
# A RESPONSABILIDADE CIVIL E CRIMINAL DO *DOXXING*

# THE CIVIL AND CRIMINAL LIABILITY OF *DOXXING*

Giovanni Zanella[1]
Jandir Ademar Schmidt[2]

## RESUMO

Este artigo tem como objetivo investigar as dimensões da responsabilidade civil e criminal do *doxxing*, compreendendo suas ramificações legais e sociais. Os objetivos específicos incluem analisar os fundamentos legais da responsabilidade civil do *doxxing*, avaliar as implicações criminais desta prática sob a legislação brasileira, identificar os principais impactos psicossociais nas vítimas, e identificar medidas preventivas e estratégias legais para mitigar o *doxxing*. Metodologicamente a pesquisa classifica como dedutiva, descritiva e bibliográfica. Conclui-se que o *doxxing* viola a privacidade e tem consequências graves para as vítimas, exigindo uma abordagem multidisciplinar para prevenção e combate. Apesar da escassez de estudos, percebe-se a urgência de debates doutrinários, jurisprudenciais e legislativos para enfrentar esse problema, garantindo a proteção dos direitos fundamentais no ambiente digital. A ausência de diretrizes claras pode enfraquecer os mecanismos de prevenção e combate ao abuso digital, expondo os usuários a riscos cada vez maiores de violação da privacidade e danos emocionais. Portanto, é essencial promover um diálogo interdisciplinar para desenvolver políticas e estratégias adequadas para proteger os cidadãos online.

**Palavras-Chave**: abuso digital; *doxxing;* responsabilização civil; responsabilização penal; privacidade.

## ABSTRACT

This article aims to investigate the dimensions of civil and criminal liability related to doxxing, understanding its legal and social ramifications. Specific objectives include analyzing the legal foundations of civil liability for doxxing, evaluating the criminal implications of this practice under Brazilian legislation, identifying the main psychosocial impacts on victims, and identifying preventive measures and legal

[1] Acadêmico do Curso de Direito da Universidade do Contestado (UNC). Campus Concórdia. Santa Catarina. Brasil. E-mail: giovannizanella10@gmail.com
[2] Mestre em Direito pela Universidade Federal de Santa Catarina (UFSC). Graduado pela Universidade Regional do Noroeste do Estado do Rio Grande do Sul (UNIJUÍ). Advogado e Professor do Curso de Direito da Universidade do Contestado (UNC). Campus Concórdia. Santa Catarina. Brasil. Email: jandir@unc.br



Acad. Dir. (ISSN: **2763-6976**)
v. 6, p. 3348-3372, 2024

strategies to mitigate doxxing. Methodologically, the research is classified as deductive, descriptive, and bibliografia. It is concluded that doxxing violates privacy and has serious consequences for victims, requiring a multidisciplinary approach to prevention and combating. Despite the scarcity of studies, there is an urgency for doctrinal, jurisprudential, and legislative debates to address this problem, ensuring the protection of fundamental rights in the digital environment. The absence of clear guidelines can weaken mechanisms for preventing and combating digital abuse, exposing users to increasing risks of privacy violations and emotional harm. Therefore, it is essential to promote interdisciplinary dialogue to develop appropriate policies and strategies to protect online citizens.

**Keywords**: digital abuse; doxxing; civil liability; criminal liability; privacy.

**Artigo recebido em**: 15/08/2024
**Artigo aceito em:** 11/10/2024
**Artigo publicado em**: 11/12/2024
Doi: https://doi.org/10.24302/acaddir.v6.3.5557

## 1 INTRODUÇÃO

O presente artigo tem como tema a ser explorado a responsabilidade civil e criminal do *doxxing*, analisando os fundamentos legais, avaliando as implicações criminais, investigando os impactos psicossociais nas vítimas e identificando medidas preventivas e estratégicas legais para mitigar o *doxxing*.

É importante que se compreenda, inicialmente, que tal prática envolve a divulgação de informações pessoais sensíveis de um indivíduo na internet sem o seu consentimento, desde o endereço residencial, número de telefone, informações de contato, detalhes de emprego e até mesmo informações sobre familiares.

Em meio a esse cenário tem-se que o objetivo do *doxxing* pode variar, desde intimidar ou assediar a vítima até causar danos à sua reputação ou até mesmo colocá-la em risco físico, assim como também pode ser incentivada por fatores diversos, como a vingança ou mesmo a simples vontade que comprometer o bem-estar físico e psíquico de outrem, motivações políticas ou ideológicas, dentre outras.

Portanto, percebe-se que o *doxxing* pode ser compreendido como violação de privacidade que pode ter consequências graves, incluindo assédio online, perseguição e até mesmo crimes mais sérios, sendo considerado uma forma de abuso digital e é ilegal, ainda que inexista, no ordenamento jurídico brasileiro, disposições na legislação civil e penal sobre este fenômeno.

Exatamente por isso o *doxxing*, prática cada vez mais comum na era digital, levanta questões sobre a responsabilidade civil e criminal dos indivíduos envolvidos. Diante disso, é fundamental investigar as implicações legais do *doxxing*, seus impactos nas vítimas e as medidas preventivas e punitivas disponíveis. Assim, dar-se-á seguimento ao estudo pautando-se no seguinte problema de pesquisa: Como vem se posicionando o ordenamento jurídico brasileiro diante da prática do *doxxing*, no que tange a responsabilização civil e criminal do agente?

Desta feita, tem-se como objetivo geral investigar as dimensões da responsabilidade civil e criminal do *doxxing*, compreendendo suas ramificações legais e sociais. Assim, o presente artigo tem como tema à ser explorado a responsabilidade civil e criminal do *doxxing*, analisando os fundamentos legais, avaliando as implicações criminais, investigando os impactos psicossociais nas vítimas e identificando medidas preventivas e estratégicas legais para mitigar o *doxxing*.

E, como objetivos específicos busca-se analisar os fundamentos legais que regem a responsabilidade civil do *doxxing*; avaliar as implicações criminais do *doxxing*, examinando a aplicação da legislação penal brasileira; identificar os principais impactos psicossociais do *doxxing* nas vítimas, com ênfase nos danos à reputação, suscetíveis de reparação civil; e, ainda, identificar medidas preventivas e estratégias legais para mitigar o *doxxing*, destacando a importância da proteção de dados, educação pública e recursos legais disponíveis para vítimas e autoridades.

Destarte, e para alcançar os objetivos supra adota-se, como método de abordagem, o dedutivo, partindo de premissas gerais para específicas. E, como método de procedimento pauta-se no método descritivo. No que tange a técnica de pesquisa, pauta-se o estudo na revisão bibliográfica, pois a doutrina, artigos, legislação, são as principais fontes de pesquisa.

## 2 FUNDAMENTOS LEGAIS

*Doxxing*, também conhecido como *doxxing*, é um termo que deriva da expressão coloquial "dropping dox", uma abreviação de "documents" (documentos), e refere-se ao ato de revelar a identidade de uma pessoa que estava operando sob anonimato. Como observam Menezes et al (2022), essa prática, comumente realizada online, envolve a divulgação de informações pessoais sensíveis de um indivíduo,

como nome completo, endereço, número de telefone, informações de contato e até mesmo detalhes sobre familiares.

Ao tratar do conceito do fenômeno em análise, Menezes *et al*. (2022, p. 828) assim o define:

> O *doxxing* pode ser compreendido como a divulgação intencional e pública, na internet, de informações de um determinado indivíduo, sem a sua permissão, e geralmente ocorre com a intenção de humilhar, ameaçar, intimidar ou punir a pessoa identificada.

