CURSO DE DIREITO

JOSÉ LUIS PARANHOS DA SILVA

CRIMES CONTRA A HONRA NAS REDES SOCIAIS: OS LIMITES DA LIBERDADE DE EXPRESSÃO NO MUNDO VIRTUAL

Cuiabá/MT

2025

CURSO DE DIREITO

JOSÉ LUIS PARANHOS DA SILVA

CRIMES CONTRA A HONRA NAS REDES SOCIAIS: OS LIMITES DA LIBERDADE DE EXPRESSÃO NO MUNDO VIRTUAL

Trabalho de Conclusão de Curso apresentado à Banca Avaliadora do Departamento de Direito, da Faculdade FASIPE Cuiabá, como requisito parcial para a obtenção do título de Bacharel em Direito.

Orientadora: Prof. Ma. Giovana César Scherner.

Cuiabá/MT

2025

JOSÉ LUIS PARANHOS DA SILVA

CRIMES CONTRA A HONRA NAS REDES SOCIAIS: OS LIMITES DA LIBERDADE DE EXPRESSÃO NO MUNDO VIRTUAL

Trabalho de Conclusão de Curso apresentado à Banca Avaliadora do Curso de Direito da Faculdade Fasipe Cuiabá como requisito parcial para a obtenção do título de Bacharel em Direito.

Aprovado em _____/_____/_____.

Prof. Ma. GIOVANA CÉSAR SCHERNER
Professora Orientadora
Departamento de Direito – FASIPE CPA

NOME EXAMINADOR
Professor Avaliador
Departamento de Direito – FASIPE CPA

NOME EXAMINADOR
Professor Avaliador
Departamento de Direito – FASIPE CPA

OLMIR BAMPI JÚNIOR
Coordenador do curso de Direito – FASIPE CPA

Cuiabá/MT

2025

DEDICATÓRIA

Dedico este trabalho primeiramente a Deus, Aquele que guia meus passos, ilumina meu caminho e, em todos os momentos de angústia, nunca deixa de estar ao meu lado.
À minha família, especialmente a minha mãe e meu pai, que me acompanham desde o início de minha existência e, com amor incondicional, não medem esforços para me ver feliz e realizado.
Também, a todos os amigos que fiz ao longo desta jornada, cuja amizade é um bem valioso, pelo qual sou grato.
Por fim, agradeço aos docentes desta faculdade, que compartilharam seus conhecimentos e me inspiraram a me tornar o profissional que almejo ser.

AGRADECIMENTOS

- Primeiramente agradeço a Deus pelo dom da vida, por ter permitido chegar até aqui e por sempre estar me abençoando.

- Agradeço a minha mãe, Nilma Ferreira da Silva, e ao meu pai, Luis Paranhos da Silva, por sempre estarem presentes, por todo esforço e sacrifício que realizaram para que eu pudesse estudar e por sempre me apoiar.

- Agradeço aos meus amigos de classe, pelo companheirismo durante esse ciclo.

- Por fim, agradeço a todos os professores que contribuíram para o meu crescimento ao longo dessa jornada.

EPÍGRAFE

Praticar a justiça é alegria para o justo, mas espanto para os que praticam a iniquidade.

Provérbios 21:15.

DA SILVA, José Luis Paranhos. **Crimes Contra a Honra nas Redes Sociais: Os Limites da Liberdade de Expressão no Mundo Virtual.** 2025. 50 folhas. Trabalho de Conclusão de Curso – Faculdade Fasipe Cuiabá.

RESUMO

Este Trabalho de Conclusão de Curso tem como objetivo analisar os crimes contra a honra cometidos nas redes sociais, destacando a complexa relação entre tais condutas e os limites da liberdade de expressão no ambiente virtual. A metodologia utilizada foi a revisão bibliográfica, de pesquisa qualitativa, dialogando com doutrinadores e estabelecendo uma conexão com a legislação e entendimentos jurisprudenciais. Ao longo da pesquisa, foi apresentada uma fundamentação teórica acerca da origem da internet, das redes sociais, do conceito de honra e da tipificação penal da calúnia, difamação e injúria. Também se discutiu a forma como esses crimes se manifestam no mundo digital e o impacto da massificação da informação nas redes sociais. Por fim, abordou-se a colisão entre os direitos fundamentais da honra e da liberdade de expressão, utilizando-se da teoria da ponderação para demonstrar a necessidade de equilíbrio na aplicação desses direitos, sem que um anule o outro. O estudo revelou que, embora a internet seja um espaço de ampliação da comunicação, também se tornou terreno fértil para práticas ofensivas, exigindo respostas jurídicas e sociais coerentes com os princípios constitucionais.

Palavras chaves: Crimes contra a honra; Crimes Virtuais; Liberdade de Expressão.

DA SILVA, José Luis Paranhos. **Crimes Against Honor on Social Networks: The Limits of Freedom of Expression in the Virtual World.** 2025. 50 sheets. Law Course Conclusion Paper – FASIPE CPA – University of Cuiabá.

ABSTRACT

This Final Undergraduate Paper aims to analyze crimes against honor committed on social media, highlighting the complex relationship between such conduct and the limits of freedom of expression in the virtual environment. The methodology employed was a bibliographic review with a qualitative research approach, engaging with legal scholars and establishing a connection with legislation and jurisprudential interpretations. Throughout the research, a theoretical foundation was presented regarding the origin of the internet, social networks, the concept of honor, and the legal classification of slander, defamation, and insult. The study also discussed how these crimes manifest in the digital world and the impact of the mass dissemination of information through social networks. Finally, it addressed the conflict between the fundamental rights to honor and freedom of expression, applying the balancing theory to demonstrate the need for equilibrium in the enforcement of these rights, ensuring that one does not nullify the other. The study revealed that, although the internet is a space that enhances communication, it has also become fertile ground for offensive practices, requiring legal and social responses that are consistent with constitutional principles.

Keywords: Crimes Against Honor; Cybercrimes; Freedom of Expression.

SUMÁRIO

1. INTRODUÇÃO **10**
2. REVISÃO DE LITERATURA **13**
2.1 A Origem da Internet **14**
2.2 O Ciberespaço **15**
2.3 As Redes Sociais **16**
2.3.1 Redes Sociais no Ambiente Digital 17
2.4 Dos Crimes Virtuais **19**
2.5 Da Contextualização da Honra **21**
2.6 Dos Tipos de Crime Contra a Honra **23**
2.6.1 Do Crime de Calúnia 23
2.6.2 Do Crime de Difamação 25
2.6.3 Do Crime de Injúria 27
2.7 Dos Crimes Contra a Honra nas Redes Sociais **28**
2.8 Da Liberdade de Expressão **31**
2.8.1 Colisão de Direitos Fundamentais: Ponderação entre Liberdade de Expressão e Proteção à Honra 32
2.9 A Legislação Brasileira Frente aos Crimes Cibernéticos **34**
2.9.1 Da chamada Lei "Carolina Dieckmann" 35
2.9.2 Do Marco Civil da Internet 38
2.9.3 Da Lei Geral de Proteção de Dados (LGPD) 39
3. RESULTADOS ESPERADOS **43**
4. CONSIDERAÇÕES FINAIS **44**
REFERÊNCIAS **46**

1. INTRODUÇÃO

A realização desta pesquisa visa abordar os crimes contra a honra cometidos nas redes sociais e como eles se conciliam com os limites da liberdade de expressão no mundo virtual. O estudo explorará as implicações jurídicas e sociais desses crimes, de modo a compreender como as interações na internet podem resultar em ofensas à honra das pessoas.

A facilidade com que informações se disseminam no ambiente virtual, combinada com a sensação de anonimato que permeia as interações online, transforma as redes sociais em um espaço propício para a prática de delitos que ferem a honra e a dignidade das pessoas. Essa dinâmica não apenas facilita a propagação de ofensas, mas também cria um ambiente onde as vítimas frequentemente se sentem desprotegidas e vulneráveis. Portanto, compreender as nuances desse fenômeno é essencial para o desenvolvimento de estratégias eficazes de prevenção e resposta.

A legislação brasileira, apesar de evoluir para acompanhar as tecnologias, ainda possui desafios que comprometem a proteção da honra no ambiente digital como, por exemplo, a identificação dos autores dos crimes que utilizam perfis falsos a fim de cometer atos ilícitos e prejudicar outros usuários.

A rápida criação de novas plataformas exige uma constante atualização das normas para acompanhar a dinâmica virtual. Além disso, a falta de clareza em algumas disposições legais pode dificultar a aplicação da justiça, deixando vítimas sem recursos adequados. Por isso, é essencial que o sistema jurídico se adapte de forma ágil e eficaz às novas realidades da internet.

Os crimes contra a honra nas redes sociais podem causar danos psicológicos graves, afetando a reputação, as relações sociais e o bem-estar emocional das vítimas. A divulgação de informações falsas ou ofensivas pode gerar consequências duradouras, inclusive no campo profissional, prejudicando oportunidades de emprego e interações pessoais. Por isso, é essencial reconhecer os impactos desses crimes e promover uma cultura de respeito e

responsabilidade online.

Outro aspecto relevante é a responsabilidade das plataformas de redes sociais. Essas empresas desempenham um importante papel na moderação de conteúdos e, consequentemente, na prevenção de crimes, uma vez que são responsáveis por implementar políticas e ferramentas que auxiliam o monitoramento de conteúdos compartilhados, bem como a identificação e exclusão de postagens de cunho ofensivo, difamatórias ou relacionadas a outros tipos de crimes contra a honra.

A principal problemática nesse contexto é a dificuldade de conciliar a liberdade de expressão com a proteção da honra e da imagem das pessoas. A rápida disseminação de informações nas redes sociais, somada à falsa sensação de anonimato, torna essas plataformas propícias para crimes contra a honra. Diante disso, a pesquisa busca responder à questão: qual a melhor forma de equilibrar esses direitos em um ambiente marcado pela massificação das redes sociais?

O objetivo geral da pesquisa visa analisar a complexa relação entre os crimes contra a honra nas redes sociais e os limites da liberdade de expressão, buscando compreender como a legislação atual se adapta a essa nova realidade e quais são as implicações sociais e jurídicas dessa dinâmica para a proteção da honra e da imagem no ambiente digital.

Para a realização da pesquisa, adotou-se o método qualitativo. Nesse sentido, Mirian Goldenberg (2004, p. 14) explica que “na pesquisa qualitativa a preocupação do pesquisador não é com a representatividade numérica do grupo pesquisado, mas com o aprofundamento da compreensão de um grupo social, de uma organização, de uma instituição, de uma trajetória etc.”. Goldenberg (2004, p. 53) complementa que "os dados qualitativos consistem em descrições detalhadas de situações com o objetivo de compreender os indivíduos em seus próprios termos".

A pesquisa qualitativa, portanto, trata-se de uma abordagem investigativa que busca compreender a profundidade dos significados, experiências e fenômenos sociais. Foram consultadas, assim, legislações pertinentes, livros, artigos e demais materiais relevantes disponíveis em bases de dados acadêmicas e fontes confiáveis na internet. Essa escolha metodológica permite captar nuances e interpretações que não seriam alcançadas por meio de dados numéricos.

Com o objetivo de aprofundar o conhecimento sobre o tema proposto, a metodologia empregada consistiu na pesquisa bibliográfica, que é o processo de levantamento, análise e interpretação de informações já publicadas sobre um determinado tema. Em suma, a leitura crítica da bibliografia e a identificação das categorias centrais são passos necessários para que

o pesquisador tenha uma fundamentação teórica sólida e defina claramente sua posição no campo de estudo, possibilitando que sua pesquisa seja bem estruturada.

2. REVISÃO DE LITERATURA

O presente capítulo tem como objetivo apresentar o embasamento teórico que sustenta a análise dos crimes contra a honra no ambiente virtual, com especial atenção aos limites da liberdade de expressão nas redes sociais. Para tanto, a revisão de literatura será organizada de forma a proporcionar uma compreensão gradual e estruturada do tema, desde os aspectos tecnológicos até os fundamentos jurídicos e sociais envolvidos.

Inicialmente, será abordada a origem da internet e sua evolução até os dias atuais, oferecendo uma visão geral do surgimento desse espaço digital. Em seguida, discorre-se sobre o conceito de ciberespaço como ambiente de interação humana mediada por tecnologias, e o papel das redes sociais como espaços privilegiados de comunicação, onde se manifestam tanto o exercício da liberdade de expressão quanto condutas potencialmente lesivas à honra.

A partir desse contexto, o capítulo explora a noção de crimes virtuais, destacando a complexidade da responsabilização penal nesse novo cenário. Em seguida, será feita a contextualização do conceito de honra, analisando seus aspectos históricos, sociais e jurídicos, para então classificar e discutir os tipos de crimes contra a honra previstos no ordenamento jurídico brasileiro.

