REVISTA DIREITO MACKENZIE

ISSN 2317-2622 | RDM | Revista Direito Mackenzie | São Paulo | SP | 18(3) | e17058 | 2024
http://dx.doi.org/10.5935/2317-2622/direitomackenzie.v18n317058

DOXING COMO FERRAMENTA PARA A PRÁTICA DE ILÍCITOS E REGULAÇÃO

RECEBIDO EM:	5.5.2024
APROVADO EM:	13.11.2024

Mateus de Oliveira Fornasier

https://orcid.org/0000-0002-1617-4270
Universidade Regional do Noroeste do Estado do Rio Grande do Sul
Ijuí, RS, Brasil
E-mail: mateus.fornasier@gmail.com

Fernanda Viero da Silva

https://orcid.org/0000-0002-3978-7395
Universidade Regional do Noroeste do Estado do Rio Grande do Sul
Ijuí, RS, Brasil
E-mail: fefeviero@gmail.com

Benhur Aurélio Formentini Nunes

https://orcid.org/0000-0002-3572-7504
Universidade Regional do Noroeste do Estado do Rio Grande do Sul
Ijuí, RS, Brasil
E-mail: benhur41@hotmail.com

Para citar este artigo: FORNASIER, M. O.; SILVA, F., V.; NUNES, B. A. F. *Doxing* como ferramenta para a prática de ilícitos e regulação. *Revista Direito Mackenzie*, São Paulo, SP, v. 18, n. 3, e17058, 2024. http://dx.doi.org/10.5935/2317-2622/direitomackenzie.v18n317058.

REVISTA DIREITO MACKENZIE
RDM | São Paulo | SP | 18(3) | e17058
2024 | v. 18 | n. 3 | p. 1-27 | ISSN 2317-2622. http://dx.doi.org/10.5935/2317-2622/direitomackenzie.v18n317058

· MATEUS DE OLIVEIRA FORNASIER
· FERNANDA VIERO DA SILVA
· BENHUR AURÉLIO FORMENTINI NUNES

RESUMO: A presente pesquisa tem por objetivo investigar a prática de *doxing* e identificar os conflitos e ilicitudes daí oriundas sob o contexto do tratamento de dados pessoais, considerando demais direitos fundamentais, pilares democráticos, que permeiam a atividade de *doxing*, bem como analisar a regulação vigente desta matéria nacional e globalmente. Para tanto, partimos dos seguintes problemas de pesquisa: poderia o *doxing* ser uma ferramenta para prática de ilícitos no contexto digital, de quais formas e como as principais legislações globais legislam acerca deste fenômeno? Como hipótese preliminar, temos que o *doxing* pode ser utilizado como ferramenta ou meio para a perpetração de diversos crimes cibernéticos, desde crimes como extorsão, perseguição, assédio e ameaças, até crimes que resultam em danos físicos reais, como ataques, linchamentos e ciberterrorismo, bem como diversos outros propósitos maliciosos. Ainda, preliminarmente, entende-se que o *doxing* não é necessariamente criminalizado como uma prática única, mas várias ações envolvidas em sua execução podem ser alvo de sanções legais que necessariamente estão profundamente ligadas ao contexto social em que essas leis são aplicadas. Os objetivos específicos são dois, quais sejam: a) analisar de quais maneiras o *doxing* pode ser utilizado para prática de ilícitos; e, b) compreender de qual forma as principais legislações globais tem enfrentado essa temática. Ao final, confirma-se a hipótese preliminar elencada. Aplicou-se no presente trabalho a metodologia hipotético-dedutiva, com método de abordagem qualitativo e abordagem bibliográfica.

PALAVRAS-CHAVE: *Doxing*; proteção de dados; regulação.

DOXING AS A TOOL FOR ILLEGAL PRACTICES AND REGULATION

ABSTRACT: The present research aims to investigate the practice of doxing and identify the conflicts and illegalities arising therefrom in the context of the processing of personal data, considering other fundamental rights, democratic pillars, which allow the activity of doxing, as well as analyzing the current regulation of this matter at national and global level. To do so, we start from the following research problems: could doxing be a tool for committing illegal acts in the digital context, in what ways and how do the main global laws regulate this influence? As preliminary hypotheses, we have that doxing can be used as a

tool or means for the perpetration of various cybercrimes, from crimes such as extortion, stalking, harassment and threats, to crimes that result in real physical harm, such as attacks, lynchings and cyberterrorism, as well as as well as several other malicious purposes. Even so, it is preliminarily understood that doxing is not necessarily criminalized as a single practice, but several actions involved in its execution can be the target of legal sanctions that are necessarily deeply linked to the social context in which these laws are applied. The specific objectives are two, which are: a) to analyze how doxing can be used to commit illegal acts; and, b) understand how the main global legislations that have addressed this issue. It ends by confirming the preliminary hypothesis listed. Methodology: hypothetical-deductive, with a qualitative approach and bibliographical approach.

KEYWORDS: Data protection; doxing; regulation.

1. Introdução

A presente pesquisa busca compreender o fenômeno do *doxing*, que é "a divulgação pública intencional na Internet de informações pessoais sobre um indivíduo por terceiros" (Douglas, 2016, p. 199), no contexto do direito humano e fundamental à proteção de dados. Leva-se em consideração que esse fenômeno pode se originar de meios legítimos ou ilegítimos, por pessoas ou organizações, contra pessoas determinadas ou organizações públicas ou privadas, com intuitos diversos, também legítimos ou ilegítimos, por interesse de particulares ou organizações governamentais. A prática do *doxing* origina-se nas relações privadas entre usuários de internet, que por motivos diversos buscavam compilar dossiês, ou seja, reunir informações contidas na rede uns dos outros para utilizá-las para quaisquer motivos. Desde os meios e motivos mais nefastos, até a simples confirmação de reputação de certa pessoa ou organização, o *doxing* se constitui, em última análise, de uma ferramenta utilizada por indivíduos e grupos para obter certos tipos de informações úteis para os fins a que se destinam.

Dessa forma, este trabalho tem como objetivo investigar a prática de *doxing* e identificar os conflitos e ilicitudes daí oriundas sob o contexto do tratamento de dados pessoais, considerando demais direitos fundamentais, pilares democráticos, que permeiam a atividade de *doxing*, bem como analisar a regulação vigente desta matéria nacional e globalmente.

REVISTA DIREITO MACKENZIE
RDM | São Paulo | SP | 18(3) | e17058
2024 | v. 18 | n. 3 | p. 1-27 | ISSN 2317-2622. http://dx.doi.org/10.5935/2317-2622/direitomackenzie.v18n317058

Partimos da compreensão de que a proteção aos dados pessoais é direito humano fundamental que se solidifica à medida que a sociedade enfrenta uma nova realidade, em que não há mais como separar o mundo virtual e o mundo real, considerando que há uma dependência cada vez maior das ferramentas digitais para a vida cotidiana. Essa realidade, por sua vez, traz à tona confrontos entre novas formas de exercício das liberdades individuais, em que o acesso à informação e as possibilidades de expressar-se livremente em ambientes que estimulam a interação entre pessoas crescem e se multiplicam. Isso significa dizer que a internet é ambiente que permite o fluxo cada vez mais livre de informação. O problema, entretanto, é que o caminho percorrido neste novo mundo deixa um rastro de fragmentos de informação sobre cada indivíduo, que pode ser exibido instantaneamente através de uma busca no Google (Solove, 2007).

Assim, partimos do seguinte problema de pesquisa: Poderia o *doxing* ser uma ferramenta para prática de ilícitos no contexto digital? De quais formas e como as principais legislações globais legislam acerca deste fenômeno? Como hipótese preliminar temos que o *doxing* pode ser utilizado como ferramenta ou meio para a perpetração de diversos crimes cibernéticos, desde crimes como extorsão, perseguição, assédio e ameaças, até crimes que resultam em danos físicos reais, como ataques, linchamentos e ciberterrorismo, bem como diversos outros propósitos maliciosos. Preliminarmente entende-se que o *doxing* não é necessariamente criminalizado como uma prática única, mas várias ações envolvidas em sua execução podem ser alvo de sanções legais que estão profundamente ligadas ao contexto social em que essas leis são aplicadas.

Com isso, a pesquisa se dividirá em dois momentos, sob forma de objetivos específicos: inicialmente o *doxing* será explorado enquanto ferramenta para prática de outros ilícitos, ou seja, definirá em que circunstâncias a prática pode ser utilizada para cometer atos criminosos. Conforme se verificará, o *doxing* pode não ser um crime em si, mas há circunstâncias em que isso se verifica e aí o trabalho vai enfrentar os desafios de regulação da prática em diversos países, que possuem abordagens variadas em seus sistemas legais. Na sequência, abordaremos questões atinentes a sua regulação, ou seja, iremos investigar legislações que visem a limitar, proibir ou regular essa prática no cenário brasileiro, norte-americano, europeu e asiático.

Por fim, para a realização desta pesquisa o estudo mescla procedimentos monográficos, históricos e comparativos, a fim de fornecer uma pesquisa satisfatoriamente completa em torno do tema, ao mesmo tempo que delimitada e específica. Para tanto,

o trabalho utilizou a técnica de pesquisa bibliográfica, investigando fontes mediatas e imediatas. A metodologia empregada é a hipotético-dedutiva.

