crime, além de dificultar a coleta de provas digitais que podem se perder com o tempo.

Os crimes cibernéticos também desafiam a tipificação penal tradicional, exigindo interpretações atualizadas e, muitas vezes, a criação de novas leis. A flexibilidade com que os agentes se adaptam às tecnologias supera, em muitos momentos, a capacidade do legislador. Silva (2023) aponta que o Direito Penal precisa se tornar mais dinâmico e conectado à realidade digital para enfrentar com eficácia essa nova criminalidade.

A responsabilização dos autores também passa pelo fortalecimento de políticas de educação digital. Prevenir os crimes cibernéticos exige formar cidadãos conscientes sobre os riscos, deveres e limites no uso da internet. Traz a análise de Silva (2023) que a educação, quando aliada à tecnologia e à legislação, é a principal arma contra a expansão do cibercrime.

Outro ponto sensível envolve a atuação das plataformas tecnológicas. Embora sejam apenas intermediárias, muitas vezes deixam de cumprir seu papel de moderação e resposta rápida a conteúdos ilícitos. Conforme alerta Silva (2023), a omissão dessas empresas pode contribuir para a perpetuação do crime e para a sensação de impunidade no ambiente virtual.

Além do aspecto penal, os crimes virtuais geram efeitos civis e psicológicos profundos. Vítimas de golpes financeiros, exposições indevidas ou perseguições online enfrentam danos que vão além do prejuízo econômico. Silva (2023) reforça que a reparação deve considerar não apenas o dano objetivo, mas também o abalo emocional causado pelas agressões digitais.

A especialização dos órgãos públicos no combate a esse tipo de crime é um passo importante. Delegacias especializadas, perícias digitais e varas com competência específica são mecanismos que fortalecem o enfrentamento. Conforme argumenta Silva (2023), a formação de agentes públicos em tecnologia e investigação digital é indispensável para acompanhar o ritmo da criminalidade cibernética.

Por fim, é necessário reconhecer que o combate aos crimes virtuais não depende apenas do Estado, mas da sociedade como um todo. A denúncia, o uso consciente da internet e a valorização do respeito digital são atitudes que ajudam a prevenir e a inibir práticas ilícitas. Silva (2023) conclui que o enfrentamento da criminalidade digital é uma missão coletiva, que exige ação conjunta, permanente e estratégica.

O Código Penal brasileiro também passou por adaptações para tratar dos crimes cibernéticos, principalmente com a inclusão da Lei dos Crimes Informáticos (Lei n.º 12.737/2012), popularmente conhecida como Lei Carolina Dieckmann, que tipifica crimes como a invasão de dispositivos eletrônicos, a interceptação de comunicações e a violação de dados pessoais. A partir dessa lei, a invasão de dispositivos de informática, com ou sem obtenção de conteúdo de comunicações privadas, tornou-se crime, sujeitando os responsáveis a penas de reclusão e multa. Conforme assinala Eliezer e Garcia (2015), essa lei foi crucial para preencher uma lacuna existente no ordenamento jurídico, considerando a crescente sofisticação dos crimes cometidos por meio de recursos tecnológicos.

. A decisão reforça a tendência de que, embora os provedores não sejam obrigados a realizar uma filtragem prévia do conteúdo postado pelos usuários, uma vez que a empresa tenha conhecimento da ilicitude, ela tem o dever de agir rapidamente para remover o conteúdo ofensivo, sob pena de responsabilidade civil, conforme denota Ferreira (2019).

No que diz respeito à proteção de dados, a jurisprudência também tem evoluído no sentido de aplicar a LGPD em crimes relacionados ao vazamento de informações pessoais. Em um caso recente, a 1ª Câmara de Direito Privado do Tribunal de Justiça de São Paulo decidiu pela condenação de uma empresa de tecnologia que não protegeu adequadamente os dados pessoais de seus clientes, resultando em um vazamento que expôs informações sensíveis. Essa decisão foi uma das primeiras a aplicar as sanções previstas na LGPD, como a imposição de multas, evidenciando o rigor com que os tribunais brasileiros têm tratado a proteção de dados no ambiente digital (FERREIRA, 2019).

Em termos de legislação comparada, o Brasil ainda está em processo de adaptação às novas demandas de regulamentação do ambiente digital. Países da União Europeia, por exemplo, adotam legislações mais rigorosas em relação à responsabilidade dos provedores de internet e plataformas digitais, especialmente com a implementação do Regulamento Geral de Proteção de Dados (GDPR), que impõe regras rígidas sobre o tratamento de dados e responsabiliza as empresas por violações. De acordo com Pompeu, Trindade e Sato (2024), a LGPD brasileira foi amplamente inspirada pelo GDPR europeu, o que evidencia uma

tendência global de proteção da privacidade dos usuários como resposta ao avanço dos crimes cibernéticos.

Uma discussão importante é a relação entre a liberdade de expressão e a responsabilidade dos provedores, especialmente no que tange à moderação de conteúdo. O Marco Civil da Internet e a LGPD buscam um equilíbrio entre a proteção dos direitos dos usuários e a responsabilização dos intermediários digitais, mas há quem argumente que as disposições legais atuais podem gerar uma censura indireta, na medida em que as plataformas podem adotar uma postura excessivamente cautelosa ao moderar conteúdos (POMPEU, TRINDADE E SATO, 2024).

Por fim, o papel do Judiciário brasileiro tem sido fundamental na interpretação e aplicação dessas normas, consolidando entendimentos sobre a responsabilidade civil, penal e administrativa dos provedores. As decisões judiciais mais recentes mostram uma tendência em responsabilizar os intermediários digitais por omissões na remoção de conteúdo ilícito ou por falhas na proteção dos dados pessoais dos usuários, contribuindo para o fortalecimento da jurisprudência sobre crimes cibernéticos no Brasil (LIMA, 2019).