O foco se volta, então, para a ocorrência desses crimes no ambiente das redes sociais, onde a velocidade, a informalidade e o amplo alcance das publicações intensificam os efeitos dessas condutas. Na sequência, será analisada a liberdade de expressão, com ênfase em sua dimensão constitucional e nos limites impostos quando esse direito colide com outros bens jurídicos, como a honra e a dignidade.

Por fim, o capítulo apresenta uma síntese da legislação brasileira aplicável aos crimes cibernéticos, destacando os principais marcos normativos e as atualizações legislativas voltadas à proteção da honra no mundo virtual. Essa estrutura visa fornecer uma base teórica sólida para a compreensão dos desafios jurídicos contemporâneos relacionados ao tema.

2.1 A Origem da Internet

A internet é, sem dúvida, um dos avanços tecnológicos que mais contribuem para a humanidade, uma vez que oferece um leque de possibilidades que facilitam a vida das pessoas, principalmente no que diz respeito à comunicação. O nascimento desta tecnologia ocorreu entre os anos de 1960 e 1970, durante a Guerra Fria, com o objetivo de ser uma ferramenta alternativa de comunicação militar, prezando a durabilidade e preservação das informações.

Stephen Segaller argumenta que "[...] *we see the creation of the Internet as one of the twentieth century's most productive acidentes.*"[1] (SEGALLER, 1998, p. 29). Com essa afirmação, o autor enfatiza a improbabilidade de que um meio de comunicação tão avançado tenha sido desenvolvido de forma intencional e planejada desde o início.

Isso significa que, ao contrário do senso comum, a internet não foi fruto de um planejamento meticuloso, mas sim o resultado inesperado de testes, experimentações e inovações acumuladas ao longo do tempo. Por isso, sua evolução pode ser compreendida como um "acidente produtivo", uma vez que sua criação emergiu da convergência de diversos projetos e descobertas que, gradualmente, se integraram.

A partir dos experimentos e das inovações que contribuíram para o nascimento da internet, os cientistas norte-americanos desenvolveram a ARPANet (*Advanced Research Projects Agency Network*), que consistia na conexão de quatro computadores, buscando rapidez, eficácia e segurança no envio de informações. Assim, ARPANet, que era um projeto financiado pelo governo dos Estados Unidos, revolucionou a forma com que as pessoas se conectam pelo mundo.

No Brasil, essa tecnologia chegou em setembro de 1988, quando foi restabelecida uma conexão internacional dedicada e contínua, unindo, assim, a emergente iniciativa brasileira de redes acadêmicas ao restante do mundo. Os primeiros usuários da internet foram, na sua maioria, pesquisadores, professores e alunos, onde tiveram contato com ferramentas inovadoras, como o correio eletrônico, as bases de dados internacionais e, por conseguinte, à rede mundial de computadores.

No entanto, esse acesso ainda não era a internet que é utilizada nos dias atuais, como afirma Getschko (2009), "Não era, ainda, a Internet. A essa só nos conectamos em 1991, ainda sem saber da magnitude do impacto que estava por vir" (GETSCHKO, 2009, n.p).

---

[1] "[...] vemos a criação da Internet como um dos acidentes mais produtivos do século XX." (SEGALLER, 1998, p. 29, tradução nossa).

Ou seja, foi apenas em 1991, que o Brasil começou a utilizar a verdadeira conexão com a Internet, vivenciando um crescimento exponencial no uso da rede, o surgimento do *World Wide Web* (WWW) e a criação de provedores de acesso, facilitando a inclusão de novos usuários e ampliando o alcance da Internet. Isso causou uma revolução na comunicação, consumo e trabalho das pessoas.

2.2 O Ciberespaço

O termo "ciberespaço" (*cyberspace*) nasce por intermédio de William Gibson, que cunhou a palavra em sua obra literária "Neuromancer", publicada em 1984. Para Gibson, o ciberespaço tratava-se de:

> Uma alucinação consensual vivida diariamente por bilhões de operadores autorizados, em todas as nações, por crianças aprendendo altos conceitos matemáticos... Uma representação gráfica de dados abstraídos dos bancos de dados de todos os computadores do sistema humano. Uma complexidade impensável. Linhas de luz abrangendo o não-espaço da mente; nebulosas e constelações infindáveis de dados. Como marés de luzes da cidade [...] (GIBSON, 2003, n.p.).

A citação de William Gibson, em Neuromancer, expressa de forma poética e visionária o conceito de ciberespaço, muito antes de sua consolidação prática na realidade tecnológica atual. Ao descrever o ciberespaço como "uma alucinação consensual vivida diariamente por bilhões de operadores autorizados", o autor antecipa uma dimensão virtual compartilhada por usuários ao redor do mundo, uma rede digital que ultrapassa limites físicos e conecta pessoas por meio da informação.

Gibson transforma o abstrato em imagens sensoriais: "linhas de luz abrangendo o não-espaço da mente", "nebulosas e constelações infindáveis de dados", "marés de luzes da cidade". Essas metáforas sugerem que o universo digital se constrói não apenas com códigos e circuitos, mas também com experiências humanas, percepções, interações e aprendizados. Em suma, a realidade virtual não se limita a uma ferramenta, mas configura-se em uma extensão simbólica e quase sensorial da própria consciência coletiva da humanidade.

Por outro ponto de vista, para Pierre Lévy (1999, p. 92), o ciberespaço é "[...] o espaço de comunicação aberto pela interconexão mundial dos computadores e das memórias dos computadores.", tal ideia implica que a internet cria um novo espaço de interação humana que se desenvolve de maneira significativa, promovendo, assim, a troca de informações e a expressão de ideias em um contexto que, idealmente, é democrático e acessível a todos.

Lévy destaca que:

> Uma das principais funções do ciberespaço é o acesso a distância aos diversos recursos de um computador. Por exemplo, contanto que eu tenha esse direito, posso, com a ajuda de um pequeno computador pessoal, conectar-me a um enorme computador situado a milhares de quilômetros e fazer com que ele execute, em alguns minutos ou algumas horas, cálculos (cálculos científicos, simulações, síntese de imagens etc.) que meu computador pessoal levaria dias ou meses para executar. (LÉVY, 1999, p. 93).

Interpretando a ideia de Lévy, compreende-se que o ciberespaço amplia as possibilidades de uso e a inclusão digital, pois traz a democratização do acesso à tecnologia, permitindo que indivíduos com equipamentos não tão modernos possam usufruir da capacidade computacional avançada, possibilitando o acesso a recursos que seriam inacessíveis se dependessem apenas de computadores locais, como a conexão à distância e a transferência de arquivos, por exemplo.

A definição de ciberespaço não é exclusiva apenas a redes de computadores, isto é, também se trata de um espaço desenvolvido pelas interações de várias tecnologias de telemática e comunicação, não se restringindo apenas às experiências online. Essa ideia é defendida por Mario J. L. Guimarães Jr., que diz:

> O termo "Ciberespaço" pode ser definido como o locus virtual criado pe1a conjunção das diferentes tecnologias de te1ecomunicação e telemática, em especial, mas não exc1usivamente, as mediadas por computador. E importante sublinhar que esta definição não circunscreve o Ciberespaço a redes de computadores, mas sim percebe como suas instancias diferentes aparatos de te1ecomunicação, desde teleconferências anal6gicas, passando por redes de computadores, "pagers", comunicação entre radio-amadores e por serviços do tipo "tele-amigos". (GUIMARÃES JÚNIOR, 2000, p. 142).

Mediante o pensamento dos autores, extrai-se que o ciberespaço é um território informacional, social, dinâmico, acessível e em constante expansão. Ele supera o simples conceito de ser uma conexão entre computadores, configurando-se como um ambiente de interação humana, que permite a troca de informações, culturas e saberes de forma ampla e descentralizada. Trata-se, portanto, de um espaço que redefine os limites da experiência social e tecnológica.

2.3 As Redes Sociais

O termo “rede social” tem sua origem em fundamentos diversificados, que se baseiam em situações específicas vivenciadas. De acordo com Barnes (1987, p. 161), “cada

analista, além de dar uma interpretação diferente às análises feitas por seus predecessores, apresenta versões mais refinadas à ideia de rede social a fim de adequá-las ao seu problema particular".

Essa interpretação de Barnes (1987) reflete na riqueza do conceito sobre o tema, bem como sua adaptabilidade a diferentes situações e contextos. Dentre as vertentes que definem o que é rede social, Musso (2006, p. 34) define o termo como "uma das formas de representação dos relacionamentos afetivos, interações profissionais dos seres humanos entre si ou entre seus agrupamentos de interesses mútuos.".

Tal definição enfatiza como as redes sociais identificam e representam formas de interação, conectando pessoas com interesses ou objetivos comuns e, assim, moldando relações e experiências no mundo.

2.3.1 Redes Sociais no Ambiente Digital

No âmbito virtual, as redes sociais emergem como uma resposta às necessidades de comunicação e interação em um mundo cada vez mais digital. Nesse sentido, Raquel da Cunha Recuero (2009, p. 94) diz que "as redes sociais analisadas na Internet podem ser de dois tipos: as redes emergentes e as redes de filiação ou redes de associação".

As redes sociais emergentes, segundo a autora, "são aquelas expressas a partir das interações entre os atores sociais. São redes cujas conexões entre os nós emergem através das trocas sociais realizadas pela interação social e pela conversação por meio da mediação do computador." (RECUERO, 2009, p. 94). Entende-se, portanto, que as conexões entre as pessoas nesse tipo de rede não são pré-estabelecidas ou fixas, mas nascem e crescem através de diálogos e interações online.

Sobre as "Redes de Filiação ou Redes Associativas", Recuero desta que:

> [...] há apenas um conjunto de atores, mas são redes de dois modos porque é estudado um conjunto de eventos aos quais um determinado ator pertence.
> Chama-se rede de dois modos porque são medidas duas variáveis: além dos atores-indivíduos são observados os eventos. Cada um desses eventos é, ainda, um elemento de conexão de um conjunto de atores. As redes de filiação seriam, assim, constituídas de dois tipos de nós: os atores e os grupos. Esses nós se relacionariam por conexões de pertencimento. (RECUERO, 2009, p. 97).

À luz do pensamento da autora, é possível descrever que as redes de filiação ou associação são estruturadas de forma mais estável e formal. Tal rede, geralmente, reflete laços

sociais estabelecidos que possam incluir grupos de amizades, interesses comuns ou até mesmo relações profissionais. Essas redes podem ser facilmente identificáveis em plataformas que permitem a configuração de relacionamentos de forma explícita, como o *Facebook, Instagram* ou *LinkedIn*.

Atualmente, as redes sociais online estão mais fortes que nunca. O compartilhamento de mensagens, fotos, vídeos e outros conteúdos **é** cada vez mais massivo, sendo impulsionado pelo aumento do acesso à internet ao longo dos anos. Essa conectividade constante transformou as redes em espaços de influência, opinião e mobilização social. Além disso, moldam comportamentos, tendências e até decisões políticas em escala global.

Segundo a Pesquisa Nacional por Amostra de Domicílios (PNAD) de 2019, realizada pelo IBGE e divulgada em 14/04/2021 pelo Ministério das Comunicações, 82,7% dos domicílios brasileiros possuem acesso à internet, um aumento de 3,6 pontos percentuais em relação a 2018, evidenciando o constante crescimento da conectividade no país. Esse avanço reflete a popularização das tecnologias digitais e a ampliação do acesso às redes móveis e fixas, ocasionando um maior consumo de conteúdo no ambiente digital.

Outro fator que contribuiu para o aumento do uso das redes sociais foi à popularização dos celulares com acesso à internet. Segundo dados do Instituto Brasileiro de Geografia e Estatística - IBGE “em 2023, 87,6% das pessoas de 10 anos ou mais de idade tinham telefone móvel celular para uso pessoal, crescimento de 1,1 p.p. em relação a 2022 (86,5%)” (BRASIL, 2024). Logo, a facilidade de acessar tais redes em qualquer lugar e a qualquer momento, contribui para o crescimento constante do uso dessas plataformas.

Além disso, o período de isolamento, devido à pandemia do Covid-19, que ocorreu entre 2020 ao início de 2022, atuou, também, como um catalisador significativo para o aumento do uso das redes sociais. Dada a necessidade de distanciamento social, bem como o fechamento de ambientes públicos, boa parte da população utilizou as redes sociais como uma válvula de escape, justamente para suprir a falta de interação com outras pessoas.

Márcio Migon, coordenador do Comitê Gestor da Internet no Brasil (CGI.br), destaca que:

> A internet e os dispositivos móveis passaram a desempenhar papel central durante a pandemia, possibilitando a continuidade de atividades empresariais com o home office, do comércio com as vendas online, prestação de serviços públicos, atividades educacionais com o ensino remoto e de saúde com as teleconsultas. (NITAHARA, 2021).

