REVISTA DA FACULDADE DE DIREITO DA UNIVERSIDADE DE LISBOA

LISBON LAW REVIEW

Número Temático: Tecnologia e Direito

ANO LXIII 2022 NÚMEROS 1 E 2

REVISTA DA FACULDADE DE DIREITO
DA UNIVERSIDADE DE LISBOA
Periodicidade Semestral
Vol. LXIII (2022) 1 e 2

LISBON LAW REVIEW

PROPRIEDADE E SECRETARIADO

Faculdade de Direito da Universidade de Lisboa
Alameda da Universidade – 1649-014 Lisboa – Portugal

EDIÇÃO, EXECUÇÃO GRÁFICA E DISTRIBUIÇÃO
LISBON LAW EDITIONS

Alameda da Universidade – Cidade Universitária – 1649-014 Lisboa – Portugal

ISSN 0870-3116 Depósito Legal n.º 75611/95

Data: Outubro, 2022

ÍNDICE 2022

LIVROS & ARTIGOS

Cyberbullying por divulgação de dados pessoais

Cyberbullying by doxxing

Renata Oliveira Almeida Menezes[*] | Luís Eduardo e Silva Lessa Ferreira[**]

Resumo: O conteúdo jurídico do direito à privacidade é desafiado na sociedade da comunicação pelo constante armazenamento e compartilhamento de dados e informações sobre os usuários da rede de computadores, ações que podem causar exposição não desejada, e que repercutem de forma evidente no mundo *offline*. Conforme a necessidade de controle do usuário da internet sobre as suas próprias informações, questionou-se se a divulgação não autorizada de informações pessoais na internet, conhecida como *doxxing*, é espécie autônoma ou apenas um meio para a prática de *cyberbullying*. Após análise dos fenômenos descritos como *doxxing*, identificou-se três possíveis correntes doutrinárias sobre a sua natureza, concluiu-se que a teoria dualista é a mais adequada para as funções jurídicas de integração, criação e decisão, no intuito de prevenir e enfrentar o *cyberbullying*. Por fim, comprovou-se a pertinência na criação pelos Estados de leis específicas para o combate ao *doxxing*.

Palavras-chave: *Cyberbullying*. *Doxxing*. Dados pessoais. Autodeterminação informacional. Privacidade.

Abstract: The legal content of the right to privacy is challenged in the communication society by the constant storage and sharing of data and information regarding computer network users. These actions can cause unwanted exposure and have evident repercussion in the offline world. Considering the internet need of internet users of controlling their own information, it is questioned whether the unauthorized disclosure of personal information on the internet, known as doxxing, is an autonomous type of crime or just a means of practicing cyberbullying. After typological analysis and categorization of the phenomena described as doxxing, three possible doctrinal currents about its nature were identified. It is concluded that the dualist theory is the most appropriate and should be used in the legal functions of integrating, creating, and deciding, to prevent and combat cyberbullying. Finally, the relevance of the creation by States of specific laws to combat doxxing was proved.

Keywords: Cyberbullying. Doxxing. Personal data. Informational self-determination. Privacy.

[*] Professora Adjunta da Universidade Federal do Rio Grande do Norte. Doutora em Direito Privado pela Universidade Federal de Pernambuco. Doutora em Ciências Jurídicas e Sociais pela Universidade Federal de Campina Grande e Universidad del Museo Social Argentino. E-mail: renata.biodireito@gmail.com.
[**]Doutorando e Mestre em Direito Privado pela Universidade Federal de Pernambuco. Advogado. E-mail: lessaluiseduardo@gmail.com.

Sumário: 1. Introdução. 2. Fundamentos normativos da proteção de dados. 3. *Cyberbullying* por divulgação de dados pessoais. 4. Delimitação conceitual de *doxxing*. 5. Espécies de *doxxing*. 5.1 *Doxxing* por desanonimização. 5.2 *Doxxing* por segmentação. 5.3 *Doxxing* por desmoralização. 6. Categorização de *doxxing*: violação de privacidade ou forma de prática de violência. 7. Conclusões.

1. Introdução

Segundo a Conferência da Organização das Nações Unidas sobre Comércio e Desenvolvimento, apenas 66% dos países salvaguardam os dados e a privacidade dos seus cidadãos, a despeito do aumento do número de leis aprovadas nesta área entre 2015 e 2020. Os resultados são ainda mais baixos entre os países menos desenvolvidos, onde apenas 43% dos Estados-membros o fazem[1]. A ONU recomenda que os países adotem leis de proteção de dados na internet como condição para o desenvolvimento, já que as ferramentas digitais são cada vez mais o único veículo para ter acesso a bens e serviços.

O reconhecimento de um direito humano e de um direito fundamental à proteção de dados pessoais ainda é um processo em curso, e que não ostenta uniformidade quando considerados os sistemas jurídicos plurais. Enquanto muitos países da Europa, e, recentemente o Brasil, reconhecem o direito à proteção de dados como direito autônomo, expressamente positivado nas suas respectivas constituições, em outras realidades jurídicas ele pode ser reconhecido de modo exclusivamente implícito, como derivado dos direitos à privacidade e à liberdade.

A extensão dos efeitos do direito fundamental à proteção de dados e à autodeterminação informacional à seara virtual mostra-se necessária em prol da eficácia social dos direitos, no contexto de sociedades complexas e da cibercultura.

---

[1] Segundo a Unctad, os países menos desenvolvidos estão em pior situação. Globalmente, 81% dos países têm uma lei sobre transações eletrônicas. A Europa tem a maior participação, 98%, seguida pelas Américas, 91%. Com 61%, África é a região com a proporção mais baixa. Cerca de 79% dos países possuem legislação sobre crimes cibernéticos, sendo a participação mais alta na Europa, 89%, e mais baixa na África, 72%. Leis de proteção do consumidor on-line variam entre 73% na Europa, 72% nas Américas a 46% na África. Já em relação a dados e privacidade, 66% dos países possuem legislação, com 96% na Europa, 69% nas Américas, 57% na Ásia e Pacífico e 50% na África. UNCTAD, *Summary of Adoption of E-Commerce Legislation Worldwide,* 2020. Disponível em: unctad.org. Consulta em: 9 de agosto de 2022.

É possível observar alguns aspectos das mudanças sociais desencadeadas pelo avanço das tecnologias digitais, potencializando a complexidade social e revelando o contraste entre perspectivas do sistema jurídico e a dinâmica social, que colocam em evidência as fragilidades jurídicas na realização de direitos, em especial no que diz respeito ao livre desenvolvimento da personalidade.

