Revista Ibero-Americana de Humanidades, Ciências e Educação — REASE

doi.org/10.51891/rease.v12i6.27736

CRIMES CONTRA A HONRA NO AMBIENTE DIGITAL: A EFETIVIDADE DOS MECANISMOS DE IDENTIFICAÇÃO DE USUÁRIOS ANÔNIMOS E OS OBSTÁCULOS AO ACESSO À JUSTIÇA

CRIMES AGAINST HONOR IN THE DIGITAL ENVIRONMENT: THE EFFECTIVENESS OF MECHANISMS FOR IDENTIFYING ANONYMOUS USERS AND OBSTACLES TO ACCESS TO JUSTICE

Eloizy Cristini Dave de Assis[1]
Andréia Alves de Almeida[2]

RESUMO: O avanço tecnológico e as redes sociais tornaram o ciberespaço o principal meio de comunicação, impulsionando também os crimes contra a honra sob anonimato. Diante disso, a problemática central desta pesquisa consiste em verificar se a atribuição à vítima do ônus de identificar o agressor e produzir as provas digitais necessárias para o ajuizamento da demanda judicial constitui obstáculo ao princípio constitucional do acesso à justiça. O objetivo geral deste estudo é analisar a efetividade dos mecanismos jurídicos nacionais voltados à quebra do anonimato na internet. Como objetivos específicos, busca-se delimitar os conceitos de honra no contexto digital, examinar as obrigações de guarda de registros pelos provedores e identificar alternativas para mitigar as barreiras financeiras na fase probatória. Metodologicamente, a pesquisa caracteriza-se como qualitativa, do tipo teórico-bibliográfica e documental, amparada no método de abordagem dedutivo. Conclui-se que a volatilidade dos dados e o alto custo da ata notarial geram uma barreira técnica e financeira que promove a exclusão processual de vulneráveis, tornando imperativa a adoção de soluções acessíveis, como redes *blockchain* e o fortalecimento da atuação das Defensorias Públicas.

Palavras-chave: Crimes Cibernéticos. Anonimato. Prova Digital. Hipossuficiência.

ABSTRACT: The technological advancement and social networks have made cyberspace the primary means of communication, also driving crimes against honor under anonymity. Given this scenario, the central problem of this research consists in verifying whether assigning the burden of identifying the offender and producing the digital evidence necessary to initiate legal proceedings to the victim constitutes an obstacle to the constitutional principle of access to justice. The general objective of this study is to analyze the effectiveness of national legal mechanisms aimed at breaking anonymity on the internet. As specific objectives, it seeks to define the concepts of honor in the digital context, examine the record-keeping obligations of internet providers, and identify alternatives to mitigate financial barriers during the evidentiary phase. Methodologically, the research is characterized as qualitative, theoretical-bibliographic, and documentary, supported by the deductive approach method. It concludes that data volatility and the high cost of notarial acts generate technical and financial barriers that promote the procedural exclusion of vulnerable individuals, making the adoption of accessible solutions imperative, such as blockchain networks and the enhancement of Public Defense Offices' performance.

Keywords: Cybercrimes. Anonymity. Digital Evidence. Unprivileged Victims.

[1] Faculdade Católica de Rondônia, Graduanda de Direito.
[2] Professora Orientadora. Doutora em Ciência Jurídica DINTER entre FCR e UNIVALI. Mestre em Direito Ambiental pela UNIVEM/SP. Especialista em Direito Penal UNITOLEDO/SP. Especialista em Segurança Pública e Direitos Humanos pela UNIR/RO. Especialista em Direito Militar pela Verbo Jurídico/RJ.

INTRODUÇÃO

O avanço tecnológico e a consolidação das redes sociais como principal meio de comunicação resultaram em um aumento exponencial dos crimes contra a honra, como calúnia, difamação e, especialmente, a injúria, praticados no ambiente virtual. Essa nova forma de ofensa apresenta características agravantes, dentre as quais se destacam a rápida viralização, o alcance massivo e a utilização estratégica do anonimato como instrumento de impunidade.

A crescente utilização das redes sociais como principal meio de comunicação ampliou significativamente a ocorrência de crimes contra a honra no ambiente digital, especialmente aqueles praticados sob anonimato. Nesse cenário, a rápida disseminação das ofensas, a dificuldade de identificação dos autores e a volatilidade dos registros eletrônicos impõem novos desafios à tutela jurisdicional. A problemática central desta pesquisa consiste em verificar se a atribuição à vítima do ônus de identificar o agressor e produzir as provas digitais necessárias para o ajuizamento da demanda judicial constitui obstáculo ao princípio constitucional do acesso à justiça.

A hipótese que orienta este estudo sustenta que a legislação vigente e os procedimentos adotados revelam-se insuficientes, uma vez que o sistema de justiça demonstra maior concentração de esforços na fase decisória em detrimento do adequado suporte à fase de produção e preservação de provas digitais. Nesse contexto, a obtenção de provas torna-se um privilégio daqueles que dispõem de recursos financeiros e técnicos, o que contribui para a exclusão das vítimas em situação de vulnerabilidade e compromete a efetividade do acesso à justiça diante da volatilidade das informações no ciberespaço.