Diante dessa concepção, o cenário pandêmico promoveu o aumento no uso das

tecnologias digitais e, consequentemente, intensificou a presença das redes sociais na vida cotidiana de milhões de brasileiros. Assim, as redes sociais como *WhatsApp, Facebook, X* (antigo *Twitter*), *TikTok* e o *Instagram* consolidaram-se entre as mais populares do mundo, conforme evidencia a pesquisa da Agência *We Are Social* (2023), reforçando sua influência no dia a dia das pessoas.

2.4 Dos Crimes Virtuais

O acesso em ambientes virtuais tornou-se cotidiano na vida das pessoas, uma vez que as informações, entretenimento, descontração e interação social atraem todo o tipo de indivíduo, inclusive aqueles de má conduta. Devido à sensação de anonimato e impunidade, criminosos praticam todo o tipo de delito, corrompendo um espaço que deveria ser voltado para o desenvolvimento e o benefício da humanidade. Nesse contexto, a expansão do uso dos meios digitais trouxe avanços, mas também desafios à integridade e segurança dos usuários.

De acordo com a pesquisa e reportagem de Antonio Barros (2006), divulgada pela Agência Câmara, os primeiros registros de crimes no âmbito da informática ocorreram nos Estados Unidos, no ano de 1960, em que a nova modalidade de criminosos praticava atividades ilícitas como sabotagem e espionagem utilizando a combinação perfeita: computadores e a internet. Assim, as pesquisas científicas sobre esse tipo de crime só foram iniciadas na década seguinte, isto é, a partir de 1970.

Foi em 1980 que ocorreu a “explosão” dos crimes cibernéticos, as atividades criminosas tiveram um aumento significativo, principalmente nos crimes de cópia não autorizados de programas de computador, comumente conhecido como pirataria; abusos nas telecomunicações e crimes relacionados a pornografia infantil. Esse período marcou o começo de uma nova era de desafios para a segurança digital, onde tais delitos passaram a ocorrer com maior frequência, exigindo, portanto, regulamentação específica e atualizada.

Assim como os crimes comuns, os crimes cibernéticos são condutas corriqueiras, antijurídicas e culpáveis, no entanto, diferem no fato de serem praticados contra ou com a utilização de sistemas de informática. Corroborando com esta ideia, Augusto Rossini (2004) diz:

> [...] o conceito de “delito informático” poderia ser talhado como aquela conduta típica e ilícita, constitutiva de crime ou contravenção, dolosa ou culposa, comissiva ou omissiva, praticada por pessoa física ou jurídica, com o uso da informática, em ambiente de rede ou fora dele, e que ofenda, direta ou indiretamente, a segurança

> informática, que tem por elementos a integridade, a disponibilidade a confidencialidade. (ROSSINI, 2004, p. 110.).

Partindo dessa premissa, os criminosos virtuais usam todas as sua expertise e conhecimentos de informática para infringir a Lei e prejudicar bens ou a integridade de terceiros. Por outro lado, não é necessário ter um vasto conhecimento e manuseio dos sistemas da informação para cometer um crime, tendo em vista que uma palavra proferida com o intuito de ofender a outrem pode configurar um crime. Nessa perspectiva, Cassanti (2014) defende que:

> Os crimes virtuais não são praticados apenas por atacantes com conhecimento sofisticado de informática. Ameaças cometidas por e-mails como calúnia (acusar alguém de um crime que não cometeu), agressão e desrespeito por motivo de cor, raça, etnia ou religião são cada vez mais frequentes entre os usuários, que utilizam na maioria das vezes redes sociais como Facebook, Twitter, YouTube ou os blogs para práticas desses delitos. Muitas vezes os autores acreditam que suas ações ficarão impunes. (CASSANTI, 2014, p. 49.).

Com base na argumentação de Cassanti (2014), entende-se que qualquer indivíduo, independentemente de sua formação ou conhecimento técnico, pode se envolver em atividades ilícitas online devido a grande e massiva acessibilidade à internet. Além disso, um dos fatores principais que contribuem para a prática de crimes cibernéticos é a falsa sensação de impunidade, em que os usuários infratores acreditam que seus atos não terão consequências legais, por acharem que estão escondidos atrás do anonimato, conforme destaca Cassanti (2014):

> O maior incentivo aos crimes virtuais é dado pela falsa sensação de que o meio digital é um ambiente sem leis, mas é importante saber que quando o computador é uma ferramenta para prática dos delitos, suscita a possibilidade de se amoldar aos tipos penais já existentes. Por exemplo, a calúnia pode ser praticada tanto em um jornal quanto na internet: é o mesmo crime, mudando apenas o meio de sua efetivação, potencializando a sua comunicação. Neste caso, as penas aplicadas são as mesmas, independentemente do meio utilizado para a prática do crime. (CASSANTI, 2014, p. 49.).

Apesar de a classificação de cibercrimes resultar de várias interpretações na doutrina jurídica, destaca-se o entendimento de Vicente Greco Filho (2000), que defende:

> Em matéria penal, 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. (GRECO, 2000).

Em resumo, com base na análise de Greco Filho, é possível compreender a variabilidade dos crimes cometidos no ambiente virtual e a necessidade de adequação da legislação para garantir a proteção da infraestrutura digital e, principalmente, dos indivíduos. Nesse norte, sumarizando a ideia do autor supracitado, a classificação dos crimes se divide em dois tipos: crimes próprios e impróprios.

Os crimes próprios referem-se aos que são praticados diretamente contra os sistemas de informática, uma vez que têm como objetivo invadir ou danificar computadores, dados ou redes, independentemente dos motivos do agente. Por exemplo, um ataque que visa invadir bancos de dados para alterar ou roubar informações é considerado um crime próprio.

Já os crimes impróprios são práticas direcionadas contra outros bens jurídicos através de um sistema de informática, ou seja, crimes que focam na propriedade, privacidade ou honra de uma pessoa. A calúnia, por exemplo, é esse tipo de crime. Essa classificação é de suma importância, tendo em vista que ajuda a compreender a natureza dos atos ilícitos no âmbito digital, bem como a necessidade de legislações adequadas que abordem cada tipo de crime, focando suas particularidades e impactos.

2.5 Da Contextualização da Honra

Além de sua relevância moral e social, a honra possui status de direito fundamental na ordem constitucional brasileira. O artigo 5º, inciso X, da Constituição Federal de 1988, estabelece que “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”.

Esse dispositivo evidencia que a proteção à honra ultrapassa o campo ético, sendo juridicamente resguardada como um dos pilares da dignidade da pessoa humana. Assim, a honra integra o núcleo essencial dos direitos fundamentais da personalidade, sendo tutelada tanto na esfera civil quanto penal.

Antes de abordar o assunto dos crimes contra a honra, é imprescindível a compreensão do conceito de honra no ordenamento jurídico. Partindo dessa premissa, Noronha (1988, p. 116) define a honra como um “complexo ou conjunto de predicados ou condições da pessoa que lhe conferem condição social e estima própria", ou seja, a honra não

se trata de somente uma característica individual, mas também de um reflexo da posição social do indivíduo na sociedade.

Por sua vez, Pagliuca (2006, p. 82) defende que a honra "pode ser definida como o conjunto de particularidades de uma pessoa que lhe atribuem consideração, estima e dignidade, não apenas pessoal, como ainda no âmbito social". Nesse sentido, ao utilizar a expressão "conjunto de particularidades" para se referir à honra, o autor indica que a honra é uma combinação de comportamento, personalidade e valores morais, sendo essas particularidades essenciais para a formação da percepção que os outros têm de um indivíduo.

De uma forma geral, a doutrina destaca a honra sobre duas perspectivas: a honra objetiva e a subjetiva. Assim, Prado descreve essas perspectivas da seguinte forma:

> A honra, do ponto de vista objetivo, seria a reputação que o indivíduo desfruta em determinado meio social, a estima que lhe é conferida; subjetivamente, a honra seria o sentimento da própria dignidade ou decoro. A calúnia e a difamação atingiriam a honra no sentido objetivo (reputação, estima social, bom nome); já a injúria ofenderia a honra subjetiva (dignidade, decoro). (PRADO, 2009, p. 213).

À luz do pensamento de Prado, a honra objetiva refere-se à reputação e o reconhecimento social, enquanto a honra subjetiva trata-se da autoimagem e dignidade que o indivíduo possui de si mesmo. Ambos os aspectos de honra são fundamentais para a dignidade das pessoas, pois influenciam a forma em que os indivíduos se percebem e são percebidos pelos outros.

A fim de coibir e ofensas e garantir a integridade das pessoas, é preciso a proteção legal dos aspectos de honra, conforme destacado pelo Art. 5°, inciso X da Constituição Federal de 1988, o qual diz que "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".

No entanto, nenhum direito é absoluto, estando todos sujeitos a possíveis limitações normativas. Tanto a liberdade de expressão quanto o direito à honra, por exemplo, podem ser restringidos para garantir a convivência harmônica entre os direitos fundamentais. A Constituição Federal, em seu artigo 53[2], estabelece que deputados e senadores não podem ser responsabilizados, nas esferas civil ou penal, por suas opiniões ou palavras, o que garante a esses parlamentares ampla liberdade de manifestação no exercício de seus mandatos.

Porém, essa prerrogativa não deve ser interpretada como uma autorização irrestrita para ofensas pessoais. Ainda que haja imunidade formal, os congressistas não estão

[2] Art. 53. Os Deputados e Senadores são invioláveis, civil e penalmente, por quaisquer de suas opiniões, palavras e votos. (BRASIL, 1988).

totalmente isentos de responsabilização quando suas manifestações extrapolam os limites do razoável, configurando abuso de direito ou violação à dignidade de terceiros.

2.6 Dos Tipos de Crime Contra a Honra

Os crimes contra a honra estão previstos no Código Penal brasileiro como formas de proteção à dignidade, à reputação e à imagem do indivíduo. Essa categoria de delitos se divide em três tipos principais: calúnia, difamação e injúria, cada um com características próprias e elementos específicos. A seguir, serão analisados separadamente esses tipos penais, com destaque para suas definições legais, requisitos, distinções entre si e suas implicações práticas.

2.6.1 Do Crime de Calúnia

A calúnia é um dos crimes contra a honra previstos no ordenamento jurídico brasileiro e se caracteriza pela falsa imputação de um fato definido como crime a alguém. Trata-se de uma conduta que atinge diretamente a honra objetiva da vítima, causando-lhe danos morais e sociais, ao atribuir-lhe, de forma inverídica, a prática de um ato criminoso. Esse delito está tipificado no artigo 138 do Código Penal, que diz:

> Art. 138 - Caluniar alguém, imputando-lhe falsamente fato definido como crime: Pena - detenção, de seis meses a dois anos, e multa.
> § 1º - Na mesma pena incorre quem, sabendo falsa a imputação, a propala ou divulga.
> § 2º - É punível a calúnia contra os mortos.
> [...] (BRASIL, 1940)

Partindo dessa premissa, Rogério Greco (2017, p. 615) defende que “A calúnia é o mais grave de todos os crimes contra a honra previstos pelo Código Penal.” Com base nessa perspectiva, a calúnia configura uma ofensa especialmente grave, por imputar falsamente à vítima a prática de um crime. Diferente da difamação e da injúria atinge a esfera penal, podendo gerar consequências jurídicas concretas. Por isso, é considerada mais danosa, tanto moral quanto juridicamente, justificando o destaque dado por ambos os autores.

Greco destaca que:

> Assim, podemos indicar os três pontos principais que especializam a calúnia com relação às demais infrações penais contra a honra, a saber: a) a imputação de um fato; b) esse fato imputado à vítima deve, obrigatoriamente, ser falso; c) além de

> falso, o fato deve ser definido como crime. (GRECO, 2017, p. 615).

Ou seja, para a configuração do crime de calúnia, é essencial que se atribua falsamente a alguém um fato concreto e definido como crime pela legislação penal. Não se trata apenas de apontar uma conduta ofensiva ou imoral, mas sim de imputar, de forma mentirosa, um fato que esteja tipificado como infração penal.

Nesse sentido, não é suficiente uma acusação vaga ou genérica. A imputação deve conter elementos que individualizam o suposto crime, como a identificação da vítima, o local do acontecimento ou as circunstâncias em que se teria dado. A ausência desses detalhes compromete a caracterização do delito, pois impede a precisão necessária à sua tipificação.

Um exemplo seria quando alguém, sem base concreta, afirma que um conhecido "cometeu um crime", sem especificar qual, contra quem ou em que circunstâncias. Por ser vaga, tal acusação dificilmente configura calúnia. No entanto, se a imputação for falsa, mas contiver detalhes que configure a conduta e descrevam fato tipificado como crime, poderá haver responsabilização penal, nos termos do artigo 138 do Código Penal.