O Marco Civil da Internet, a LGPD e o Código Penal brasileiro constituem o arcabouço jurídico que regula o ambiente digital no Brasil, estabelecendo diretrizes claras sobre a responsabilidade dos provedores de internet e plataformas digitais. O avanço da jurisprudência e a aplicação prática dessas leis demonstram que o Brasil está evoluindo na proteção dos direitos dos usuários e na responsabilização por crimes cibernéticos, embora desafios ainda permaneçam, especialmente no equilíbrio entre liberdade de expressão, proteção de dados e segurança no ambiente digital.

O papel das plataformas digitais e provedores de internet, portanto, é multifacetado, abrangendo desde a oferta de infraestrutura até a moderação de conteúdo e a proteção dos usuários. Conforme ressalta Ferreira (2019), essas empresas enfrentam um delicado equilíbrio entre a facilitação da comunicação livre e a prevenção de abusos e crimes cibernéticos, sendo constantemente pressionadas a desenvolver políticas e tecnologias que aumentem a segurança sem comprometer os direitos fundamentais.

A discussão sobre a responsabilidade contratual e legal desses intermediários no Brasil e no exterior destaca a necessidade de um marco regulatório que proteja tanto os usuários quanto as empresas. Segundo Viana (2015), a busca por um equilíbrio entre liberdade e segurança deve ser o foco das futuras reformas legislativas, considerando o impacto das decisões jurídicas e políticas públicas no desenvolvimento da economia digital e na proteção dos direitos dos cidadãos.

Por fim, o estudo da função e natureza dos provedores de internet e plataformas digitais mostra que, à medida que a sociedade avança na digitalização, a responsabilidade desses intermediários torna-se cada vez mais central. Como aponta Ferreira (2019), o futuro da internet dependerá da capacidade de esses atores se adaptarem às novas demandas por segurança e privacidade, ao mesmo tempo em que garantem um ambiente digital livre e acessível para todos.

O Código Penal brasileiro também passou por adaptações para tratar dos crimes cibernéticos, principalmente com a inclusão da Lei dos Crimes Informáticos (Lei n.º 12.737/2012), popularmente conhecida como Lei Carolina Dieckmann, que tipifica crimes como a invasão de dispositivos eletrônicos, a interceptação de comunicações e a violação de dados pessoais. A partir dessa lei, a invasão de dispositivos de informática, com ou sem obtenção de conteúdo de comunicações privadas, tornou-se crime, sujeitando os responsáveis a penas de reclusão e multa. Conforme assinala Eliezer e Garcia (2015), essa lei foi crucial para preencher uma lacuna existente no ordenamento jurídico, considerando a crescente sofisticação dos crimes cometidos por meio de recursos tecnológicos.

A fiscalização de crimes cibernéticos tem se tornado um desafio constante para as autoridades, especialmente diante do avanço acelerado das tecnologias de informação. A internet se tornou um espaço fértil para práticas criminosas, e a atuação dos órgãos competentes exige o domínio de técnicas investigativas específicas, muitas delas dependentes de acesso a registros eletrônicos e da colaboração de empresas de tecnologia. Lima (2019) traz que a efetividade da repressão aos delitos virtuais exige uma abordagem técnica, coordenada e atualizada.

Entre os crimes mais comuns no ambiente digital, a difamação merece atenção especial por sua alta incidência e pelo impacto direto na dignidade da vítima. A facilidade com que conteúdos são disseminados em plataformas online amplia os danos morais e dificulta a contenção dos prejuízos. Conforme diz Ferreira (2019), as ofensas à honra, quando publicadas nas redes sociais, ganham proporção coletiva e quase irreversível, o que reforça a necessidade de fiscalização ágil e eficaz.

Os métodos tradicionais de investigação criminal nem sempre são suficientes para lidar com as nuances do ambiente virtual. Por isso, ferramentas tecnológicas passaram a ser incorporadas às rotinas investigativas, como softwares de rastreamento de endereço virtual, análise de metadados e monitoramento de publicações em redes sociais. Conforme diz Lima (2019), o uso desses instrumentos permite a identificação da autoria com maior precisão e

rapidez, mesmo quando os criminosos tentam ocultar sua identidade.

A atuação das delegacias especializadas em crimes digitais tem sido uma das principais frentes de fiscalização. Elas contam com profissionais capacitados para lidar com as particularidades do cibercrime e com a coleta de provas digitais, que muitas vezes estão armazenadas em nuvem ou em locais de difícil acesso. Conforme Ferreira (2019) consigna, a qualificação técnica dos agentes é fator determinante para o sucesso das apurações, especialmente em casos de difamação com autoria anônima.

A cooperação entre órgãos públicos e empresas privadas, como provedores de internet e plataformas de redes sociais, é fundamental para o avanço das investigações. Essa parceria permite a obtenção de registros de acesso, conteúdos apagados e informações sobre usuários que tenham praticado atos ilícitos. Conforme Lima (2019), sem essa colaboração, grande parte dos crimes cibernéticos terminaria arquivada por falta de provas ou de autoria definida.

A preservação da cadeia de custódia das evidências digitais é outro aspecto relevante nos métodos de fiscalização. Qualquer falha nesse processo pode comprometer a validade da prova e inviabilizar a responsabilização do autor. Nos termos da literatura de Ferreira (2019), os dados obtidos devem ser armazenados com segurança, sem alterações ou manipulações, de forma que possam ser utilizados no processo judicial com legitimidade.

No que se refere à difamação, Lima (2019) traz que a atuação do Ministério Público tem se mostrado essencial. Muitas vezes, o promotor requer medidas urgentes, como a quebra de sigilo telemático ou a retirada imediata de conteúdo ofensivo das redes. O combate à difamação online exige respostas rápidas, pois a permanência da ofensa publicada intensifica o dano à imagem da vítima.

Além das ações repressivas, a fiscalização também envolve ações preventivas. Programas de conscientização sobre o uso responsável da internet têm sido realizados por escolas, instituições públicas e organizações não governamentais. Conforme diz Ferreira (2019), a prevenção é uma ferramenta eficaz contra crimes cibernéticos, na medida em que informa a população sobre os limites legais da liberdade de expressão e os riscos de condutas ofensivas.