Assim, o objetivo geral desta pesquisa consiste em analisar se a transferência do ônus probatório digital à vítima de crimes contra a honra na internet atua como barreira ao acesso à justiça, propondo medidas que simplifiquem a identificação de infratores anônimos. Como objetivos específicos, busca-se delimitar os conceitos de honra no contexto digital; examinar as obrigações dos provedores e os prazos de guarda de registros; investigar as respostas da jurisprudência contemporânea diante dos obstáculos econômicos na produção da prova eletrônica; e, por fim, identificar alternativas tecnológicas e institucionais capazes de mitigar a exclusão processual da vítima hipossuficiente.

A metodologia aplicada no desenvolvimento deste estudo caracteriza-se como uma pesquisa qualitativa de natureza teórico-bibliográfica e documental. Como método de abordagem científica, adota-se o método dedutivo, partindo-se da análise geral do arcabouço

regulatório da internet e das garantias constitucionais dos direitos da personalidade para, de forma particular, investigar a viabilidade técnica e financeira de identificação do agressor nos crimes de injúria online. A coleta de dados ampara-se na revisão sistemática de posicionamentos doutrinários, legislações vigentes e entendimentos jurisprudenciais correlatos ao tema.

Para a estruturação do trabalho, o primeiro capítulo aborda a evolução legislativa, a vedação ao anonimato e a tipicidade dos crimes contra a honra no ambiente digital. O segundo capítulo examina o regime de guarda de registros do Marco Civil da Internet e as barreiras econômicas da prova, confrontando a fragilidade técnica do *print screen* com o custo da ata notarial. Por fim, o terceiro capítulo dedica-se à análise da jurisprudência dos tribunais superiores e à proposição da tecnologia *blockchain* como alternativa viável para assegurar uma instrução probatória democrática e efetiva.

2. EVOLUÇÃO LEGISLATIVA E CONTEXTO HISTÓRICO DA PROTEÇÃO DA HONRA E DA DIGNIDADE HUMANA

A proteção jurídica da honra não constitui fenômeno recente, mas representa uma construção histórica vinculada à própria evolução das sociedades civis e à necessidade de preservação da convivência social. A tutela da dignidade pessoal percorreu um longo caminho até alcançar a atual dimensão digital, especialmente diante da expansão das redes sociais e do ambiente virtual.

Suas origens remontam ao Direito Romano, período em que surgiu a actio iniuriarum, reconhecida como uma das primeiras manifestações jurídicas voltadas à proteção da honra e da dignidade individual. Na antiga Lei das Doze Tábuas, datada do século V a.C., as respostas às ofensas físicas e morais possuíam natureza predominantemente corporal e retaliatória, influenciadas pela lógica da Lei de Talião.

Com o desenvolvimento do direito pretoriano romano, entretanto, a repressão física passou gradativamente a ser substituída pela reparação pecuniária do dano moral sofrido, por meio da injúria. Nesse contexto, a injúria deixou de abranger apenas agressões físicas, passando a compreender qualquer ato ofensivo à dignidade, ao decoro e à consideração social do indivíduo, formando as bases do atual conceito de honra subjetiva.

A influência romano-germânica refletiu diretamente no ordenamento jurídico luso-brasileiro por meio das Ordenações do Reino de Portugal. As Ordenações Filipinas, promulgadas em 1603 e aplicadas no Brasil colonial, disciplinavam severamente as ofensas à

honra, prevendo penas corporais, multas, desterros e punições rigorosas para aqueles que proferirem palavras injuriosas ou desonrosas contra terceiros. A honra, nesse período, possuía caráter fortemente hierárquico e elitista, estando diretamente ligada à posição social, à honra familiar e à condição econômica do indivíduo (Lopes, 2014; Wolkmer, 2019). Após a independência do Brasil, o Código Criminal do Império de 1830 promoveu significativo avanço humanista ao abolir penas cruéis e inserir, de forma sistematizada, os crimes de calúnia e injúria no ordenamento jurídico nacional. Mais tarde, o Código Penal Republicano de 1890 manteve a proteção penal da honra, mas foi o Código Penal de 1940 (Brasil, 1940), atualmente em vigor, que consolidou definitivamente a clássica divisão dos crimes contra a honra em calúnia, difamação e injúria, previstas respectivamente nos artigos 138, 139 e 140 do referido diploma legal.

Com a promulgação da Constituição Federal de 1988 (Brasil, 1988), a proteção da honra adquiriu status constitucional, sendo elevada à categoria de direito fundamental vinculado diretamente ao princípio da dignidade da pessoa humana, previsto no artigo 1º, inciso III, da Constituição da República. O artigo 5º, inciso X, passou a assegurar a inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas, garantindo ainda o direito à indenização pelos danos materiais e morais decorrentes de sua violação. A partir dessa constitucionalização, a honra deixou de ser vista apenas como um interesse patrimonial ou penalmente protegido, passando a integrar o núcleo essencial dos direitos da personalidade. Nesse contexto, consolidou-se a distinção doutrinária entre honra objetiva e honra subjetiva. A honra objetiva refere-se à reputação e ao conceito social do indivíduo perante terceiros, enquanto a honra subjetiva corresponde ao sentimento íntimo de dignidade, autoestima e respeito próprio (Bitencourt, 2020; Prado, 2019). No crime de injúria, previsto no artigo 140 do Código Penal (Brasil, 1940), o bem jurídico tutelado é precisamente a honra subjetiva, uma vez que a ofensa atinge diretamente a dignidade pessoal da vítima, independentemente da imputação de fato determinado ou da necessidade de exposição pública perante terceiros.