Além disso, Greco defende que:

> A calúnia se consuma quando um terceiro, que não o sujeito passivo, toma conhecimento da imputação falsa de fato definido como crime.
> Dependendo do meio pelo qual é executado o delito, há possibilidade de se reconhecer a tentativa (GRECO, 2017, p. 617).

A partir da análise do pensamento do referido autor, chega-se à conclusão que calúnia é um crime que se consuma no momento em que um terceiro, diferente da pessoa falsamente acusada, toma conhecimento da imputação de um fato que a lei define como crime. Em termos claros, não basta que o agente formule a acusação falsa; é necessário que essa acusação chegue ao conhecimento de outra pessoa para que se configure a consumação.

No entanto, dependendo da forma como o agente tenta praticar o crime, por exemplo, por carta, mensagem ou outros meios, pode ocorrer a interrupção do ato antes que o terceiro tome conhecimento da imputação. Nesses casos, é possível reconhecer a forma tentada do delito, já que o agente iniciou os atos de execução, mas não conseguiu consumá-los por circunstâncias alheias à sua vontade.

É importante ressaltar que, para configurar a calúnia, exige-se a imputação falsa de um fato tido como crime, desde que tenha a mínima verossimilhança. Em outras palavras, se a acusação é absurda ou impossível, não há configuração do crime, pois o fato é inverossímil e não afeta a honra de forma penalmente relevante.

Essa também é uma perspectiva abordada por Rogério Greco, em que comenta: “Também não poderá configurar-se como calúnia a imputação de fatos inverossímeis, como no exemplo daquele que atribui a alguém a subtração da estátua do Cristo Redentor, afixada no morro do Corcovado, na cidade do Rio de Janeiro” (GRECO, 2017, p. 616).

Há de se comentar, ainda, que o crime de calúnia exige, necessariamente, o dolo, ou seja, a intenção de ofender a honra da vítima (*animus caluniandi*), sendo possível tanto o dolo direto quanto o eventual. Em suma, não há previsão de calúnia na modalidade culposa, à luz da jurisprudência do Superior Tribunal de Justiça: “O dolo específico (*animus calumniandi*), ou seja, a vontade de atingir a honra do sujeito passivo, é indispensável para a configuração do delito de calúnia. (BRASIL, STJ, Apn 473/DF, Rel. Min. Gilson Dipp, 5ª T., DJe 8/9/2008).

2.6.2 Do Crime de Difamação

A difamação é caracterizada pela atribuição de um ato que prejudica a reputação de uma pessoa, imputando uma conduta que compromete sua honra perante a sociedade, independentemente de essa conduta ser considerada um crime. A veracidade da acusação é irrelevante, isto é, a mera alegação já constitui o delito, conforme dita o artigo 139 do Código Penal:

> Art. 139 - Difamar alguém, imputando-lhe fato ofensivo à sua reputação:
> Pena - detenção, de três meses a um ano, e multa.
> Exceção da verdade
> Parágrafo único - A exceção da verdade somente se admite se o ofendido é funcionário público e a ofensa é relativa ao exercício de suas funções. (BRASIL, Código Penal, 1940).

Conforme o entendimento do Supremo Tribunal Federal – STF, “O delito de difamação considera-se perpetrado por quem, afirmando fato certo e definido, ofende a honra de outrem, ainda que se repisem fatos sobre aquilo que os outros reputam a respeito do cidadão, no tocante a seus atributos físicos, intelectuais e morais.” (BRASIL, STF, Inq. 2915/PA, Rel. Min. Luiz Fux, Pleno, DJe 31/5/2013).

A difamação se distingue da calúnia e da injúria, conforme descreve Jesus (2007):

> Enquanto a calúnia existe imputação de fato definido como crime, na difamação o fato é meramente ofensivo a reputação do ofendido. Além disso, o tipo de calúnia exige elemento normativo da falsidade da imputação, o que é irrelevante no delito da

> difamação. Enquanto na injúria o fato versa sobre qualidade negativa da vítima, ofendendo-lhe a honra subjetiva, na difamação há ofensa à reputação do ofendido, versando sobre fato a ela ofensivo. (JESUS, 2007, p. 225).

Com base no pensamento do autor acima, entende-se que, na calúnia, ocorre a imputação de um fato específico que a lei considera crime, enquanto na difamação o fato atribuído é apenas ofensivo à reputação da pessoa, sem necessariamente constituir crime. Além disso, a calúnia exige que o fato imputado seja falso, sendo esse elemento essencial ao tipo penal, o que não é exigido na difamação.

Já a injúria se diferencia por atingir diretamente a dignidade ou o sentimento pessoal da vítima, com ofensas que recaem sobre características negativas dela, afetando sua honra subjetiva. Por outro lado, a difamação atinge a honra objetiva, relacionada à imagem social da vítima.

Semelhante à calúnia, para que a difamação seja considerada consumada é preciso que terceiros, além da vítima, também tenham conhecimento da ofensa, ou seja, não basta que apenas a vítima saiba do fato ofensivo. Isso se dá porque o dano à honra ou à reputação tem um sentido social, dependente da divulgação para outras pessoas além da vítima.

Corroborando com essa ideia, Rogério Greco destaca:

> Às vezes nos soa um pouco ilógico entender que a consumação se dá quando terceiro toma conhecimento dos fatos ofensivos à reputação da vítima, mas exigimos, em geral, que esses mesmos fatos cheguem ao conhecimento dela para que, se for da sua vontade, possa ser proposta ação penal contra o agente difamador, no prazo de 6 (seis) meses, sob pena de ocorrer a decadência do seu direito de ação. (GRECO, 2017, p. 632).

Ou seja, mesmo que o crime já tenha se consumado perante terceiros, a contagem do prazo de seis meses para a propositura da queixa-crime só começa quando a vítima tiver conhecimento da ofensa. Caso ela não tome nenhuma providência nesse período, ocorre a decadência, simplificando, ela perde o direito de ingressar com a ação penal.

Assim como ocorre no crime de calúnia, não se admite a modalidade culposa na difamação, conforme entendimento consolidado na jurisprudência do Superior Tribunal de Justiça, que afirma:

> A denúncia deve estampar a existência de dolo específico necessário à configuração dos crimes contra a honra, sob pena de faltar-lhe justa causa, sendo que a mera intenção de caçoar (animus jocandi), de narrar (animus narrandi), de defender (animus defendendi), de informar ou aconselhar (animus consulendi), de criticar (animus criticandi) ou de corrigir (animus corrigendi) exclui o elemento subjetivo e, por conseguinte, afasta a tipicidade desses crimes. (BRASIL, STJ, HC 234134/MT,

Rel. Min. Laurita Vaz, j. 06 nov. 2012, DJe 16 nov. 2012).

É válido ressaltar que, segundo o entendimento do STF "A pessoa jurídica pode ser vítima de difamação, mas não de injúria e calúnia" (BRASIL, STF. RHC 83091 / DF. Relator: Min. Marco Aurélio. 2003). Portanto, o STF entende que somente a difamação pode atingir a honra objetiva da pessoa jurídica, uma vez que é possível "manchar" sua reputação pública. Por outro lado, a calúnia e injúria são tipos penais que exigem características pessoais, por isso não se aplicam à pessoa jurídica.

2.6.3 Do Crime de Injúria

Conforme o artigo 140 do Código Penal, o crime de injúria consiste em "Injuriar alguém, ofendendo-lhe a dignidade ou o decoro" (BRASIL, 1940), em suma, quando alguém faz um comentário que desrespeita ou menospreza outra pessoa, configura-se a injúria. Partindo desse contexto, Pagliuca (2006, p. 88) diz que a injúria "consiste também em mais um escudo à honra, sendo o delito uma manifestação de desrespeito e deboche a outrem", isto é, a injúria reflete a opinião do autor da ofensa, o qual sempre representa um desprezo pelo injuriado.

Embora seja tida como a menos grave entre os crimes contra a honra, a injúria revela-se uma das mais complexas em razão da sua estrutura normativa. Ao se analisar o dispositivo legal que a define, observa-se que esse delito se desdobra em três modalidades distintas, conforme explica Rogério Greco, ao afirmar que "[...] o Código Penal trabalha com três espécies de injúria: a) injúria simples, prevista no caput do art. 140; b) injúria real, consignada no § 2º do art. 140; c) injúria preconceituosa, tipificada no § 3º do art. 140" (GRECO, 2017, p.639).

Nesse sentido, a chamada injúria simples, prevista no caput do art. 140, é a forma básica do delito e, de fato, a menos grave entre os crimes contra a honra. Isso porque consiste unicamente na ofensa à dignidade ou ao decoro da vítima, sem imputação de fato determinado, sem uso de violência ou motivação discriminatória. Trata-se, portanto, de um ataque à honra subjetiva, geralmente por meio de palavras ou gestos, limitando-se à detenção de um a seis meses, ou multa.

Em uma posição intermediária está a injúria real, descrita no § 2º do mesmo artigo, que ocorre quando a ofensa é praticada mediante violência ou outro meio que torne mais grave a agressão à dignidade da vítima. A pena aplicada nesse caso é semelhante àquela

prevista para o crime de difamação, o que demonstra um maior rigor em comparação com a injúria simples.

Por fim, a modalidade mais grave é a injúria preconceituosa, prevista no § 3º, que envolve ofensas motivadas por discriminação relacionada à raça, cor, etnia, religião, origem, idade ou deficiência. Essa última é tratada com maior severidade pelo ordenamento jurídico, refletindo uma preocupação com a proteção de grupos que são, historicamente, mais vulneráveis.

Uma característica exclusiva da injúria, entre os crimes analisados, é a possibilidade de concessão do perdão judicial. Essa hipótese está prevista nos incisos I e II do §1º do art. 140 do Código Penal e consiste na faculdade conferida ao magistrado de deixar de aplicar a pena, mesmo diante da configuração do tipo penal, nos casos em que houver provocação ou retorsão entre as partes envolvidas no processo criminal. Nessas circunstâncias, a punibilidade do agente é extinta.

A consumação do crime de injúria, diferentemente do que ocorre na calúnia e na difamação, dá-se no momento em que a vítima toma conhecimento das expressões ofensivas dirigidas à sua dignidade ou ao seu decoro. Nesse contexto, Greco observa que “Considerando que o delito atinge a honra subjetiva, consuma-se a injúria no momento em que a vítima toma conhecimento das palavras ofensivas à sua dignidade ou decoro” (GRECO, 2017, p. 641).

Sumarizando, a presença da vítima no instante em que a ofensa é proferida não é condição necessária para a configuração do delito. Basta que, mesmo ausente, ela venha a tomar ciência da agressão à sua honra, como no caso em que terceiros reproduzem as palavras ofensivas posteriormente.

2.7 Dos Crimes Contra a Honra nas Redes Sociais

A internet, a princípio, deveria ser encarada como um espaço democrático, onde diversas formas de opiniões e pensamentos coexistissem, proporcionando, assim, debates sobre uma variedade de temas. No entanto, os usuários da internet precisam assumir a responsabilidade por suas opiniões e terem ciência das consequências de suas palavras, pois as expressões feitas no mundo virtual podem gerar efeitos significativos e irreversíveis na vida das pessoas.

O mundo informático trouxe muitos benefícios e facilidades à humanidade, conforme destaca Aras (2001):

> Um novo ramo do Direito nasceu — e logo passou a ser sistematizado — quando os computadores se tornaram uma ferramenta indispensável ao cotidiano das pessoas e das empresas e do próprio Estado. A importância da informática na sociedade tecnológica é incontestável. (ARAS, 2001, p. 1).

Em outra perspectiva, a informatização gerou uma significativa insegurança em relação à confiabilidade do armazenamento de dados, principalmente aqueles que são sigilosos e que são relacionados a assuntos financeiros de indivíduos e instituições do ramo financeiro. Seguindo essa linha de pensamento, Lima defende que:

> Essa nova era da informação não traz somente vantagens, a segurança das informações armazenadas nos sistemas computadorizados ganha gigantesca importância quando, no mundo todo, as instituições financeiras passam a fazer toda espécie de transações monetárias com uso de computadores. (LIMA, 2006, p. 2).

Dessa forma, percebe-se que o avanço tecnológico, especialmente no que se refere à informatização dos sistemas e à digitalização de dados, trouxe consigo uma série de benefícios relacionados à agilidade e à eficiência dos serviços. No entanto, é imprescindível reconhecer que tais avanços também impõem novos desafios, sobretudo no que tange à segurança da informação.

Conforme destacado por Lima (2006, p. 2), a era da informação não se resume às vantagens proporcionadas pelo uso da tecnologia, mas também acarreta preocupações significativas, especialmente no contexto das instituições financeiras, que passaram a realizar praticamente todas as suas transações por meio de sistemas informatizados.