Douglas (2016) salienta que, na atualidade, o termo *doxxing* tem uma aplicação ampla e é frequentemente empregado para descrever um conjunto de atos que envolvem a exposição de informações pessoais na internet sem o consentimento da vítima, geralmente com intenções maliciosas de causar danos à pessoa e/ou ao seu patrimônio.

Portanto, essa conduta é retratada como o uso abusivo de informações pessoais e sensíveis do sujeito, seguido pelo seu compartilhamento com terceiros, com a finalidade de causar dano, perturbação ou obter vantagem indevida. Essas informações podem incluir dados como nome completo, endereço, número de telefone, informações de contato, detalhes sobre familiares, entre outros (MOTA *et al*., 2016).

Segundo Ramos (2022), o *doxxing* é uma forma extremamente invasiva de assédio online que envolve a divulgação deliberada de informações privadas ou identificação pessoal de um indivíduo, como telefone, e-mail ou endereço, cuja finalidade é expor a vítima, mas, ainda, intimidar, ameaçar ou difamar. E o autor complementa:

> [...] campanhas de assédio online e o que foi nomeado como *doxxing* – prática de procurar e divulgar informações privadas ou informações de identificação pessoal de um indivíduo, como seu telefone, e-mail ou endereço, sabidamente em um ambiente que encoraja ou necessariamente culmina na intimidação ou ameaça à pessoa exposta [...]. O *doxxing* se tornou um clássico do assédio on-line contra jornalistas mulheres e estava presente neste primeiro caso, em 2010, mas já era prática de trolls, assim como o envio de pizzas à residência da pessoa (RAMOS, 2022, p. 14).

Complementam Menezes *et al.* (2022) que tal prática é frequentemente utilizada como uma tática de intimidação contra jornalistas, especialmente mulheres,

e está intrinsecamente ligada a campanhas de assédio online. Logo, ao divulgar essas informações sensíveis em um ambiente virtual, os perpetradores pretendem criar um clima de hostilidade e medo na vida da vítima.

Não se pode ignorar, ainda, que o *doxxing* também pode se manifestar em outras formas de assédio online, como envio de mensagens intimidadoras ou ofensivas. Esse comportamento é muitas vezes associado a *trolls* da internet, que realizam ataques coordenados para causar danos emocionais e psicológicos às suas vítimas.

Por isso Ramos (2022) observa que, por meio da tipologia dos trolls, o *doxxing* é classificado como "IRL Trolling" (trollagem na vida real), evidenciando como essa prática se estende para além do ambiente virtual, impactando diretamente a vida cotidiana das pessoas expostas.

Porém, Douglas (2016) lembra que o *doxxing* é um tipo de violência que envolve a divulgação não autorizada de informações sensíveis, como endereço residencial, número de telefone e outros dados pessoais, com o propósito de prejudicar a vítima. Por exemplo, uma mulher que recebe ameaças online pode ter seu endereço exposto, o que pode intensificar seu medo e ansiedade em relação à sua segurança pessoal.

Lado outro, o termo *trolling* é utilizado para descrever o comportamento de indivíduos que publicam mensagens deliberadamente provocativas ou confusas, com o intuito de induzir as pessoas a uma resposta emocional ou para perturbar uma discussão normal (RAMOS, 2022).

À luz das informações anteriores, é evidente que o *doxxing* e o trolling, embora possam ocorrer em contextos semelhantes dentro do espaço digital, são distintos em sua natureza e motivação. Enquanto o *doxxing* envolve a divulgação não autorizada de informações pessoais sensíveis com o objetivo de causar danos à vítima, o trolling refere-se à prática de postar mensagens provocativas ou desorientadoras com o propósito de induzir uma resposta emocional ou perturbar uma discussão. Em outras palavras, enquanto o *doxxing* busca expor e intimidar, o trolling busca provocar e perturbar.

Portanto, é fundamental distinguir entre esses dois fenômenos para compreender adequadamente os diferentes tipos de abusos e comportamentos prejudiciais que ocorrem online, até mesmo porque, embora tenham pontos de

interseção, para fins de responsabilização, principalmente criminal, precisam ser bem delimitados.

Já Menezes *et al.* (2022) apontam que o *doxxing*, enquanto espécie do gênero assédio digital, pode ser compreendido também como uma espécie de *cyberbullying*, no que diz respeito à divulgação de dados pessoais no mundo virtual. Significa dizer que para os retromencionados autores, o assédio digital é uma modalidade ampla, que contempla outras, como o *cyberbullying*. Este, por sua vez, tem dentre suas modalidades o *doxxing.*

Verifica-se, nesse contexto, que assim como acontece com os termos *doxxing* e trolling, também se observa menções ao *doxxing* como uma forma específica de *cyberbullying*. Nesse sentido, o *doxxing* é visto como uma prática que se enquadra dentro do espectro mais amplo do *cyberbullying*, no qual indivíduos utilizam a internet e outras tecnologias para assediar, intimidar ou causar danos a outros.

Independentemente dessas divergências, que encontram terreno fértil até mesmo pelo fato de não ser o fenômeno objeto de disciplina legal, o *doxxing*, ao expor informações privadas e sensíveis de uma pessoa sem consentimento, pode ter um impacto devastador sobre a vítima, levando a consequências emocionais, psicológicas e até mesmo físicas.

Exatamente por nisso Menezes *et al*. (2022) chamam a atenção para o fato de que o *doxxing* claramente vai de encontro à tutela da privacidade, e demonstra-se cada vez mais desafiador no cenário jurídico, seja pela ampla difusão de informações nos mais diversos meios de comunicação, seja pela utilização inadequada da internet por vários usuários, que ignoram os limites legais e éticos da utilização de plataformas digitais, blogs, congêneres.

A privacidade é fundamental para assegurar a dignidade, liberdade e autonomia do indivíduo, permitindo o controle sobre as próprias informações pessoais e a decisão sobre como e com quem compartilhá-las. Essa proteção é crucial para o desenvolvimento da identidade individual e para o estabelecimento de relações pautadas em confiança e respeito à individualidade (DONEDA, 2017).

A doutrina tende a definir a privacidade como um dos direitos da personalidade, destacando que se trata do "conjunto de informações sobre o indivíduo que ele pode manter sob seu controle exclusivo, ou comunicar, decidindo para quem, quando, onde e em que condições, sem que isso seja legalmente imposto" (SILVA, 2024, p. 208).

Ao analisar o tema, Bittar (2017), em sua obra clássica sobre os direitos da personalidade, enfatiza a importância do direito à privacidade nesse campo. Portanto, esses são direitos essenciais, vitalícios e intransferíveis, que protegem valores inerentes à pessoa humana, como a vida, a honra, a identidade, o segredo e a liberdade.

Nas últimas décadas, houve uma mudança significativa no perfil da privacidade devido à interação de vários interesses ao seu redor. Por esse motivo, Bittar (2017) entende que a privacidade não está mais centrada na pessoa, na informação e no segredo, mas sim em um novo eixo, composto pela estruturação da pessoa, da informação, da circulação e do controle.

Outra visão esclarecedora é apresentada por Brito (2011), que relaciona a privacidade às manifestações de algumas pessoas. Ou seja, na visão do autor, algumas manifestações do indivíduo não devem ser acessíveis ao conhecimento de outros, são secretas, e não é lícito divulgá-las, revelá-las ou dar conhecimento delas, independentemente da forma e do número de pessoas.