2.1 Conceito de Crimes Contra a Honra no Ambiente Virtual

No ambiente virtual, a ofensa deixa de ser um evento local para se tornar uma agressão de alcance global, onde a arquitetura das redes sociais permite que o dano se perpetue no tempo. A facilidade de disseminação de conteúdos ofensivos em plataformas digitais não apenas amplia

o abalo psicológico, mas dificulta a contenção do ilícito, uma vez que o conteúdo escapa ao controle total das autoridades judiciárias após a sua publicação (Peck, 2021; Siqueira, 2017).

Somado a isso, observa-se que o ambiente digital potencializou o surgimento de um verdadeiro "tribunal do júri virtual", onde a massa de usuários assume simultaneamente os papéis de acusadora, julgadora e executora da pena reputacional. Nos linchamentos virtuais, a injúria deixa de ser uma mera ofensa isolada para se converter em uma punição coletiva desproporcional. Diferente do rito processual geométrico e analógico do Poder Judiciário, que observa o contraditório e a ampla defesa, o julgamento realizado nas redes sociais ocorre sob a lógica do algoritmo e do engajamento. Nesse ecossistema, a viralização da ofensa atua como uma sentença condenatória instantânea e irremediável, impondo à vítima severos danos à sua reputação e convivência social digital antes mesmo que qualquer autoridade possa investigar a autoria ou a veracidade dos fatos (Silva; Cruz, 2024).

Neste contexto, o crime de injúria, tipificado no artigo 140 do Código Penal (Brasil, 1940), ganha contornos dramáticos quando praticado sob o manto do pseudonimato. Diferente da calúnia e da difamação, a injúria fere o âmago da vítima, atacando os seus valores mais íntimos sem necessariamente imputar um fato falso ou determinado. A problemática central reside na distinção entre o anonimato constitucionalmente vedado (Brasil, 1988) e o uso de perfis simulados que, embora deixem rastros digitais como endereços de IP, impõem uma barreira técnica de acesso para o cidadão comum. Desse modo, a identificação do infrator torna-se um percurso tortuoso, pois o sistema jurídico impõe barreiras probatórias que muitas vezes ignoram a rapidez com que os dados podem ser apagados (Cavalcanti, 2025).

Ademais, a transitoriedade das informações nas redes sociais impõe um obstáculo crítico à instrução processual. Enquanto no mundo físico a prova costuma estar limitada ao testemunho, no virtual ela é documental e volátil, exigindo uma agilidade técnica que a vítima frequentemente não possui. Este cenário evidencia que o ônus da prova digital acaba por segregar os jurisdicionados, uma vez que a preservação de metadados torna-se um privilégio de quem detém recursos, deixando a parcela hipossuficiente desamparada perante a perda do suporte material da sua pretensão (Alexandre; Araújo, 2023). Assim, a fase de instrução e a coleta de provas tornaram-se o verdadeiro campo de batalha jurídico, onde a identificação do agressor é condição indispensável para que o Judiciário cumpra o seu papel de julgar a lide.

2.2 A Engenharia de Redes e a Dinâmica de Guarda de Registros no Marco Civil da Internet

Para compreender o gargalo processual que envolve a identificação de autoria nos crimes de injúria virtual, faz-se imperioso analisar, preliminarmente, a infraestrutura técnica e regulatória que viabiliza o fluxo de dados na internet brasileira. Sob a égide da Lei nº 12.965/2014, conhecida como o Marco Civil da Internet (MCI), a rede foi estruturada juridicamente a partir de duas figuras fundamentais: os provedores de conexão e os provedores de aplicação (Brasil, 2014). Os primeiros são as empresas de telecomunicação que fornecem o acesso físico do terminal do usuário à rede mundial de computadores, ao passo que os segundos correspondem às plataformas que disponibilizam serviços, funcionalidades e redes sociais onde as interações, e, consequentemente, as ofensas, ocorrem (Teixeira; Limberger, 2020).

Ao analisar detidamente a engenharia de dados desenhada pela Lei nº 12.965/2014, constata-se que a segmentação entre provedores de conexão e de aplicação não é mera escolha caprichosa do legislador, mas reflexo da própria arquitetura técnica da grande rede. O prazo de 6 (seis) meses estipulado pelo artigo 15 do Marco Civil da Internet para a guarda de logs de acesso funciona como um ponto de equilíbrio regulatório (Brasil, 2014). Argumenta-se na doutrina jurídica que este limite atende tanto à necessidade de persecução de ilícitos quanto ao direito ao esquecimento e à não retenção perpétua de dados dos usuários (Tomasevicius Filho, 2016).

Essa separação técnica dita o rastro da prova digital. A identificação de um agressor que se oculta sob o manto do anonimato não se dá por meio de um ato único ou imediato, mas sim através de uma cadeia sucessiva e complexa de requisições de dados que exige a cooperação de múltiplos agentes. No desenho técnico-jurídico estabelecido pelo Marco Civil da Internet (Brasil, 2014), a vítima de uma ofensa moral perpetrada por um perfil anônimo precisa trilhar um caminho de duas etapas distintas.