Em outro sentido, há uma clara oportunidade para questionamentos, aprendizados e inovação. Os desafios podem ressignificar a importância da convergência de normas de direitos humanos, constitucionais de direitos fundamentais e das legislações infraconstitucionais para acentuar o desenvolvimento humano, frente aos fenômenos que são próprios da realidade virtual.

A transitoriedade é uma característica muito marcante nos modos de interação social, um meio que é utilizado massivamente pode facilmente ser substituído por outro, que passa a ser preferido por alguns, e, em pouco tempo, pode ser adotado pelos demais, sob a ação do "efeito manada"[2]; em seguida, ante o surgimento de uma outra plataforma de troca de dados, informações e materiais, aquele meio ora massivamente utilizado, passa a ser tido como defasado, e é substituído.

Essa realidade se mostrou mais evidente com o advento da internet, que, ao mesmo tempo em que acelerou e otimizou interações pessoais, presencia a fluidez da instabilidade das suas plataformas. Como o que acontece on-line tem repercussão na sociedade, especialmente em âmbito externo ao virtual, acaba por desafiar o Direito a acompanhar tais alterações, no intuito de garantir a efetividade da tutela dos direitos fundamentados no princípio da dignidade humana, especialmente dos direitos da personalidade.

Como a intensificação das atividades sociais em rede é síncrona com o desenvolvimento de poderosas ferramentas de busca e quase ilimitada capacidade de armazenamento de dados, grandes desafios são criados para estabelecer o equilíbrio e a proporção entre a autonomia individual e o direito à autodeterminação informacional[3]; e para precisar o conteúdo jurídico do direito à privacidade, dada à necessidade de controle do usuário da internet sobre as suas próprias informações.

Todavia, a arquitetura e o desenvolvimento de novas aplicações móveis dificultam o controle do acervo digital, já que a economia da internet, baseada em serviços oferecidos com suposta gratuidade, cria um modelo de negócios opaco a muitos

---

[2] Entendido na área da psicologia como um comportamento humano comum derivado das atitudes coletivas.

[3] David Lindsey. 'The 'Right to Be Forgotten' in European data protection law. in *Emerging Challenges in Privacy Law: Comparative Perspectives,* Normann Witzlebb *et al.* Cambridge: Cambridge University Press, 2014, pp. 290-337, p. 332.

dos usuários que, cientes ou não, compartilham informações pessoais com uma miríade de outros sujeitos[4]. Nessa realidade, novas ferramentas são desenvolvidas à míngua de uma clara estabilidade dos conteúdos jurídicos nos ambientes virtuais, sob o argumento furtivo do conflito de jurisdições.

Surgem novas modalidades de danos a terceiros, dentre elas a divulgação não autorizada de imagens em aplicativos e *sites* de compartilhamento de conteúdo; criação de perfis falsos em redes sociais virtuais; indexação por provedores de pesquisa de conteúdo em desacordo com as características atuais do indivíduo; criação de página com conteúdo ofensivo a determinada pessoa ou com atribuição de características em desacordo com a atual personalidade do retratado; e a exposição abusiva da imagem de alguém em notícia jornalística ou em quadro de humor. Atreladas ao uso indevido de atributos da personalidade encontram-se também práticas de intimidação e de agressão a terceiros na internet, como o *cyberbullying*.

Ante aos novos fenômenos virtuais, típicos do ciberespaço, a doutrina diverge e se divide em correntes de pensamento. Algumas classificam a internet apenas como um meio para se causar danos já conhecidos e tipificados nas categorias tradicionais, como à honra, ao recato e à respeitabilidade das pessoas. Outras defendem que os fenômenos cibernéticos são peculiares e consubstanciados em formas típicas autônomas de violência, que carecem de regulação específica, aprofundamento científico com suporte na multidisciplinariedade e políticas públicas voltadas ao seu combate.

O conceito ampliado da sociedade de informação revela que o direito à proteção de dados ultrapassa a tutela da privacidade e da autodeterminação informativa, cuidando-se, de tal sorte, de um direito fundamental autônomo, diretamente vinculado à proteção da personalidade.

O fato é que o objeto do direito à proteção de dados pessoais, com base num conceito ampliado de informação, abarca todos os dados que dizem respeito a um determinado sujeito em um contexto dinâmico de interações virtuais, e que a delimitação temática desafia as tradições jurídicas em seu enquadramento. Ainda que existam as categorias de direitos fundamentais, à autodeterminação informacional e da personalidade, podem ser observadas também algumas inovações legislativas específicas quanto a alguns fatos sociais específicos da cibercultura, dentre os quais, leis para o combate ao *doxxing*.

É sob esse contexto que, conforme a teoria dos direitos fundamentais e da personalidade, indaga-se, no presente artigo, se o fato em si, de dados pessoais serem divulgados na internet sem consentimento dos seus titulares – conduta denominada

[4] Åste Corbridge. *Responding to doxing in Australia*: *Towards a right to informational self-determination.* "UniSA Student Law Review", III-3, 2017/2018, pp. 01-28, p. 14.

como *doxxing* –, já fere a mencionada classe de direitos, ou se será preciso que, em decorrência da divulgação, houvesse outros atos mais atentatórios à privacidade e à integridade das vítimas, para que tal conduta seja considerada modalidade de *cyberbullying*. Então, é preciso delimitar se o *doxxing* é um meio para a prática do *cyberbullying,* ou se, por si só, já caracteriza a violência, o *cyberbullying* de fato.

A hipótese de o *doxxing* ser tratado apenas como meio repercute na possibilidade de funções jurídicas de integração, criação e decisão considerarem o ambiente virtual e suas especificidades como circunstâncias judiciais para aplicação das sanções ao caso concreto. Em outra vertente, quando da categorização da espécie como tipo autônomo de violência, há de se reconhecer a fonte material, que inova o ordenamento jurídico, e reclama tratamento legislativo específico, em razão dos princípios e garantias fundamentais, principalmente, do direito penal, enquanto *ultima ratio.*

Neste sentido, é necessário demarcar o conceito de *doxxing* com vistas à realização do Direito ante os problemas prático-sociais propostos pelo recorte do objeto do exame, a proteção da intimidade no ambiente virtual e o direito à autonomia informacional.

Nesse desiderato, a partir de uma perspectiva metodológica de promoção da aplicação do direito em respeito aos valores da dignidade da pessoa humana e das liberdades; e, enfática preocupação com o exercício das funções jurídicas; propõe-se a revisão da bibliografia especializada para a prática jurídica, definições de políticas públicas, pesquisas científicas e programas de prevenção e enfrentamento ao *cyberbullying*, com foco em fomentar a eficácia social dos direitos da personalidade inclusive no ambiente virtual.

Por isso, considerando a importância da perspectiva jurídica, interessa compreender os desafios da sociedade complexa e da Cibercultura, tanto para o aprimoramento do Direito, como para as condições de realização do desenvolvimento humano.