Assim, a proteção de dados sensíveis e a adoção de mecanismos eficazes de segurança tornam-se elementos essenciais para garantir a integridade, a confidencialidade e a disponibilidade das informações. Este cenário reforça a necessidade de regulamentações específicas e de constante atualização das práticas de segurança cibernética.

Segundo o Ministério da Justiça e Segurança Pública, com base em dados divulgados pela Delegacia de Repressão aos Crimes Informáticos (DRCI) e em conformidade com o Código Penal, os crimes mais comuns praticados na internet são: o crime de ameaça, calúnia, difamação, injúria e o crime de falsa identidade.

Devido a esses crimes, a honra e integridade das pessoas são feridas todos os dias, pois as redes sociais se tornam uma ferramenta de propagação de ofensas por pessoas más intencionadas. Dessa forma, a disseminação dessas ofensas impacta diretamente na vida das pessoas em escala global, devido sua rápida propagação pelo planeta. Nesse norte, na atualidade, as agressões não ocorrem apenas fisicamente, mas também virtualmente, atingindo

diretamente a dignidade do indivíduo.

O uso das redes sociais se intensificou durante a pandemia de COVID-19, já que, devido ao isolamento social, as pessoas passaram a se comunicar principalmente por meio dessas plataformas, que se tornaram ainda mais relevantes nesse período de distanciamento necessário para combater o vírus. Assim, para Martins (2020):

> [...] apenas o meio eletrônico que na verdade parece irradiar com maior facilidade e velocidade dimensionando drasticamente os efeitos da conduta danosa já que a internet, também para condutas reprováveis, consegue ser um facilitador na medida em que dá voz àqueles que, em outro contexto, talvez não fariam. (MARTINS, 2020, n.p).

Por sua vez, Teixeira argumenta que:

> Crimes contra a honra, quando são praticados em ambiente virtual, como é a internet, podem provocar às vítimas danos em extensão bem maior do que se praticados nas vias ordinárias da vida real. Isso porque uma informação circulando na rede e/ou colocada em comunidades virtuais (redes sociais) alcança um número ilimitado de pessoas, uma vez que houve uma ampliação do espaço "público" por onde os efeitos do crime poderiam percorrer. (TEIXEIRA, 2020, n.p).

Sintetizando a argumentação de Teixeira, constata-se que a internet, com sua característica de ampliação do espaço público, permite que os efeitos de crimes como difamação, injúria ou calúnia se espalhem de forma muito mais rápida e abrangente, intensificando o impacto na vida das vítimas. Dessa forma, os crimes contra a honra ganham uma dimensão nova e mais perigosa devido à facilidade de disseminação da informação e à dificuldade de controlar seu alcance.

É importante destacar que o artigo 141 do Código Penal estabelece hipóteses específicas de aumento de pena para os crimes contra a honra, quando cometidos em determinadas circunstâncias qualificadas. Assim, com foco nas redes sociais, o §2º do referido artigo, dispões que: "Se o crime é cometido ou divulgado em quaisquer modalidades das redes sociais da rede mundial de computadores, aplica-se em triplo a pena.".

Tal disposição normativa reforça o entendimento de que a internet, ao ampliar exponencialmente o alcance e a repercussão das ofensas, exige uma resposta penal proporcional aos danos gerados. Assim, conclui-se que os crimes contra a honra, quando praticados em redes sociais, assumem uma dimensão mais lesiva, justificando o tratamento jurídico mais severo atribuído pelo ordenamento atual.

2.8 Da Liberdade de Expressão

"Uma das primeiras aspirações na modernidade (século XVIII), no que se refere à dignidade humana foi a afirmação da liberdade como valor essencial à condição humana." (DE FREITAS; DE CASTRO, 2013, p. 330). Nesse contexto, a liberdade passou a ser reconhecida como um dos pilares centrais da dignidade da pessoa.

Tal concepção surgiu como resposta a regimes autoritários e estruturas sociais que limitavam a autonomia dos indivíduos. A afirmação da liberdade como valor essencial refletia a busca por uma sociedade mais justa, em que cada pessoa pudesse exercer sua vontade, expressar suas ideias e fazer escolhas sem coerção externa. Assim, a liberdade foi consolidada como fundamento indispensável para o pleno desenvolvimento humano e para a construção de uma ordem jurídica e social baseada no respeito à pessoa.

A respeito da liberdade de expressão, De Freitas e De Castro comentam:

> Em verdade, a Liberdade de Expressão, desdobrada em diferentes modalidades (Liberdade de Imprensa e Liberdade Religiosa), adquire relevância extrema para a afirmação da burguesia no período das Revoluções Liberais, quer como um instrumento de propagação das ideias revolucionárias (Liberdade de Imprensa), quer para a afirmação do Estado Laico, repelindo qualquer subordinação ou influência da Igreja Católica (Liberdade Religiosa). (DE FREITAS; DE CASTRO, 2013, p. 328).

A liberdade de imprensa permitiu a difusão das ideias revolucionárias, contribuindo para a mobilização social e política, uma vez que permitiu pensamentos, críticas e propostas contrárias ao regime vigente pudessem ser publicados e disseminados sem censura ou repressão estatal.

Já a liberdade religiosa foi essencial para a consolidação do Estado laico, ao estabelecer a separação entre Igreja e Estado e rejeitar a influência da Igreja Católica sobre os assuntos políticos. Dessa forma, a liberdade de expressão consolidou-se como um instrumento de afirmação de novos valores sociais e de reorganização do poder.

Mundialmente, o direito à liberdade de expressão está amparado no Artigo 19º da Declaração Universal dos Direitos Humanos, que diz "Todo o indivíduo tem direito à liberdade de opinião e de expressão, o que implica o direito de não ser inquietado pelas suas opiniões e o de procurar, receber e difundir, sem consideração de fronteiras, informações e ideias por qualquer meio de expressão." (ORGANIZAÇÃO DAS NAÇÕES UNIDAS, 1948).

Já no Brasil, além do Artigo 19º da Declaração Universal dos Direitos Humanos, a liberdade de expressão tem fundamentação legal na Constituição Federal de 1988, mais

especificadamente nos artigos:

> Art. 5º, IV - é livre a manifestação do pensamento, sendo vedado o anonimato;
> Art. 5º, IX - é livre a expressão da atividade intelectual, artística, científica e de comunicação, independentemente de censura ou licença;
> Art. 220. A manifestação do pensamento, a criação, a expressão e a informação, sob qualquer forma, processo ou veículo não sofrerão qualquer restrição, observado o disposto nesta Constituição. (BRASIL, 1988).

Nesse sentido, a liberdade de expressão pode ser observada como um conjunto de direitos vinculados às liberdades de comunicação. Seguindo essa linha de raciocínio, Magalhães (2008, p. 74) argumenta que "liberdades fundamentais que devem ser asseguradas conjuntamente para se garantir a liberdade de expressão no seu sentido total". Portanto, esse conjunto de direitos tem como objetivo proteger tanto aqueles que transmitem quanto aqueles que recebem informações, críticas e opiniões.

2.8.1 Colisão de Direitos Fundamentais: Ponderação entre Liberdade de Expressão e Proteção à Honra

No contexto constitucional contemporâneo, a colisão entre direitos fundamentais não é uma anomalia, mas sim um fenômeno estrutural de grande magnitude, como ressalta Robert Alexy "não existe catálogo de direitos fundamentais sem colisão de direitos fundamentais e também um tal não pode existir. Isso vale tanto para colisões de direitos fundamentais em sentido estrito como também para tais em sentido amplo." (ALEXY, 1999, p. 68).

Essa realidade exige a adoção de um método que possibilite a harmonização dos direitos em tensão. Para tanto, Alexy propõe a teoria dos princípios, segundo a qual os direitos fundamentais são normas que não se aplicam de forma absoluta, mas sim "ordenam que algo seja realizado em uma medida tão ampla quanto possível relativamente a possibilidades fáticas ou jurídicas" (ALEXY, 1999, p. 74).

Dessa forma, ao invés de se resolver os conflitos por meio da simples subsunção, típica das regras, utiliza-se a ponderação, que é o processo metodológico que avalia a proporcionalidade entre os princípios envolvidos. A ponderação se dá, segundo Alexy, em três fases sucessivas: "Na primeira fase deve ser determinada a intensidade da intervenção. Na segunda fase se trata, então, da importância das razões que justificam a intervenção. Somente na terceira fase sucede, então, a ponderação no sentido estrito e próprio." (ALEXY, 1999, p. 78).

Essa estrutura culmina no que o autor denomina lei da ponderação, segundo a qual "quanto mais intensiva é uma intervenção em um direito fundamental tanto mais graves devem ser as razões que a justificam" (ALEXY, 1999, p. 78). Tais premissas são essenciais para analisar o embate entre a liberdade de expressão e a proteção à honra, pois permitem que o intérprete constitucional avalie, à luz do caso concreto, qual princípio deve prevalecer sem a supressão total do outro, garantindo, assim, a máxima efetividade dos direitos fundamentais em conflito.

A liberdade de expressão constitui um dos pilares do Estado Democrático de Direito, sendo garantida pelo artigo 5º[3], inciso IV[4], IX[5] e, também, no art. 220[6] da Constituição Federal de 1988. Contudo, não se trata de um direito absoluto, pois encontra limites tanto de natureza moral quanto jurídica, especialmente quando seu exercício compromete outros direitos fundamentais.

O Supremo Tribunal Federal, ao julgar o Habeas Corpus n. 82.424/RS, reafirmou esse entendimento ao destacar que "o direito à livre expressão não pode abrigar, em sua abrangência, manifestações de conteúdo imoral que implicam ilicitude penal.", ressaltando ainda que: "As liberdades públicas não são incondicionais, por isso devem ser exercidas de maneira harmônica, observados os limites definidos na própria Constituição Federal (CF, artigo 5º, § 2º, primeira parte)." (BRASIL, STF, HC 82.424/RS, 2003).

Nesse contexto, discursos que ultrapassam o campo da opinião e incidem na esfera da ilicitude, como a incitação ao racismo, a calúnia, a injúria ou a difamação, não são protegidos pelo manto da livre manifestação do pensamento. A ponderação entre os direitos envolvidos deve levar em consideração não apenas a formalidade da liberdade de expressão, mas, sobretudo, os impactos concretos que determinadas manifestações podem gerar na esfera jurídica e pessoal dos indivíduos atingidos, especialmente quando comprometam sua honra, imagem ou integridade moral.

Fortalecendo essa ideia, o STF entende que:

> O preceito fundamental de liberdade de expressão não consagra o "direito à incitação ao racismo", dado que um direito individual não pode constituir-se em

---

[3] Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:

[4] IV - é livre a manifestação do pensamento, sendo vedado o anonimato;

[5] IX - é livre a expressão da atividade intelectual, artística, científica e de comunicação, independentemente de censura ou licença;

[6] Art. 220. A manifestação do pensamento, a criação, a expressão e a informação, sob qualquer forma, processo ou veículo não sofrerão qualquer restrição, observado o disposto nesta Constituição.
(BRASIL, 1988)

> salvaguarda de condutas ilícitas, como sucede com os delitos contra a honra. Prevalência dos princípios da dignidade da pessoa humana e da igualdade jurídica. [...] No estado de direito democrático devem ser intransigentemente respeitados os princípios que garantem a prevalência dos direitos humanos. (BRASIL, STF, HC 82.424/RS, 2003).

Esse entendimento demonstra a aplicação do princípio da prevalência dos direitos humanos, segundo o qual o ordenamento jurídico deve, em caso de conflito, priorizar valores fundamentais que assegurem o respeito à pessoa humana em detrimento de liberdades que venham a ser usadas como escudo para discursos de ódio ou práticas discriminatórias. Em suma, a liberdade de expressão deve coexistir com outros direitos e valores protegidos pela Constituição, como a dignidade humana e os direitos de personalidade.

Além das normas constitucionais, o ordenamento jurídico brasileiro conta com legislações infraconstitucionais que tipificam condutas ilícitas relacionadas à discriminação. A título de exemplo, a Lei nº 7.716/1989, em seu artigo 20, criminaliza a prática, induzimento ou incitação ao preconceito e à discriminação por motivos de raça, cor, etnia, religião ou procedência nacional. Essa norma impõe limites objetivos à liberdade de expressão, ao vedar manifestações que promovam o ódio ou a intolerância, assegurando, assim, a proteção de grupos historicamente vulnerabilizados.

É imprescindível, então, que as pessoas possuam plena consciência das implicações de suas expressões e opiniões, especialmente quando estas são divulgadas na internet. A liberdade de expressão é um direito fundamental, mas deve ser exercida com responsabilidade, evitando qualquer prática criminosa que possa violar a honra e a dignidade de terceiros.