As denúncias anônimas também têm papel importante no processo de fiscalização. Plataformas digitais e canais governamentais permitem que qualquer cidadão informe irregularidades ou comportamentos suspeitos no ambiente virtual. Conforme diz Lima (2019), essas ferramentas democratizam o acesso à justiça e ampliam o alcance da fiscalização sobre crimes cometidos na internet.

A legislação brasileira tem avançado na tentativa de acompanhar a evolução tecnológica e os novos formatos de conduta ilícita. A criação de normas específicas voltadas aos crimes digitais contribuiu para o fortalecimento da fiscalização, a existência de tipificações claras e adequadas é essencial para a segurança jurídica e a responsabilização dos agressores.

A fiscalização também se depara com entraves quando os dados estão hospedados em servidores de outros países. Nesses casos, é necessário acionar mecanismos de cooperação internacional, como acordos bilaterais e convenções multilaterais. Conforme diz Lima (2019), o tempo de resposta pode ser um obstáculo, e muitas vezes os dados se perdem antes de serem obtidos pelas autoridades brasileiras.

Já denota Lima (2019) que o trabalho conjunto entre a advocacia, a magistratura e os peritos técnicos é indispensável para que a fiscalização se concretize de forma justa e eficiente. A compreensão multidisciplinar dos elementos envolvidos nos crimes cibernéticos, especialmente os que envolvem difamação, fortalece as ações punitivas e reparatórias, a atuação integrada entre os atores do sistema de justiça é um dos pilares do combate aos crimes virtuais.

A análise de comportamento em redes sociais também tem sido adotada como método de investigação. Com o auxílio de algoritmos e inteligência artificial, é possível identificar padrões de conduta ofensiva ou a criação de perfis falsos para fins ilícitos. Essas tecnologias contribuem para mapear redes de difamação e grupos que se organizam com o objetivo de atacar a imagem de pessoas públicas ou anônimas (LIMA, 2019).

Em casos de difamação, o mais importante é garantir à vítima a possibilidade de exercer plenamente seu direito de defesa e de reparação moral. A fiscalização atua, portanto, também como forma de preservar a dignidade da pessoa humana. Nos termos de Ferreira (2019), a honra não pode ser relativizada pelo anonimato da internet, e a responsabilização deve ser proporcional ao dano causado.

A repressão a crimes cibernéticos não deve ser vista apenas como tarefa do Estado, mas como um compromisso coletivo. Empresas, usuários e instituições têm papel ativo na criação de um ambiente digital mais seguro e respeitoso. Conforme diz Lima (2019), a eficácia da fiscalização depende do engajamento social na denúncia e no combate de práticas ofensivas, como a difamação, que têm efeitos devastadores sobre a vida das pessoas.

Esses métodos, quando aplicados com rigor técnico e respeito aos direitos fundamentais, formam o conjunto de ferramentas indispensáveis para enfrentar os desafios da

criminalidade virtual. A difamação digital, por sua natureza difusa e de fácil propagação, exige um aparato fiscalizador dinâmico, atualizado e humano tecnologia é um meio, mas o fim deve sempre ser a proteção da dignidade humana e a promoção da justiça (FERREIRA, 2019).

Em termos de jurisprudência, a aplicação dessas leis em crimes cibernéticos tem sido progressivamente consolidada pelos tribunais brasileiros. Um caso notório ocorreu no julgamento do Recurso Especial 1.660.168/SP, no qual o Superior Tribunal de Justiça (STJ) reconheceu a responsabilidade de um provedor de aplicação por não remover conteúdo ofensivo, mesmo após notificação judicial. O tribunal reafirmou que, ao ser devidamente notificado, o provedor tem a obrigação de tomar as providências necessárias para retirar o material infrator, e, caso não o faça, pode ser responsabilizado pelos danos causados à parte ofendida (ELIEZER E GARCIA, 2015).

4 CRIME DE DIFAMAÇÃO

A difamação representa um dos ataques mais recorrentes à honra objetiva do indivíduo, sendo caracterizada pela imputação de fato ofensivo à reputação de alguém, ainda que tal fato seja verdadeiro. Como observa Gominho (2022), trata-se de uma conduta que ultrapassa o direito à livre expressão e atinge diretamente a imagem pública da vítima, sendo juridicamente reprovável.

Nos meios digitais, essa prática ganha contornos ainda mais preocupantes. De acordo com Filho (2024), as redes sociais transformaram-se em instrumentos velozes e potentes para a propagação de discursos difamatórios, muitas vezes com irreparável dano à imagem de pessoas que sequer têm oportunidade de defesa prévia.

A honra, nesse contexto, é colocada em constante risco, sobretudo diante da ilusão de impunidade que o ambiente virtual proporciona aos usuários. Gominho (2022) pontua que, na prática, muitos acreditam estar protegidos por um suposto anonimato digital, o que acaba incentivando a prática reiterada de ofensas públicas e irresponsáveis.

> A 3ª Turma chegou a decisão de queações indenizatórias por danos morais poderão ter ajuizamentoem nome do proprietário da organização vitimada de mensagens de difamação em comunidades do site de relacionamentos Orkut. O tribunal levou em consideração legítima a ação com proposição partindo de um empresário do estado de Minas Gerais contra dois indivíduos que difamaram seu negócio de criar avestruzes, causando-lhediversos prejuízos. De acordo com a ministra Nancy Andrighi, as mensagens com divulgação não foram apenas consideradas ofensivas ao empresário e seu filho, mas também ao seu comércio de ave (RODRIGUES, 2021, p. 11).

Filho (2024) explica que, ao contrário do que muitos pensam, a liberdade de expressão não é um direito absoluto. Quando a manifestação de pensamento ultrapassa os limites do respeito e compromete a reputação alheia, configura-se abuso de direito, atraindo a responsabilização civil e penal de seu autor.

Ainda segundo Gominho (2022), a legislação brasileira foi construída para garantir a convivência harmônica entre os direitos fundamentais, de modo que a proteção à honra e à dignidade da pessoa humana não pode ser relativizada sob a justificativa de liberdade de manifestação.