No desenho técnico-jurídico estabelecido pelo Marco Civil da Internet, a vítima de uma ofensa moral perpetrada por um perfil anônimo precisa trilhar um caminho de duas etapas distintas. O ponto de partida consiste em acionar judicialmente o provedor de aplicação para obter o registro de acesso à aplicação correspondente. Esse registro, conforme preceitua o artigo 15 do MCI, consiste no conjunto de informações referentes à data, hora, fuso horário e, crucialmente, ao endereço de Protocolo de Internet (IP) utilizado para criar ou aceder à conta que proferiu a injúria (Brasil, 2014). Contudo, o fornecimento do IP e da porta lógica de origem pelo provedor de aplicação não revela de imediato a identidade civil do infrator; indica apenas

a "matrícula" da conexão utilizada no momento exato do ilícito, demandando uma segunda etapa de quebra de sigilo junto ao provedor de conexão para a efetiva individualização do usuário. Torna-se indispensável, então, uma segunda etapa de quebra de sigilo: a propositura de uma nova pretensão em face do provedor de conexão (as operadoras de telefonia). De posse do IP e do fuso horário precisos, esta operadora é intimada a identificar qual linha telefônica ou contrato residencial estava associado àquela assinatura de dados.

O grande gargalo prático que inviabiliza a responsabilização e alimenta a impunidade reside no descompasso temporal entre a volatilidade da prova cibernética e a burocracia do sistema de justiça nacional. O artigo 15 do Marco Civil da Internet compele os provedores de aplicação a conservarem os registros de acesso sob sigilo pelo prazo exíguo de apenas 6 (seis) meses (Brasil, 2014). No entanto, o tempo técnico da internet colide diretamente com o tempo burocrático das instituições jurídicas brasileiras. Desde o momento em que a vítima toma ciência da agressão à sua honra subjetiva, inicia-se um decurso temporal severo: a realização do boletim de ocorrência, a instauração e tramitação do inquérito policial, a busca por representação jurídica (seja por advogado particular ou pela sobrecarregada Defensoria Pública), o protocolo da petição inicial e a posterior apreciação do pedido de liminar pelo magistrado.

O que a doutrina especializada evidencia é que essa janela temporal curta acaba por exigir do aparato estatal e dos causídicos uma diligência quase instantânea, sob pena de esvaziamento do objeto da demanda pela eliminação lícita das informações (Crespo, 2021). Frequentemente, quando a ordem judicial de quebra de sigilo é finalmente expedida e o oficial de justiça intima a plataforma digital, o prazo legal de seis meses já se exauriu. Como o descarte de dados após esse período é uma conduta lícita autorizada pela própria legislação, os provedores procedem à eliminação das informações, resultando na perda definitiva do rastro digital da autoria. Essa volatilidade probatória demonstra que a janela temporal oferecida pelo atual sistema normativo é insuficiente para dar amparo à vítima de injúria online, transformando o direito de resposta e de responsabilização numa promessa legal ineficaz para a imensa maioria dos casos de ofensas virtuais.

2.3. O Aparente Conflito com a Lei Geral de Proteção de Dados: Ponderação entre Privacidade e Efetividade da Tutela

A promulgação da Lei Geral de Proteção de Dados (Lei nº 13.709/2018, conhecida como LGPD) adicionou uma nova camada de complexidade jurídica ao tratamento dos registros de

conexão e acesso à internet (Brasil, 2018). A LGPD erigiu a privacidade, a autodeterminação informativa e a proteção de dados pessoais ao patamar de direitos fundamentais no ordenamento brasileiro. Entre os pilares dessa legislação, destacam-se os princípios da finalidade, da adequação e da minimização dos dados, os quais determinam que o tratamento de dados pessoais deve ser limitado ao mínimo necessário para a realização de suas finalidades específicas, impondo o descarte dessas informações assim que o objetivo do tratamento for atingido (Brasil, 2018).

Sob uma leitura descontextualizada ou excessivamente restritiva, poder-se-ia argumentar que a guarda massiva e preventiva de logs de acesso e de conexões por provedores de internet violaria o espírito protetivo da LGPD, uma vez que tais metadados têm a capacidade de individualizar e traçar o perfil comportamental dos cidadãos na rede. Configura-se, desse modo, um aparente conflito de normas entre o dever de retenção de dados imposto pelo Marco Civil da Internet (Brasil, 2014) e as restrições ao tratamento de dados consagradas pela LGPD (Brasil, 2018).

No entanto, a doutrina civil-constitucional contemporânea adverte que o direito à proteção de dados e à privacidade não possui caráter absoluto, devendo coexistir de forma harmônica com outros direitos de igual envergadura, como a inviolabilidade da honra, da imagem e o amplo acesso à justiça. Sob a óptica desse cruzamento normativo, argumenta-se na doutrina especializada que o armazenamento compulsório desses metadados pelos provedores não configura violação à autodeterminação informativa dos internautas.