Destarte, a necessidade de limitar certos atos de manifestações, quando estes se tornam preconceituosos ou ilegais, é uma medida cabível para garantir o respeito e a integridade dos indivíduos nos ambientes virtuais. Assim, todos devem estar cientes de que suas palavras e ações online têm consequências, e é fundamental que assumam a responsabilidade por elas.

2.9 A Legislação Brasileira Frente aos Crimes Cibernéticos

Com fundamento no art. 5º, inciso XXXIX, da Constituição Federal de 1988, o qual consagra o princípio da legalidade penal ao dispor que “não há crime sem lei anterior que o defina, nem pena sem prévia cominação legal” (BRASIL, 1988), infere-se que a responsabilização penal de qualquer indivíduo exige a descrição prévia, clara e minuciosa, na

norma penal incriminadora, de todos os elementos que configuram a conduta delituosa.

Assim, atos criminosos praticados por meio de sistemas informatizados, dispositivos de comunicação ou redes de computadores também devem estar expressamente tipificados em lei, sob pena de violação ao referido princípio constitucional.

Dessa forma, diante da crescente digitalização da sociedade, a legislação brasileira tem buscado se adaptar para enfrentar os desafios impostos pelos crimes cibernéticos, que vão desde fraudes eletrônicas até o vazamento de dados pessoais. A promulgação da Lei 12.737/2012 (Lei Carolina Dieckmann), do Marco Civil da Internet (Lei nº 12.965/2014) e da Lei Geral de Proteção de Dados (Lei nº 13.709/2018) representou importantes avanços no sentido de garantir direitos e deveres no ambiente virtual.

Além disso, o Código Penal foi atualizado pela Lei nº 14.155/2021 para aumentar as penas de crimes como estelionato e invasão de dispositivos eletrônicos, especialmente quando praticados por meio da internet. Ainda assim, a rapidez com que surgem novas formas de delitos digitais exige constante atualização normativa, bem como investimentos em capacitação de agentes públicos e em tecnologia, para que o sistema jurídico brasileiro seja eficaz na prevenção e repressão dessas condutas.

Outra alteração relevante foi promovida pela Lei nº 13.964/2019 (conhecida como Pacote Anticrime), que ampliou as penas dos crimes contra a honra, como calúnia, difamação e injúria, quando praticados por meio de redes sociais ou outros meios digitais que potencializem a divulgação da ofensa. Essa previsão está disposta no § 2º do art. 141 do Código Penal, que estabelece: “Se o crime é cometido ou divulgado em quaisquer modalidades das redes sociais da rede mundial de computadores, aplica-se em triplo a pena.”.

Ainda assim, a rapidez com que surgem novas formas de delitos digitais exige constante atualização normativa, bem como investimentos em capacitação de agentes públicos e em tecnologia, para que o sistema jurídico brasileiro seja eficaz na prevenção e repressão dessas condutas.

2.9.1 Da chamada Lei “Carolina Dieckmann”

Até o ano de 2012, inexistia no ordenamento jurídico brasileiro uma legislação específica voltada à proteção das vítimas de crimes cibernéticos. Contudo, um episódio de grande repercussão nacional impulsionou mudanças legislativas: a invasão do computador pessoal da atriz Carolina Dieckmann, seguida do vazamento de suas fotos íntimas.

O autor do crime tentou extorquir a atriz, ameaçando divulgar os conteúdos na internet. Em vez de ceder à chantagem, Carolina optou por denunciar o caso às autoridades, o que contribuiu significativamente para o debate público e a posterior aprovação da chamada "Lei Carolina Dieckmann" (Lei nº 12.737/2012).

No entanto, apesar de famosa e de grande influência, Dieckmann encontrou obstáculos para propor mudanças na legislação, conforme explica Crespo (2013, apud POMPEU, 2022, p. 24):

> A ação judicial promovida por Carolina deparou-se, porém, com um obstáculo jurídico, o mesmo que vem atenuando a punição em casos semelhantes que ocorreram há mais de uma década no Brasil. "Se eu invadisse uma máquina e me valesse de informações confidenciais para ter um proveito financeiro, eu poderia responder por concorrência desleal, por extorsão, mas não pela invasão". [...], por isso, os invasores responderão por crimes que a legislação brasileira já tipifica: furto, extorsão e difamação. (CRESPO, 2013, apud POMPEU, 2022, p. 24).

Desdobrando o comentário do autor Crespo, observa-se que o caso envolvendo a atriz Carolina Dieckmann evidenciou um importante entrave jurídico existente à época no ordenamento brasileiro: a ausência de tipificação penal específica para crimes cometidos em ambiente virtual.

Devido a isso, a ação judicial por ela proposta enfrentou empecilhos. Isso porque, mesmo diante de uma conduta claramente ofensiva, como a invasão de dispositivos eletrônicos e o uso indevido de dados pessoais, a legislação vigente não previa, de forma expressa, a criminalização da prática da invasão digital em si.

Dessa forma, os operadores do direito eram obrigados a enquadrar tais condutas em tipos penais tradicionais já previstos no Código Penal, como furto, extorsão e difamação. Ou seja, a conduta do agente invasor era punida não pelo ato de invasão propriamente dito, mas sim pelas consequências derivadas desse ato, como a obtenção indevida de vantagens, a exposição da vítima ou a coação exercida mediante chantagem.

Tal lacuna legal gerava insegurança jurídica e dificultava a responsabilização adequada dos autores desses delitos, exigindo a adoção de interpretações extensivas e nem sempre satisfatórias do ponto de vista técnico e social.

Todavia, devido à sua condição de figura pública e à sua significativa influência, o Poder Legislativo precisou dedicar a devida atenção ao tema dos crimes virtuais, resultando na sanção da Lei 12.737/2012, que aborda especificamente os crimes cibernéticos e promoveu alterações em alguns delitos já existentes.

A Lei nº 12.737/2012, que ficou popularmente conhecida como "Lei Carolina

Dieckmann", foi sancionada em 30 de novembro de 2012, publicada no Diário Oficial da União em 3 de dezembro do mesmo ano e entrou em vigor em 2 de abril de 2013. Sendo assim, ela foi criada com o intuito de proteger bens jurídicos ligados à liberdade individual, à privacidade e ao sigilo profissional e pessoal, especialmente no contexto digital.

Sua promulgação representou um marco no Direito Penal brasileiro, ao introduzir os artigos 154-A[7] e 154-B [8] ao Código Penal, os quais passaram a tipificar condutas relacionadas à invasão de dispositivos informáticos, suprindo uma importante lacuna legislativa frente ao avanço dos crimes cibernéticos.

Além disso, a referida norma alterou os artigos 266[9] e 298[10] do Código Penal, ampliando sua aplicação para o contexto digital, sobretudo no que tange à segurança da informação e ao uso indevido de dados e conteúdos de caráter íntimo, como fotos e vídeos, veiculados indevidamente na internet. O artigo 154-A, em especial, passou a tratar diretamente da conduta de invadir, sem autorização, dispositivo informático alheio.

Com isso, a Lei nº 12.737/2012 passou a preencher uma lacuna legislativa até então existente no ordenamento jurídico brasileiro, permitindo uma resposta penal mais precisa diante de condutas praticadas em ambiente virtual. A inclusão do artigo 154-A representou um avanço no enfrentamento aos crimes cibernéticos, pois tornou possível a responsabilização direta daqueles que, por meio da violação de dispositivos eletrônicos, comprometem a privacidade e a integridade de dados pessoais.

A tipificação específica da invasão de dispositivos informáticos não apenas reforça a proteção à intimidade e ao sigilo das comunicações, como também sinaliza o reconhecimento, pelo legislador, da importância da segurança digital como direito fundamental na sociedade contemporânea.

---

[7] Art. 154-A. Invadir dispositivo informático de uso alheio, conectado ou não à rede de computadores, com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do usuário do dispositivo ou de instalar vulnerabilidades para obter vantagem ilícita:
Pena – reclusão, de 1 (um) a 4 (quatro) anos, e multa.

[8] Art. 154-B. Nos crimes definidos no art. 154-A, somente se procede mediante representação, salvo se o crime é cometido contra a administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviços públicos.

[9] Art. 266 - Interromper ou perturbar serviço telegráfico, radiotelegráfico ou telefônico, impedir ou dificultar-lhe o restabelecimento:
Pena - detenção, de um a três anos, e multa.

[10] Art. 298 - Falsificar, no todo ou em parte, documento particular ou alterar documento particular verdadeiro:
Pena - reclusão, de um a cinco anos, e multa.
(BRASIL, 1940)

2.9.2 Do Marco Civil da Internet

De acordo com o Comitê Gestor da Internet no Brasil – CGI.br, "o Marco Civil da Internet é um projeto de lei que visa a consolidar direitos, deveres e princípios para a utilização e o desenvolvimento da Internet no Brasil" (CGI.br, 2013). Isto é, a proposta do Marco Civil surgiu diante da necessidade de responder aos desafios impostos pela rápida disseminação da Internet em diversos setores da sociedade.

À medida que empresas, órgãos públicos, entidades civis e a população em geral passaram a utilizar massivamente a rede, tornou-se evidente a urgência de estabelecer parâmetros claros para garantir a proteção de direitos fundamentais no ambiente digital. Assim, além de assegurar a liberdade e a abertura da Internet, busca-se criar uma base normativa que promovesse a inovação, o desenvolvimento social e econômico, e fortalecesse a diversidade cultural no ambiente virtual.

O CGI.br complementa que:

> Após mais de um ano de trabalho e inúmeras interações com a sociedade brasileira, em 24 de agosto de 2011, o projeto de lei (PL) foi finalmente apresentado à Câmara dos Deputados, recebendo o número 2.126/2011. A Câmara formou então Comissão Especial para apreciação do PL e de outros projetos correlatos que passaram a tramitar apensados ao Marco Civil da Internet. O processo que se seguiu incluiu, mais uma vez, uma série de audiências públicas, além de disponibilizar todo o material em discussão no sítio da Câmara para sugestões e consultas de toda a sociedade. (CGI.br, 2013).

Em resumo, o processo legislativo que consolidou tal lei, evidenciou o compromisso com a construção coletiva de normas que garantissem não apenas a liberdade e a neutralidade da rede, mas também a proteção da privacidade, o estímulo à inovação e o fortalecimento da democracia digital. Foi assim, então, que a aprovação da Lei Federal nº 12.965, em 2014, representou um marco regulatório fundamental para o ordenamento do ciberespaço brasileiro, assegurando direitos essenciais como a proteção dos dados pessoais e o respeito à privacidade dos usuários.

Dentre as disposições da lei, destaca-se o artigo 7º[11] que, por exemplo, aborda

[11] Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos: I - inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação; II - inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei; III - inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial; [...] VII - não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei; [...]. (BRASIL, 2014).

direitos como a proteção da intimidade e da vida privada, o sigilo e a inviolabilidade do fluxo de comunicações na internet, a proteção e o sigilo das comunicações privadas armazenadas, salvo decisão judicial e a proibição do fornecimento de dados pessoais a terceiros, incluindo registros de conexão e de acesso a aplicações, salvo consentimento ou previsão legal.

Segundo informações do Ministério da Justiça e Segurança Pública, consta que:

> O Marco Civil da Internet também determinou que os Juizados Especiais são os responsáveis pela decisão sobre a ilegalidade ou não dos conteúdos. Isto se aplica aos casos de ofensa à honra ou injúria, que serão tratados da mesma forma como ocorre fora da rede mundial de computadores. (BRASIL, 2024).

Isso significa que essas infrações, mesmo ocorrendo no ambiente virtual, devem ser tratadas de maneira semelhante ao que acontece no mundo real, garantindo assim que as regras e procedimentos judiciais aplicados fora da internet também se apliquem no contexto digital. Dessa forma, o Marco Civil busca assegurar proteção jurídica às vítimas, promovendo a responsabilização adequada dos autores de conteúdos ilegais na rede.

A determinação da competência judicial não depende da localização do provedor de acesso, mas sim do local onde o delito foi consumado, conforme o artigo 70[12] do Código de Processo Penal. Por outro lado, crimes que envolvem violação de privacidade ou que afetam bens, interesses ou serviços da União, ou de suas autarquias e empresas públicas, são de competência da Justiça Federal. O mesmo se aplica aos crimes previstos em convenções internacionais, como tráfico, tortura e falsificação de moeda.

2.9.3 Da Lei Geral de Proteção de Dados (LGPD)

Antes de 2018, o Brasil carecia de uma legislação específica voltada à proteção de dados particulares. Embora o Marco Civil da Internet representasse um avanço ao estabelecer princípios e diretrizes para o uso da internet, ainda persistiam diversos obstáculos à efetiva proteção das informações pessoais.