2. Fundamentos normativos da proteção de dados

O reconhecimento de um direito humano fundamental à proteção dos dados pessoais não ocorreu de modo uniforme ao longo das tradições jurídicas[5]. Em sede

[5] No âmbito do direito internacional público, no sistema universal de proteção da ONU, o direito à proteção de dados tem sido extraído principalmente do direito à privacidade, com a exemplo da A/RES/68/167, que dispõe sobre o direito à privacidade na era digital e define os princípios de proteção aos dados pessoais e à privacidade.

de direito internacional público, no sistema universal de proteção da Organização das Nações Unidas e no âmbito do direito europeu, é do direito à privacidade que tem sido deduzido o direito à proteção de dados, embora não constituam sinônimos[6].

O direito à proteção de dados é reconhecido de forma clara e abrangente na Constituição da República Portuguesa[7]. Entretanto, outros países ainda não o reconhecem de forma expressa, embora haja casos em que é possível sustentar a presença desse direito de forma implícita, especialmente com base na teoria estruturante dos direitos fundamentais.

No âmbito das relações privadas em que as atividades virtuais se desenvolvem, não raramente ocorrem conflitos de liberdades e garantias constitucionais. Entram em linha de colisão as garantias de liberdade, igualdade material e intimidade, de um lado; e de outro, as liberdades relacionadas às garantias do discurso e da liberdade de expressão. É possível reconhecer, *prima facie*, a possibilidade dos conflitos de direitos da intimidade com: a) a liberdade de expressão; b) liberdade de imprensa; c) segurança pública e persecução criminal; d) livre iniciativa e exploração de atividade econômica; e, e) liberdade de pesquisa científica.

No Direito Internacional Público é possível se verificar que o direito à proteção de dados tem sido extraído principalmente do direito à privacidade, a partir da relação conflituosa com a liberdade de expressão e a liberdade informacional.

Nesse sentido, podem ser citados como principais marcos regulatórios do direito à proteção de dados pessoais: a) Declaração dos Direitos do Homem e do Cidadão,

---

[6] Ingo Wolfgang Sarlet. "Nesse sentido, a orientação adotada pela Comissão da ONU para Direitos Humanos, interpretando o alcance do artigo 17 do Pacto Internacional de Direitos Civis e Políticos, assim como a jurisprudência da Corte Europeia de Direitos Humanos (CEDH) e do Tribunal de Justiça da União Europeia (TJUE), forte no artigo 8º da Convenção Europeia. Foi somente na Convenção nº 108 para a Proteção de Indivíduos com Respeito ao Processamento Automatizado de Dados Pessoais (1981), comumente intitulada de Convenção de Estrasburgo, bem como, quase vinte anos mais tarde, no artigo 8º da Carta de Direitos Fundamentais da União Europeia (doravante CDFUE), do ano 2000 – que o direito à proteção de dados finalmente alçou a condição de direito fundamental de natureza autônoma, mas vinculando, como tal, apenas os estados integrantes da União Europeia, o que se deu apenas com a entrada em vigor do Tratado de Lisboa, em 2009". *Proteção de dados pessoais: para além da privacidade e autodeterminação informacional*, Revista Consultor Jurídico, 2021. Disponível em: www.conjur.com.br, Consulta feita em: 09 de agosto de 2022.

[7] Portugal. "Artigo 35.º (Utilização da informática) (...) 6. A todos é garantido livre acesso às redes informáticas de uso público, definindo a lei o regime aplicável aos fluxos de dados transfronteiras e as formas adequadas de protecção de dados pessoais e de outros cuja salvaguarda se justifique por razões de interesse nacional". *Constituição da República Portuguesa de 1976* (versão actualizada). Disponível em: pgdlisboa.pt, Consulta em: 9 de agosto de 2022.

1789[8]; b) Declaração Americana dos Direitos e Deveres do Homem, 1948[9]; c) Declaração Universal de Direitos do Homem, 1948[10]; d) Convenção Europeia dos Direitos Humanos, 1950[11]; e) Pacto Internacional dos Direitos Civis e Políticos, 1966[12]; f) Conferência Nórdica sobre o Direito à Intimidade, 1967[13]; g) Pacto de San José da Costa Rica (Convenção Americana sobre Direitos Humanos), 1969.

No contexto normativo europeu, a evolução temática desenvolvida a partir da década de 1950, mais precisamente após a Convenção Europeia dos Direitos Humanos, enfrentou o desafio de estabelecer um equilíbrio entre a proteção da vida privada e a livre circulação de dados pessoais na União Europeia. Os meandros eram consequentemente enfrentados por meio da interpretação ampla do artigo 8º, intitulado "direito ao respeito à vida privada e familiar"[14], na jurisprudência do Tribunal Europeu dos Direitos Humanos.

---

[8] Por força do artigo 11º, instituiu-se que: "a livre comunicação dos pensamentos e das opiniões é um dos mais preciosos direitos do Homem; todo o cidadão pode, portanto, falar, escrever, imprimir livremente, respondendo, todavia, pelos abusos desta liberdade nos termos previstos na Lei.".

[9] A referida Declaração mencionava em seu artigo V que: "toda pessoa tem direito à proteção da lei contra os ataques abusivos a sua honra, a sua reputação e a sua vida privada e familiar".

[10] Também em 1948, aprovada pela Assembleia Geral das Nações Unidas, a Declaração Universal de Direitos do Homem, que enunciava em no artigo 12 que: "Ninguém sofrerá intromissões arbitrárias na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem ataques à sua honra e reputação. Contra tais intromissões ou ataques toda a pessoa tem direito a protecção da lei.".

[11] Instituiu, no artigo 6º, 1, o direito à intimidade, quando da exposição pública por ocasião da persecução criminal, nos seguintes termos: "(...) o acesso à sala de audiências pode ser proibido à imprensa ou ao público durante a totalidade ou parte do processo, quando a bem da moralidade, da ordem pública ou da segurança nacional numa sociedade democrática, quando os interesses de menores ou a protecção da vida privada das partes no processo o exigirem, ou, na medida julgada estritamente necessária pelo tribunal, quando, em circunstâncias especiais, a publicidade pudesse ser prejudicial para os interesses da justiça.".

[12] Determinou em seu artigo 19 que o direito à liberdade de expressão implicará deveres e responsabilidades especiais. Consequentemente, poderá estar sujeito a certas restrições, que devem, entretanto, ser expressamente previstas em lei e que se façam necessárias para assegurar o respeito dos direitos e da reputação das demais pessoas; e proteger a segurança nacional, a ordem, a saúde ou a moral públicas.