2. *Doxing* como ferramenta para praticar outros ilícitos e como forma direta de violação de direitos

Douglas (2016) apresentou um dos principais estudos conceituais sobre o assunto, descrevendo *doxing* como a divulgação intencional na internet de informações pessoais sobre um indivíduo, realizada por terceiros. O termo tem suas raízes nas expressões *dropping documents* ou *dropping dox*, que significam basicamente divulgar documentos. Oriundo da cultura *hacker* dos anos 1990, o *doxing* envolve revelar a identidade de pessoas que operam anonimamente, através da publicação na internet de informações privadas, proprietárias ou de identificação pessoal sem o consentimento da parte envolvida e geralmente com intenções maliciosas (Anderson; Wood, 2021; Douglas, 2016; Snyder *et al.*, 2017).

O *doxing* é considerado um processo de comunicação complexo, no qual uma ou várias pessoas buscam informações privadas ou pessoais sobre outro indivíduo e as divulgam de forma ampla em canais de mídia *on-line* sem o consentimento dessa pessoa, tornando-a, portanto, vulnerável pela exposição nos meios de comunicação de massa (Eckert; Metzger-Riftkin, 2020).

A complexidade do fenômeno, conforme Anguita (2021), pode ser compreendida pela necessidade de utilizar inteligência, criatividade e habilidades para buscar informações de terceiros armazenadas em vários locais da internet. Os dados podem ser de acesso público, mas apresentados de forma complicada ou incompreensível para o público em geral e, além disso, podem resultar de violações de segurança ou mesmo serem fornecidos pelo próprio alvo, mesmo que este não tenha consciência de que esteja compartilhando-os com terceiros.

Embora o *doxing* possa ser estudado como conduta, não necessariamente o mesmo deve ser entendido como um fim em si, conforme já exposto. Tais atos podem levar à roubo de identidade, perseguição, chantagem, assédio e danos físicos, bem como sofrimento psicológico (Tan, 2022). Há também uma série de outros delitos que podem ser cometidos a partir do *doxing* que se encaixam na definição de cibercrime, crime informático ou crime cibernético. A peculiaridade dessa modalidade reside no fato de que

REVISTA DIREITO MACKENZIE
RDM | São Paulo | SP | 18(3) | e17058
2024 | v. 18 | n. 3 | p. 1-27 | ISSN 2317-2622. http://dx.doi.org/10.5935/2317-2622/direitomackenzie.v18n317058

são crimes cometidos usando dispositivos computadorizados, dados e redes, incluindo a internet (Klymenko; Gutsalyuk; Savchenko, 2020).

Existem cibercrimes baseados no dispositivo informático como ferramenta, como pornografia infantil, fraude, lavagem de dinheiro e perseguição (*stalking*), enquanto outros são focados e totalmente dependentes do dispositivo, como *hacking*, *phishing* e desfiguração de sites (Al-Khater *et al.*, 2020). Crimes que usam computadores como ferramenta são apenas variantes de crimes já existentes, enquanto outros só podem existir por causa do uso da informática (Yar; Steinmetz, 2019).

Conforme asseveram Yar e Steinmetz (2019), o estudo dos cibercrimes se coloca no contexto de uma nova construção social internacional, em que o ambiente virtual é marcado sobre a queda das barreiras de espaço e de tempo, comunicação muitos-para-muitos e também um certo nível de possibilidade de permanecer anônimo, que levam a um cenário no qual se pode cometer novos tipos de crimes desapegados do mundo terrestre físico.

Al-Khater *et al.* (2020) trazem, ainda, uma extensa divisão de tipos de cibercrimes, notadamente: (1) ciberterrorismo - ação ilegal que envolve violência contra pessoas e propriedades. Muitas vezes tem propósito político e racial ou ideológico; (2) guerra cibernética – um tipo de guerra que não utiliza armas, mas sim ataques cibernéticos. Pode ser realizado por organizações ou grupos de *hackers* sem permissão do governo; (3) espionagem cibernética – refere-se a qualquer ação que envolva espiões e roubo de informações importantes e sensíveis em benefício de empresas rivais ou governos estrangeiros, mediante uso de ferramentas tecnológicas; (4) pornografia infantil – pode referir-se a proliferação e armazenamento de fotos, vídeos e gravações de áudio de crianças em contextos sexuais; e (5) *ciberbullying* – que, neste contexto, significa todo tipo de ataque que inflige dano emocional e mental, afetando a personalidade da pessoa, incluindo o recebimento de mensagens com sugestão de violência, assédio, ameaça ou manipulação psicológica (Al-Khater *et al.*, 2020).

Além desses, há ainda formas sofisticadas de crimes como *phishing*, *SQL injection* e ataque DoS ou DDoS; este último serve para comprometer a disponibilidade de sistemas através da geração artificial de múltiplos acessos simultâneos (Al-Khater *et al.*, 2020).

Independentemente da divisão ou classificação que se faça para o estudo do tema, é necessário apenas compreender que existe uma gama de crimes que podem ser cometidos aliados ao uso do *doxing*. Como os motivos para o *doxing* são diversos, partindo desde questões políticas e ideológicas, passando por vingança, ódio ou o simples desejo

de prejudicar alguém (Tan, 2022), muitos dos crimes citados acima podem ser cometidos através do acesso e da divulgação de dados pessoais.

Quando se fala em formas de violência cibernética, conforme refere Yar (2019), também podem ser identificadas práticas de *doxing* para perpetrar esse tipo de crime. Por exemplo: um chantagista só vai divulgar a informação se a vítima não concordar com as suas exigências, ou seja, *doxing* pode servir como ferramenta de chantagem. Nesse exemplo, os dados em posse do chantagista podem ter sido conseguidos por meio de *phishing*, que é uma forma de cibercrime na qual os criminosos utilizam-se de técnicas para enganar usuários e conseguir acesso aos dados, muitas vezes através da própria confiança da vítima, como e-mails fraudulentos. Essa é uma presunção válida, tendo em vista que a vasta maioria dos ataques que violam segurança de dados inicia com esta prática (Varshney *et al.*, 2024).

A partir do vazamento de dados pessoais de determinado indivíduo através de *doxing*, este pode ser vítima, ainda, de crimes de ódio, que são crimes cometidos por motivos de repulsa contra determinado grupo, em razão de gênero, orientação sexual, etnia, nacionalidade, religião, dentre outros fatores (Frós, 2022). Ou seja, contravenções diferentes dos considerados crimes "normais", tendo em vista a presença de um viés ideológico com relação à vítima, uma motivação diretamente relacionada com a identidade da vítima (Canini, 2020).

Em 2023, um jornalista brasileiro, William de Lucca, teve seus dados vazados em grupos do aplicativo Telegram, incluindo CPF e local de residência. O motivo do vazamento teria sido um conflito do jornalista, identificado com uma pauta LGBTQIA+, com grupos de extrema-direita após uma piada sobre prisão de apoiadores do ex-presidente Jair Bolsonaro (Teixeira, 2023).

A dinâmica parece também funcionar de forma contrária: grupos que disseminam discursos de ódio podem usar *doxing* para intimidar quem os enfrenta ou sanciona. Em 2018, uma juíza do Rio de Janeiro teve seus dados pessoais publicados na internet após determinar que um site denominado "Rio de Nojeira" fosse retirado do ar após denúncias de veiculação de mensagens de ódio e racismo (Conjur, 2018).

Percebe-se que essas práticas resultam em efeitos na reputação, na posição social, no bem-estar familiar e econômico, na perda de um emprego ou relacionamento (Tan, 2022), podendo levar até mesmo ao suicídio (Murphy, 2012; Hancocks, 2012).

Recentemente, o Legislativo brasileiro aprovou uma série de alterações legais que criminalizam o *cyberbullying*, alterando dispositivos do Código Penal, do Estatuto da

REVISTA DIREITO MACKENZIE
RDM | São Paulo | SP | 18(3) | e17058
2024 | v. 18 | n. 3 | p. 1-27 | ISSN 2317-2622. http://dx.doi.org/10.5935/2317-2622/direitomackenzie.v18n317058

Criança e do Adolescente e da Lei de Crimes Hediondos, resultando na Lei nº 14.811, de 12 de janeiro de 2024 (Brasil, 2024). O texto aprovado traz dois novos tipos penais, chamados de "intimidação sistemática" e "intimidação sistemática virtual".

A "intimidação sistemática virtual" é compatível com a classificação proposta por Al-Khater *et al.* (2020), no entanto se distancia da categorização do crime de ódio, tendo em vista a ausência de motivação na previsão legal (Brasil, 2024). Crimes de ódio, inclusive, não possuem regulação legal direcionada no Brasil (Caye, 2022), mas a própria Constituição Federal estabelece, em seus objetivos, a punição contra discriminações de raça, sexo, cor; ou quaisquer outros e crimes desta natureza são previstos na Lei Federal nº 7.716, de 5 de janeiro de 1989, que diz que "[...] serão punidos [...] crimes resultantes de discriminação de raça, cor, etnia, religião ou procedência nacional (Brasil, 1989).

Para fechamento do ponto, em tom conclusivo e já preparando a sequência do estudo, imagine a seguinte situação: uma pessoa está em processo de seleção para ser contratada por uma empresa. O chefe dessa empresa determina a seus funcionários que pesquisem a vida do candidato. Na pesquisa em redes sociais, descobrem que o candidato emitiu opiniões impopulares acerca de determinado tema, em postagem feita há alguns meses e ainda disponível na rede. Sabendo dessa informação, o chefe, que discorda da opinião do candidato, resolve não contratá-lo. Tem-se, aí, uma prática no contexto privado, e, em primeira análise, seria aceitável que determinado particular não aceite dar emprego a outro particular com o qual discorda em um assunto polêmico.