Esse cenário começou a mudar com a sanção da Lei Geral de Proteção de Dados (LGPD), em 14 de agosto de 2018, que passou a disciplinar de forma abrangente o tratamento de dados pessoais no país. A LGPD tem como finalidade assegurar os direitos fundamentais à liberdade, à privacidade e ao livre desenvolvimento da personalidade da pessoa natural.

---

[12] Art. 70. A competência será, de regra, determinada pelo lugar em que se consumar a infração, ou, no caso de tentativa, pelo lugar em que for praticado o último ato de execução. (BRASIL, 1941).

Tal Lei foi elaborada com forte influência do regulamento europeu conhecido como GDPR (*General Data Protection Regulation*), traduzido como Regulamento Geral sobre a Proteção de Dados (RGPD). Conforme destaca os autores abaixo:

> Efetivamente, a LGPD tem sido reiteradamente exposta como sendo uma "espécie de projeção" do Regulamento (UE) 2016/679, do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares [físicas] no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (Regulamento Geral sobre a Proteção de Dados), o RGPD, na terra de Vera Cruz. (MASSENO; MARTINS; FALEIROS JÚNIOR, 2020, p. 3).

Como já dito, observa-se que a Lei Geral de Proteção de Dados brasileira (LGPD) apresenta forte correspondência com o Regulamento Geral sobre a Proteção de Dados da União Europeia (RGPD), sendo frequentemente interpretada como uma adaptação nacional daquele regulamento europeu. Essa relação se revela tanto na estrutura normativa quanto nos princípios fundamentais que regem o tratamento de dados pessoais.

Assim como o RGPD, a LGPD busca assegurar a proteção dos direitos fundamentais da pessoa natural, especialmente no que diz respeito à privacidade, à autodeterminação informativa e à liberdade no uso dos dados.

Ao adotar diretrizes semelhantes às da União Europeia, o Brasil alinha-se aos padrões internacionais de proteção de dados, promovendo segurança jurídica e fortalecendo a confiança nas relações digitais, inclusive no cenário global. A escolha por seguir o modelo europeu não foi apenas técnica, mas estratégica, uma vez que o RGPD é amplamente reconhecido como um dos marcos mais avançados e abrangentes em matéria de privacidade e governança da informação.

Complementando, Wachowicz destaca que "o RGPD é um regulamento do direito europeu sobre privacidade e proteção de dados pessoais, aplicável a todos os indivíduos na União Europeia (UE) e Espaço Econômico Europeu (EEE). Regulamenta também a exportação de dados pessoais para fora da UE e EEE." (WACHOWICZ, 2020, p. 14).

Foi em agosto de 2018 que o Brasil promulgou a Lei 13.709, conhecida como Lei Geral de Proteção de Dados (LGPD), que se inspira na legislação europeia (RGPD). A Lei 13.709 de 2018 tem como objetivo primordial a proteção do direito fundamental à privacidade e ao livre desenvolvimento da personalidade dos indivíduos, abrangendo tanto o setor privado quanto a administração pública, conforme o pensamento de Wachowicz (2020), que diz:

> A LGPD aplica-se ao tratamento de dados pessoais por pessoas singulares ou colectivas de direito privado ou autoridades públicas (artigo 1º). O objetivo desta lei

> é proteger o direito fundamental à privacidade, por um lado, e o livre desenvolvimento da personalidade de uma pessoa interessada (art. 1º), por outro. A lei aplica-se, portanto, tanto ao setor privado quanto à administração pública. (WACHOWICZ, 2020, p. 28)

Ainda de acordo com Wachowicz (2020), a LGPD estabelece um conjunto de normas que regulam o tratamento de dados pessoais, definindo claramente as bases legais que legitimam esse tratamento, sendo elas:

> (1) Consentimento do titular dos dados;
> (2) Cumprimento das exigências legais ou regulamentares do órgão de processamento;
> (3) Implementação de atos administrativos;
> (4) Realização de estudos por instituições de pesquisa;
> (5) Execução do contrato ou medidas pré-contratuais, ambas a pedido da pessoa interessada;
> (6) Declaração de direitos próprios em processos judiciais;
> (7) Proteção do corpo e da saúde da pessoa interessada ou de terceiros;
> (8) Proteção da saúde pelas autoridades sanitárias;
> (9) A existência de um interesse legítimo, exceto quando prevalecerem os direitos fundamentais do titular dos dados;
> (10) Para proteger os empréstimos. (WACHOWICZ, 2020, p. 31).

Entre as dez bases legais previstas na Lei Geral de Proteção de Dados, destacam-se o consentimento do titular, o cumprimento de obrigações legais e a proteção de interesses vitais, que juntos compõem os fundamentos que autorizam o tratamento de dados pessoais de forma legítima.

O consentimento, por exemplo, é uma manifestação livre, informada e inequívoca do titular, permitindo que seus dados sejam tratados apenas quando houver uma autorização expressa.

Já o cumprimento de exigências legais ou regulamentares representa hipóteses em que o tratamento se faz necessário para atender obrigações impostas ao controlador, como nos casos de cadastro fiscal, previdenciário ou trabalhista.

A proteção de interesses vitais, por sua vez, abrange situações emergenciais em que o tratamento é indispensável para salvaguardar a vida ou a integridade física do titular ou de terceiros.

Além dessas, a LGPD prevê outras bases legais igualmente relevantes, como a execução de contratos, que permite o tratamento de dados quando necessário para a formalização ou cumprimento de obrigações contratuais solicitadas pelo próprio titular; e a realização de estudos por instituições de pesquisa, desde que garantido o anonimato dos dados.

A lei também contempla a defesa de direitos em processos judiciais, permitindo o uso de dados para fins de exercício regular de direitos em disputas legais. No âmbito da saúde, o tratamento pode ocorrer tanto para proteção da saúde de pessoas quanto por autoridades sanitárias, especialmente em contextos de interesse público, como campanhas de vacinação ou controle de epidemias.

Outra base legal relevante é o interesse legítimo do controlador, desde que este não viole os direitos e liberdades fundamentais do titular. Por fim, a lei prevê a hipótese específica de tratamento para proteção do crédito, assegurando a legalidade de operações financeiras como concessões de empréstimos.

Essa diversidade de bases legais reflete a preocupação do legislador em garantir que o tratamento de dados pessoais ocorra de maneira ética, equilibrando os interesses legítimos dos agentes de tratamento com a proteção dos direitos fundamentais dos indivíduos.

A LGPD também exige que entidades que tratam dados sistematicamente nomeiem um Encarregado de Dados (*Data Protection Officer - DPO*), reforçando a responsabilidade das organizações na proteção dessas informações. Desse modo, a LGPD não apenas moderniza a legislação brasileira de proteção de dados, mas eleva o padrão de segurança, alinhando-se às melhores práticas internacionais e reconhecendo a relevância da privacidade em um mundo digitalizado.

3. RESULTADOS ESPERADOS

Com base nos capítulos desenvolvidos ao longo desta pesquisa, os resultados esperados consistem em proporcionar uma compreensão ampla, crítica e atualizada sobre os crimes contra a honra no contexto das redes sociais e os desafios enfrentados para garantir a proteção desses direitos fundamentais sem comprometer a liberdade de expressão. Ao abordar desde a origem da internet e o conceito de ciberespaço até a estrutura jurídica dos crimes de calúnia, difamação e injúria, pretende-se construir um panorama teórico robusto que auxilie acadêmicos, profissionais do Direito e operadores do sistema de justiça.

Espera-se, também, evidenciar as peculiaridades da prática desses crimes no ambiente digital, destacando como a massificação do uso das redes sociais potencializou os danos causados à honra das vítimas, exigindo uma resposta mais eficaz do ordenamento jurídico. A inserção do art. 141, §2º do Código Penal e os efeitos práticos da sua aplicação reforçam a necessidade de atualização constante das leis frente à realidade tecnológica.

Além disso, busca-se fomentar o debate sobre a responsabilidade das plataformas digitais e o papel que estas exercem na mediação dos conflitos relacionados à honra e à liberdade de expressão. As análises das legislações específicas, como o Marco Civil da Internet, a Lei Carolina Dieckmann e a LGPD, contribuem para uma reflexão crítica sobre a eficácia normativa na proteção da dignidade da pessoa humana no ambiente virtual.

Por fim, como resposta à problemática central apresentada na introdução, espera-se demonstrar que a melhor forma de equilibrar os direitos fundamentais em colisão — como a liberdade de expressão e o direito à honra — é por meio da aplicação da teoria da ponderação proposta por Robert Alexy. A adoção desse método proporciona uma análise proporcional, adequada e contextualizada de cada situação concreta, promovendo decisões jurídicas que respeitem o Estado Democrático de Direito e os valores constitucionais.

4. CONSIDERAÇÕES FINAIS

Este estudo explorou as complexidades que envolvem os crimes contra a honra no ambiente digital, sobretudo nas redes sociais, analisando suas particularidades, implicações jurídicas e sociais. Com o avanço tecnológico, a comunicação instantânea e de amplo alcance tem se tornado uma ferramenta fundamental na interação social, ao mesmo tempo em que evidencia desafios relacionados à responsabilização por ofensas virtuais.

Primeiramente, foi possível compreender a origem e evolução da internet e do ciberespaço, contextualizando o crescimento das redes sociais como espaços privilegiados de expressão e comunicação. Esses ambientes, por sua natureza, promovem uma liberdade de expressão que, embora indispensável para a democracia, apresenta limites legais claros para a proteção da honra e da dignidade dos indivíduos.

A revisão de literatura demonstrou que os crimes contra a honra, divididos tradicionalmente em calúnia, difamação e injúria, assumem novas configurações no ambiente virtual, onde a velocidade, informalidade e alcance das publicações potencializam os impactos dessas condutas. Além disso, a análise mostrou que há uma forte necessidade de delimitação entre liberdade de expressão e proteção à honra, especialmente em plataformas digitais, considerando a vulnerabilidade e o anonimato que muitas vezes favorecem condutas ofensivas.

A legislação brasileira, incluindo marcos normativos como a Lei “Carolina Dieckmann”, o Marco Civil da Internet e a LGPD, busca equilibrar esses direitos e proteger os indivíduos de ataques virtuais. No entanto, as hipóteses de responsabilização ainda enfrentam desafios devido às particularidades do ambiente digital, como a dificuldade de identificação do infrator e a rápida propagação das ofensas.

Por fim, é possível, agora, responder à pergunta central desta pesquisa: qual a melhor forma de equilibrar os direitos à liberdade de expressão e à proteção da honra em um

ambiente marcado pela massificação das redes sociais? A resposta encontra-se na ponderação entre princípios constitucionais, conforme propõe Robert Alexy, que defende que os direitos fundamentais devem ser harmonizados caso a caso, buscando a máxima efetividade de cada um, sem que haja anulação total do outro.

Assim, embora a liberdade de expressão seja um dos pilares do Estado Democrático de Direito, ela não pode ser usada como escudo para práticas ilícitas que ofendam a dignidade de terceiros. A jurisprudência do Supremo Tribunal Federal reforça que esse direito, como os demais, não é absoluto e deve ser exercido de forma compatível com os limites constitucionais.

Além disso, o §2º do art. 141 do Código Penal, ao triplicar a pena nos casos de crimes contra a honra praticados em redes sociais, demonstra a preocupação do legislador com os danos potencializados nesse ambiente. Portanto, o equilíbrio entre os direitos exige não apenas a atuação do Poder Judiciário por meio da ponderação, mas também políticas públicas eficazes e a responsabilidade das plataformas digitais.

Desse modo, a melhor forma de equilibrar tais direitos está na conjugação entre interpretação constitucional adequada, legislação atualizada e comprometimento institucional com a proteção da dignidade humana, sem restringir indevidamente a participação social no espaço virtual. Esse caminho permite um ambiente digital mais seguro, justo e compatível com os valores democráticos.

REFERÊNCIAS

ALEXY, R. **Colisão de direito fundamentais e realização de direitos fundamentais no Estado de Direito democrático**. Revista de Direito Administrativo, [S. l.], v. 217, p. 67–79, 1999. DOI: 10.12660/rda.v217.1999.47414. Disponível em: https://periodicos.fgv.br/rda/article/view/47414. Acesso em: 28 jun. 2025.

ARAS, Vladimir. **Crimes de informática: uma nova criminalidade**. Revista Jus Navigandi, ISSN 1518-4862, Teresina, ano 6, n. -639, 1 out. 2001. Disponível em: https://jus.com.br/artigos/2250. Acesso em: 5 nov. 2024.

BARNES, J. A. **Redes sociais e processo político**. In: FELDMAN-BIANCO, Bela (org.). Antropologia das sociedades contemporâneas. São Paulo: Global, 1987. p. 159-93.