A resolução dessa aparente antinomia passa pela aplicação das próprias bases autorizativas previstas no artigo 7º da LGPD. A guarda obrigatória de registros de conexão e de acessos a aplicações, prevista nos artigos 13 e 15 do Marco Civil da Internet (Brasil, 2014), encontra perfeita sustentação na hipótese do inciso II do referido artigo 7º da LGPD, que autoriza o tratamento de dados pessoais para o "cumprimento de obrigação legal ou regulatória pelo controlador" (Brasil, 2018). Portanto, os provedores não apenas podem, mas têm o estrito dever legal de manter esses registros sob custódia pelo prazo legal.

A proteção de dados pessoais estabelecida pela LGPD não foi concebida para atuar como um salvo-conduto ou um escudo de impunidade para a prática de crimes de injúria ou difamação no ambiente cibernético. A privacidade do usuário anônimo termina onde começa o direito fundamental da vítima de buscar a reparação pelos danos sofridos na sua dignidade. O ordenamento jurídico não pode tolerar que a tutela da privacidade seja distorcida a ponto de

impedir o exercício do direito de ação e de defesa do ofendido. A devida ponderação entre a preservação da intimidade coletiva na internet e a necessidade de responsabilização individual por atos ilícitos exige que os dados de conexão continuem a ser preservados de maneira segura, servindo como a ferramenta indispensável para que o Judiciário possa desmascarar os agressores e restabelecer a justiça no ciberespaço.

3. A JURISPRUDÊNCIA DOS TRIBUNAIS E A BARREIRA ECONÔMICA DA PROVA

Ao analisar a resposta do Poder Judiciário brasileiro frente ao fenômeno da injúria online, percebe-se uma jurisprudência consolidada que privilegia a livre manifestação do pensamento e a facilidade de navegação na rede em detrimento de uma proteção mais ágil à honra subjetiva das vítimas. O Superior Tribunal de Justiça (STJ) pacificou o entendimento de que os provedores de aplicação de internet não possuem a obrigação legal de exigir dados rígidos de cadastro, tais como a validação de CPF, de RG ou a verificação de identidade facial, quando um usuário cria uma conta nas suas plataformas. Conforme decidido em sede de recursos repetitivos, a exemplo do REsp 1.784.098/SP (Brasil, 2020), o tribunal considera que a exigência de identificação prévia e rigorosa representaria um obstáculo ao livre fluxo de informações e ao direito de acesso à rede, sufocando a liberdade de expressão em nível global.

Parte da doutrina sustenta, ainda, que a imposição de mecanismos excessivos de identificação poderia comprometer garantias constitucionais relacionadas à liberdade de expressão, à manifestação do pensamento e ao acesso democrático à informação, especialmente em contextos de denúncias sociais, participação política e proteção contra perseguições ideológicas. Sob essa perspectiva, o anonimato relativo no ambiente digital funcionaria como instrumento de proteção da livre manifestação em determinadas situações sensíveis. Contudo, embora tais preocupações sejam juridicamente relevantes, a proteção à liberdade de expressão não pode ser utilizada como escudo para práticas ilícitas que violem a honra, a dignidade e os direitos da personalidade de terceiros.

Apesar de fundamentada na proteção de princípios democráticos, essa jurisprudência gera reflexos severos e desproporcionais para o indivíduo que sofre agressões virtuais. Na prática, a desobrigação de cadastros validados transfere integralmente para a vítima o fardo e a complexidade técnica de identificar o agressor. Uma vez que qualquer pessoa pode criar múltiplos perfis utilizando endereços de e-mail temporários ou nomes fictícios, a internet transforma-se num terreno fértil para a proliferação de perfis falsos (*fakes*) voltados

exclusivamente para a prática de ofensas morais e linchamentos virtuais. A vítima, desprovida de conhecimentos técnicos e de recursos jurídicos céleres, vê-se diante de uma barreira de impunidade, enquanto o agressor desfruta de uma posição de confortável ocultação proporcionada pela própria arquitetura jurídica validada pelos tribunais.

Ademais, a discussão sobre a responsabilidade das plataformas e a remoção de conteúdos ofensivos atinge o seu ápice no julgamento do Tema 987 de Repercussão Geral pelo Supremo Tribunal Federal (STF), que discute a constitucionalidade do artigo 19 do Marco Civil da Internet (Brasil, 2014). Atualmente, sob a vigência do referido artigo, as redes sociais somente respondem civilmente por danos decorrentes de conteúdos gerados por terceiros se, após ordem judicial específica, não tomarem as providências para indisponibilizar o material apontado como ofensivo (Brasil, 2014). Este modelo de notificação judicial prévia é amplamente criticado pela doutrina especializada, pois ignora a velocidade avassaladora com que um conteúdo injurioso se propaga e viraliza nas redes sociais (Costa; Costa, 2024; Rodrigues; Farias; Freitas, 2020).

Enquanto a vítima aguarda a lenta tramitação de uma medida liminar para que a ofensa seja removida, o dano à sua integridade moral e psicológica é perpetuado e multiplicado a cada partilha. Defender a necessidade de intervenção judicial prévia para a remoção de manifestas ofensas morais, em casos em que não há debate político ou de interesse público, acaba por infligir à vítima uma severa vitimização secundária, forçando-a a suportar o escárnio público enquanto o sistema de justiça opera no seu ritmo ordinário e analógico (Pollak; Borges, 2023).