Schreiber (2014) também contribui para a definição de privacidade, afirmando que consiste no direito de manter o controle sobre as próprias informações e o poder de determinar as modalidades da própria esfera privada. A partir desse conceito, as informações pessoais tornam-se o objetivo e a construção da esfera privada, a finalidade.

Privacidade e proteção de dados pessoais são agora reconhecidas como direitos fundamentais que asseguram a liberdade e a dignidade do indivíduo, protegendo-o contra usos indevidos de suas informações pessoais e garantindo a autonomia sobre seus dados num mundo cada vez mais interconectado (MENDES *et al*., 2018).

É interessante observar a abordagem de Silva (2024) sobre a ideia inicial de privacidade. Para o autor, o conceito de privacidade que predominou por muitos anos não é mais capaz de abranger as complexas relações inerentes à sociedade atual da informação. Isso se deve à disseminação do uso da tecnologia, o que torna a violação da privacidade mais intensa e silenciosa, sendo este um "fantasma embutido na ferramenta que se tornou indispensável para a eficiência nas atividades cotidianas do homem: o computador" (SILVA *et al*., 2020, p. 07).

De fato, com a o grande avanço tecnológico vivenciado nas últimas décadas, sobretudo a facilidade do acesso à informação gerada pelo uso de ferramentas como tablets, celulares e computadores, as redes sociais (facebook, X, instagram, WhatsApp, etc.) assumiram lugar de destaque e de grande repercussão nas relações interpessoais.

De fato, a internet contribui para romper com a barreira temporal e pôr fim aos obstáculos de acesso ao conhecimento e difusão de informações (GIACCHETTA *et al*., 2014). Não obstante, também enfatiza que todo o processo de inovação tecnológica, voltada à mais rápida difusão de informações, trouxe problemas, principalmente porque a liberdade de expressão e de informação não são direitos fundamentais absolutos.

A internet é a interligação de redes de computadores espalhados pelo mundo, que passam a funcionar como uma só rede, possibilitando a transmissão de dados, sons e imagens de forma rápida (ALMEIDA *et al*., 2015). Nesse sentido, convém observar que, apesar de já ser rotina para todos nós executar ações como enviar um e-mail, falar ao celular, ler uma notícia online, escrever um conteúdo no blog, participar de um chat, fazer uma compra online, tirar uma foto digital, dentre outras coisas, para muitos não são claros os limites e as responsabilidades envolvidas nessas atividades da era virtual.

Nesse passo, possuindo a internet um imenso efeito multiplicador, que potencializa os danos, tornando não apenas mais rápida sua efetivação como mais amplos os seus estragos, a atuação e utilização de maneira indevida da rede dentre os indivíduos é real, uma vez que as relações jurídicas realizadas através das redes de computadores ocorrem dentro daquilo que se denomina espaço virtual (CASTRO, 2014).

As redes sociais, em breves linhas, são um meio de se conectar a outras pessoas na internet, cujo principal objetivo é juntar um grupo de pessoas com quem se esteja interconectado por um ou mais fatores, surgindo uma verdadeira interação social (NAPOLITANO *et al*., 2018).

De fato, algumas redes sociais estão preparadas especificamente ao redor dos interesses especiais, tais como o *Facebook* e *X*. Esses sites existem para compartilhar experiências, conhecimentos e formar grupos sobre tópicos específicos, para difundir

informações, servindo, como lembram Napolitando *et al*., (2018, p. 323), para ampliar o alcance do discurso, senão veja:

> Para além da possibilidade de manifestar o pensamento, opiniões e sentimentos, atualmente, o acesso à internet e, sobretudo, às redes sociais intensificou o dissenso ao assegurar que grupos, historicamente afastados da esfera de debate público, pudessem divulgar os seus conteúdos, com extrema rapidez e abrangência.

Na Internet, as redes sociais são todo e qualquer site de relacionamento cujo principal atrativo é conectar pessoas de diferentes locais a redor do mundo a fim de criar laços afetivos e fraternos, podendo, a partir daí, conectar-se com amigos em comum, criar novos e até mesmo se relacionar fisicamente com novos conhecidos. Trata, em síntese, de uma ferramenta social pela qual há a interação de pessoas através de seus perfis com o fim de trocar experiências, de maneira virtual, com outros indivíduos conectados na mesma rede (NAPOLITANO *et al*., 2018).

Nestas redes online, a capacidade básica para os usuários é criar e compartilhar seu perfil pessoal, onde podem ser inseridas informações e gostos pessoais, bem como a publicação de fotos e vídeos no perfil criado. Porém, cada rede social possui a sua peculiaridade de regras e métodos de busca e contato com amigos em potencial, apesar de quase a sua totalidade possuir a mesma finalidade (NAPOLITANO *et al*., 2018). Nessa esteira, diversos foram os sites que, aproveitando-se da popularidade da internet, criaram sites com o intuito de promover as relações sociais dos internautas, tendo por escopo a facilidade que a rede transporta seus usuários através de contatos por todo o mundo através de fácil acesso.

Com a intensa demanda que geraram centenas de milhares de cadastros e perfis criados, foi oportunizado, além da criação de diversos contatos e relacionamentos virtuais, o lado negativo de toda essa popularidade: a dos usuários que acabam cometendo ilícitos, dentre os quais se destaca a difusão de falsas informações, os discursos de ódio, dentre outras (REBS *et al*., 2017). Logo, instaura-se um conflito entre a privacidade e a difusão de informações, em sentido amplo, nas redes sociais.

Sem dúvida, o direito à privacidade é a possibilidade que cada indivíduo tem de evitar a intromissão de estranhos em sua vida privada e familiar, assim como de impedir o acesso e a divulgação de informações sobre a privacidade de cada um.

Nesse contexto, o direito ao esquecimento ganha destaque, pois se a privacidade é o direito de manter certos fatos para si, ser constantemente "lembrado" deles não é viável.

Leonardi (2012) concorda com a abordagem anteriormente mencionada, no sentido de que a privacidade deve ser vista de uma perspectiva plural, já que a definição tradicional acaba por dificultar a compreensão do que está incluído em sua proteção, o que pode prejudicar sua importância em caso de conflito com outros direitos e interesses.

É incontestável que a privacidade desempenha um papel de extrema relevância em questões políticas em toda a sociedade, no sentido de que o respeito a todas as formas de liberdade individual e a busca por meios adequados para sua proteção são de grande importância para os direitos de associação e também para evitar a limitação do controle governamental em relação aos pensamentos e ações de toda a sociedade (SILVA, 2024).

Por fim, como demonstra Leonardi (2012) ao conceituar a privacidade, é de grande importância a ideia de controle sobre informações e dados pessoais. As pessoas reivindicam o direito de determinar como suas informações são utilizadas, e a elas cabe decidir o que é aceitável ou não, considerando que todas as informações são repassadas e comercializadas para uma variedade de terceiros.

Superada tal questão, passa-se à análise das implicações criminais e cíveis do *doxxing*, objeto da próxima seção.

## 3 IMPLICAÇÕES CRIMINAIS E CÍVEIS DO *DOXXING*

Lima *et al.* (2014, p. 230) partem do mesmo pressuposto de que vivemos em uma sociedade de classificação, na qual o homem está constantemente exposto através dos meios tecnológicos. Todas as suas características, ou seja, aquilo que ele mais gosta, de acordo com suas preferências, podem ser facilmente acessadas através de um clique, o que abre acesso aos seus dados pessoais.