Nesse mesmo exemplo, um funcionário da empresa que possui *expertise* em informática consegue, por meio de *hacking* ou *phishing*, acessar o e-mail do candidato e encontra na caixa de entrada uma série de e-mails contendo mensagens privadas nas quais ele revela a prática de um crime horrendo. Além de comunicar ao chefe, que decide não contratar o candidato, o funcionário decide expor a identidade do cidadão na internet, denunciando o crime reprovável e jogando-o ao conhecimento público, para que não fique impune. A pessoa, então, sofre uma série de ataques de ódio nas redes sociais e acaba se suicidando.

Nasce, então, no simples exemplo, a grande controvérsia: esse funcionário adentrou ao meio de comunicação privado do candidato por meio de uma violação de sua privacidade e agora resolveu expor a identidade da pessoa na internet por meio de divulgação de um dossiê contendo informações privadas. Independentemente da natureza odiosa do crime praticado, tem-se, nesse segundo exemplo, a prática do *doxing* por

meio de violação de uma série de direitos que culminou em lesão irreversível à vida da vítima, e este é o embate que será explorado adiante.

Primeiro, deve ser explorada a possibilidade de responsabilização criminal do agente que pratica *doxing*, através das regulações em matéria penal para a prática em diversos países. Em seguida, a face social e política será devidamente confrontada, visando a enquadrar circunstâncias em que o *doxing* não é puramente ferramenta para cometer ilícito, tampouco ilícito em si, mas pensada a partir de uma perspectiva de ferramenta social.

A principal ideia a ser desenvolvida neste ponto é o *doxing* como violação de direitos e uma forma de violência perpetrada no ambiente *on-line*. Desse modo, na sequência iremos investigar legislações que visem a limitar, proibir ou regular essa prática. Ao longo desta pesquisa, foram considerados de maneira marcante três contextos legais e jurisprudenciais, que são o caso brasileiro, europeu e norte-americano. Portanto, esses serão os paradigmas utilizados na análise a seguir, além de uma especial investigação sobre legislações de países asiáticos que demonstram proeminência na regulação do *doxing*.

2. *Doxing* e regulação

A prática do *doxing* envolve, conforme visto anteriormente, os atos de obter e divulgar os dados. A obtenção pode se dar de forma legal, através de dados já disponíveis na internet, ou ilegal, através de violações de segurança. Já a divulgação precisa ter certos objetivos ou, pelo menos, potencial lesivo à pessoa que tem seus dados expostos. Esses serão os principais requisitos analisados a partir de agora, em diferentes contextos.

Inicialmente temos que não há legislação brasileira específica que criminalize a conduta de *doxing* e, por esse motivo, é necessário desmembrar os momentos de obtenção e divulgação para averiguar as possibilidades de violações e responsabilidades. Embora o diploma que trate por excelência do tema proteção de dados pessoais no Brasil seja a LGPD, o Código Penal é o primeiro refúgio para a exploração do *doxing* no sistema legal brasileiro, trazendo a previsão do crime de "divulgação de segredo".

Em seu artigo 153, enuncia que divulgar alguém, sem justa causa, conteúdo de documento particular ou de correspondência confidencial, de que é destinatário ou detentor, e cuja divulgação possa produzir dano a outrem gera pena de detenção de um a seis meses. Ainda, dispõe que divulgar, sem justa causa, informações sigilosas ou reservadas, assim definidas em lei, contidas ou não nos sistemas de informações ou banco

REVISTA DIREITO MACKENZIE
RDM | São Paulo | SP | 18(3) | e17058
2024 | v. 18 | n. 3 | p. 1-27 | ISSN 2317-2622. http://dx.doi.org/10.5935/2317-2622/direitomackenzie.v18n317058

de dados da Administração Pública, além de ensejar pena de detenção de um a quatro anos (mais multa), se resultar prejuízo para a Administração Pública, a ação penal será incondicionada (Brasil, 1940).

Na sequência , o mesmo diploma traz em seu artigo 154-A o tipo "violação de dispositivo informático". A principal implicação lógica do texto desses dispositivos é que eles pressupõem que exista uma violação de sistema que, de alguma forma, armazena ou transmite dados, tendo em vista que a informação deve ser particular ou confidencial. Com isso, temos que *in verbis*

> [...] invadir dispositivo informático de uso alheio, conectado ou não à rede de computadores, com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do usuário do dispositivo ou de instalar vulnerabilidades para obter vantagem ilícita (Brasil, 1940),

além de ensejar pena de reclusão, aumenta-se a pena de um terço a dois terços se da invasão resulta prejuízo econômico.

Destaca-se também que há previsão de aumento de pena se o crime foi praticado contra o presidente da República, governadores, prefeitos, presidentes do Supremo Tribunal Federal, Câmara de Deputados, Senado Federal e outros entes federativos. É marcante que o objeto da conduta prevista no artigo 154-A (Brasil, 1940) é o dispositivo informático, seja qual for, conectado ou não à internet. O propósito do agente desse tipo penal deve ser obter vantagem ilícita (Nucci, 2023), o que contemplaria, em tese, apenas parte da conduta do *doxing*, necessitando a combinação do tipo com o artigo 153 (Brasil, 1940), que trata da divulgação de um segredo. Percebe-se que há, nesses dispositivos, claro direcionamento para proteção do bem jurídico dos dados pessoais, em conexão com o direito à privacidade e liberdade individual (Greco, 2022), todos previstos na Constituição Federal (Brasil, 1988), conforme já explorado.

As previsões constantes no artigo 154-A do Código Penal Brasileiro são fruto de um marco legal na tipificação de crimes informáticos, que é a Lei Federal nº 12.737, de 30 de novembro de 2012, conhecida como Lei Carolina Dieckmann (Brasil, 2012). Em 2011, a atriz brasileira Carolina Dieckmann teve seu computador invadido e diversas fotos íntimas foram divulgadas em redes sociais após a atriz não ceder à extorsão praticada pelos criminosos, o que gerou uma resposta legislativa concretizada pela rápida aprovação da nova legislação em 2012.

Em 2017, uma série de personalidades públicas envolvidas na política tiveram dados compilados e postados no site Ghostbin: Luis Inácio Lula da Silva e Dilma Roussef, o então presidente Michel Temer, ministros, deputados e até mesmo o *youtuber* Felipe Neto. As informações envolviam: nome completo, data de nascimento, endereços de residência e trabalho, número de CPF, números telefônicos, valores de bens declarados ao governo, renda presumida, nomes completos de familiares, participações societárias, *score* do Serasa etc. (G1, 2020).

Já em 2020, uma prática semelhante atingiu o então presidente Jair Bolsonaro, seus filhos e ministros de Estado. A maioria das informações divulgadas em forma de compilado eram públicas, mas também houve divulgação de números de telefone pessoais, contas de e-mail e endereços (G1, 2020). Considerando essa forma de tratamento legal e que o *doxing* pode ser entendido não como uma prática ilegal em si, conclui-se que só podem ser criminalmente puníveis, no Brasil, os efeitos ou os meios (ilegais) de obtenção dos dados, isoladamente, e não a prática do *doxing*.

Doxing como conduta e fenômeno individual é virtualmente inexistente para a Justiça brasileira, tendo em vista que, até o momento em que este texto é redigido, não existem registros do termo "*doxing*" ou "*doxxing*" nas pesquisas públicas de jurisprudências dos sites do Supremo Tribunal Federal, do Superior Tribunal de Justiça, Justiça Federal, tampouco nas Justiças Estaduais de São Paulo e do Rio Grande do Sul.

Embora não tenha trazido disposições especificamente penais, a LGPD (Brasil, 2018) trouxe uma série de responsabilidades, direitos e deveres com poder regulatório que podem causar reflexos e implicações criminais, além das administrativas e cíveis. Alguns países serão tomados como referência para o presente estudo, com vistas a desenvolver os conceitos até aqui apresentados. Da mesma forma que o Brasil, a Europa possui uma legislação destinada à proteção de dados por excelência, o RGPD. Porém, alguns países possuem peculiaridades nas suas legislações locais penais que merecem ser abordadas para a boa compreensão do tema.

De forma muito parecida com o caso brasileiro, a Espanha regula os atos de descoberta e revelação de informações secretas em seu Código Penal. A semelhança não é surpresa, tendo em vista que os sistemas jurídicos dos dois países pertencem à família do sistema romano-germânico e se situam em um chamado círculo dogmático e doutrinário que compreende ainda Itália, Portugal e América Latina como um todo, sob influência do direito penal alemão (Oliveira, 2020).

REVISTA DIREITO MACKENZIE
RDM | São Paulo | SP | 18(3) | e17058
2024 | v. 18 | n. 3 | p. 1-27 | ISSN 2317-2622. http://dx.doi.org/10.5935/2317-2622/direitomackenzie.v18n317058

Assim, as previsões do texto espanhol na forma do artigo 197 são no seguinte sentido:

> [...] quem, para descobrir segredos ou violar a privacidade de outrem, sem o seu consentimento, apreende os seus papéis, cartas, e-mails ou quaisquer outros documentos ou objetos pessoais, intercepta as suas telecomunicações ou utiliza dispositivos técnicos de escuta, transmissão, gravação ou reproduzir som ou imagem, ou qualquer outro sinal de comunicação, será punido com pena de prisão de um a quatro anos e multa de doze a vinte e quatro meses (Espanha, 1995, tradução nossa).
>
> As punições serão aplicadas da mesma forma a qualquer pessoa que, sem autorização, capture, utilize ou altere para prejudicar terceiros, dados privados, pessoais ou familiares de outras pessoas, contidos em arquivos ou suportes informáticos, eletrônicos ou telemáticos, ou em qualquer outro tipo de registro público ou privado (Espanha, 1995, tradução nossa).