[13] Pela primeira vez o tema intimidade foi trabalhado em abrangência internacional e teve repercussão nos diversos sistemas jurídicos sobre os limites da ingerência sobre a vida privada, definindo padrões de ofensas à intimidade.

[14] O dispositivo estabelece que: "1. Qualquer pessoa tem direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência. 2. Não pode haver ingerência da autoridade pública no exercício deste direito senão quando esta ingerência estiver prevista na lei e constituir uma providência que, numa sociedade democrática, seja necessária para a segurança nacional, para a segurança pública, para o bem-estar económico do país, a defesa da ordem e a prevenção das infracções penais, a protecção da saúde ou da moral, ou a protecção dos direitos e das liberdades de terceiros.".

A Corte Europeia compreende que o artigo 8° da Convenção para a Proteção dos Direitos Humanos, em um sentido amplo, protege o desenvolvimento individual do ser humano. Por isso, essa garantia não elimina o reconhecimento da dimensão relacional da pessoa natural, principalmente porque essa corte considera que o indivíduo estabelece e desenvolve relações com outros seres humanos e com o mundo exterior, devendo ser tutelada sua vida privada, familiar, seu domicílio e sua correspondência.

Outros documentos também devem ser destacados, como: a) Convenção para a Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados de Carácter Pessoal, 1981[15]; b) Diretiva 95/46/CE, 1995[16]; c) Carta de Direitos Fundamentais da União Europeia, 2000[17]; e d) Regulamento UE de 2016/679[18], 2016.

Este último, mais conhecido como Regulamento Geral sobre a Proteção de Dados, demonstra um esforço para a adoção de um ato legislativo único, no intuito de combater a fragmentação resultante da coexistência de sistemas nacionais diferentes e com encargos administrativos desnecessários. Trata da proteção das pessoas singulares, no que diz respeito ao tratamento de dados pessoais e à livre circulação desses; e é medida essencial para reforçar os direitos fundamentais das pessoas na era digital.

As regras, todavia, não se aplicam ao tratamento de dados por motivos exclusivamente pessoais ou no exercício de atividades domésticas. O que pode representar lacunas na concretização do direito à proteção de dados quando do enfrentamento de conflitos na esfera privada, como acontece nos casos de uso de informações pessoais por um particular para causar danos à terceiro. Restando o tema a ser tratado nos contornos internos das jurisdições dos países integrantes da União Europeia.

No caso do Brasil, apesar de uma proteção constitucional explícita à intimidade e à vida privada, a proteção de dados pessoais no ambiente virtual foi densificada pela atuação

---

[15] Parte da necessidade de conciliar os valores fundamentais do respeito pela vida privada e da livre circulação de informação entre os povos.

[16] Institui um quadro regulamentar a fim de estabelecer um equilíbrio entre um nível elevado de proteção da vida privada das pessoas e a livre circulação de dados pessoais no interior da União Europeia. Para este efeito, fixou limites estritos à recolha e à utilização de dados pessoais e solicita a criação, em cada Estado-Membro, de um organismo nacional independente encarregado do controle de todas as atividades relacionadas com o tratamento de dados pessoais.

[17] Merece especial atenção o artigo 8°, intitulado "Protecção de dados pessoais", o qual dispõe que: "1. Todas as pessoas têm direito à protecção dos dados de carácter pessoal que lhes digam respeito. 2. Esses dados devem ser objecto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei. Todas as pessoas têm o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respectiva rectificação. 3. O cumprimento destas regras fica sujeito a fiscalização por parte de uma autoridade independente".

[18] É o Regulamento Geral sobre a Proteção de Dados, do Parlamento Europeu e do Conselho de 27 de abril de 2016.

legislativa infraconstitucional. Inicialmente, com a edição da Lei 12.965 de 2014, ao estabelecer princípios, garantias, direitos e deveres para o uso da internet no Brasil.

Com forte inspiração no Regulamento Geral sobre a Proteção de Dados, o legislativo brasileiro editou a Lei nº 13.709 de 2018, a Lei Geral de Proteção de Dados Pessoais – LGPD, que tem como um dos seus objetivos proteger os direitos e liberdades fundamentais, em particular o direito à proteção de seus dados pessoais, ao assegurar o respeito à privacidade e garantir a propriedade de cada indivíduo sobre suas próprias informações. Desta forma, cumpre sublinhar, que tanto o Regulamento Geral, quanto a LGPD têm âmbito de aplicação voltado à atividade de tratamento que tenha por objetivo a oferta ou o fornecimento de bens ou serviços.

Apenas recentemente, a Constituição da República Federativa do Brasil foi alterada por meio da Emenda Constitucional nº 115, de 2022, que acresceu um inciso LXXIX ao artigo 5º, dispondo que "é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais".

O *status* constitucional da proteção aos dados pessoais garante efeitos positivos substanciais em relação ao atual estado da arte nos países que os reconhecem, posto que, embora possíveis as interseções e articulações com outros direitos, fica assegurada à proteção de dados a condição de direito fundamental autônomo, com âmbito de proteção próprio. Ademais, ao direito à proteção de dados passa a ser atribuído de modo inquestionável o pleno regime jurídico-constitucional, relativo ao seu perfil de direito fundamental em sentido material e formal.

Dentre os principais aspectos do reconhecimento de um direito fundamental autônomo à proteção de dados, destaca-se o fato de que as normas relativas ao direito à proteção de dados são dotadas de aplicabilidade imediata e vinculam diretamente todos os atores públicos, bem como privados, em razão de sua eficácia horizontal.

Ademais, ante a existência de uma série de lacunas regulatórias; já que a LGPD não contempla os setores da segurança nacional e pública, investigação criminal e execução penal; tal dispositivo mostra-se particularmente relevante. Além de passar a ser um direito com uma expressa reserva legal simples, possibilitando que legisladores infraconstitucionais estabeleçam intervenções restritivas no âmbito de proteção do direito, ao tempo em que se obriga a observar as exigências da reserva de lei[19].

Quando o direito à proteção de dados passa a integrar a categoria de direito e garantia fundamental, a compreensão do seu conteúdo jurídico e as formas de interpretação e aplicação devem ser entendidas de forma ampla e sistemática.

---

[19] Ingo Wolfgang Sarlet. *Proteção de dados pessoais: para além da privacidade e autodeterminação informacional*, Revista Consultor Jurídico, 2021. Disponível em: www.conjur.com.br, Consulta feita em: 9 de agosto de 2022.

O direito em questão deve ser analisado em cotejo com outros princípios, garantias e direitos fundamentais, a ponto de definir qual é o seu real âmbito de proteção e quais são os seus limites.

Dentre os conflitos emergentes, a liberdade de expressão é a principal zona de colidência, e a ponderação de valores essenciais é feita em grande medida por meio de atividades legislativas no âmbito infraconstitucional.