O dano decorrente de uma difamação não reside apenas no conteúdo proferido, mas também no alcance que esse conteúdo adquire após sua divulgação. Filho (2024) destaca que o potencial de viralização das mensagens ofensivas agrava a lesão, o que exige, por parte do Poder Judiciário, um olhar mais atento e célere.

Além disso, Gominho (2022) esclarece que a tipificação da difamação prescinde da falsidade do fato imputado, pois a simples exposição de fato ofensivo à reputação já é suficiente para configurar o delito, bastando que a conduta tenha sido dirigida a terceiro ou a um grupo de pessoas.

Na seara da responsabilidade civil, Filho (2024) ressalta que a vítima da difamação pode buscar reparação pelos danos morais sofridos, sendo irrelevante se houve ou não prejuízo material, uma vez que o abalo à honra e à imagem já configura, por si só, lesão indenizável.

Gominho (2022) também chama atenção para o papel da sociedade na contenção da prática difamatória, defendendo que a educação digital e o incentivo ao respeito no ambiente virtual são medidas tão relevantes quanto a repressão penal, sobretudo diante da cultura de linchamento moral nas redes.

O crime de difamação no ambiente virtual ganhou proporções alarmantes nos últimos anos, principalmente em razão do uso desenfreado das redes sociais. A facilidade com que se publica conteúdo e a rapidez com que ele se espalha contribuem para a propagação de ofensas que atingem diretamente a reputação das vítimas. Traz a análise de Ferreira (2019) que a internet se tornou um espaço fértil para a destruição da imagem pública de indivíduos, muitas vezes sem qualquer fundamento factual.

A tipificação da difamação está prevista no Código Penal brasileiro e se refere à imputação de fato ofensivo à reputação de alguém, ainda que esse fato não configure crime. No meio digital, essa imputação é frequentemente feita em tom jocoso, irônico ou de denúncia pública, ampliando o alcance e os efeitos da ofensa. Lima (2019) destaca que a configuração do crime independe da veracidade da informação, bastando que ela comprometa a imagem da pessoa diante da coletividade.

Com a naturalização dos ataques verbais e da cultura de exposição nas redes, tornou-se comum a prática de linchamento moral digital, em que grupos inteiros se voltam contra

uma pessoa. Isso agrava o dano à vítima e torna o controle da difamação mais difícil. Ferreira (2019) afirma que o alcance coletivo da difamação virtual provoca danos morais de proporção incomum e duradoura.

A fiscalização da difamação digital depende de métodos técnicos e jurídicos de identificação do autor da publicação. Isso inclui o rastreamento do endereço IP, a quebra de sigilo de dados mediante ordem judicial e a análise de perfis em redes sociais. Traz a análise de Lima (2019) que o anonimato no meio virtual é ilusório, sendo plenamente possível localizar o responsável pela ofensa com a devida autorização judicial.

Outro ponto importante é que a difamação digital, diferentemente do que ocorre em conversas privadas, se perpetua no tempo. Mesmo que o conteúdo seja excluído posteriormente, ele já foi visualizado, replicado e armazenado em diversos dispositivos. Ferreira (2019) conclui que a natureza duradoura da difamação online exige resposta judicial imediata, sob pena de irreparabilidade do dano.

O Judiciário tem sido provocado com frequência para lidar com ações penais e cíveis decorrentes de difamações em ambientes digitais. As ações buscam não apenas a responsabilização penal, mas também a reparação por danos morais. Traz a análise de Lima (2019) que a via cível tem sido cada vez mais utilizada como instrumento de justiça restaurativa nesse tipo de infração.

Importante destacar que, ao contrário do que muitos acreditam, a liberdade de expressão não é um salvo-conduto para ofender. Existe um limite jurídico claro entre crítica e difamação. Quando se ultrapassa esse limite e se atinge a reputação de alguém com afirmações pejorativas ou inverídicas, configura-se o crime. Ferreira (2019) ressalta que o direito à honra é tão protegido quanto o direito de se expressar, sendo ambos tutelados constitucionalmente.

Outro aspecto que merece atenção é o papel das plataformas digitais. Ainda que não sejam responsáveis diretas pelo conteúdo, elas têm o dever de colaborar com a Justiça e de adotar medidas eficazes para coibir a propagação de conteúdos difamatórios. Lima (2019) explica que a ausência de uma política de controle contribui para a sensação de impunidade dos ofensores virtuais.

A cultura do cancelamento é um fenômeno moderno que frequentemente beira ou ultrapassa os limites da difamação. Pessoas são expostas publicamente, com ataques à sua honra e reputação baseados em versões parciais ou falsas de fatos. Traz a análise de Ferreira (2019) que essa prática agrava o dano moral e configura linchamento digital, muitas vezes irreparável para a vítima.

Nos casos em que a vítima identifica a publicação ofensiva, o ideal é reunir provas antes de qualquer exclusão. Prints de tela, URLs e dados de postagem são essenciais para a instrução da ação penal ou cível. Lima (2019) orienta que a preservação de provas digitais deve ser feita com cuidado técnico, respeitando a cadeia de custódia e a autenticidade das informações.

Quando o conteúdo é publicado em grupos privados de mensagens, como aplicativos de conversas, a difamação ainda assim pode ser caracterizada. Basta que mais de uma pessoa tenha acesso à mensagem e que esta contenha imputação ofensiva à reputação do ofendido. Ferreira (2019) destaca que o espaço onde ocorre a difamação, seja público ou restrito, não altera sua natureza penal.

O crime de difamação, previsto no artigo 139 do Código Penal Brasileiro, consiste na imputação de fato ofensivo à reputação de alguém perante terceiros. De acordo com Gominho (2022), trata-se de uma ofensa que atinge diretamente a honra objetiva da vítima, ou seja, a percepção social sobre sua conduta, valores e integridade.