Ainda, aquele que, sem consentimento da pessoa afetada, compartilhar, divulgar ou transferir a terceiros imagens ou gravações audiovisuais da pessoa (mesmo que originalmente obtidas com a autorização dela) será sujeito a uma pena de prisão de três meses a um ano ou a uma multa de seis a doze meses. Isso se aplica tanto quando a divulgação ocorre em domicílio ou em qualquer outro local fora do alcance de terceiros, e quando a exposição prejudicar gravemente a privacidade pessoal da pessoa retratada (Espanha, 1995).

As formas previstas na legislação espanhola, portanto, guardam estreita relação com a legislação brasileira ao definirem punições para os atos que envolvem a prática do *doxing*, de forma isolada, porém sem assertividade na abordagem específica do fenômeno. A disposição do anexo 7 do artigo 197 é mais direcionada à proteção da privacidade ao incriminar a divulgação de imagens e gravações audiovisuais no contexto íntimo, o que tem sido alvo de críticas da doutrina espanhola, eis que se a troca de mensagens foi consensual, ou seja, se os dados foram transferidos de maneira voluntária, se criaria um dever jurídico de sigilo injusto. Por outro lado, outros autores consideram que consentir com a realização de uma gravação para uso privado de duas pessoas não é o mesmo que consentir com a sua divulgação, deixando o consentimento abranger um aspecto importante da privacidade (Ibarra, 2019).

Curiosamente, a atual redação do texto espanhol também foi modificada com a inclusão do anexo 7 após um escândalo envolvendo uma celebridade local. Nesse caso,

Olvido Hormigos enviou um vídeo sexual explícito gravado por ela própria a um terceiro que divulgou a terceiros sem o seu consentimento (Barrio, 2019). O caso acabou indo à Justiça e restou arquivado, uma vez que a conduta não estava prevista no Código Penal em 2012, época dos fatos, pois exigia a necessidade de que o material fosse obtido de forma ilícita para que se considerasse um crime contra a privacidade (Barrul Fuentes, 2020).

De qualquer forma, são previsões demasiadamente genéricas que não enfrentam de forma satisfatória a prática do *doxing* em si, senão seus efeitos e alguns de seus meios (ou meios de obtenção dos dados), conectando-se mais com outros tipos de crimes cibernéticos, uma vez que se distanciam das categorizações de Douglas (desanonimização, *targeting*, deslegitimização) e de MacAllister (intenção maliciosa, fim político, desmascarar membro anônimo).

A Holanda aprovou, em 2023, legislação que trata da matéria de forma específica. A principal falha legislativa corrigida foi no sentido de que, embora muitas formas de intimidação já fossem ilegais no país, as tentativas de punição de *doxing* frequentemente esbarravam na ausência de ameaça específica do autor da conduta (Reuters, 2023). A inovação legislativa foi motivada pelo crescimento da prática contra agentes de polícia, políticos e cientistas no país (Reuters, 2023), mas principalmente contra jornalistas mulheres que relataram sofrer diversos tipos de abuso e ameaças *on-line*. Assim está formulado o novo diploma legal, em vigor desde janeiro de 2024 *in verbis:*

> Artigo 285d
>
> 1. Qualquer pessoa que obtenha dados pessoais de outra pessoa ou de terceiro, distribua esses dados ou os disponibilize de outra forma com a intenção de assustar ou causar medo a essa outra pessoa, causar sérios incômodos ou fazer com que lhe sejam causados ou gravemente impedir ou permitir ser gravemente prejudicado no exercício do seu cargo ou profissão, será punido com pena de prisão não superior a dois anos ou com pena de multa da quarta categoria.
>
> 2. Se o crime descrito no primeiro parágrafo for cometido contra pessoa na qualidade de Ministro, Secretário de Estado, Comissário do Rei, deputado, presidente da Câmara, vereador, membro de órgão de representação geral, funcionário judicial, advogado, jornalista ou publicitário no contexto da recolha de notícias, do agente policial ou do agente especial de investigação, a pena de prisão imposta pelo crime será aumentada em um terço (Holanda, 2023, tradução nossa).

REVISTA DIREITO MACKENZIE
RDM | São Paulo | SP | 18(3) | e17058
2024 | v. 18 | n. 3 | p. 1-27 | ISSN 2317-2622. http://dx.doi.org/10.5935/2317-2622/direitomackenzie.v18n317058

O caso holandês parece ser a principal conexão, até o momento, entre as legislações internas da Europa e os estudos conceituais do fenômeno do *doxing*. Isso porque a lei pune de forma específica a utilização de dados de terceiros através da obtenção (independentemente se legal ou não) e a publicação com a intenção de causar dano à vítima.

De modo muito parecido com o contexto brasileiro, a Europa possui uma extensa legislação específica de proteção de dados, que pode ser considerada paradigmática para a legislação brasileira, porém ainda falha ao tentar criminalizar, pelo menos, uma forma de *doxing* que promova violação a direitos fundamentais como um fim em si própria, tratando a prática mais como um meio para cometimento de outras modalidades de crimes virtuais.

No contexto de alguns países asiáticos, o *doxing* vem sendo tratado de forma específica. Na Coreia do Sul, há uma série de previsões legais que atacam a prática, principalmente as previstas na "Lei sobre a promoção da utilização da rede de informação e comunicação e proteção da informação" (Coreia do Sul, 1986, tradução nossa):

> Artigo 44
> (1) Nenhum usuário pode circular qualquer informação que viole os direitos de outras pessoas, incluindo invasão de privacidade e difamação, através de uma rede de informação e comunicação.
> (2) Cada fornecedor de serviços de informação e comunicações deverá envidar esforços para impedir que qualquer informação nos termos do parágrafo (1) circule através da rede de informação e comunicações operada e gerida pelo fornecedor.
> [...]
> Artigo 44-7
> (1) Ninguém pode circular qualquer uma das seguintes informações através de uma rede de informação e comunicação:
> [...]
> 2. Informações com conteúdo que difame outras pessoas, divulgando fato ou informação falsa, de forma aberta e com intenção de denegrir a reputação da pessoa;
> [...]
> 4. Informações cujo conteúdo comprometa, destrua, altere ou falsifique um sistema de informação e comunicação, dados, programa ou similar ou que interfira no funcionamento de tal sistema, dados, programa ou similar sem motivo justificável;
> [...]

> 6-2. Informações sobre o conteúdo de transações de informações pessoais que violem esta Lei ou outros estatutos e regulamentos relativos à proteção de informações pessoais
> [...]
> Artigo 49.º (Proteção de Segredos)
> Ninguém deverá mutilar as informações de outra pessoa processadas, armazenadas ou transmitidas através de uma rede de informação e comunicação, nem deverá infringir, apropriar-se indevidamente ou divulgar o segredo de outra pessoa.
> Artigo 49-2 (Proibição de Coleta de Informações Pessoais por Atos Enganosos)
> (1) Ninguém deverá coletar informações de outra pessoa ou incitar outra pessoa a fornecer informações através de uma rede de informação e comunicação por meio de um ato de engano.
> (2) Sempre que um fornecedor de serviços de informação e comunicação descobre uma violação do parágrafo (1), ele ou ela reporta imediatamente ao Ministro da Ciência e TIC, à Comissão de Comunicações da Coreia ou à Agência Coreana de Internet e Segurança (Coreia do Sul, 1986, tradução nossa).

O caso sul-coreano é similar às amostras já exploradas, principalmente da Europa, no sentido de que a punição é feita para as condutas isoladas. Entretanto, as previsões entrelaçadas dos artigos 44 e 49 (Coreia do Sul, 1986) conseguem abranger de forma mais completa a prática de *doxing*, proibindo que seja circulada qualquer informação que ofenda direitos de personalidade, incluindo-se aí a proteção dos dados e a intimidade, além de proibir a coleta fraudulenta dos dados, ou seja, criminaliza a violação de dados pessoais. O ato legal ainda dá ênfase, nesses artigos, à responsabilidade dos fornecedores dos serviços de armazenamento.

O contexto da Coreia do Sul apresenta uma característica peculiar: o país asiático exibe altíssima taxa de suicídios, amplamente noticiada como uma das maiores do mundo e a maior entre países desenvolvidos (Ha, 2023; Hadjimatheou, 2022). Por guardar relação direta com a saúde mental, muitos estudos buscam interpretar as causas desse fenômeno, como: uso de smartphone (Woo *et al.*, 2021), qualidade de sono (Kwon *et al.*, 2020), situações relacionadas a emprego, desemprego ou trabalho excessivo (Ahn *et al.*, 2021), uso de álcool (Kim, 2023) e quarentena durante a pandemia de Covid-19 (Lee, 2020).

Dentre esses fatores, o *cyberbullyng* também aparece, principalmente em relação aos mais jovens, como um grande causador de problemas emocionais e mentais (Yoo, 2021; Kim; Lee; Jennings, 2022), inclusive fator que pode levar a suicídio (Lee, 2021).