Diferentemente do que ocorre no Brasil e em muitos países da Europa, que garantem a proteção da privacidade por motivação essencial da defesa da dignidade da pessoa humana, nos Estados Unidos o fundamento axial das tutelas é a liberdade individual.

A privacidade nos Estados Unidos é protegida através de um ordenamento de direitos que funciona como uma "colcha de retalhos"[20], através do sistema jurídico do *common law*, do reconhecimento na Constituição de aspectos da personalidade de forma expressa[21] e, implicitamente, pela formulação de uma cláusula geral baseada na liberdade, leis federais, leis estaduais e as constituições de alguns estados.

As previsões sobre a privacidade existem na interpretação integrativa e criativa do sistema do *common law,* na Constituição Federal e dos estados, além de uma variedade de estatutos que versam sobre questões específicas referentes a setores e jurisdições específicas[22]. Em comparação com outros sistemas legais, a construção norte-americana

---

[20] A associação é feita por Steffano Scoglio. *Transforming privacy: a transpersonal philosophy of rights.* Westport: Praeger Publishers, 1976, p. 102.

[21] A Constituição dos Estados Unidos não contém previsão expressa do direito à privacidade. A Carta de Direitos e Liberdades, todavia, albergou as preocupações dos constituintes – principalmente James Madison – quanto a proteção de alguns e específicos aspectos da privacidade, como o direito à liberdade de crença (Primeira Emenda); a privacidade da residência contra a passagem não autorizada de soldados durante os tempos de paz (Terceira Emenda); o direito do povo à inviolabilidade de suas pessoas, casas, papéis e haveres contra busca e apreensão arbitrárias (Quarta Emenda); além da proteção contra a própria incriminação (Quinta Emenda), o que protege em essência as informações íntimas do sujeito.

[22] Como exemplo, vide *The Children's on-line Privacy Protection Act of 1998* – COPPA, lei criada para a proteção das informações dos menores da obtenção abusiva e uso ilegítimo para finalidades comerciais. A lei criou a obrigação de que os domínios eletrônicos construídos para os menores devem buscar informar a finalidade comercial e buscar consentimento dos pais ou responsáveis para a obtenção dos dados do menor. Em estudo comparado, Valentina Vicenza Cuocci aduz que apesar de existir a tutela específica dos menores nos Estados Unidos, não se pode constatar, em relação à normativa federal, COPPA, tratamento voltado para considerar os menores como sujeitos vulneráveis no ambiente virtual. Recentemente, todavia, é possível constatar tutela específica a nível estadual, a exemplo da que existe na Califórnia, onde há normativas como o CCPA, *California Consumer Privacy Act,* largamente inspiradas no RGPD. As regulações estaduais adotam técnicas de proteção e tratamento diverso em relação aos dados dos menores no ambiente virtual, ao proibirem expressamente a venda desses dados, ainda que tenham sido compartilhados pelos próprios titulares. *Vulnerabilità, dati personali e mitigaion measures. Oltre la protezioni dei minori,* "Revista da Faculdade de Direito da Universidade de Lisboa – Lisbon Law Review", LXII, 2021, pp. 963-990, pp. 973-975.

para a proteção da privacidade numa perspectiva individual e intersubjetiva é algo imprevisível. Como consequência, é difícil a articulação de teorias legais sobre o respeito à vida privada do sujeito de direitos, especialmente, no ambiente virtual.

Como a eficácia social do direito fundamental à proteção de dados e do direito à autodeterminação informacional requerem que a proteção seja estendida ao âmbito virtual, é importante analisar o atual estado da arte, no qual os fatos sociais no ambiente on-line são caracterizados pelo ineditismo, riscos imensuráveis e difícil descrição técnica[23].

É justamente sob esse viés de efetivação dos direitos de proteção de dados pessoais e de observância aos ditames da segurança jurídica, que ganha especial relevância a discussão sobre a exposição de dados pessoais no ambiente virtual como forma de se atingir a dignidade da pessoa humana.

3. *Cyberbullying* por divulgação de dados pessoais

Para compreender o fenômeno social do *cyberbullying* por divulgação de dados pessoais é necessário considerar a existência de uma tríade conceitual[24] composta pelo *bullying,* cibercultura e o *cyberbullying* propriamente dito.

Bullying pode ser compreendido como uma subcategoria do comportamento agressivo que ocorre entre pares, quando no relacionamento interpessoal há um desequilíbrio de forças e o alvo da agressão percebe-se física ou mentalmente vulnerável à vista do perpetrador.

No *bullying* existe a intenção de prejudicar e/ou humilhar, e tal comportamento, que pode ocorrer de várias maneiras, persiste por certo tempo. A duração deve-se à manutenção do poder exercido sobre a vítima, seja pela diferença de idade, força ou gênero. Existem três elementos cruciais que caracterizam o *bullying*: a repetição, o prejuízo e a desigualdade de poder[25].

A tutela inibitória do *bullying* encontra base jurídica na inviolabilidade da dignidade da pessoa humana, na proteção dos direitos da personalidade, especialmente dos direitos à intimidade, honra, imagem e integridade, e na promoção da igualdade e segurança.

---

[23] Simone Fischer-Hübner *et al. Online Privacy: Towards Informational Self-Determination on the Internet, "*Dagstuhl Manifestos", I-1, 2011, pp. 1-20, pp. 3-4.

[24] Luzia de Oliveira Pinheiro. *Cyberbullying em Portugal*: uma perspectiva sociológica. Braga, Universidade do Minho, 2009, p. 12.

[25] Cláudia de Moraes Bandeira / Claudio Simon Hutz. *Bullying: prevalência, implicações e diferenças entre os gêneros*, "Revista Semestral da Associação Brasileira de Psicologia Escolar e Educacional", Vol. XVI-1, Janeiro/Junho de 2012, pp. 35-44, p. 36. Disponível em: www.scielo.br, Consulta feita em: 11 de julho de 2022.

Já a cibercultura é entendida como um neologismo que representa o momento atual da cultura, pautada na utilização de novas tecnologias, que promove a compreensão de que, cada vez mais, a população habita em uma aldeia global, onde fatores sociais, econômicos, políticos e culturais estão interligados. A informação torna-se, nesse cenário, "um elemento estratégico decisivo da evolução social e fator com capacidade determinante do comportamento dos indivíduos". É nesse sentido que é preferível falar em 'sociedade da comunicação', ao invés de 'sociedade da informação', já que a pretensão é de impulsionar a comunicação, e apenas em um sentido amplo se pode entender que toda mensagem é informação[26].