Diferentemente da calúnia, a difamação não exige que o fato seja falso ou que constitua crime. Como pontua Filho (2024), o núcleo da conduta é a exposição de um fato que, ainda que verdadeiro, diminua a estima social da pessoa, comprometendo sua imagem diante da comunidade ou de um grupo específico.

Para a configuração da difamação, é essencial que a imputação chegue ao conhecimento de terceiros. Gominho (2022) enfatiza que não há crime quando a ofensa é proferida exclusivamente à vítima, sem qualquer divulgação ou repercussão, situação que caracteriza apenas injúria, por atingir a honra subjetiva.

Filho (2024) destaca que a difamação se consuma no instante em que terceiros tomam conhecimento da imputação ofensiva. Isso significa que a conduta torna-se típica independentemente da extensão da divulgação, bastando que uma única pessoa, além da vítima, receba a informação ofensiva.

Outro ponto relevante é que, na difamação, não se exige a falsidade do fato imputado. Conforme explica Gominho (2022), ainda que o conteúdo divulgado seja verdadeiro, sua exposição pública com o intuito de desprestigiar a vítima é suficiente para configurar o crime, pois o ordenamento jurídico também protege a privacidade e a reputação.

A ação penal nos crimes de difamação é, via de regra, privada, o que significa que somente o ofendido, ou seu representante legal, pode ajuizar a queixa-crime. Filho (2024) ressalta que o prazo para a propositura da ação é de seis meses, contados a partir do conhecimento da autoria do fato, sob pena de decadência.

No tocante à pena, o artigo 139 do Código Penal prevê detenção de três meses a um ano, e multa. Gominho (2022) observa que, apesar de parecer branda, a pena pode ser aumentada em razão de agravantes, como o uso de meios que facilitem a divulgação da difamação, a exemplo da internet e redes sociais.

A vítima de difamação pode buscar tutela judicial por meio de representação ao Ministério Público ou ingresso direto com ação penal privada. Há ainda a possibilidade de ajuizar ação de reparação por danos morais. Traz a análise de Lima (2019) que, além da responsabilização, a Justiça deve oferecer meios eficazes de remoção de conteúdo e proteção à integridade psicológica da vítima.

Há casos em que a difamação é associada a motivações discriminatórias, como gênero, raça, religião ou orientação sexual, o que agrava a responsabilidade do autor. Essas ofensas, quando feitas com dolo específico de humilhação, ultrapassam o limite do aceitável e podem configurar outros crimes em concurso. Ferreira (2019) sustenta que a análise do contexto é fundamental para aplicação justa da pena.

O tempo de resposta das autoridades também é essencial. A demora pode resultar na perda de provas, no agravamento dos danos ou até mesmo na inutilidade da futura sanção penal. Traz a análise de Lima (2019) que a Justiça precisa se adequar à velocidade da comunicação digital para não ser ineficaz.

A difamação digital pode afetar qualquer pessoa, mas celebridades e autoridades públicas costumam ser alvos mais frequentes. Ainda que figuras públicas estejam sujeitas a maior exposição, isso não autoriza a disseminação de inverdades ou ataques pessoais. Ferreira (2019) observa que a exposição pública não reduz o direito à honra, apenas aumenta a necessidade de vigilância e fiscalização.

As vítimas, muitas vezes, enfrentam também um segundo sofrimento ao serem desacreditadas quando denunciam a difamação. Isso pode inibir novas denúncias e reforçar a cultura de permissividade. Traz a análise de Lima (2019) que a naturalização da difamação em ambientes digitais constitui obstáculo à promoção de justiça e respeito.

O combate à difamação deve ocorrer em três frentes: repressiva, preventiva e educativa. A repressiva atua sobre o fato consumado, com responsabilização e reparação. A preventiva envolve mecanismos de controle e denúncias em plataformas. E a educativa diz respeito à formação de usuários conscientes e respeitosos. Ferreira (2019) argumenta que, sem educação digital, a repressão isolada será sempre insuficiente.

É possível observar que a reincidência de difamações, quando não punida, gera efeito de contágio. Outros usuários se sentem encorajados a agir da mesma forma, criando ondas de

ofensas virtuais. Traz a análise de Lima (2019) que o exemplo de impunidade alimenta o ciclo do crime e enfraquece a confiança da sociedade na Justiça.

Nos ambientes de trabalho e estudo, a difamação digital pode ser ainda mais destrutiva, afetando o rendimento e as relações pessoais. Além do dano emocional, há prejuízos profissionais e sociais. Ferreira (2019) sustenta que o espaço virtual não está dissociado da realidade, sendo muitas vezes o gatilho para processos de exclusão e marginalização.

A prática da difamação, mesmo que sob o pretexto de humor ou crítica, precisa ser analisada com rigor. O dano causado por uma piada ofensiva ou um “exposed” irresponsável pode ser permanente. Traz a análise de Lima (2019) que o humor não pode ser escudo para crimes contra a honra, especialmente quando vinculado a conteúdos virais de ampla repercussão.

> Especificando mais sobre a difamação, ela ocorre quando alguém divulga, ou fala um fato negativo sobre outra pessoa que possa prejudicar sua reputação, assim causando constrangimento e vergonha na vítima, mesmo que esse fato não constitua um crime. Em outras palavras, a difamação é a ato de transmitir informações ou rumores que podem manchar a imagem e a reputação da pessoa que é alvo da difamação, causando-lhe danos morais. Para que haja a difamação, é necessário que haja a imputação de um fato que seja ofensivo à reputação da pessoa. A diferença determinante entre difamação e injúria é que, na difamação, o fato ofensivo deve ser divulgado a terceiros, enquanto na injúria é uma ofensa direta à pessoa. O crime de difamação implica que o fato ofensivo seja levado ao conhecimento de outras pessoas além da vítima. A mera ofensa privada, sem divulgação, não configura difamação. O fato imputado deve ser capaz de afetar a imagem da pessoa na sociedade, prejudicando a forma como ela é vista pelos outros (GANASSINI, 2024, p. 09).