REVISTA DIREITO MACKENZIE
RDM | São Paulo | SP | 18(3) | e17058
2024 | v. 18 | n. 3 | p. 1-27 | ISSN 2317-2622. http://dx.doi.org/10.5935/2317-2622/direitomackenzie.v18n317058

Tal contexto social é determinante para compreender a abordagem legal específica destinada a combater o *doxing* como forma de violação de direitos no país, considerando a preocupação com a saúde da população e os possíveis reflexos das más práticas adotadas pelos usuários na internet.

Na China, em 1º de março de 2020, entrou em vigor o Regulamento sobre a Governança Ecológica do Conteúdo de Informação On-line (República Popular da China, 2019), que traz previsões direcionadas ao *doxing*. Em seu artigo 21, enuncia-se que os utilizadores de serviços de conteúdos *on-line*, os produtores de serviços de conteúdos *on-line* e as plataformas de serviços de conteúdos *on-line* não devem empregar redes e tecnologias de informação relacionadas para realizar condutas ilegais, como insultar, difamar, ameaçar, espalhar boatos ou divulgar maliciosamente informações privadas de terceiros, prejudicando seus direitos e interesses legítimos (República Popular da China, 2019, tradução nossa).

As disposições do referido regulamento ainda proíbem que os usuários das plataformas *on-line* na China publiquem informações geradas por produtores de conteúdos que contrariem princípios constitucionais ou que difamem outras pessoas, infrinjam a honra, privacidade ou outros direitos e interesses legais (República Popular da China, 2019).

A forma com que a lei é redigida no caso chinês possui ligação intrínseca com a maneira com que a internet é regulada no país. Diferentemente da abordagem mais livre dos Estados Unidos ou da regulação intervencionista geral da União Europeia, as políticas chinesas para a internet são forte e historicamente inseparáveis do controle estatal (Miao; Jiang; Pang, 2021; Mueller; Tan, 1996; Yang; Mueller, 2014).

A China possui, portanto, um modelo que no qual o governo controla a internet, desde a infraestrutura até o conteúdo (Negro, 2017). O controle se dá de forma ampla através de um grande número (116) de agências governamentais que elaboram ou participam das políticas para a internet (Li *et al.*, 2018), sendo marcante a presença de uma vigilância estatal implementada através de diversos mecanismos que possuem como escopo fornecer segurança coletiva aos cidadãos chineses (Fornasier; Borges, 2023).

No contexto chinês, as legislações da internet vão priorizar os interesses nacionais, para depois se preocupar com a regulação dos produtores de conteúdo e dos fornecedores de serviço, e só então dar atenção ao usuário e à proteção de dados (Li *et al.*, 2018), como se percebe no Regulamento sobre a Governança Ecológica do Conteúdo de Informação On-line (China Law Translate, 2019, tradução nossa).

Apesar da abordagem claramente diferente dos governos ocidentais em geral, no que diz respeito ao assunto da regulação do *doxing* na legislação chinesa, pode-se concluir que a mesma parece cobrir de forma satisfatória os potenciais riscos de violações a direitos que podem ser causados, principalmente ao proibir a divulgação de informações pessoais em meio de comunicação *on-line*.

Em Hong Kong, leis mais severas tipificando o *doxing* estão em vigor desde 2021. A lei criminaliza a conduta de divulgar, de forma intencional ou imprudente, dados pessoais obtidos sem consentimento, desde que haja possibilidade de danos à vítima ou a pessoas de sua família (Hong Kong, 2023). O caso é emblemático, uma vez que a legislação emerge como resposta governamental a uma onda de protestos iniciada em 2019 contra extradições de cidadãos para a China, o que acabou por causar grande número de casos de *doxing* como forma de combate e resistência dos manifestantes contra a violência policial que se perpetrou nas ruas (Cheung, 2021). Essa é uma faceta da prática de *doxing* que será investigada em detalhes no próximo ponto do presente estudo.

De maneira semelhante a muitos outros países já explorados até aqui, os Estados Unidos não possuem uma regulação específica para o tema, portanto o problema ainda não ocupa um espaço explícito nos diplomas legais criminais nem civis (Lindvall, 2019). Em termos de estatutos federais, há os chamados interestaduais (válidos para todos os Estados americanos) sobre comunicações e *stalking*. Esses diplomas, no entanto, são inconclusivos ou não são suficientemente abrangentes para combater o *doxing*, raramente sendo aplicados (Lindvall, 2019).

Existe, ainda, a Lei de Decência nas Comunicações (do inglês, *Communications Decency Act*, CDA). A CDA apresenta uma limitação ao enfrentamento do *doxing*, uma vez que produz uma espécie de "escudo" para os fornecedores de serviços *on-line*, ou seja, as plataformas contra a responsabilidade pelos conteúdos postados pelos usuários – o que seria um potencial caminho para uma solução contra o *doxing* malicioso. A lei regulamenta conteúdos obscenos (embora constitucionais) e também aqueles que não são protegidos pela Constituição, eximindo o fornecedor de serviços, ou seja, as plataformas da responsabilidade em hospedar tais informações, dados, imagens ou quaisquer outras informações. Essa prática é desencorajadora para que exista um controle ou remoção de tais conteúdos (MacAllister, 2016).

Embora haja falta de "motivação legal" para remoção dos conteúdos, algumas ferramentas, entretanto, possuem mecanismos próprios que visam a atacar o problema. O X, por exemplo, possui medidas para remover conteúdo oriundo de *doxing* e

REVISTA DIREITO MACKENZIE
RDM | São Paulo | SP | 18(3) | e17058
2024 | v. 18 | n. 3 | p. 1-27 | ISSN 2317-2622. http://dx.doi.org/10.5935/2317-2622/direitomackenzie.v18n317058

restringir a atuação de *doxers* (aqueles que realizam a prática), muito a partir de relatórios de usuários e outros métodos de detecção, inclusive através de soluções automatizadas, por meio de inteligência artificial, ainda que de forma não totalmente otimizada (Karimi; Squicciarini; Wilson, 2022).

Em geral, as plataformas de redes sociais sofrem para moderar com eficácia o comportamento dos usuários, tendo em vista que os conteúdos e comportamentos escapam dos filtros de moderação, encontrando barreiras de contexto cultural, de escala (grande número de postagens) ou de preocupações com censura (Schoenebeck; Lampe; Triêu, 2023).

Logicamente, o argumento de responsabilização da plataforma se baseia na presunção de que as companhias iriam buscar aprimorar seus sistemas de remoção de conteúdo indesejado, incluindo-se o *doxing*. Sem nenhuma responsabilização, as redes sociais podem ser telas em branco prontas para a atuação de indivíduos mal-intencionados (MacAllister, 2016; Quon, 2009).

Especificamente no caso norte-americano, a Suprema Corte decidiu, em anos recentes, pela impossibilidade de responsabilização das plataformas pelos conteúdos postados pelos usuários. No caso *Twitter, Inc v. Taamneh et al.* (Estados Unidos, 2023), a família de um cidadão morto durante ataque atribuído ao Estado Islâmico em Istambul processou o Twitter, o Google e o Facebook, argumentando que não havia controle de conteúdo terrorista em seus sites (CBS News, 2022). O caso foi julgado em conjunto com *Gonzalez et al. v. Google LLC* (Estados Unidos da América, 2023), em que a família de uma americana de 23 anos que estudava em Paris processou a empresa tendo em vista que, através do sistema de recomendação do Youtube, a plataforma levou aos usuários vídeos de recrutamento para o Estado Islâmico, que acabou realizando um ataque terrorista no ano de 2015, ocasionando a morte da jovem. A família considerou que o site de vídeos seria, então, parcialmente responsável pela morte (CBS News, 2022).

No julgamento conjunto, a Corte considerou que não há responsabilidade das plataformas pelos conteúdos. Os demandantes argumentaram no sentido de limitar o alcance da proteção prevista na Seção 230 da CDA. Já as plataformas argumentaram (entre outras coisas) que a seção citada protegeria o uso de algoritmos para recomendar conteúdo específico a usuários específicos, que foi o entendimento da decisão (Estados Unidos da América, 2023).

Embora a discussão desses casos esteja focada em outros tipos de ataques *on-line*, é possível considerar a responsabilização no contexto do doxing. Apesar de o doxing

não ser tipificado como crime de forma autônoma, ele pode ser usado como ferramenta para viabilizar outras formas de violência. Isso é evidente a partir das análises já mencionadas (Schoenebeck; Lampe; Triêu, 2023), que demonstram como a prática pode facilitar ações prejudiciais.

Para além da CDA, existem duas legislações federais que abordam, ainda que de forma indireta ou insuficiente, o *doxing* (MacAllister, 2016). O Estatuto das Comunicações Interestaduais criminaliza a transmissão, pela internet, de qualquer comunicação que contenha ameaça de sequestro ou ameaça de ferir outra pessoa, caso no qual os agentes da lei poderiam utilizar a legislação para responsabilizar atores que usam o *doxing* para realizar as ameaças (MacAllister, 2016). Entretanto, a legislação faz referências apenas a comunicações que transbordem fronteiras entre os Estados ou para fora do país, o que limita sua aplicação.