Por isso, dentre questões inúmeras, a responsabilização civil e criminal em caso de *doxxing* precisa ser discutida pela ótica da proteção de dados, da efetiva tutela da privacidade, da responsabilização ante as novas tecnológicas da informação, da responsabilização civil dos agentes, dentre outras. Significa dizer que a privacidade

merece a tutela do Estado, seja no que tange a responsabilização civil, quando violada a honra, a imagem, quando há exposição demasiada de dados, etc., seja a responsabilidade criminal, pois o assédio virtual, online, não raras vezes também configura delitos como calúnia, difamação, injúria e outros.

A injúria refere-se a ofensas e xingamentos dirigidos a alguém, atacando sua honra e dignidade. Nas redes sociais e em fóruns online, é comum encontrar comentários agressivos e desrespeitosos, muitas vezes ultrapassando os limites do aceitável.

Já a difamação envolve a divulgação de informações falsas ou distorcidas sobre uma pessoa, prejudicando sua reputação. Na internet, notícias falsas, boatos e comentários difamatórios podem se espalhar rapidamente, causando danos irreparáveis à imagem da vítima.

A calúnia, por sua vez, consiste em imputar falsamente a alguém a prática de um crime, afirmando que essa pessoa cometeu algo ilegal. A disseminação de acusações infundadas na internet pode levar a graves consequências para a reputação e a vida pessoal do indivíduo caluniado.

Assim, como lecionam Mota *et al.* (2016, p. 128):

> Ocorre injúria quando se ofende a honra ou o decoro do indivíduo (Art. 140 do Código Penal). Calúnia acontece quando se imputa um fato criminoso a um indivíduo que não o praticou (Art. 138 do Código Penal); se o acusado praticou, não há crime, pois se trata de falar a verdade (exceção da verdade). Já a difamação ocorre quando se imputa a prática de um ato desonroso e não criminoso ao indivíduo que não o cometeu de fato (Art. 139 do Código Penal), ressalvada a exceção da verdade.

Portanto, o *doxxing*, ao divulgar informações pessoais sensíveis de um indivíduo sem consentimento, muitas vezes com o objetivo de causar danos à vítima, pode estar intrinsecamente ligado a crimes contra a honra, como calúnia, difamação e injúria. Quando as informações divulgadas são falsas e prejudiciais à reputação da pessoa exposta, isso pode configurar calúnia, que consiste na imputação falsa de um crime a alguém. Logo, configurará a calúnia e poderá levar o agente a ser condenado criminalmente se o *doxxing* consistir na falsa imputação de crime.

Da mesma forma, se as informações são verdadeiras, mas divulgadas com o intuito de prejudicar a reputação da vítima, caracteriza-se difamação, que é a divulgação de fato ofensivo à reputação de alguém. E, ainda, o *doxxing* pode resultar

em injúria, que é a ofensa à dignidade ou ao decoro de alguém, causando-lhe constrangimento ou vexame perante terceiros.

Portanto, o *doxxing* pode ser considerado uma forma de conduta criminosa que viola os direitos fundamentais de uma pessoa, sendo passível de responsabilização legal nos termos da legislação referente a esses crimes contra a honra.

É importante destacar que, além dos crimes contra a honra, o *doxxing* também pode estar relacionado a outras infrações legais, como invasão de privacidade, *stalking* (perseguição), ameaça, extorsão e até mesmo crimes cibernéticos. Wermuth *et al.* (2021), por exemplo, apontam que o *doxxing* pode configurar o crime previsto no art. 147-A do Código Penal Brasileiro, numa modalidade de *cyberstalking*.

Complementam Wermuth *et al.* (2021) que o *doxxing*, quando envolve a publicação não autorizada de dados pessoais da vítima em espaços digitais, como redes sociais, com o propósito de ridicularizá-la, menosprezá-la ou incitar assédio contra ela, configura-se como uma prática que viola a integridade moral e emocional da pessoa exposta. Tal comportamento pode ser caracterizado como uma forma de cyberbullying, como mencionado antes; e, de acordo com o artigo 147-A do Código Penal Brasileiro, pode ser considerado crime de perseguição, também conhecido como *stalking*, conduta criminosa cuja finalidade é intimidar, ameaçar ou importunar a vítima, causando-lhe medo, desconforto e angústia.

Não obstante tais considerações, a questão precisará, contudo, ser analisada no caso concreto, pois como inexiste um tipo penal específico, que trate do *doxxing*, tornando a conduta criminosa em si, elencando os requisitos e pena, é preciso que o interprete amolde a prática abusiva a um delito previsto no Código Penal ou legislação esparsa.

Isso se deve porque a divulgação não autorizada de informações pessoais sensíveis pode violar a privacidade da vítima e causar danos emocionais, psicológicos e, em alguns casos, físicos. Portanto, é fundamental que as autoridades estejam atentas a esse tipo de comportamento e que haja leis e medidas de proteção adequadas para prevenir e punir o *doxxing*, garantindo assim a segurança e a integridade das pessoas no ambiente digital. Nesse contexto surge a necessidade de se verificar a responsabilização civil por danos, seja ele material, seja moral.

A responsabilidade civil refere-se à obrigação legal de reparar os danos causados a outra pessoa ou seu patrimônio como resultado de uma conduta

negligente, imprudente ou deliberada. Dentro desse contexto, os danos podem ser classificados em duas categorias principais: dano material e dano moral. O dano material diz respeito aos prejuízos financeiros tangíveis sofridos pela vítima, como danos à propriedade, despesas médicas, perda de lucros ou danos materiais diretos (VENOSA, 2019).

Por outro lado, o dano moral refere-se aos prejuízos não financeiros, como sofrimento emocional, dor, angústia, humilhação, constrangimento ou perda da reputação. Embora o dano moral não seja facilmente mensurável em termos monetários, ele é igualmente reconhecido pela lei como uma forma legítima de dano que pode exigir compensação (GAGLIANO *et al*., 2020).

Ademais, cumpre registrar que a responsabilidade civil, para ser estabelecida, clama a presença de três elementos fundamentais são demonstrados: a existência de um ato ilícito ou negligente (conduta), o dano sofrido pela vítima e o nexo causal entre o ato e o dano. Nesse sentido, aquele que causa danos a outra pessoa ou seu patrimônio pode ser responsabilizado legalmente e obrigado a reparar os danos, tanto materiais quanto morais, causados pela sua conduta (GONÇALVES, 2018).

É importante ressaltar que a responsabilidade civil pode surgir de diversas situações, incluindo acidentes de trânsito, negligência profissional, danos ambientais, violação de direitos autorais, entre outros (GONÇALVES, 2018). Logo, não há dúvidas de que a responsabilidade civil desempenha um papel crucial no sistema jurídico ao garantir que as vítimas sejam devidamente compensadas pelos danos que sofreram e ao incentivar a prevenção de condutas prejudiciais à sociedade como um todo (VENOSA, 2019).

Anote-se, ainda, que na responsabilidade civil subjetiva, a culpa desempenha uma grande relevância na determinação da responsabilidade legal. Nesse contexto, a culpa refere-se à conduta negligente ou imprudente do agente que resulta em danos para a vítima. Para que a responsabilidade seja estabelecida, é necessário demonstrar que o agente agiu com negligência, ou seja, que ele falhou em agir com o cuidado e a diligência esperados em uma determinada situação. Essa negligência pode se manifestar de várias maneiras, como a falta de atenção, a violação de normas de segurança ou o descumprimento de deveres legais ou contratuais. No entanto, é importante ressaltar que a culpa deve ser comprovada com base em evidências

objetivas, levando-se em consideração o padrão de cuidado razoável esperado de uma pessoa comum nas mesmas circunstâncias (GAGLIANO *et al*., 2020).