Ao se qualificar a sociedade como da comunicação, o fluxo de mensagens compartilhadas sobre o indivíduo passa a ter um enfoque especial, já que a comunicação pode ser determinante para o posicionamento do sujeito na sociedade. Na cibercultura, o *bullying* pode ser praticado justamente por meio do compartilhamento de informações pessoais na internet, ou seja, *cyberbullying*.

É possível afirmar que o termo *cyberbullying* é polissêmico[27], mas merece destaque a definição técnica proposta pelo Fundo das Nações Unidas para a Infância – UNICEF, segundo o qual ele é o *bullying* realizado por meio das tecnologias digitais e pode ocorrer nas mídias sociais, plataformas de mensagens, jogos e celulares[28]. As características do *cyberbullying;* incluídas sua definição, riscos associados, índices de prevalência, fatores de risco e proteção, e estratégias de enfrentamento, ainda que relacionadas ao *bullying;* guardam aspectos que lhe são únicos e que permitem uma diferenciação metodológica[29].

O comportamento em âmbito virtual, exercido de modo repetido, com intuito de assustar, enfurecer ou envergonhar as vítimas[30], faz com que os seus efeitos possam ser duradouros e afetem as pessoas mentalmente, emocionalmente e

---

[26] José de Oliveira Ascensão. *Sociedade da Informação e mundo globalizado*, "Boletim da Faculdade de Direito da Universidade de Coimbra, *Studia Juridica"*, LXIII, Coimbra: Editora Coimbra, 2003, pp. 163-179, p. 167.

[27] Taiza Ramos Ferreira / Suely Ferreira Deslandes. *Cyberbullying: conceituações, dinâmicas, personagens e implicações à saúde*, "Ciência & Saúde Coletiva", volume 23, n°. 10, 2018, pp. 3369-3379, p. 3372. Disponível em: www.scielo.br, Consulta feita em: 12/07/2022.

[28] Mario Viola de Azevedo Cunha. *Child Privacy in the Age of Web 2.0 and 3.0: Challenges and opportunities for policy.* "Innocenti Discussion Papers", 2017, pp. 1-23, p. 9.

[29] Nadia S. Ansary. *Cyberbullying: Concepts, theories, and correlates informing evidence-based best practices for prevention,* "Aggression and Violent Behavior", L, 2020, pp. 1359-1789, pp. 1363-1364. Disponível em: www.sciencedirect.com/, Consulta feita em: 15/07/2022.

[30] Mariya Stoilova / Sonia Livingstone / Rana Khazbak. *Investigating Risks and Opportunities for Children in a Digital World: A rapid review of the evidence on children's internet use and outcomes,* "Innocenti Discussion Papers" no. 2020-3, 2021, pp. 01-81, p. 34.

fisicamente. Ainda que seja possível identificar, nas condutas, uma intersecção em termos de direitos da personalidade violados, a proporção e a velocidade da expansão do dano em ambiente virtual tendem a ser maiores.

A ubiquidade tecnológica na vida cotidiana, em especial nos grupos etários mais jovens, revela a possibilidade de o indivíduo ser vítima de danos ininterruptamente (24 horas ao dia), em razão da exposição de suas informações pessoais e dados sensíveis na internet. O fato de que os agentes causadores do dano muitas vezes se protegem no anonimato e têm a percepção de que dificilmente serão punidos, realça preocupações objetivas, demonstradas por maiores taxas de associação de psicopatologias ao *cyberbullying,* em comparação com o *bullying* tradicionalmente descrito[31], o que pode ser confirmado por pesquisas quantitativas[32] de referência.

Nesse sentido, a proteção dos dados pessoais, que "tem sido compreendida como o direito de o indivíduo autodeterminar as suas informações pessoais: autodeterminação informacional"[33] ganha especial relevância na sociedade tecnológica. O reconhecimento de um direito humano fundamental à proteção dos dados pessoais, contudo, é disforme ao longo das tradições jurídicas.

À exceção dos exemplos da Constituição da República Portuguesa de 1976 e Espanhola de 1978, outros países ainda não reconhecem o direito à proteção de dados de forma clara e abrangente. No Brasil, a Lei 13.709 de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD), é a que mais se aproxima de um regramento mais aprofundado sobre o tema. O dispositivo teve sua redação alterada pela Lei 13.853, de 8 de julho de 2019 e entrou em vigor em 18 de setembro de 2020.

Note-se que ainda existem Estados onde o direito fundamental à proteção de dados não é expressamente positivado em suas constituições. Muito embora, em alguns casos, tal direito seja tido como implicitamente positivado, sem prejuízo de uma maior ou menor regulação legislativa e administrativa, além de significativo desenvolvimento na esfera jurisprudencial.

---

[31] Nadia S. Ansary. *Cyberbullying* cit. (nt. 29), pp. 1364-1366.

[32] Sobre os estudos quantitativos, ver: Evelina Landstedt / Susanne Persson. *Bullying, cyberbullying, and mental health in young people*, "Scandinavian journal of public health", XLII-4, 2014, pp. 393-399, pp. 394-395. Sara Mota Borges Bottino *et al. Cyberbullying and adolescent mental health: systematic review.* "Cadernos de Saúde Pública", XXXI-3, 2015, pp. 463-475, pp. 467-470. Disponível em: www.scielo.br, Consulta feita em: 12/07/2022.

[33] Bruno Ricardo Bioni. *Proteção de dados pessoais: a função e os limites do consentimento*. Rio de Janeiro: Forense, 2020, p. XXVII.

A proteção de dados pessoais é respaldada pelos princípios e direitos fundamentais de caráter geral e especial, como é o caso do princípio da dignidade da pessoa humana, do direito fundamental ao livre desenvolvimento da personalidade, direito geral de liberdade e direitos especiais de personalidade mais relevantes no contexto, quais sejam, os direitos à privacidade e intimidade e, com particular ênfase, à autodeterminação informativa[34].

Como a eficácia social da autodeterminação informacional requer que a proteção seja estendida ao âmbito virtual, é importante analisar se a exposição não consentida de informações pessoais em tal meio é suficiente para caracterizar uma modalidade de *cyberbullying*.

4. Delimitação conceitual de *doxxing*

Na seara da discussão acerca do *cyberbullying* e suas modalidades, mostra-se relevante um neologismo norte-americano, típico da cultura *hacker* da década de 1990. *Doxing* (ou, *doxxing*) deriva da expressão linguística coloquial *dropping dox (documents),* e significa o ato de revelar a identidade de quem atuava sob anonimato[35].

Na atualidade, o termo tem aplicação ampla e é empregado para descrever um conjunto de atos que expõe informações pessoais na internet sem o consentimento da vítima, usualmente com intenções maliciosas de causar danos à pessoa e/ou ao patrimônio. A conduta é retratada como o uso abusivo de informações pessoais e sensíveis do sujeito e seu compartilhamento com terceiros, com a finalidade de causar dano, perturbação ou obter vantagem indevida.