Por sua vez, o Estatuto Interestadual contra *Stalking* proíbe o uso de dispositivo informático para colocar uma pessoa em estado de medo razoável de morte ou lesões graves, o que poderia abranger alguns casos de *doxing* (Lindvall, 2019). O problema, no entanto, reside na necessidade de que um agente realize a conduta de maneira reiterada para caracterizar perseguição, e, no caso do *doxing*, muitas vezes, há mais de um indivíduo agindo isoladamente e nem sempre com coordenação (MacAllister, 2016).

Essas previsões demonstram a ineficácia das legislações em lidar com os atos de *doxing*, considerando a ausência da previsão específica de escolha de uma vítima e a publicação de seus dados pessoais na internet. Uma situação de *doxing*, portanto, dificilmente será compatível com uma acusação de *stalking*, uma vez que a perseguição se consuma através de diversas ameaças de colocar outra pessoa em perigo, não necessariamente pelo uso de dados pessoais obtidos de forma ilegal (McIntyre, 2016).

No tocante a leis estaduais, existem algumas previsões que cobrem casos de *doxing*, mas a maioria dos dispositivos possui lacunas (MacAllister, 2016). Na Califórnia, uma lei local proíbe a distribuição ou publicação de informações de identificação pessoal com a intenção de colocar a vítima em situação de risco à sua segurança (McIntyre, 2016), o que cobre parcialmente a conduta do *doxing*, não se preocupando com o meio de obtenção das informações.

Com isso, resta evidente que tais previsões elencadas são bastante amplas e não abordam de maneira adequada e taxativa o próprio ato do *doxing*, focando mais em seus efeitos e em alguns métodos de obtenção de dados. Elas se relacionam mais com outros tipos de crimes cibernéticos, pois se afastam das categorias previamente definidas

REVISTA DIREITO MACKENZIE
RDM | São Paulo | SP | 18(3) | e17058
2024 | v. 18 | n. 3 | p. 1-27 | ISSN 2317-2622. http://dx.doi.org/10.5935/2317-2622/direitomackenzie.v18n317058

como a desanonimização, *targeting*, *deslegitimização*, intenção maliciosa, objetivo político, revelação de membros anônimos.

3. Conclusão

A presente pesquisa objetivou em linhas gerais investigar a prática de *doxing* e identificar os conflitos e ilicitudes daí oriundas sob o contexto do tratamento de dados pessoais, considerando demais direitos fundamentais, pilares democráticos, que permeiam a atividade de *doxing*, bem como analisar a regulação vigente dessa matéria a nível nacional e globalmente. Quanto ao primeiro objetivo específico, podemos concluir que o *doxing* pode ser utilizado como ferramenta para a prática de diversos outros ilícitos. Assim, demonstrou-se que a prática pode servir de instrumento para cometimento de diversos crimes cibernéticos. A gama de crimes cibernéticos foi explorada e confrontada com o *doxing*, sendo estabelecida a forma com que cada ilícito se relaciona com o fenômeno.

Desde crimes como extorsão, perseguição, assédios, ameaças, até crimes com reais danos físicos, como ataques, linchamentos, ciberterrorismo, entre diversos outros fins maliciosos podem ser cometidos através do uso de *doxing*, ainda que sob forma de ameaça. O que se identificou foi, enfim, a força de que a posse injusta e a divulgação injusta de dados pessoais de terceiros podem exercer para perpetrar fins maliciosos.

No que tange o segundo objetivo específico, o *doxing* foi analisado como um ilícito em si. Várias legislações do mundo foram trazidas à baila, demonstrando que, devido à complexidade do fenômeno, o *doxing* não é necessariamente criminalizado como prática em si, mas diversos fragmentos dos atos necessários para sua prática podem ser alvo de previsão legal. Assim, ao cotejar as previsões legais de países como Brasil, Estados Unidos, Holanda, Coreia do Sul e China, restou demonstrado que a criminalização do *doxing* ou de seus atos separadamente tem profunda ligação com o contexto social em que se inserem as referidas legislações e são, sobretudo, leis que possuem uma forte simbologia de resposta a acontecimentos marcantes e, no caso da China, profundamente marcadas pela forma com que a internet e as ferramentas digitais são geridas pelo governo.

A presente pesquisa portanto conclui sua hipótese preliminar tendo em vista que o entendimento fragmentado do núcleo duro do conceito *doxing* compreende, na realidade, a obtenção ilegal de dados em um sistema de armazenamento e a posterior divulgação. Armazenar dados e divulgar informações são fenômenos que existem tanto no

mundo analógico quanto no digital, assim como os demais atos que permeiam a prática, tais como os crimes abordados.

Entretanto, como o trabalho não visa a um total esgotamento da temática, alguns aspectos podem ser abordados de maneira mais ampla para compreender de forma ainda mais completa o fenômeno do *doxing*. O primeiro deles, percebido ao longo do desenvolvimento, foi a possibilidade de amplo debate do tema sob o olhar do direito ao esquecimento, uma vez que o ambiente digital é marcado fortemente por um fluxo de dados e um grande volume de informações. Tais informações podem, ao longo do tempo, se tornar obsoletas, mas difíceis de serem apagadas, motivo pelo qual, em algum momento, podem ser utilizadas em um contexto que pode vir a lesar o patrimônio subjetivo dos alvos da prática de *doxing*.

REFERÊNCIAS

AHN, J. *et al.* Comparison of the physical and mental health problems of unemployed with employees in South Korea. *Archives of Environmental & Occupational Health*, v. 76, n. 3, p. 163- 172, 2021. Disponível em: https://www.tandfonline.com/doi/abs/10.1080/19338244.2020.1783503. Acesso em: 18 jan. 2024.

ALEMANHA. Bundersministerium der Justiz. *Bundesdatenschutzgesetz*. Berlim, 2023. Disponível em: https://www.gesetze-im-internet.de/bdsg_2018/. Acesso em: 3 jan. 2024.

AL-KHATER, W. A. *et al.* Comprehensive review of cybercrime detection techniques. *IEEE Access*, v. 8, p. 137293-137311, 2020. Disponível em: https://ieeexplore.ieee.org/abstract/document/9146148/. Acesso em: 18 jan. 2024.

ANDERSON, B.; WOOD, M. A. Doxxing: a scoping review and typology. *In*: BAILEY, J.; FLYNN, A.; HENRY, N. *The emerald international handbook of technology-facilitated violence and abuse*. Bingley: Emerald Publishing Limited, 2021. Disponível em: https://www.emerald.com/insight/publication/doi/10.1108/9781 839828485. Acesso em: 20 nov. 2023.

ANGUITA, R. P. Freedom of expression in social networks and doxing. *In*: CORREDOIRA, L.; MALLÉN, I. B.; PRESUEL, R. C. *The handbook of communication rigts, law, and ethics*. New York: John Wiley & Sons, Inc., 2021. Disponível em: https://onlinelibrary.wiley.com/doi/10.1002/9781119719564.ch23. Acesso em: 8 jan. 2024.

BARRIO, A. del. Así se cambió el Código Penal por el video sexual de Olvido Hormigos. *El Mundo*. Madrid, 2019. Disponível em: https://www.elmundo.es/madrid/2019/05/30/5cee6365fc6c83ae2a8b45a6.html. Acesso em: 18 jan. 2024.

BARRUL FUENTES, M. A. *Intimidad, sexting y derecho penal*. Facultade de Dereito, Universidade da Coruña, 2020. Disponível em: https://ruc.udc.es/dspace/handle/2183/26978. Acesso em: 18 jan. 2024.

REVISTA DIREITO MACKENZIE
RDM | São Paulo | SP | 18(3) | e17058
2024 | v. 18 | n. 3 | p. 1-27 | ISSN 2317-2622. http://dx.doi.org/10.5935/2317-2622/direitomackenzie.v18n317058

BRASIL. *Constituição Federal do Brasil de 1988*. Brasília, DF: Presidência da República, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm. Acesso em: 1º nov. 2023.

BRASIL. *Decreto-Lei nº 2.848, de 7 de dezembro de 1940*. Código Penal. Brasília, DF: Presidência da República, 1940. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 18 jan. 2024.

BRASIL. *Lei nº 7.716, de 5 de janeiro de 1989*. Brasília, DF: Presidência da República, 1989. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l7716.htm. Acesso em: 10 dez. 2023.

BRASIL. *Lei nº 12.737, de 30 de novembro de 2012*. Brasília, DF: Presidência da República, 2012. Disponivel em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 18 jan. 2024.

BRASIL. *Lei nº 13.709, de 14 de agosto de 2018*. Brasília, DF: Presidência da República, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm. Acesso em: 4 jan. 2024.

BRASIL. *Lei nº 14.811, de 12 de janeiro de 2024*. Brasília, DF: Presidência da República, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2024/lei/L14811.htm. Acesso em: 18 jan. 2024.

CANINI, R. *Os efeitos do discurso sobre a violência*: uma análise do crime de ódio no Brasil. Pontifícia Universidade Católica do Rio de Janeiro - PUC-Rio. 2020. Disponível em: https://www.econ.puc-rio.br/biblioteca.php/?titulo=&numero=&autor=&ano_inicial=&tipo=7&ano_final=&page=13. Acesso em: 29 nov. 2023.

CAYE, A. A. B. S. Crimes de ódio no sistema de justiça criminal brasileiro. *Revista da Faculdade de Direito da FMP*, v. 17, n. 1, p. 92-94, 2022. Disponível em: https://revistas.fmp.edu.br/index.php/FMP-Revista/article/view/297. Acesso em: 18 jan. 2024.