Nesse cenário, e partindo da premissa de que o *doxxing*, como uma prática que viola a privacidade ao expor informações pessoais sensíveis sem consentimento, pode, de fato, gerar a obrigação de reparar civilmente o dano causado. Ao divulgar informações privadas, sem autorização, os perpetradores do *doxxing* podem causar danos emocionais, psicológicos e até mesmo físicos às vítimas. Esses danos podem incluir angústia emocional, ansiedade, medo, humilhação e perda da sensação de segurança e privacidade. Como resultado, as vítimas podem ter direito a uma reparação financeira pelos danos sofridos.

Na esfera da responsabilidade civil, a obrigação de reparar o dano causado pelo *doxxing* pode surgir quando três elementos fundamentais são demonstrados: a conduta ilícita do agente (no caso, a divulgação não autorizada de informações privadas), o dano sofrido pela vítima e o nexo causal entre a conduta e o dano (GAGLIANO *et al*., 2020).

Se esses elementos forem comprovados, os responsáveis pelo *doxxing* podem ser considerados legalmente responsáveis pelos danos causados e obrigados a compensar as vítimas. E, presente a culpa em sentido amplo, a compensação pelos canos causados pode incluir o pagamento de indenizações por danos materiais (como despesas médicas ou perda de oportunidades de trabalho) e danos morais (como sofrimento emocional e constrangimento), dada a exposição demasiada e não autorizada.

O Marco Civil da Internet, instituído pela Lei 12.965/14, introduziu mudanças significativas na responsabilização civil dos provedores de aplicações de internet. Antes dessa legislação, os provedores podiam ser responsabilizados por conteúdos ilícitos sem a necessidade de uma ordem judicial. Com a nova lei, a responsabilidade dos provedores por danos relacionados a conteúdos gerados por terceiros agora depende do cumprimento de ordens judiciais específicas que exigem a remoção desses conteúdos (FLUMIGNAN, 2021).

A implementação do Marco Civil da Internet no Brasil é um marco significativo na regulamentação da responsabilidade dos provedores de serviço de internet, estabelecendo diretrizes claras quanto à proteção da privacidade e dos dados dos usuários. A legislação é cuidadosa ao diferenciar o papel dos provedores de conteúdo

da responsabilidade por informações publicadas por terceiros, enfatizando a importância de processos legais adequados antes de qualquer intervenção. Este enquadramento legal assegura a liberdade de expressão e limita a responsabilidade dos provedores, criando um ambiente onde práticas como o *doxxing* precisam ser claramente abordadas através de medidas judiciais específicas para cada caso. Tal abordagem fortalece a necessidade de uma revisão e ajuste constante das leis, para acompanhar a evolução das tecnologias digitais e dos novos desafios que surgem, como o *doxxing* (URIAS, 2020).

Contudo, não se pode ignorar que o *doxxing* também gera impactos psicossociais, sendo importante abordá-los, ainda que sucintamente, objeto da próxima seção.

## 4 IMPACTOS PSICOSSOCIAIS NAS VÍTIMAS

Em 2017, pesquisadores da New York University Tandon School of Engineering e da University of Illinois at Chicago conduziram o primeiro estudo em grande escala sobre *doxxing*, explorando as motivações por trás dessa forma de assédio online e seu impacto nas vítimas.

Para o estudo foi desenvolvido um classificador de texto personalizado, uma ferramenta de processamento de linguagem projetada para analisar grandes volumes de texto. Este classificador foi especialmente desenvolvido para identificar e categorizar arquivos de *doxxing*, que contêm informações pessoais publicadas ilegalmente. Focando em sites conhecidos por hospedar esses arquivos, como Pastebin.com, 4chan.org e 8ch.net, a equipe capturou mais de 1,7 milhão de arquivos de texto durante dois períodos de seis a sete semanas. Utilizando o classificador, eles identificaram e examinaram mais de 5.500 mil arquivos associados ao *doxxing*, o que permitiu uma análise detalhada das motivações para *doxxing* e dos impactos nas vítimas. Esse método automatizado usando a tecnologia facilitou o processamento e a análise de um grande volume de dados, permitindo uma compreensão aprofundada das dinâmicas e consequências do *doxxing* (SNYDER *et al*., 2017).

O estudo revelou estatísticas alarmantes sobre a prevalência dessa forma de assédio online: mais de 90% dos arquivos expostos continham o endereço das vítimas, 61% incluíam número de telefone e 53% o endereço de e-mail. Além disso,

40% dos arquivos revelaram nomes de usuários online e endereços IP das vítimas. As informações mais sensíveis também foram comprometidas, incluindo números de cartão de crédito (4,3%), números de previdência social (2,6%) e outras informações financeiras (8,8%). A exposição dessas informações teve um impacto direto na segurança online das vítimas, com 32% ajustando as configurações de privacidade do Instagram e 25% do Facebook após o ataque (SNYDER *et al*., 2017).

É evidente que, após a divulgação online de suas informações pessoais, as vítimas sentiram a necessidade de ajustar as configurações de privacidade em suas redes sociais para aumentar sua proteção. Essas alterações podem incluir tornar contas privadas, limitar visualizações de postagens e controlar quem pode enviar mensagens, refletindo a preocupação e o impacto psicológico dessas vítimas em proteger sua privacidade e evitar mais assédios.

Para compreender os impactos psicossociais em vítimas, é útil examinar estudos sobre o Cyberstalking, uma forma de assédio online anterior ao *doxxing*, mas com efeitos potencialmente similares devido às suas semelhanças.

O *doxxing* é definido como a liberação intencional de informações pessoais na internet sem consentimento, frequentemente com o objetivo de intimidar ou punir o indivíduo visado. Já o cyberstalking envolve o uso repetido de comunicações eletrônicas para assediar ou intimidar alguém, e pode incluir ameaças, monitoramento obsessivo e invasão da privacidade da vítima (ALMAGOR *et al*., 2022).

Cyberstalking envolve o uso da Internet, e-mails ou outros meios de comunicação eletrônica para assediar ou ameaçar outra pessoa. Isso pode incluir o envio de mensagens ameaçadoras, monitoramento das atividades online da vítima, divulgação de informações pessoais sem autorização e criação de perfis falsos com a intenção de causar danos (POLLARD *et al*., 2008).

“Cyberstalking pode causar mudanças nos padrões de sono e alimentação, pesadelos, hipervigilância, ansiedade, desamparo, medo pela segurança e choque e descrença.” (POLLARD *et al*., 2008, p. 103).

Em Hong Kong um estudo conduzido por Chen *et al.* (2018) teve o objetivo de investigar a vitimização por *doxxing* e seus impactos emocionais entre estudantes do ensino médio. O estudo envolveu 2.120 mil estudantes de diferentes origens socioeconômicas, que completaram questionários sobre suas experiências de vitimização por *doxxing* e seus sentimentos psicológicos na semana seguinte. As

variáveis analisadas incluíram características demográficas, tipos de informações pessoais divulgadas, a identidade dos agressores e as plataformas usadas para o *doxxing*. A análise estatística utilizou coeficientes de Spearman, uma medida de correlação que avalia a força e a direção da associação entre duas variáveis, para determinar as associações entre vitimização por *doxxing* e sintomas de depressão, ansiedade e estresse.