BARROS, Antonio. **Conheça a evolução dos crimes cibernéticos**. Agência Câmara, Brasília, 23 ago. 2006. Disponível em: https://www.camara.leg.br/noticias/116826-conheca-a-evolucao-dos-crimes-ciberneticos. Acesso em: 22 out. 2024.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Disponível em: https://planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 21 out. 2024.

BRASIL. **Decreto-Lei n.º 2.848, de 7 de dezembro de 1940. Código Penal**. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 21 out. 2024.

BRASIL. **Decreto-Lei nº 3.689, de 3 de outubro de 1941**. Código de Processo Penal. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del3689.htm. Acesso em: 26 maio 2025.

BRASIL. INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA (IBGE). **Em 2023, 88,0% das pessoas com 10 anos ou mais utilizaram Internet**. Agência IBGE Notícias, 16 ago. 2024. Disponível em: https://agenciadenoticias.ibge.gov.br/agencia-noticias/2012-agencia-de-noticias/noticias/41026-em-2023-87-2-das-pessoas-com-10-anos-ou-mais-utilizaram-internet. Acesso em: 9 abr. 2025.

BRASIL. **Lei nº 7.716, de 5 de janeiro de 1989. Define os crimes resultantes de preconceito de raça ou de cor**. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l7716.htm. Acesso em: 24 out. 2024.

BRASIL. **Lei n° 12.737, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos**. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 22 out. 2024.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil**. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 22 out. 2024.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados**

Pessoais (LGPD). Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 27 maio 2025.

BRASIL. **Lei nº 14.155, de 27 de maio de 2021. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para dispor sobre crimes cometidos por meio da internet ou de dispositivos eletrônicos.** Diário Oficial da União: seção 1, Brasília, DF, 28 maio 2021. Disponível em: https://www.in.gov.br/en/web/dou/-/lei-n-14.155-de-27-de-maio-de-2021-322698993. Acesso em: 27 maio 2025.

BRASIL. Ministério das Comunicações. **Pesquisa mostra que 82,7% dos domicílios brasileiros têm acesso à internet**. Disponível em: https://www.gov.br/mcom/pt-br/noticias/2021/abril/pesquisa-mostra-que-82-7-dos-domicilios-brasileiros-tem-acesso-a-internet. Acesso em: 19 out. 2024.

BRASIL. Ministério da Justiça e Segurança Pública. **Crimes Digitais: o que são, como denunciar e quais leis tipificam como crime?**. Disponível em: https://www.gov.br/mj/pt-br/assuntos/sua-protecao/sedigi/crimes-digitais. Acesso em: 21 out. 2024.

BRASIL. Superior Tribunal de Justiça. **Apelação nº 473/DF**. Relator: Ministro Gilson Dipp. 5ª Turma. Diário da Justiça Eletrônico, Brasília, DF, 8 set. 2008. Disponível em: https://processo.stj.jus.br/SCON/pesquisar.jsp?i=1&b=ACOR&livre=((%27APN%27.clas.+e++@num=%27473%27)+ou+(%27APn%27+adj+%27473%27).suce.)&thesaurus=JURIDICO&fr=veja. Acesso em: 17 maio 2025.

BRASIL. Superior Tribunal de Justiça. **APn 813/DF**. Rel. Min. Felix Fischer, julgado em 12 abr. 2016. Disponível em: https://scon.stj.jus.br/SCON/pesquisar.jsp?i=1&b=ACOR&livre=((%27APN%27.clas.+e+@num=%27813%27)+ou+(%27APn%27+adj+%27813%27).suce.)&thesaurus=JURIDICO&fr=veja. Acesso em: 20 maio 2025.

BRASIL. Superior Tribunal de Justiça. **AgInt no Recurso Especial n. 1.548.520/MG**. Relator: Ministro Sebastião Reis Júnior. Sexta Turma. DJe 22 jun. 2016. Disponível em: https://scon.stj.jus.br/SCON/pesquisar.jsp?i=1&b=ACOR&livre=((%27AIRESP%27.clas.+e+@num=%271548520%27)+ou+(%27AgInt%20no%20REsp%27+adj+%271548520%27).suce.)&thesaurus=JURIDICO&fr=veja. Acesso em: 19 maio 2025.

BRASIL. Superior Tribunal de Justiça. **Habeas Corpus nº 234.134/MT**. Relatora: Ministra Laurita Vaz. Quinta Turma. Julgado em 6 de novembro de 2012. Diário da Justiça Eletrônico, Brasília, DF, 16 de novembro de 2012. Disponível em: https://processo.stj.jus.br/SCON/pesquisar.jsp?i=1&b=ACOR&livre=((%27HC%27.clap.+e+@num=%27234134%27)+ou+(%27HC%27+adj+%27234134%27).suce.)&thesaurus=JURIDICO&fr=veja. Acesso em: 28 jun. 2025.

BRASIL. Supremo Tribunal Federal. **Habeas corpus n. 82.424/RS**. Relator: Min. Moreira Alves. Redator do acórdão: Min. Maurício Corrêa. Julgado em: 17 set. 2003. Publicado em: 19 mar. 2004. Tribunal Pleno. Disponível em: https://jurisprudencia.stf.jus.br/pages/search/sjur96610/false. Acesso em: 25 jun. 2025.

BRASIL. Supremo Tribunal Federal**. RHC n. 83.091/DF**. Relator: Min. Marco Aurélio.

Brasília, DF, 2003. Disponível em: https://jurisprudencia.stf.jus.br/pages/search?base=acordaos&pesquisa_inteiro_teor=false&sinonimo=true&plural=true&radicais=false&buscaExata=true&page=1&pageSize=10&sort=_score&sortBy=desc&isAdvanced=true&classeNumeroIncidente=%22RHC%2083091%22. Acesso em: 19 maio 2025.

BRASIL. Supremo Tribunal Federal. **Inquérito n. 2915/PA**. Relator: Min. Luiz Fux. Julgamento: 09 maio 2013. Publicação: 31 maio 2013. Disponível em: https://jurisprudencia.stf.jus.br/pages/search/sjur231839/false. Acesso em: 19 maio 2025.

CASSANTI, Moisés de Oliveira. **Crimes Virtuais, Vítimas Reais**. 1. ed. São Paulo: Brasport, 2014.

COMITÊ GESTOR DA INTERNET NO BRASIL (CGI.br). **O CGI.br e o Marco Civil da Internet**. São Paulo: CGI.br, 2013. Disponível em: https://www.cgi.br/publicacao/o-cgi-br-e-o-marco-civil-da-internet/. Acesso em: 26 maio 2025.

DE FREITAS, Riva Sobrado; DE CASTRO, Matheus Felipe. **Liberdade de Expressão e Discurso do Ódio: um exame sobre as possíveis limitações à liberdade de expressão**. Seqüência Estudos Jurídicos e Políticos, Florianópolis, v. 34, n. 66, p. 327–355, 2013. DOI: 10.5007/2177-7055.2013v34n66p327. Disponível em: https://periodicos.ufsc.br/index.php/sequencia/article/view/2177-7055.2013v34n66p327. Acesso em: 23 maio. 2025.

GETSCHKO, Demi. **Internet, Mudança ou Transformação?** In: CGI.br (Comitê Gestor da Internet no Brasil). Pesquisa sobre o uso das tecnologias da informação e da comunicação 2008. São Paulo, 2009, pp. 49-52.
Disponível em: https://www.cgi.br/publicacao/internet-mudanca-ou-transformacao/. Acesso em:

GIBSON, William. **Neuromancer**. Tradução de Fábio Fernandes. 1. ed. São Paulo: Aleph, 2003.

GOLDENBERG, Mirian. **A arte de pesquisar: Como fazer pesquisa qualitativa em Ciências Sociais**. 8. ed. Rio de Janeiro: Record, 2004.

GRECO FILHO, Vicente. **Algumas observações sobre o direito penal e a internet**. Boletim do IBCCrim. São Paulo. Ed. Esp., ano 8, n. 95, p. 3, 2000. Disponível em: https://arquivo.ibccrim.org.br/boletim_editorial/160-95-Outubro-Esp-2000. Acesso em: 21 out. 2024.

GRECO, Rogério. **Código Penal Comentado**. 11. ed. revista, ampliada e atualizada até 1º de janeiro de 2017. Curitiba: Impetus, 2017.

GUIMARÃES JÚNIOR, Mário José Lopes. **O Ciberespaço como Cenário para as Ciências Sociais**. Ilha Revista de Antropologia, Florianópolis, v. 2, n. 1, p. 139–154, 2000. Disponível em: https://periodicos.ufsc.br/index.php/ilha/article/view/14652. Acesso em: 8 abr. 2025.

JESUS, Damásio**. Direito Penal: Parte especial: dos crimes contra a pessoa e dos crimes contra o patrimônio**. 28. ed. rev. e atual. São Paulo: Saraiva, 2007.

LÉVY, Pierre. **Cibercultura**. Tradução de Carlos Irineu da Costa. São Paulo: Editora 34, 1999.

LIMA, Paulo Marco Ferreira. **Crimes de computador e segurança computacional**. Campinas: Millennium, 2006. 234 p.

MAGALHÃES, José Luiz Quadros de. **Direito constitucional: curso de direitos fundamentais**. 3. ed. São Paulo: Método, 2008

MARTINS, Julio. **Crimes contra a honra na internet em tempos de pandemia**. DireitoNET, 2020. Disponível em: https://www.direitonet.com.br/artigos/exibir/11710/Crimes-contra-a-honra-na-Internet-em-tempos-de-pandemia. Acesso em: 22 out. 2024.

MASSENO, M. D.; MARTINS, G. M.; FALEIROS JÚNIOR, J. L. de M. **A Segurança na Proteção de Dados: Entre o RGPD Europeu e a LGPD Brasileira**. Revista do CEJUR/TJSC: Prestação Jurisdicional, Florianópolis (SC), v. 8, n. 1, p. e346, 2020. DOI: 10.37497/revistacejur. v8i1.346. Disponível em: https://revistadocejur.tjsc.jus.br/cejur/article/view/346. Acesso em: 26 maio. 2025.

MUSSO, Pierre. **Ciberespaço, figura reticular da utopia tecnológica**. In: MORAES, Dênis de. Sociedade Midiatizada. Rio de Janeiro: Mauad, 2006.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. **Declaração Universal dos Direitos Humanos**. Tradução para o português. Genebra: Alto Comissariado das Nações Unidas para os Direitos Humanos, [s.d.]. Disponível em: https://www.ohchr.org/en/human-rights/universal-declaration/translations/portuguese?LangID=por. Acesso em: 29 jun. 2025.

NITAHARA, Akemi. **Estudo mostra que pandemia intensificou uso das tecnologias digitais**. Agência Brasil, 25 nov. 2021. Disponível em: https://agenciabrasil.ebc.com.br/geral/noticia/2021-11/estudo-mostra-que-pandemia-intensificou-uso-das-tecnologias-digitais. Acesso em: 10 abr. 2025.

NORONHA, Edgard Magalhães. **Direito Penal**. 29. ed. São Paulo: Saraiva, 1998. v. 2, 526 p.

PAGLIUCA, José Carlos Gobbis**. Direito penal: parte especial**. São Paulo: Rideel, 2006. v. 1, 288 p.

POMPEU, Ana Luiza Brandão Calil. **Crimes cibernéticos: a ineficácia da Lei Carolina Dieckmann**. 2022. Trabalho de Conclusão de Curso (Bacharelado em Direito) – Faculdade de Inhumas, Centro de Educação Superior de Inhumas, Inhumas, 2022. Disponível em: http://65.108.49.104:80/xmlui/handle/123456789/509. Acesso em: 23 maio 2025.

PRADO, L. R. **Curso de direito penal Brasileiro**: volume II, parte especial, 7 ed., 2008.

RECUERO, Raquel. **Redes sociais na internet**. Porto Alegre: Sulina, 2009.

pompeuROSSINI, Augusto Eduardo de Souza. **Informática, telemática e direito penal**. São Paulo: Memória Jurídica, 2004.

SEGALLER, Stephen. **Nerds 2.0.1: A Brief History of the Internet**. 1. ed. Nova York: TV Books, 1998.

TEIXEIRA, Tarcisio. **Direito Digital e Processo Eletrônico**. 5. ed. São Paulo: Saraiva Educação, 2020.

WACHOWICZ, Marcos. **Proteção de Dados Pessoais em Perspectiva: LGPD e RGPD na ótica do direito comparado**. GEDAI, 2020.

WE ARE SOCIAL. **The Changing World of Digital in 2023**. Disponível em: https://wearesocial.com/uk/blog/2023/01/the-changing-world-of-digital-in-2023/. Acesso em: 19 out. 2024.