Por fim, a responsabilização pelos crimes de difamação na internet precisa ser acompanhada por uma mudança de cultura. O respeito, a empatia e a responsabilidade no uso da palavra devem ser valores promovidos tanto pelo Estado quanto pela sociedade. Ferreira (2019) conclui que a internet deve ser espaço de diálogo, não de destruição da dignidade alheia.

Filho (2024) lembra que a retratação pode excluir a punibilidade do autor, desde que feita de forma espontânea antes da sentença. Contudo, para que seja aceita, a retratação deve ser completa e pública, reparando os danos causados à imagem da vítima, o que nem sempre é simples no contexto da difamação digital.

A difamação virtual, por sua vez, tem merecido especial atenção da doutrina e jurisprudência. Conforme assinala Gominho (2022), as redes sociais intensificaram o alcance dos danos causados, pois a divulgação de conteúdo ofensivo pode ser replicada em larga

escala e perpetuar-se no ambiente digital.

Nesse contexto, torna-se evidente que a evolução tecnológica exige uma reinterpretação dos institutos penais tradicionais, como é o caso da difamação. Segundo Gominho (2022), a sociedade hiperconectada amplia as possibilidades de ataque à honra, exigindo maior rigor na aplicação do direito penal e maior atenção à proteção da imagem dos indivíduos.

Ao analisar o comportamento das pessoas nas plataformas digitais, observa-se um fenômeno perigoso: a banalização da reputação alheia. Filho (2024) chama a atenção para o fato de que muitos usuários utilizam a internet como se estivessem em um espaço sem lei, desconsiderando que as consequências jurídicas das ofensas permanecem válidas mesmo em ambientes virtuais.

Um aspecto relevante apontado por Gominho (2022) é a facilidade com que conteúdos difamatórios são replicados nas redes sociais, o que intensifica a ofensa e multiplica os danos. Isso ocorre porque cada compartilhamento não apenas propaga a informação ofensiva, mas também reforça sua credibilidade perante terceiros.

Filho (2024) reforça que a viralização de conteúdos ofensivos potencializa o dano à reputação da vítima, pois a velocidade e o alcance da difamação dificultam qualquer tentativa de retratação ou reparação. O prejuízo, nesses casos, adquire proporções que ultrapassam o controle individual, tornando-se muitas vezes irreversível.

Não se pode ignorar que, em alguns casos, o autor da difamação sequer possui vínculo direto com a vítima, sendo motivado por opiniões ideológicas, rivalidades pessoais ou mesmo por mero entretenimento. Como observa Gominho (2022), esse tipo de comportamento é incentivado por uma cultura digital que promove julgamentos sumários e condenações morais sem provas.

Filho (2024) aponta que, ainda que o autor da conduta alegue intenção crítica ou satírica, o ordenamento jurídico não permite que o exercício de um direito seja utilizado como instrumento de destruição da imagem alheia. A liberdade de expressão não se sobrepõe à dignidade da pessoa humana, sendo necessário o equilíbrio entre os direitos em conflito.

Nesse sentido, a jurisprudência tem reafirmado que o dever de respeito mútuo deve orientar toda e qualquer manifestação pública. Conforme destaca Gominho (2022), a internet não é um território isento de responsabilidade jurídica, sendo plenamente aplicáveis as normas penais a condutas praticadas nesse ambiente.

> Ao contrário do que hoje se imagina, há sim normas para combater os crimes cometidos pela internet. A Lei Carolina Dieckman (12.737/2012) e a Lei Azeredo (12.735/2012) entraram em vigor no dia 02 de abril de 2013 no Código Penal Brasileiro para tipificar uma série de condutas no ambiente digital. Há também o Marco Civil da Internet (Lei no 12.965/2014) e a Lei Geral de Proteção de Dados (Lei no 13.718/2018). No entanto, estas legislações não preveem todas as possibilidades de delitos praticados pela rede mundial de computadores fazendo-se necessário, em determinadas situações, empregar a analogia para punir alguns dos crimes cometidos pela internet, além de novos delitos, que antes da internet, não eram conhecidos e que, portanto, não contam com nenhuma tipificação. No entanto, o Direito – é importante destacar – está sempre à mercê e sujeito às inovações científicas e tecnológicas, de maneira que a solução para muitos delitos digitais pode chegar tarde demais até seus destinatários (GANASSINI, 2024, p. 14).

Outro ponto importante levantado por Filho (2024) diz respeito à retratação como causa extintiva da punibilidade. Embora prevista no Código Penal, a retratação deve ser completa e espontânea, com o objetivo de restaurar a honra da vítima. Contudo, em se tratando de redes sociais, nem sempre a retratação alcança o mesmo público da ofensa.

A jurisprudência também tem reconhecido que as plataformas digitais podem ser responsabilizadas, na esfera civil, quando não adotam medidas para a remoção de conteúdo difamatório após notificação. Gominho (2022) explica que, embora o autor da ofensa seja o responsável direto, as empresas que facilitam sua disseminação também possuem deveres de vigilância e cooperação.

Filho (2024) observa ainda que a vítima de difamação pode buscar tutela jurisdicional para obter não apenas a responsabilização penal do ofensor, mas também reparação por danos morais. Em muitos casos, os tribunais reconhecem a gravidade da violação e fixam indenizações significativas, a fim de desestimular a prática e compensar o sofrimento causado.

No aspecto probatório, Gominho (2022) ressalta a importância da preservação de provas digitais, como capturas de tela, links, data e horário das publicações. Esses elementos são fundamentais para demonstrar a autoria e a publicidade da ofensa, especialmente em ambientes onde os conteúdos podem ser rapidamente excluídos.

Filho (2024) destaca que, mesmo em grupos fechados ou aplicativos de mensagens, a difamação pode se consumar, desde que o conteúdo ofensivo tenha sido comunicado a pelo menos uma pessoa além da vítima. Assim, o crime se configura ainda que a mensagem não tenha sido divulgada publicamente.