Os impactos psicossociais nas vítimas de *doxxing* foram avaliados utilizando a versão curta da Escala de Depressão, Ansiedade e Estresse (DASS-21). Esta escala de autorrelato, composta por 21 itens, mede a frequência dos sintomas de depressão, ansiedade e estresse em três dimensões distintas. A análise dos dados coletados revelou associações significativas entre a vitimização por *doxxing* e aumentos nos níveis de depressão, ansiedade e estresse, indicando que a divulgação não autorizada de informações pessoais pode causar sofrimento psicológico considerável entre os adolescentes (CHEN *et al*., 2018).

Nos Estados Unidos, em janeiro de 2024, foi realizado um estudo com 1.003 mil adultos representativos em termos de gênero, raça e idade.

Como aponta Sheridan (2024), os participantes foram questionados sobre suas preocupações e experiências com o *doxxing*. Aqueles que se identificaram como vítimas foram convidados a participar da pesquisa que explorou as circunstâncias, reações e repercussões dos ataques. O estudo revelou informações importantes sobre a prevalência e os impactos do *doxxing*, destacando as graves consequências psicossociais para as vítimas.

De acordo com as informações obtidas, 4% dos americanos, aproximadamente 11 milhões de pessoas, relataram terem sido vítimas do *doxxing*. Entre os afetados, cerca de metade teve seus endereços residenciais ou e-mails divulgados, 25% tiveram fotos ou vídeos distribuídos online, e 20% tiveram informações pessoais sobre suas famílias compartilhadas. Mais de 90% dos usuários da web estão preocupados com o *doxxing*, e 73% limitam o que compartilham online para evitar serem vítimas. Os impactos incluem estresse e ansiedade, com casos extremos de hospitalização, danos à reputação pessoal e profissional, ameaças à segurança física, como uma vítima que recebeu ameaças de morte. Além disso, 93% das pessoas estão preocupadas com a possibilidade de serem vítimas, 72% preocupam-se com a

exposição de informações pessoais, 62% com ameaças à segurança, e 37% com repercussões profissionais ou financeiras (SHERIDAN, 2024).

Um caso notório no Brasil envolvendo o *doxxing* e a jornalista Vera Magalhães, ocorrido em 2020, evidencia os perigos do uso indevido da internet para práticas como o *doxxing* e a criação de perfis falsos em redes sociais. Durante um período de intensa polarização política, Magalhães, conhecida por suas análises críticas, foi alvo de ataques e ameaças online. Suas informações pessoais foram divulgadas sem consentimento, e vários perfis falsos foram criados para ridicularizá-la, configurando uma campanha de linchamento virtual, conforme relatado pela Associação Brasileira de Jornalismo Investigativo (ABRAJI, 2020). Esse incidente ilustra a responsabilidade civil e criminal dos envolvidos na exposição não autorizada de dados pessoais e na disseminação de mensagens fraudulentas, que afetam a integridade moral e emocional da vítima, além de comprometerem sua reputação e segurança física.

Trata-se apenas de um exemplo, que demonstra a necessidade de aprofundamentos nos estudos sobre a questão, dada a gravidade das consequências do *doxxing* que, ao violar a privacidade e causar danos às vítimas.

Em um recente julgamento pelo Tribunal de Justiça do Estado de São Paulo, foi abordado um caso de *doxxing*, onde um indivíduo alegou que a publicação de suas informações pessoais em plataformas digitais afetou adversamente sua vida profissional e pessoal. No agravo de instrumento nº 2225622-68.2020.8.26.0000, o agravante argumentou que seus dados sensíveis foram expostos sem consentimento, resultando em ameaças à sua segurança e danos à sua carreira (SÃO PAULO, 2021).

Ele solicitou a remoção de URLs específicas e a desvinculação de seu nome de resultados de pesquisas em buscadores de internet, ressaltando a capacidade técnica dos operadores desses serviços em interromper tal associação em seus sistemas de indexação. No entanto, a corte tratou as alegações como um "fato novo" introduzido na fase recursal, o que é inadmissível segundo o art. 329, I, do Código de Processo Civil, enfatizando a rigidez processual e a aderência aos direitos fundamentais como a liberdade de expressão e a proteção de dados pessoais.

O tribunal seguiu precedentes do Superior Tribunal de Justiça, decidindo contra a remoção das informações, sublinhando que os provedores de pesquisa na internet não são legalmente obrigados a eliminar resultados baseados em termos específicos (SÃO PAULO, 2021).

Logo, e sendo a única decisão jurisprudencial encontra com menção ao termo "*doxxing*", não se faz possível averiguar qual o entendimento jurisprudencial sobre responsabilidade civil e criminal ante a prática do *doxxing*. Desta feita, e do até aqui exposto, não há dúvidas de que o *doxxing* representa uma forma de abuso digital que que viola a privacidade das vítimas, exigindo uma resposta eficaz e abrangente por parte das autoridades e plataformas online.

## 5 MEDIDAS PREVENTIVAS E ESTRATÉGICAS LEGAIS PARA MITIGAR O *DOXXING*

Conforme exposto por John B. Major (2012), as vítimas de assédio online enfrentam grandes dificuldades em evitar seus perseguidores ou renunciar ao uso da Internet. Em um mundo altamente interconectado, a desconexão não é uma opção viável para muitas pessoas, pois isso resultaria na perda de importantes oportunidades pessoais e profissionais.

Diante disso Snyder *et al.* (2017) propõem medidas de mitigação, como "um serviço que pode informar as pessoas quando suas contas foram compartilhadas em um arquivo de dox, ou ferramentas de notificação para informar as autoridades quando indivíduos estão em risco elevado de abuso" (SNYDER *et al*., 2017, p. 432).

Seguindo o objetivo de encontrar formas de combater o *doxxing*, MacAllister (2017) propõe que "os estados devem criminalizar a publicação maliciosa de informações pessoais e apoiar o treinamento de agentes da lei para lidar melhor com vítimas de *doxxing*" (MACALLISTER, 2017, p. 2482).

Para proteger redes internas dentro de uma organização contra ataques de *doxxing*, é essencial implementar múltiplas camadas de defesa, uma abordagem conhecida como defesa em profundidade. Isso inclui o uso de autenticação de dois fatores e gerenciadores de senhas para garantir que o acesso seja impedido (KHANNA *et al*., 2016). Além disso, Khanna *et al.,* (2016) discutem a relevância das contramedidas organizacionais para prevenir ataques de *doxxing*, destacando que "as organizações devem empregar as ferramentas de *doxxing* utilizadas contra elas mesmas para realizar auditorias de privacidade de informações através de sites, que podem rastrear a origem da informação na internet" (KHANNA *et al*., 2016, p. 462).

Isso indica uma abordagem estratégica em que as organizações podem antecipar ataques, utilizando as mesmas ferramentas de seus potenciais atacantes para fortalecer suas defesas contra violações de privacidade e exposições maliciosas de informações.

Conforme discutido anteriormente, o *doxxing* é uma prática maliciosa de expor informações pessoais online sem consentimento, representa uma ameaça grave à privacidade e à segurança dos indivíduos na era digital. Para mitigar eficazmente essa ameaça, é imperativo adotar uma abordagem abrangente que combine medidas legais, proteção de dados e educação pública.