CBS NEWS. *Supreme Court will hear two cases seeking to hold social media companies financially responsible for terrorist attacks*. 3 Oct. 2022. Disponível em: https://www.cbsnews.com/news/supreme-court-social-media-terrorism-lawsuits-nohemi-gonzalez-nawras-alassaf/. Acesso em: 22 jan. 2024.

CHEN, M.; CHEUNG, A. S. Y.; CHAN, K. L. Doxing: what adolescents look for and their intentions. *International journal of environmental research and public health*, v. 16, n. 2, p. 218, 2019. Disponível em: https://www.mdpi.com/1660-4601/16/2/218. Acesso em: 18 jan. 2024.

CHEUNG, A. Doxing and the challenge to legal regulation: when personal data become a weapon. *In*: *The emerald international handbook of technology-facilitated violence and abuse*. Bingley: Emerald Publishing Limited, 2021. p. 577-594. Disponível em: https://doi.org/10.1108/978-1-83982-848-520211041. Acesso em: 5 dez. 2023.

CHINA LAW TRANSLATE. Provisions on the Governance of the Online Information Content Ecosystem. 21 dez. 2019. Disponível em: https://www.chinalawtranslate.com/en/provisions-on-the-governance-of-the-online-information-content-ecosystem/. Acesso em: 18 jan. 2024.

CONJUR. *Após bloquear site racista, juíza tem dados vazados na internet e é ameaçada*. 26 jan. 2018. Disponível em: https://www.conjur.com.br/2018-jan-26/bloquear-site-racista-juiza-ameacada-dados-divulgados/. Acesso em: 29 nov. 2023.

COREIA DO SUL. *Act on promotion of information and communications network utilization, and information protection*. 1986. Disponível em: https://elaw.klri.re.kr/kor_service/lawView.do?hseq=50484&lang=ENG. Acesso em: 5 dez. 2023.

DOUGLAS, D. M. Doxing: a conceptual analysis. *Ethics and Information Technology*, v. 18, n. 3, p. 199–210. 2016. Disponível em: https://link.springer.com/article/10.1007/s10676-016-9406-0. Acesso em: 5 dez. 2023.

ECKERT, S.; METZGER-RIFTKIN, J. Doxxing. *In*: *The international encyclopedia of gender, media, and communication*. ROSS, K. (ed.) *et al*. New York: John Wiley & Sons, Inc, 2020. Disponível em: https://onlinelibrary.wiley.com/doi/book/10.1002/9781119429128. Acesso em: 18 jan. 2024.

ESPANHA. *Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal*. Agéncia Estatal Boletín Oficial del Estado, 1995. Disponível em: https://www.boe.es/buscar/act.php?id=BOE-A-1995-25444. Acesso em: 18 jan. 2024.

ESTADOS UNIDOS DA AMÉRICA. *Constitution of the United States*. Filadélfia, PA: Constitutional Convention, 1787. Disponível em: https://www.senate.gov/about/origins-foundations/senate-and-constitution/constitution.htm. Acesso em: 8 jan. 2024.

ESTADOS UNIDOS DA AMÉRICA. Suprema Corte. *Gonzalez et al. v. Google LLC*. Julgado em: 18 May 2023. Disponível em: https://supreme.justia.com/cases/federal/us/598/21-1333/. Acesso em: 22 jan. 2024.

ESTADOS UNIDOS DA AMÉRICA. Suprema Corte. *Twitter, Inc v. Taamneh et al.* Julgado em: 18 Maio 2023. Disponível em: https://www.supremecourt.gov/opinions/22pdf/21-1496_d18f.pdf. Acesso em: 22 jan. 2024.

FORNASIER, M. de O.; BORGES, G. S. The Chinese 'sharp eyes' system in the era of hyper surveillance: between state use and risks to privacy. *Revista Brasileira de Políticas Públicas*, v. 13, p. 440, 2023. Disponível em: https://www.gti.uniceub.br/RBPP/article/view/7997/pdf. Acesso em: 19 mar. 2024.

FRÓS, C. C. Crimes de ódio. *Revista da Faculdade de Direito da FMP*, v. 17, n. 1, p. 95-98, 2022. Disponível em: https://revistas.fmp.edu.br/index.php/FMP-Revista/article/view/298. Acesso em: 5 dez. 2023.

GRECO, R. *Curso de direito penal*: volume 2: parte especial: artigos 121 a 212 do Código Penal. 19. ed. Barueri: Atlas, 2022.

G1. *Entenda o caso de Edward Snowden, que revelou espionagem dos EUA*. São Paulo, 2013. Disponível em: https://g1.globo.com/mundo/noticia/2013/07/entenda-o-caso-de-edward-snowden-que-revelou-espionagem-dos-eua.html. Acesso em: 22 jan. 2024.

G1. *Grupo de hackers vaza em rede social supostos dados pessoais de Bolsonaro, filhos e ministros*. Brasília, 2020. Disponível em: https://g1.globo.com/politica/noticia/2020/06/02/grupo-de-hackers-vaza-em-rede-social-supostos-dados-pessoais-de-bolsonaro-filhos-e-apoiadores.ghtml. Acesso em: 22 jan. 2024.

HA, S. Por que Coreia do Sul tem os maiores índices de suicídio entre países desenvolvidos. *BBC News Brasil*, 2 nov. 2023. Disponível em: https://www.bbc.com/portuguese/articles/c4n4gjxr0e3o. Acesso em: 18 jan. 2024.

REVISTA DIREITO MACKENZIE
RDM | São Paulo | SP | 18(3) | e17058
2024 | v. 18 | n. 3 | p. 1-27 | ISSN 2317-2622. http://dx.doi.org/10.5935/2317-2622/direitomackenzie.v18n317058

HADJIMATHEOU, C. Como Coreia do Sul se tornou um dos países com mais insones. *BBC News Brasil*, 18 abr. 2022. Disponível em: https://www.bbc.com/portuguese/internacional-61138819. Acesso em: 18 jan. 2024.

HANCOKS, P. South Korea teenagers bullied to death. CNN. 26 jul. 2012. Disponível em: https://edition.cnn.com/2012/07/25/world/asia/south-korea-school-bully/index.html. Acesso em: 18 jan. 2024.

HOLANDA. Government of The Netherlands. *Use of personal data for the objective of harassment to become criminal offence*, 12 jun. 2023. Disponível em: https://www.government.nl/latest/news/2023/07/12/use-of-personal-data-for-the-objective-of-harassment-to-become-criminal-offence. Acesso em: 18 jan. 2024.

HONG KONG. *Doxing offences*. The Office of the Privacy Commissioner for Personal Data, 2023. Disponível em: https://www.pcpd.org.hk/english/doxxing/index.html. Acesso em: 18 jan. 2024.

IBARRA, J. C. H. (coord.). *Manual de derecho penal parte especial*. Adaptado a las LLOO 1/2019 y 2/2019 de Reforma del Código Penal. Doctrina y jurisprudencia con casos solucionados. 2. ed. Valência: Tirant lo Blanch, 2019.

KARIMI, Y.; SQUICCIARINI, A.; WILSON, S. Automated detection of doxing on twitter. *Proceedings of the ACM on Human-Computer Interaction*, v. 6, n. CSCW2, p. 1-24, 2022. Disponível em: https://dl.acm.org/doi/abs/10.1145/3555167. Acesso em: 18 jan. 2024.

KIM, J.; LEE, Y.; JENNINGS, W. G. A path from traditional bullying to cyberbullying in South Korea: examining the roles of self-control and deviant peer association in the different forms of bullying. *Journal of interpersonal violence*, v. 37, n. 9-10, p. 5937-5957, 2022. Disponível em: https://journals.sagepub.com/doi/abs/10.1177/08862605211067022. Acesso em: 18 jan. 2024.

KIM, S. *et al*. The effects and challenges of alcohol use disorder peer support service in South Korea: a focus group study. *International Journal of Mental Health Nursing*, 2023. Disponível em: https://onlinelibrary.wiley.com/doi/abs/10.1111/inm.13230. Acesso em: 18 jan. 2024.

KLYMENKO, O. A.; GUTSALYUK, M. V.; SAVCHENKO, A. V. Combating cybercrime as a prerequisite for the development of the digital society. *JANUS. NET e-Journal of International Relations*, v. 11, p. 18-29, 2020. Disponível em: https://repositorio.ual.pt/handle/11144/4542. Acesso em: 18 jan. 2024.

KWON, D. H. *et al*. The mental health and sleep quality of the medical staff at a hub-hospital against COVID-19 in South Korea. *Journal of Sleep Medicine*, v. 17, n. 1, p. 93-97, 2020. Disponível em: https://e-jsm.org/journal/view.php?number=281. Acesso em: 18 jan. 2024.

LEE, J. *et al*. A social-ecological approach to understanding the relationship between cyberbullying victimization and suicidal ideation in South Korean adolescents: the moderating effect of school connectedness. *International Journal of Environmental Research and Public Health*, v. 18, n. 20, p. 10623, 2021. Disponível em: https://www.tandfonline.com/doi/abs/10.1080/02185385.2020.1774409. Acesso em: 18 jan. 2024.

LEE, S. W. *et al*. Association between mental illness and COVID-19 susceptibility and clinical outcomes in South Korea: a nationwide cohort study. *The Lancet Psychiatry*, v. 7, n. 12, p. 1025-1031, 2020. Disponível em: https://www.thelancet.com/journals/lanpsy/article/PIIS2215-0366(20)30421-1/fulltext. Acesso em: 18 jan. 2024.