Outro aspecto sensível, segundo Gominho (2022), é a prática de difamação contra figuras públicas. Embora o espaço para crítica seja mais amplo nesse contexto, os limites legais continuam existindo. A crítica deve incidir sobre atos públicos, e não sobre

características pessoais ou imputações desnecessariamente ofensivas.

Filho (2024) complementa afirmando que, mesmo pessoas com notoriedade social, como políticos, artistas ou influenciadores, têm direito à proteção da honra. A crítica contundente é legítima, mas não pode se converter em ofensa pessoal, sob pena de configurar abuso e ensejar responsabilização.

Por fim, Gominho (2022) conclui que o combate à difamação exige um esforço conjunto entre educação digital, responsabilização jurídica e fomento à cultura de respeito. A dignidade da pessoa humana deve ser resguardada como valor central nas relações sociais, inclusive e sobretudo nos espaços digitais.

5 CONSIDERAÇÕES FINAIS

A análise desenvolvida ao longo deste trabalho evidenciou que o crime de difamação, quando transposto para o ambiente digital, assume proporções significativamente mais complexas e lesivas. A facilidade de disseminação de conteúdos ofensivos nas redes sociais, aliada à sensação de anonimato proporcionada pelo meio virtual, cria um terreno fértil para ataques à honra que, muitas vezes, escapam ao controle da vítima e desafiam os mecanismos tradicionais de responsabilização jurídica.

A problemática central reside justamente na dificuldade de identificar autores, preservar provas digitais e aplicar sanções eficazes em tempo hábil, o que contribui para a perpetuação de uma cultura de impunidade. Além disso, há uma banalização da reputação alheia nas plataformas digitais, onde o julgamento moral coletivo e a exposição pública se sobrepõem ao devido processo legal, causando danos profundos e, por vezes, irreversíveis às vítimas.

Para enfrentar esse cenário, é imperativo o aprimoramento da legislação penal com tipificações mais específicas para condutas reiteradas em ambientes digitais. Do mesmo modo, o Poder Judiciário deve estruturar varas especializadas e investir em tecnologia forense para garantir agilidade na remoção de conteúdos e na punição dos infratores.

Também se impõe uma responsabilização mais efetiva das plataformas digitais, que devem implementar políticas de moderação mais rigorosas, com canais céleres de denúncia e resposta a conteúdos difamatórios, sob pena de responsabilidade civil por omissão. A aplicação do artigo 19 do Marco Civil da Internet precisa ser interpretada à luz do princípio da dignidade da pessoa humana, de modo a equilibrar a liberdade de expressão com o dever de proteção à honra.

Por fim, a educação digital deve ser incorporada como política pública transversal, a partir dos currículos escolares, campanhas de conscientização e treinamentos voltados para

usuários, professores e agentes da segurança pública. É essencial formar cidadãos críticos, conscientes dos limites legais da manifestação de pensamento e das consequências de seus atos no espaço virtual.

Portanto, combater a difamação digital exige mais do que dispositivos legais: exige vontade política, atuação institucional integrada e, principalmente, uma mudança cultural que resgate o respeito no ambiente virtual e afirme, com contundência, que a honra e a dignidade da pessoa humana não podem ser relativizadas pela tecnologia.

Portanto, a repressão penal à difamação e aos crimes cibernéticos deve caminhar junto à prevenção, ao estímulo à responsabilidade digital e ao fortalecimento da cultura dos direitos humanos na internet. Não se trata de limitar a livre expressão, mas de protegê-la contra o abuso e o desvio de finalidade.

Por fim, reforça-se que a construção de um ambiente digital seguro, ético e juridicamente responsável é um desafio coletivo. Depende da ação coordenada entre instituições, operadores do direito, sociedade civil, plataformas digitais e, principalmente, da consciência individual de cada cidadão em respeitar os direitos e os limites que sustentam uma convivência democrática.

REFERÊNCIAS

BARDlN, Laurence. **Análise de conteúdo.** Lisboa edições, 1977.

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

BRASIL. Lei nº 12.737, de 30 de novembro de 2012. **Dispõe sobre a tipificação criminal de delitos informáticos.** Diário Oficial da União: seção 1, Brasília, DF, 03 dez. 2012.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. **Marco Civil da Internet.** Diário Oficial da União, Brasília, 2014.

CARNEIRO, José Manoel. **Contratos eletrônicos e a responsabilidade dos intermediários digitais.** Rio de Janeiro: Forense, 2020.

CAVALCANTE, Lívia Teixeira Canuto; DE OLIVEIRA, Adélia Augusta Souto. **Métodos de revisão bibliográfica nos estudos científicos.** Psicologia em Revista, Belo Horizonte, v. 26, n. 1, p. 83-102, abr. 2020.

CERT.br. **Relatório de Incidentes de Segurança no Brasil, 2021.** Disponível em: https://www.cert.br/.

COSTA, Roberto Renato Strauhs da; PENDIUK, Fábio. **DIREITO DIGITAL: O MARCO CIVIL DA INTERNET E AS INOVAÇÕES JURÍDICAS NO CIBERESPAÇO**. Direito Digital: o marco civil brasileiro da internet e as inovações jurídicas no ciberespaço. Disponível em: http://publica.fesppr.br/ index.php/publica/article/viewFile/129/38.

DUTRA, Maristela Ap.; SILVA, Lorena Jaqueline. **A RESPONSABILIDADE CIVIL DOS PROVEDORES DE INTERNET DIANTE DE COMENTÁRIOS OFENSIVOS INSERIDOS POR TERCEIROS NAS REDES SOCIAIS À LUZ DO MARCO CIVIL DA INTERNET.** Revista Jurídica UNIARAXÁ, Araxá, v. 20, n. 19, p. 141-168, ago. 2016. Disponível em: https://ojs.uniaraxa.edu.br/index.php/juridica/article/view/516/495

ELIEZER, Cristina Rezende; GARCIA, Tonyel de Pádua. **O novo crime de invasão de dispositivo informático**. Revista do Curso de Direito do UNIFOR, [S. l.], v. 5, n. 1, p. 69–87, 2015. Disponível em: https://revistas.uniformg.edu.br/cursodireitouniformg/article/view/242. Acesso em: 6 nov. 2024.