A proteção de dados desempenha um papel central na prevenção do *doxxing*. Empresas e plataformas online devem implementar medidas robustas de segurança cibernética para salvaguardar as informações pessoais de seus usuários contra acesso não autorizado. Isso inclui a criptografia de dados sensíveis, o uso de firewalls e a realização regular de auditorias de segurança (MOTA *et al*., 2016).

Ademais, a educação pública desempenha um papel crucial na prevenção do *doxxing*. Os usuários devem ser instruídos sobre os riscos associados à divulgação indiscriminada de informações pessoais online e sobre as medidas que podem ser tomadas para proteger sua privacidade (DOUGLAS, 2016). Isso envolve ensinar as pessoas a configurar corretamente as configurações de privacidade em suas contas online, bem como fornecer orientação sobre como reconhecer e evitar armadilhas comuns de engenharia social.

De igual forma, é essencial fortalecer os recursos legais disponíveis para vítimas e autoridades. Isso inclui a implementação de legislação específica que criminalize o *doxxing* e estabeleça penalidades proporcionais à gravidade do crime. As leis devem garantir que as vítimas tenham acesso a recursos legais adequados para buscar reparação por danos causados pelo *doxxing*, incluindo medidas de compensação financeira e proteção contra assédio (DOUGLAS, 2016).

Também é preciso que as vítimas de *doxxing* devem ser capacitadas para lidar com as consequências dessa prática e buscar justiça. Isso pode incluir o acesso a recursos legais gratuitos ou de baixo custo, bem como assistência psicológica para ajudar as vítimas a lidar com o impacto emocional do *doxxing* (DOUGLAS, 2016).

Portanto, proteger contra o *doxxing* requer estratégias abrangentes que enfatizem a proteção de dados, educação pública e recursos legais disponíveis para

vítimas e autoridades, pois somente através da implementação coordenada dessas medidas pode-se esperar mitigar eficazmente essa ameaça e proteger a privacidade e a segurança online de todos os indivíduos.

## 6 CONSIDERAÇÕES FINAIS

Este estudo teve como objetivo discorrer sobre a responsabilidade civil e criminal relacionada ao *doxxing*. Ao explorar os aspectos legais envolvidos nessa prática, busca-se compreender as repercussões jurídicas do *doxxing*, tanto em termos de responsabilização por danos causados às vítimas quanto pelas possíveis sanções penais aplicáveis aos seus perpetradores.

Constatou-se que o *doxxing* é compreendido como uma prática altamente invasiva e prejudicial, na qual informações pessoais sensíveis são expostas online sem o consentimento da vítima, exposição essa indevida e que pode ter sérias consequências para a privacidade, segurança e bem-estar emocional das pessoas afetadas.

Verificou-se, também, que o *doxxing* frequentemente ocorre com o intuito de intimidar, assediar ou difamar a vítima, tornando-se uma forma de abuso digital que desafia os direitos individuais e a liberdade na internet.

Anote-se, ainda, que a crescente conscientização sobre os impactos negativos do *doxxing* clama a uma maior discussão sobre medidas legais e políticas para prevenir e punir essa prática, destacando a necessidade de proteger a privacidade e a segurança dos usuários online.

Em que pese isso, o tema ainda é pouco debatido, sendo escassos os estudos sobre a matéria. Significa dizer que, apesar dos efeitos prejudiciais do *doxxing* serem cada vez mais reconhecidos, a compreensão completa de suas implicações legais, éticas e sociais permanece limitada. A falta de pesquisa e debate aprofundados sobre o assunto reflete a complexidade do fenômeno do *doxxing* e a rápida evolução das práticas digitais. Portanto, há uma clara necessidade de ampliar o escopo de estudos e discussões para abordar adequadamente o *doxxing* e desenvolver estratégias eficazes para lidar com essa forma de abuso digital.

Anote-se, ainda, que mesmo diante da escassez dos estudos, foi possível perceber que o *doxxing*, enquanto espécie do gênero abuso digital, viola a

privacidade, um direito fundamental consagrado em diversas legislações. A divulgação não autorizada de informações pessoais sensíveis, como endereço, número de telefone e dados de identificação, compromete a intimidade e a autonomia dos indivíduos, afetando sua dignidade e bem-estar emocional.

Exatamente nesse contexto é que se verificou que essa forma de violação da privacidade pode ter sérias consequências para as vítimas, incluindo o risco de assédio, perseguição e danos à reputação. Portanto, é crucial reconhecer o *doxxing* como uma ameaça à privacidade e promover esforços para prevenir e combater essa prática, garantindo assim o respeito aos direitos fundamentais dos usuários online.

Ademais, viu-se que, apesar de não ser tratada de forma específica pela legislação civil ou penal, o *doxxing* pode, sim, gerar a obrigação civil de reparar danos, desde que estejam presentes os elementos configuradores da responsabilidade civil, como a conduta ilícita, o dano e o nexo de causalidade. A exposição não autorizada de informações pessoais sensíveis pode causar danos emocionais, psicológicos e até mesmo materiais às vítimas, justificando assim a reparação civil.

De igual forma, constatou-se que, dependendo da natureza e das circunstâncias da conduta, o *doxxing* também pode levar à condenação por crimes como calúnia, injúria, extorsão, entre outros. A análise do caso concreto e a forma como a conduta se exterioriza são determinantes para a aplicação da legislação penal, respeitando os princípios da legalidade e da individualização da pena.

Destarte, conclui-se que embora não haja uma legislação específica para o *doxxing*, suas práticas podem ser sancionadas tanto no âmbito civil quanto no penal, de acordo com as normas vigentes e a interpretação dos tribunais.

Por fim, ressalta-se que é urgente e imprescindível promover debates doutrinários, jurisprudenciais e legislativos sobre o *doxxing*, dada a crescente prevalência dessa prática e seus impactos negativos na sociedade contemporânea. A falta de uma legislação específica para lidar com o *doxxing* deixa lacunas no sistema jurídico, dificultando a responsabilização eficaz dos infratores e a proteção das vítimas.

Posta assim a questão, tem-se que a ausência de diretrizes claras pode enfraquecer os mecanismos de prevenção e combate ao abuso digital, expondo os usuários a riscos cada vez maiores de violação da privacidade e danos emocionais. Portanto, é essencial promover um diálogo interdisciplinar entre juristas, acadêmicos,

legisladores e a sociedade civil para desenvolver políticas e estratégias adequadas para enfrentar o problema do *doxxing* e proteger os direitos fundamentais dos cidadãos no ambiente digital.

## REFERÊNCIAS

ABRAJI condena perfil falso e exposição de dados pessoais de Vera Magalhães em redes sociais. **Nota da ABRAJI**, 2020. Disponível em: https://abraji.org.br/noticias/abraji-condena-perfil-falso-e-exposicao-de-dados-pessoais-de-vera-magalhaes-em-redes-sociais. Acesso em: 04 mai. 2024.

ALMAGOR, Rafael Cohen *et al.* Internet Crime Enabling: Stalking and Cyberstalking. **Springer Link**, Arai, 2022. Disponível em: https://link.springer.com/chapter/10.1007/978-3-030-98015-3_57. Acesso em: 27 jul. 2024.

ALMEIDA, Jéssica de Jesus et al. Crimes Cibernéticos. **Ciências Humanas e Sociais Unit.** Aracaju, v. 2, nº 3, p. 215-236, mar. 2015.

BITTAR, Carlos Alberto. **Os direitos da personalidade.** 8. ed. São Paulo: Saraiva, 2017.