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. A abrangência do termo "informações pessoais" é ampla e engloba o nome, endereço residencial e profissional, telefone, informações financeiras e bancárias, fotos e vídeos, histórico criminal, correspondências privadas, dados de saúde e outros[36].

---

[34] Ingo Wolfgang Sarlet. *Proteção de dados pessoais como direito fundamental na Constituição Federal brasileira de 1988: Contributo para a construção de uma dogmática constitucionalmente adequada*, "Revista Brasileira De Direitos Fundamentais & Justiça", XVI-42, pp.179-218, p. 188.
[35] David M Douglas. *Doxing: a conceptual analysis*, "Ethics and Information Technology", XVIII-3, 2016, pp. 199-210, p. 200.
[36] Noah Berlatsky. *Doxing isn't about privacy*: *it's about abuse*, "Daily Dot", 2016. Disponível em: www.dailydot.com/, Consulta feita em: 11 de julho de 2022.

As ações invasivas para atacar as pessoas via *doxxing* incluem: a) rastreamento de nome de usuário; b) *phishing*; c) *stalking* em redes sociais; d) rastreamento de endereços IP; e) *packet sniffing*; f) uso de *data brokers;* entre outras. O rastreamento de nomes de usuários possibilita ter uma noção clara dos interesses do sujeito-alvo, saber como ele passa o tempo na internet, quais conteúdos chamam sua atenção, além da extração de informações que compõem o seu perfil sociopolítico e econômico.

Por meio do *phishing,* a atenção do usuário é atraída por um conteúdo malicioso que lhe é atrativo, e que, ao ser acessado, permite ao *hacker* obter acesso às informações, dispositivos eletrônicos, dados importantes e senhas do usuário.

No *stalking* cibernético o agente reiteradamente persegue, vigia e mapeia as informações disponibilizadas pelo próprio sujeito-alvo, com o objetivo de descobrir aspectos de sua personalidade, como: preferências, hábitos de vida, constituição familiar, local de residência e de trabalho.

Por meio da engenharia social, é possível que a localização do sujeito-alvo seja revelada via rastreamento do endereço de IP. O termo *packet sniffing* concerne à interceptação, por parte dos criminosos, dos dados móveis na internet; é uma busca por todos os tipos de dados, incluindo senhas, números de telefone, informações de conta bancária e mensagens de e-mail. É uma intervenção por meio da violação das medidas de segurança, o que permite a captura do fluxo de dados dentro e fora da rede.

Já *data brokers,* também conhecidos como agentes de informações, são os sujeitos maliciosos especializados na coleta, armazenamento e venda de dados pessoais. Eles coletam tais informações e elaboram pacotes de dados que são vendidos a terceiros.

Desse modo, o *doxxing* pode representar ataques de reduzida relevância, como o envio de e-mails ou *delivery* de produtos não solicitados; ou ameaças de grandes proporções como, por exemplo, quando destinado a enviar as informações indevidamente coletadas para membros da família ou empregadores.

Tal divulgação de informações pessoais de modo indevido pode resultar em *cyberbullying,* quando causar um destacado constrangimento, ou até mesmo implicar em violações físicas à pessoa. Independentemente da motivação, seu principal objetivo é violar a privacidade, e isso pode colocar as pessoas em uma situação desconfortável, o que, algumas vezes, pode ter consequências graves.

5. Espécies de *doxxing*

A partir de uma análise conceitual, David Douglas[37] faz a distinção de três formas de *doxxing*, a) por desanonimização; *b)* por segmentação; *e, c)* por desmoralização. Cada uma delas definida de acordo com o bem jurídico lesado, quais sejam o anonimato, o "direito a ser deixado de lado" e a reputação, respectivamente.

5.1 *Doxxing* por desanonimização

As condutas de desanonimização visam expor a pessoa que tem o direito e/ou a intenção de se manter no anonimato, ou ter sua privacidade protegida por meio de um pseudônimo. O uso das tecnologias e o acesso aos dados sensíveis por meio de expedientes lícitos ou ilícitos ganharam destaque nos últimos anos. A exposição da identidade pode não ser relevante, em alguns casos se mostrar irreversível, ou até mesmo justificada pelo interesse público, como ocorre nos casos em que um sujeito faz uso de um pseudônimo para causar danos a terceiros, para fins de obtenção de vantagens econômicas ou prestígio pessoal.

Para fins de exemplificação, destaca-se o caso da escritora Elena Ferrante, o qual, no ano de 2016, ganhou atenção com as afirmações de que o jornalista investigativo Claudio Gatti havia descoberto sua identidade e endereço, divulgando-os em múltiplos veículos de imprensa[38]. A descoberta pautou-se no vazamento das contas bancárias da editora *Edizione* e do rastreamento da compra de várias propriedades na Itália, que o levaram a concluir que, por trás do pseudônimo literário mais citado no século XXI, estava a tradutora Anita Raja[39], esposa do escritor Domenico Starnone. Sob o argumento do direito à informação e liberdade de imprensa, a privacidade e a autodeterminação informacional da Elena Ferrante foram violadas.

Também se configurou *doxxing* por desanonimização a divulgação da identidade do criador das criptomoedas[40], ocorrida em 2014, no noticiário *Newsweek*.

---

[37] D. M. Douglas. *Doxing*, cit. (nt. 35), p. 203.

[38] No "Il Sole 24 Ore, Frankfurter Allgemeine Zeitung", "The New York Review of Books" e no site de notícias francês "Mediapart".

[39] Para maiores detalhamentos, conferir: Andrea Aguilar. "*A verdade sobre o caso Elena Ferrante*". El País, 2016. Disponível em https://brasil.elpais.com/, Consulta feita em 12/07/2022. Justificativas alegadas para o vazamento de dados encontram-se em: Katherine Angel / Claudio Gatti. *Why uncover the identity of author Elena Ferrante?*, BBC News. Disponível em www.bbc.com/news/, Consulta feita em 12/07/2022.

[40] Leah McGrath Goodman. "This is the guy who created Bitcoin? It looks like he's living a pretty humble life. I'd come here to try to find out more about Nakamoto and his humble life. It

5.2 *Doxxing* por segmentação

Em sentido lexical, a segmentação pode significar o ato de fazer de algo ou alguém, singularmente ou em conjunto, um alvo a ser atacado, capturado ou destruído[41]. As condutas de *doxxing* de segmentação física consistem na exposição de dados pessoais que permitem o acesso à localização do domicílio do indivíduo, seja residencial ou laboral, bem como a identificação de locais que a vítima costuma frequentar ou possa ser encontrada por terceiros. Ao revelar tais informações, ainda que não seja essa a intenção, o agente agrava as chances da vítima ser alvo de assédio e outras formas de perseguição e violência.