ENISA. **European Union Agency for Cybersecurity.** Cybersecurity Threat Landscape, 2022.

FBI. **Internet Crime Report, 2021.** Disponível em: https://www.ic3.gov/Home/AnnualReports.

GIL, Antônio Carlos. **Métodos e Técnicas de Pesquisa Social.** 6ª ed. São Paulo: Atlas, 2019.

FEBRABAN. **Relatório Anual de Segurança Bancária, 2022.** Disponível em: https://www.febraban.org.br/. Acesso em: 3 out. 2024.

FERREIRA, Júlio Marinho. REDES, SOCIEDADE INFORMACIONAL E INTERNET: OS USOS POLÍTICOS DO ON-LINE NA CONTEMPORANEIDADE A PARTIR DA MASSIFICAÇÃO DE PÓS-VERDADES E DE FAKE NEWS. **A generalização da ideia de empresa nas políticas sociais: características e implicações**, v. 7, n. 12. Pelotas, 2019.

FILHO, Eduardo Tomasevicius. **Marco civil da internet:** uma lei sem conteúdo normativo. Estudos avançados, v. 30, n. 86, p. 269-285, 2016. Tradução. Disponível em: https://doi.org/10.1590/s0103- 40142016.00100017. Acesso em: 03 out. 2024.

GANASSINI, Vinicius Mendes. **Responsabilidade civil por difamação online.** Pontíficia Universidade Católica: Goiânia, 2024.

GOMINHO, Victor de Coimbra Pinto. **Crimes Virtuais: O Sequestro de Dados na Doutrina Brasileira.** Portal de Trabalhos Acadêmicos, [S. l.], v. 8, n. 1, 2022. Disponível em: https://revistas.faculdadedamas.edu.br/index.php/academico/article/view/2152. Acesso em: 3 out. 2024.

HAMMERSCHMIDT, K. S. de A.; FRANCO DAVID, D. **RESPONSABILIDADE PENAL DA PESSOA COLETIVA E O PRINCÍPIO DA CULPABILIDADE NOS CRIMES INFORMÁTICOS EM REDES SOCIAIS**,2023.Disponível em: ttps://cadernopaic.fae.emnuvens.com.br/cadernopaic/article/view/559. Acesso em: 3 out. 2024.

ISTOÉ DINHEIRO. **Cibercrimes terão impacto de mais de US$ 1 trilhão na economia global em 2020. IstoÉ Dinheiro,** 2020. Disponível em: https://istoedinheiro.com.br/cibercrimes-terao-impacto-de-mais-de-us-1-trilhao-na-economia-global-em-2020/. Acesso em: 7 nov. 2024.

LIBMAN, Juliana. **Moderação de conteúdo em redes sociais:** por uma regulação que promova a liberdade de expressão. Dissertação de Mestrado (Programa de Mestrado Profissional em Direito Civil Contemporâneo e Prática Jurídica) - Pontifícia Universidade Católica. Rio de Janeiro, 2023.

LIMA, Clara Affeld Martins de; **O TRATAMENTO DE DADOS PESSOAIS PELO "LEGÍTIMO INTERESSE" DO CONTROLADOR:** análise da perspectiva europeia e brasileira. Trabalho de Conclusão de Curso (Ciências Jurídicas e Sociais) - Universidade Federal do Rio Grande do Sul. Porto Alegre, 2019.

MULHOLLAND, Caitlin; FRAJHOF, Isabella Z. Frajhof. **Entre as leis da robótica e a ética: regulação para o adequado desenvolvimento da inteligência artificial. Direito Digital e Inteligência Artificial.** Rio de Janeiro, 2021.

PINTO, Josane Daniela Freitas. **O texto multimodal e os construtos identitário-ideológicos no discurso político do Facebook.** 2020. Tese (Doutorado em Filologia e Língua Portuguesa) - Faculdade de Filosofia, Letras e Ciências Humanas, University of São Paulo, São Paulo, 2020.

PIOVESAN, F. **Crimes digitais e a responsabilidade dos intermediários:** uma análise comparada. Porto Alegre: Livraria do Advogado, 2018.

POMPEU, Bruno; TRINDADE, Eneus; SATO, Silvio Koiti. **Consumo, cidadania e vigilância: Reflexões sobre a expansão tecnológica e seus impactos no contexto brasileiro**. Estudos Avançados, v. 38, n. 110, p. 87-104, 2024.

RODRIGUES, Cláudio Araújo. **Análise da aplicação do direito penal nos crimes virtuais**. Pensar Acadêmico, Rio de Janeiro, 2021.

SILVA, Ronaldo Couto da; NOVAIS, Thyara Gonçalves. **A LEI GERAL DE PROTEÇÃO DE DADOS E SUA APLICAÇÃO NO COMBATE AOS CRIMES CIBERNÉTICOS: DESAFIOS E PERSPECTIVAS**. Revista Ibero-Americana de Humanidades, Ciências e Educação, [S. l.], v. 9, n. 10, p. 4679–4703, 2023. DOI: 10.51891/rease.v9i10.12254. Disponível em: https://periodicorease.pro.br/rease/article/view/12254. Acesso em: 3 out. 2024.

VIANNA, Geraldo Luiz. **Constitucionalismo e Democracia: O Estado Constitucional e a Permanente tensão entre Poder e Direitos.** Revista Direito em Foco, v. 7, p. 1-14, 2015.

WANDERLEY, Carlos Alberto Cardoso; COSTA, Rodrigo Silva da; RIBEIRO, Lara de Paula. **CRIMES CIBERNÉTICOS EM TEMPOS DE PANDEMIA:** O ISOLAMENTO SOCIAL COMO PROPULSOR DA VULNERABILIDADE DA POPULAÇÃO E DO AUMENTO DOS CASOS. QUALIS B1. FLUXO CONTÍNUO. JUNHO/2022. Ed. 37 V.