3.1. A Desigualdade na Produção da Prova Digital: O Custo da Fé Pública e a Exclusão da Vítima Hipossuficiente

Se a identificação do infrator anônimo nos crimes de injúria virtual já se apresenta como um caminho processual tortuoso, a colheita e a preservação da materialidade do crime revelam uma profunda desigualdade socioeconômica no acesso à justiça. No processo civil e penal, a prova digital é caracterizada pela sua extrema volatilidade: uma postagem injuriosa numa rede social pode ser apagada pelo agressor em segundos, destruindo os elementos que comprovariam a infração. Para evitar o perecimento da prova, as vítimas frequentemente recorrem à simples captura de ecrã (o popular *print screen*). No entanto, a jurisprudência pátria tem demonstrado crescente ceticismo em relação à validade jurídica dessas capturas de ecrã isoladas, uma vez que imagens digitais podem ser facilmente alteradas, simuladas por meio de códigos de inspeção de

páginas (*inspect element*) ou manipuladas por inteligências artificiais gerativas, carecendo, portanto, de integridade técnica e de preservação da cadeia de custódia (Jorge; Caselli, 2021).

Sob a perspectiva técnica especializada, o *print screen* carece de idoneidade processual por se tratar de uma mera representação gráfica desprovida de metadados essenciais, o que impossibilita a auditoria da cadeia de custódia da prova eletrônica. Manifestações nesse sentido advertem que a facilidade de manipulação de conteúdos em ambientes virtuais impede a verificação do princípio da mesmidade, tornando a prova vulnerável a contaminações e adulterações que comprometem a sua autenticidade em juízo, uma vez que a validação de uma prova digital exige o registro técnico de elementos estruturais profundos, como o código-fonte, endereços lógicos, logs e hashes criptográficos, requisitos que o cidadão comum é incapaz de capturar por meio de uma simples imagem estática.

Esse entendimento técnico encontra perfeito eco na jurisprudência pátria contemporânea. Ao julgar o Recurso Especial nº 1.903.252/RS, a Sexta Turma do Superior Tribunal de Justiça pacificou o entendimento de que a simples captura de tela é uma prova vulnerável e desprovida de rigidez fenomênica, uma vez que a ausência de espelhamento técnico e a quebra da cadeia de custódia impedem a verificação de sua integridade (Brasil, 2021). O Tribunal Superior assentou que, pela facilidade de adulteração e exclusão de mensagens ou postagens sem deixar vestígios, o *print screen* isolado não possui força probatória suficiente para subsidiar uma condenação (Brasil, 2021).

Para que a prova digital seja dotada de indiscutível valor probatório em juízo, a via tradicional e recomendada pelo artigo 384 do Código de Processo Civil (Brasil, 2015) é a lavratura de uma ata notarial. Trata-se de um instrumento público por meio do qual o tabelião de notas, dotado de fé pública, acede à página da internet onde consta a injúria, descreve minuciosamente o facto presenciado, regista o endereço eletrônico (URL) e atesta a existência do conteúdo ofensivo. Ocorre que a ata notarial é um ato cartorário de custo financeiro extremamente elevado. As tabelas de emolumentos estaduais fixam taxas que frequentemente ultrapassam centenas de reais por folha ou por hora de diligência. Para um cidadão de baixa renda ou de classe média baixa, o custo para registar uma simples ofensa no ambiente virtual em cartório torna-se uma barreira financeira intransponível.

Esta realidade escancara o fenómeno da elitização da prova digital, onde a defesa da dignidade e da honra subjetiva no ambiente virtual se converte num privilégio econômico de poucos. Enquanto vítimas de alto poder aquisitivo consegue mobilizar recursos financeiros

imediatos para blindar as suas provas através de atas notariais robustas, a parcela hipossuficiente da população é compelida a assistir passivamente à destruição das evidências das suas agressões morais pela impossibilidade de arcar com as custas cartorárias.

O sistema de justiça, ao exigir ferramentas de alto custo para garantir a autenticidade da prova e ao desconsiderar meios mais simples, acaba por promover uma exclusão social silenciosa. Cria-se, assim, uma grave distorção democrática: a honra dos mais abastados goza de tutela e preservação efetivas, enquanto os cidadãos vulneráveis veem as suas pretensões de responsabilização civil e penal rejeitadas por insuficiência probatória, perpetuando o anonimato virtual como um refúgio seguro para a impunidade dos agressores na internet.

3.2. A Tecnologia Blockchain como Alternativa Disruptiva na Validação e Preservação de Evidências Digitais

A superação do cenário de exclusão processual que afeta a vítima hipossuficiente exige a transição para um modelo de instrução probatória que rompa com o monopólio financeiro da fé pública tradicional. Nesse horizonte, as soluções baseadas na tecnologia *blockchain* surgem como uma alternativa viável para a preservação de evidências digitais. Ao registrar metadados, hashes criptográficos e logs de acesso em uma rede descentralizada, distribuída e imutável, essas plataformas conferem anterioridade, integridade e autenticidade à prova por uma fração ínfima do custo de uma ata notarial. Trata-se de uma evolução técnica que substitui a necessidade de um tabelião pela validação matemática de algoritmos inteiramente auditáveis.