LI, J. *et al*. Examining China's internet policies through a bibliometric approach. *Journal of Contemporary Eastern Asia*, v. 17, n. 2, p. 237-253, 2018. Disponível em: https://koreascience.kr/article/JAKO201816936726878.page. Acesso em: 18 jan. 2024.

LINDVALL, A. J. Political hacktivism: doxing & the first amendment. *Creighton Law Review*, v. 53, p. 1, 2019. Disponível em: https://heinonline.org/HOL/LandingPage?handle=hein.journals/creigh53&div=5&id=&page=. Acesso em: 18 jan. 2024.

MACALLISTER, J. M. The doxing dilemma: seeking a remedy for the malicious publication of personal information. *Fordham Law Review*, v. 85, p. 2451, 2016. Disponível em: https://heinonline.org/HOL/LandingPage?handle=hein.journals/flr85&div=98&id=&page=. Acesso em: 18 jan. 2024.

MCINTYRE, V. Do (x) you really want to hurt me?: adapting IIED as a solution to doxing by reshaping intent. *Tulane Journal of Technology & Intellectual Property*, v. 19, p. 111, 2016. Disponível em: https://heinonline.org/HOL/LandingPage?handle=hein.journals/tuljtip19&div=8&id=&page=. Acesso em: 22 jan. 2024.

MIAO, W.; JIANG, M.; PANG, Y. Historicizing internet regulation in China: a meta-analysis of Chinese internet policies (1994–2017). *International Journal of Communication*, v. 15, p. 24, 2021. Disponível em: https://ijoc.org/index.php/ijoc/article/view/15944. Acesso em: 18 jan. 2024.

MUELLER, M. L.; TAN, Z.. *China in the information age*: telecommunication and the dilemmas of reform. Westport: Greenwood Publishing Group Inc., 1996.

MURPHY, L. Did anonymous unmask the wrong guy in its hunt for the man who allegedly drove a teen to suicide? *Slate.com*. 17 out. 2012. Disponível em: https://slate.com/technology/2012/10/amanda-todd-suicide-did-anonymous-dox-the-wrong-guy.html. Acesso em: 18 jan. 2024.

NEGRO, G. *Internet in China*. London: Palgrave Macmillan, 2017.

NEUBAUM, G. *et al*. United in the name of justice: how conformity processes in social media may influence online vigilantism. *Psychology of Popular Media Culture*, v. 7, n. 2, p. 185, 2018. Disponível em: https://psycnet.apa.org/record/2016-11413-001. Acesso em: 22 jan. 2024.

NUCCI, G. de S. *Manual de direito penal*: volume único. 19. ed. Rio de Janeiro: Forense, 2023.

OLIVEIRA, X. de. Estudo de direito penal comparado acerca da jurisdição universal nos sistemas penais brasileiro e espanhol. *INTER*: Revista de Direito Internacional e Direitos Humanos da UFRJ. v. 3, n. 1, 2020. Disponível em: https://revistas.ufrj.br/index.php/inter/article/view/35018. Acesso em: 18 jan. 2024.

PORTUGAL. *Constituição da República Portuguesa*. Disponível em: https://www.parlamento.pt/Parlamento/Documents/CRP1976.pdf. Acesso em: 10 dez. 2023.

QUON, K. Implementing a standard of care to provide protection from a lawless internet. *Whittier Law Review*, v. 31, p. 589, 2009. Disponível em: https://heinonline.org/HOL/LandingPage?handle=hein.journals/whitlr31&div=25&id=&page=. Acesso em: 18 jan. 2024.

REPÚBLICA POPULAR DA CHINA. The "Regulations on ecological governance of internet information content" clearly prohibit illegal activities such as human flesh searches and traffic fraud. *Xinhua News Agency*. 21 dez. 2019. Disponível em: https://www.gov.cn/xinwen/2019-12/21/content_5462826.htm. Acesso em: 18 jan. 2024.

REVISTA DIREITO MACKENZIE
RDM | São Paulo | SP | 18(3) | e17058
2024 | v. 18 | n. 3 | p. 1-27 | ISSN 2317-2622. http://dx.doi.org/10.5935/2317-2622/direitomackenzie.v18n317058

REUTERS. Dutch Senate votes to make "doxing" a crime. *Reuters*. [Amsterdam], 11 jul. 2023. Disponível em: https://www.reuters.com/world/europe/dutch-senate-votes-make-doxing-crime-2023-07-11/. Acesso em: 18 jan. 2024.

SCHOENEBECK, S.; LAMPE, C.; TRIỆU, P. Online harassment: assessing harms and remedies. *Social Media+ Society*, v. 9, n. 1, p. 20563051231157297, 2023. Disponível em: https://journals.sagepub.com/doi/full/10.1177/20563051231157297. Acesso em: 18 jan. 2024.

SNOWDEN, E. *Eterna vigilância*: como montei e desvendei o maior esquema de espionagem do mundo. São Paulo: Planeta, 2019. Edição do Kindle.

SNYDER, P. *et al*. Fifteen minutes of unwanted fame: Detecting and characterizing doxing. *In*: 2017 INTERNET MEASUREMENT CONFERENCE, 2017, London. *Anais* [...]. London, 2017. p. 432-444. Disponível em: https://dl.acm.org/doi/abs/10.1145/3131365.3131385. Acesso em: 19 dez. 2023.

SOLOVE, D. J. *The future of reputation*: gossip, rumor, and privacy on the internet. Yale: Yale University Press, 2007.

SORCE, G.; DUMITRICA, D. Transnational dimensions in digital activism and protest. *Review of Communication*, v. 22, n. 3, p. 157-174, 2022. Disponível em: https://www.tandfonline.com/doi/full/10.1080/15358593.2022.2107877. Acesso em: 22 jan. 2024.

TAN, A. *To dox or not to dox, that is the question.* 1º fev. 2022. Disponível em: https://ssrn.com/abstract=4369643 or http://dx.doi.org/10.2139/ssrn.4369643. Acesso em: 20 dez. 2023.

TEIXEIRA, P. S. O que é doxing? Entenda prática que expõe pessoas, mas não é crime no Brasil. *Folha de São Paulo*. São Paulo, 26 jan. 2023. Disponível em: https://www1.folha.uol.com.br/tec/2023/01/o-que-e-doxing-entenda-pratica-que-expoe-pessoas-mas-nao-e-crime-no-brasil.shtml. Acesso em: 18 jan. 2024.

VARSHNEY, G. *et al*. Anti-phishing: a comprehensive perspective. *Expert Systems with Applications*, v. 238, 2024. Disponível em: https://www.sciencedirect.com/science/article/abs/pii/S095741742302701X. Acesso em: 18 jan. 2024.

WOO, K. S. *et al*. Mental health, smartphone use type, and screen time among adolescents in South Korea. *Psychology research and behavior management*, p. 1419-1428, 2021. Disponível em: https://www.tandfonline.com/doi/full/10.2147/PRBM.S324235. Acesso em: 18 jan. 2024.

YANG, F.; MUELLER, M. L. Internet governance in China: a content analysis. *Chinese Journal of Communication*, v. 7, n. 4, p. 446-465, 2014. Disponível em: https://www.tandfonline.com/doi/abs/10.1080/17544750.2014.936954. Acesso em: 18 jan. 2024.

YAR, M.; STEINMETZ, K. *Cybercrime and society*. New York: Sage Publications, 2019. Edição do Kindle.

YOO, C. What are the characteristics of cyberbullying victims and perpetrators among South Korean students and how do their experiences change? *Child Abuse & Neglect*, v. 113, p. 104923, 2021. Disponível em: https://www.sciencedirect.com/science/article/abs/pii/S0145213420305780. Acesso em: 18 jan. 2024.

Mateus de Oliveira Fornasier

Doutor em Direito pela Universidade do Vale do Rio dos Sinos (Unisinos), com Pós-doutorado em Direito e Teoria pela University of Westminster (Reino Unido). Professor do Programa de Pós-Graduação (Mestrado e Doutorado) em Direito da Universidade Regional do Noroeste do Estado do Rio Grande do Sul (UnIjuí). Advogado.
Universidade Regional do Noroeste do Estado do Rio Grande do Sul
Ijuí, RS, Brasil
E-mail: mateus.fornasier@gmail.com

Fernanda Viero da Silva

Doutoranda e mestra em Direito pela Universidade Regional do Noroeste do Estado do Rio Grande do Sul (UnIjuí).
Universidade Regional do Noroeste do Estado do Rio Grande do Sul
Ijuí, RS, Brasil
E-mail: fefeviero@gmail.com

Benhur Aurélio Formentini Nunes

Mestre em Direito pela Universidade Regional do Noroeste do Estado do Rio Grande do Sul (UnIjuí).
Universidade Regional do Noroeste do Estado do Rio Grande do Sul
Ijuí, RS, Brasil
E-mail: benhur41@hotmail.com

Equipe editorial

Editor Acadêmico Felipe Chiarello de Souza Pinto
Editor Executivo Marco Antonio Loschiavo Leme de Barros

Produção editorial

Coordenação Editorial Andréia Ferreira Cominetti
Preparação de texto Mônica de Aguiar Rocha
Diagramação Libro Comunicação
Revisão Vera Ayres
Estagiária editorial Isabelle Callegari Lopes