BRITO, Ronaldo Figueiredo. Direito da personalidade: pessoa e indivíduo. **Justiça e Direito,** v. 1, n. 1, p. 136-151, jan./jun. 2011.

CANCELIER, Mikhail Vieira de Lorenzi. O direito à privacidade hoje: perspectiva histórica e o cenário brasileiro. **Seqüência**: Estudos Jurídicos e Políticos, v. 38, n. 76, p. 213, 2017. Doi: http://dx.doi.org/10.5007/2177-7055.2017v38n76p213.

CASTRO, Carla Rodrigues Araújo de. **Crimes de Informática e seus Aspectos Processuais.** Rio de Janeiro, Lúmen Júris, 2014.

CHEN, Qiqi et al. Doxing Victimization and Emotional Problems among Secondary School Students in Hong Kong**. International Journal of Environmental Research and Public Health**, v. 15, n. 12, p. 2665, 2018.

DOUGLAS, David. Doxing: a conceptual analysis, **"Ethics and Information Technology"**, v. 18, n. 3, p. 199-210, p. 2016.

FLUMIGNAN, Wévertton. Análise da responsabilidade civil no âmbito do Marco Civil da Internet e da Lei Geral de Proteção de Dados. *In:* **Migalhas**, 2021. Disponível em: https://www.migalhas.com.br/coluna/migalhas-de-protecao-de-dados/343301/responsabilidade-civil-no-ambito-do-marco-civil-da-internet-e-da-lgpd. Acesso em: 14 jul. 2024.

GAGLIANO, Pablo Stolze *et al*. **Novo curso de direito civil**: responsabilidade civil, v. 3. 19. ed. São Paulo: Saraiva Jur, 2020.

GIACCHETTA, André Zonaro et al. Marco Civil da Internet põe fim a lacunas na legislação. **Revista Consultor Jurídico**, abr. 2014. Disponível em: https://www.conjur.com.br/2014-abr-30/marco-civil-internet-poe-fim-lacunas-existentes-legislacao/. Acesso em: 20 abr. 2024.

GONÇALVES, Carlos Roberto. **Direito civil brasileiro**: responsabilidade civil. 13. ed. São Paulo: Saraiva, 2018.

KHANNA, Parul et al. Experimental Analysis of Tools Used for Doxing and Proposed New Transforms to Help Organizations Protect against Doxing Attacks. **Procedia Computer Science**, v. 94, p. 459-464, 2016. Disponível em: http://www.sciencedirect.com/science/article/pii/S1877050916311505. Acesso em: 28 jul. 2024.

LEONARDI, Marcel. **Tutela e Privacidade na Internet.** São Paulo: Saraiva, 2012.

LIMA, Cíntia Rosa Pereira de *et al.* **Estudos avançados de Direito Digital.** Rio de Janeiro: Editora Elsevier, 2014.

MAJOR, John B. **Cyberstalking**, Twitter, and the Captive Audience: A First Amendment Analysis of 18 U.S.C. § 2261A(2). California: Southern California Law Review, 2012.

MACALLISTER, Julia M. The Doxing Dilemma: Seeking a Remedy for the Malicious Publication of Personal Information. *In***: Fordham University School of Law,** v. 85, 2451, 2017.

MENDES, Laura Schertel *et al.* Reflexões iniciais sobre a nova Lei Geral de Proteção de Dados. **Revista de Direito do Consumidor**. v. 120. A. 27. p. 469-483, 2018.

MENEZES, Renata Oliveira Almeida *et al.* Cyberbullying por divulgação de dados pessoais. **Revista da Faculdade de Direito da Universidade de Lisboa,** v. 63, p. 815-838, 2022. Disponível em: https://repositorio.ul.pt/bitstream/10451/62136/1/Renata-Oliveira-Almeida-Menezes-Lui%CC%81s-Eduardo-e-Silva-Lessa-Ferreira.pdf. Acesso em: 06 abr. 2024.

POLLARD, Nicolle Parsons *et al.* **Controversies in Victimology.** New York: Routledge, 2008.

MOTA, Bárbara Maria Farias et al. Hacking político: crime cibernético ou manifestação legal de protesto? ***Argumentum***, v. 8, n. 3, p. 122-132, 2016. Disponível em: https://periodicos.ufes.br/argumentum/article/view/13396. Acesso em: 11 maio 2024.

NAPOLITANO, Carlo José et al. O Supremo Tribunal Federal e o discurso de ódio nas redes sociais: exercício de direito versus limites à liberdade de expressão. **Revista Brasileira de Políticas Públicas,** v. 7, n. 3, p. 313-332, 2018.

RAMOS**,** Daniela Osvald. Origens da misoginia online e a violência digital direcionada a jornalistas mulheres. **RuMoRes**, v. 16, n. 32, p. 39-57, 2022. Disponível em: https://repositorio.usp.br/item/003113494. Acesso em: 13 abr. 2024.

REBS, Rebeca Recuero et al. Haters e o discurso de ódio: entendendo a violência em sites de redes sociais. **Diálogo das Letras**, v. 6, n. 02, p. 24–44, 2017. Disponível em: https://periodicos.apps.uern.br/index.php/DDL/article/view/1014. Acesso em: 26 mai. 2024.

SÃO PAULO. Tribunal de Justiça do Estado de São Paulo. **Apelação Cível nº 2021. 0000097671,** Relator Inah de Lemos e Silva Machado, 6ª Câmara de Direito Privado, julg. 16 fev. 2021. Disponível em: https://esaj.tjsp.jus.br/cjsg/resultadoCompleta.do;jsessionid=E26888D7B1C89F6171985A9BD2B0D710.cjsg2. Acesso em: 28 mai. 2024.

SCHREIBER, Anderson. **Direitos da personalidade**. 3. ed. São Paulo: Atlas, 2014.

SHERIDAN, Max**.** Doxxing Statistics in 2024: 11 Million Americans Have Been Victimized. *In*: **SafeHome.org**, 2024. Disponível em: https://www.safehome.org/family-safety/doxxing-online-harassment-research/. Acesso em: 28 jul. 2024.

SILVA, José Afonso da. **Curso de direito constitucional positivo**. 45. ed. São Paulo: Malheiros, 2024.

SILVA, Simone de Assis Alves et al. Herança da informação digital e direito ao esquecimento em redes sociais on-line: uma revisão sistemática de literatura. **Em Questão**, v. 26, n. 1, p. 357-401, 2020.

SNYDER, Peter *et al*. Fifteen Minutes of Unwanted Fame: Detecting and Characterizing Doxing. *In*: **Proceedings of IMC '17**, London, United Kingdom. New York: ACM, 2017.

URIAS, Rodrigo. Responsabilidade Civil e o Marco Civil da Internet (Lei n.º 12.965 de 2014). *In*: **JusBrasil**, 2020. Disponível em: https://www.jusbrasil.com.br/artigos/responsabilidade-civil-e-o-marco-civil-da-internet-lei-n-12965-de-2014/1134307738. Acesso em: 20 jul. 2024.

VENOSA, Silvio de Salvo. **Direito civil**: obrigações e responsabilidade civil, v. 2. 19. ed. Rio de Janeiro: Atlas, 2019.

WERMUTH, Maiquel Angelo Dezordi et al. Staking e Cyberstalking: considerações críticas sobre o delito tipificado no art. 147-A do Código Penal brasileiro. **Revista Brasileira de Ciências Criminais**, v. 186, n. 2021, p. 105-126, 2021.