A viabilidade jurídica dessa ferramenta encontra amparo no próprio ordenamento nacional, especialmente a partir de uma interpretação progressista do artigo 411, inciso II, do Código de Processo Civil (Brasil, 2015), que admite a autenticidade do documento quando a autoria estiver identificada por qualquer meio legal de certificação. O amplo reconhecimento judicial dessas plataformas assegura que a evidência coletada na internet permaneça idêntica até o momento de sua apreciação pelo magistrado, resguardando perfeitamente a idoneidade da cadeia de custódia (Teixeira, 2021). Desconstrói-se, assim, a premissa de que a segurança jurídica do documento eletrônico é um privilégio econômico, democratizando os meios de defesa contra os ilícitos virtuais

CONSIDERAÇÕES FINAIS

A presente pesquisa teve como escopo analisar de forma crítica e fundamentada a efetividade dos mecanismos jurídicos nacionais na identificação de infratores anônimos na internet, tomando como base os impactos gerados pelo ônus probatório digital sobre a vítima em situação de hipossuficiência técnica e financeira nas redes sociais.

A partir da problemática proposta, verificar se a atribuição à vítima do ônus de identificar o agressor e produzir as provas digitais necessárias para o ajuizamento da demanda judicial constitui obstáculo ao princípio constitucional do acesso à justiça, buscou-se compreender de que maneira o Estado tem (ou não) garantido a plena atuação da tutela jurisdicional, à luz da legislação vigente e da proteção aos direitos da personalidade. O estudo foi estruturado em três capítulos principais que, em conjunto, permitiram uma abordagem integrada da temática.

No primeiro capítulo, foram discutidos os fundamentos normativos e conceituais que asseguram a proteção jurídica da honra no contexto digital, com ênfase na distinção entre honra objetiva e subjetiva, na vedação constitucional ao anonimato e na tipicidade dos crimes de calúnia, difamação e injúria. Demonstrou-se que, embora tais institutos possuam sólida base penal tradicional, a agressão virtual multiplica o dano de forma exponencial devido ao potencial de viralização, exigindo respostas que superem os limites da era analógica. No segundo capítulo, foram analisadas as condições práticas e regulatórias impostas pelo Marco Civil da Internet no tocante à guarda de registros pelos provedores, revelando-se a insuficiência do prazo exíguo de seis meses de armazenamento e a complexidade técnica de individualização do usuário a partir do fornecimento isolado do endereço de IP.

Constatou-se que a classificação da "matrícula" da conexão constitui apenas uma etapa inicial que depende de conhecimentos periciais avançados, distanciando o cidadão comum da via reparatória. O terceiro capítulo tratou das implicações jurídicas da barreira econômica na produção da prova eletrônica, considerando a jurisprudência contemporânea do Superior Tribunal de Justiça, que retirou o valor probatório absoluto do simples *print screen* por sua fácil manipulação. Também se adotou como suporte o princípio da mesmidade e a cadeia de custódia, demonstrando-se que a exigência de mecanismos rígidos de preservação, como a ata notarial, opera como um entrave processual intransponível devido aos custos proibitivos dos emolumentos cartorários.

Nesse sentido, as hipóteses da pesquisa foram confirmadas: a insuficiência do sistema de justiça decorre do fato de que o ordenamento vigente concentra esforços na fase decisória em detrimento do suporte à produção inicial da prova eletrônica. Conforme o que foi analisado, verificou-se que a atribuição integral desse ônus tecnológico transforma a preservação da evidência em um privilégio econômico, beneficiando o agressor anônimo e promovendo a exclusão processual das vítimas vulneráveis.

Diante desse cenário, conclui-se que a efetivação do princípio constitucional do acesso à justiça diante dos crimes cibernéticos exige uma atuação mais ativa e comprometida por parte do Estado.

É fundamental que sejam instituídas ferramentas tecnológicas descentralizadas e acessíveis para a fixação de evidências digitais, com atenção especial à viabilidade da tecnologia *blockchain* e de carimbos de tempo como alternativas democráticas e de baixo custo para assegurar a integridade da cadeia de custódia sem a dependência dos altos custos dos cartórios.

Além disso, é urgente o fortalecimento das estruturas institucionais, com a ampliação da atuação da Defensoria Pública na fase pré-processual por meio de núcleos especializados em Direito Digital, de forma a romper com a lógica da exclusão que ainda marca o litígio no ciberespaço. A superação desse quadro demanda não apenas recursos materiais, mas sobretudo vontade política e sensibilidade social para garantir que a identificação do infrator na internet não seja condicionada à capacidade financeira do ofendido, assegurando a todos o respeito e a dignidade que lhes são devidos.

REFERÊNCIAS BIBLIOGRÁFICAS

ALEXANDRE, F. L.; ARAÚJO, L. C. A evolução dos crimes cibernéticos e os desafios da legislação brasileira. **RevistaFT**, v. 31, n. 119, p. 701–716, 2023. Disponível em: https://revistaft.com.br/a-evolucao-dos-crimes-ciberneticos-e-os-desafios-da-legislacao-brasileira/. Acesso em: 24 sep. 2025.

BITENCOURT, Cezar Roberto. **Tratado de Direito Penal**: Crimes contra a Pessoa. 20. ed. São Paulo: Saraiva Educação, 2020.

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República, 1988. Disponível em: http://www.planalto.gov.br. Acesso em: 21 maio 2026.

BRASIL. Decreto-Lei nº 2.848, de 7 de dezembro de 1940. **Código Penal**. Disponível em: https://www.jusbrasil.com.br/topicos/10622974/artigo-138-do-decreto-lei-n-2848-de-07-de-dezembro-de-1940. Acesso em: 24 set. 2025.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil (Marco Civil da Internet). Brasília, DF: Presidência da República, 2014. Disponível em: http://www.planalto.gov.br. Acesso em: 21 maio 2026.

BRASIL. Lei nº 13.105, de 16 de março de 2015. **Código de Processo Civil**. Brasília, DF: Presidência da República, 2015. Disponível em: http://www.planalto.gov.br. Acesso em: 21 maio 2026.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD)**. Brasília, DF: Presidência da República, 2018. Disponível em: http://www.planalto.gov.br. Acesso em: 21 maio 2026.

BRASIL. Superior Tribunal de Justiça (2. Seção). **Recurso Especial nº 1.784.098/SP**. (Tema 987 dos Recursos Repetitivos). Relator: Ministro Luis Felipe Salomão. Julgado em: 11 mar. 2020. *Diário da Justiça Eletrônico*, Brasília, DF, 18 mar. 2020.

BRASIL. Superior Tribunal de Justiça (6. Turma). **Recurso Especial nº 1.903.252/RS**. Relator: Ministro Nefi Cordeiro. Julgado em: 23 fev. 2021. Diário da Justiça Eletrônico, Brasília, DF, 26 fev. 2021. Disponível em: https://www.stj.jus.br. Acesso em: 21 mai. 2026.

CAVALCANTI, Francisco Roberto T. **Crimes contra a honra nas redes sociais sob o anonimato**: algumas abordagens sociojurídicas em defesa da honra e os desafios legais e institucionais da identificação e da responsabilidade à luz do Marco Civil da Internet e de outros dispositivos normativos. 2025. 89 f. Monografia (Curso de Direito) – Universidade Federal da Paraíba, Santa Rita, 2025.

COSTA, Fernanda; COSTA, Rodrigo. Calúnia digital e fake news: desafios legais e jurisprudenciais no Brasil. **Revista Vista**, v. 10, n. 2, p. 45-62, 2024.

COSTA, José Manuel de Velasco. **História do Direito Romano**. 4. ed. Coimbra: Almedina, 2018.

CRESPO, Marcelo. **Crimes Digitais e os Desafios da Investigação Cibernética**. São Paulo: Editora Jurídica, 2021.

JORGE, Higor Vinicius Nogueira; CASELLI, Guilherme. **Prova Digital**: Teoria e Prática. 2. ed. Salvador: Juspodivm, 2021.

LOPES, José Reinaldo de Lima. **O Direito na História**: Lições de História do Direito. 5. ed. São Paulo: Atlas, 2014.

PECK, Patrícia. **Direito Digital**. 7. ed. São Paulo: Saraiva Educação, 2021.

POLLAK, Natália; BORGES, Felipe. Direitos humanos e crimes contra a honra na era digital. **Revista Vista**, v. 9, n. 1, p. 23-39, 2023.

PRADO, Luiz Regis. **Tratado de Direito Penal Brasileiro**: Parte Especial. 3. ed. Rio de Janeiro: Forense, 2019.

RODRIGUES, M.; FARIAS, I.; FREITAS, R. D. Crimes cibernéticos à luz dos crimes contra a honra. In: CONGREGA MIC. **Anais [...]**, v. 16, n. 0, p. 354–359, 2020.

SANTANA, Katiene G.; SANTOS, Keila O. **Crimes contra a honra no ambiente virtual**. 2017. Monografia (Curso de Direito) – Centro Universitário Uninabuco, Paulista, 2017.

SILVA, João; CRUZ, Mariana. Crimes digitais: a linha tênue entre liberdade de expressão e crimes contra a honra cometidos no meio digital. **Revista Vista**, v. 10, n. 1, p. 15-30, 2024.

SIQUEIRA, Aldo. **Direito e Internet**: Responsabilidade Civil dos Provedores e Tutela da Honra. Rio de Janeiro: Forense, 2017.

SYDOW, Spencer Toth. **Exposição pornográfica não consentida na internet**: análise jurídica da vingança pornográfica. São Paulo: Almedina, 2019.

TEIXEIRA, Tarcísio. **Direito Digital e Processo Eletrônico**. 5. ed. São Paulo: Saraiva Educação, 2021.

TEIXEIRA, Tarcisio; LIMBERGER, Têmis. **Marco Civil da Internet**: Comentários à Lei nº 12.965/2014. 4. ed. São Paulo: Revista dos Tribunais, 2020.

TOMASEVICIUS FILHO, Eduardo. Marco Civil da Internet: uma lei sem conteúdo normativo. **Estudos Avançados**, v. 30, n. 86, p. 269-284, 2016.

WOLKMER, Antônio Carlos. **Fundamentos de História do Direito**. 9. ed. Belo Horizonte: Del Rey, 2019.