Não há justificativa para a conduta de permitir a violação de direitos da pessoa exposta, por se tratar de ação com evidente perigo em abstrato. Desta feita, a finalidade específica de causar dano não é elemento essencial para a sua configuração; mesmo não desejando causar mal ao sujeito, ao ter sua localização revelada, terceiros podem fazer uso da informação para perseguir seus próprios desideratos.

A forma de expor a informação certamente deve ser considerada no cotejo analítico dos fatos, no intuito de verificar se, no contexto da divulgação, há o estímulo para que terceiros persigam a vítima. Como ocorreu, segundo relato do caso, do site "arquivos de Nuremberg" (*Nuremberg Files*)[42], através do qual, na década de 1990, foi realizada a divulgação de nomes, endereços pessoais e profissionais,

---

seemed ludicrous that the man credited with inventing Bitcoin – the world's most wildly successful digital currency, with transactions of nearly $500 million a day at its peak – would retreat to Los Angeles's San Gabriel foothills, hole up in the family home and leave his estimated $400 million of Bitcoin riches untouched. It seemed similarly implausible that Nakamoto's first response to my knocking at his door would be to call the cops. Now face to face, with two police officers as witnesses, Nakamoto's responses to my questions about Bitcoin were careful but revealing.". *The Face Behind Bitcoin*, Newsweek Magazine, 2014. Disponível em: www.newsweek.com, Consulta feita em 14/07/2022.

[41] Definição de *targeting* do Dicionário Collins: "1. Military: the act of deciding to attack a particular point, area, or person physically; 2. the act of attempting to appeal to a person or group or to influence them in some way 3. the act of directing or aiming something at a particular group of people".

[42] Eric Silverberg *et al.* «Over 200 doctors opened their suit against a website called the "Nuremberg Files.". The site provided detailed personal information about doctors who provide abortions amidst images of dripping blood and aborted fetuses, and calls for "justice.". The plaintiffs contended that the site constituted a threat to the safety of the listed individuals and their families. The site owners claimed that the site's purpose was to provide information and not to incite violence. The jury found for the plaintiffs and awarded over one hundred million dollars in damages». *The Nuremberg Files*. Stanford. Disponível em: https://cs.stanford.edu/people/eroberts/, Consulta feita em: 15/07/2022.

fotos, antecedentes criminais e históricos de processos a que respondiam, dos profissionais que realizavam abortamentos nos Estado Unidos. O *doxxing* de segmentação foi realizado com finalidade clara de intimidação, mesmo porque, nas listas expostas, figuravam também informações de familiares.

Cumpre também destacar que, mesmo que algumas das informações pessoais já sejam de domínio público, elas não podem ser divulgadas em um contexto que incite a perturbação, assédio, violência emocional e ódio. Ademais, é um tipo de violação geralmente relacionada a outra modalidade de *doxxing*, o ato de desanonimizar o sujeito. Essa realidade pode ser verificada uma vez que, por vezes, a intenção de constituir um pseudônimo ou operar em anonimato é justificada com base na vontade de não ser perturbado fisicamente em espaços públicos e, fundamentalmente, privados. Assim, as duas classificações, em muitos casos, podem ser aplicadas simultaneamente.

5.3 *Doxxing* por desmoralização

Essa terceira categoria envolve a conduta de revelar informações pessoais com a intenção de causar abalos na autoestima, reputação e credibilidade do indivíduo. Seu objetivo é a intimidação ou humilhação da vítima, revelando fatos que desabonem a sua respeitabilidade

Registros médicos, históricos de buscas e navegação na internet e a sexualidade são aspectos frequentemente utilizados para perpetrar ataques à honra das vítimas, principalmente por serem dados sensíveis, que, quando expostos, tem o grande potencial de intimidar, causando fortes abalos emocionais. A exemplo dos casos de pornografia de revanche, que, por vezes, são associados à exposição segmentária com a divulgação de informações pessoais das vítimas, para a promoção de ataques perpetrados por terceiros.

Um caso relevante que ilustra o *doxxing* por desmoralização é o da revelação da identidade de um dentista de Minnesota (EUA), que ilegalmente caçou e matou um leão que vivia em um reserva protegida do Zimbábue. A estratégia utilizada por alguns foi a de desqualificar o profissional em suas redes profissionais (no *website* YELP, por exemplo), expondo o fato da caça ilegal, mas também inserindo falsas avaliações negativas sobre seus serviços profissionais[43].

[43] Megan Condis. "The story of Walter Palmer, the Minnesota dentist who poached the beloved, human-friendly lion named Cecil in Zimbabwe, is going viral. Outraged animal lovers have been making their displeasure over what appears to have been an illegal and unethical hunt known online. Some have found productive and clever ways to register their protest, from deluging the Yelp page

6. Categorização de *doxxing*: violação de privacidade ou forma de prática de violência

No desiderato de promover a tutela adequada e a proteção suficiente dos bens jurídicos, algumas inovações legislativas são pautadas em fatos virtuais específicos, como é o caso das recentes leis que tratam particularmente da prática de *doxxing* para garantia da proteção dos dados pessoais e/ou à privacidade, com é o caso da Austrália[44], Hong Kong[45] e alguns estados norte-americanos, como Califórnia[46], Colorado[47], Oregon[48], Connecticut[49] e Nevada[50].

---

for Palmer's dentistry practice with negative reviews to raising awareness on Twitter through hashtags ranging in tone from earnest and heartfelt". *Cecil the Lion's hunter becomes the hunted*: *Online activists must reject doxxing terror tactics.* Aljazeera America, 2015, Disponível em: http://america.aljazeera.com, Consulta feita em: 13/07/2022.

[44] Sobre a atividade legislativa australiana, ver: Online Safety Bill 2021, aprovada nas duas casas legislativas em 23 Junho 2021: "Summary: Introduced with the Online Safety (Transitional Provisions and Consequential Amendments) Bill 2021, the bill: retains and replicates certain provisions in the Enhancing Online Safety Act 2015, including the non-consensual sharing of intimate images scheme; specifies basic online safety expectations; establishes an online content scheme for the removal of certain material; creates a complaints-based removal notice scheme for cyber-abuse being perpetrated against an Australian adult; broadens the cyber-bullying scheme to capture harms occurring on services other than social media; reduces the timeframe for service providers to respond to a removal notice from the eSafety Commissioner; brings providers of app distribution services and internet search engine services into the remit of the new online content scheme; and establishes a power for the eSafety Commissioner to request or require internet service providers to disable access to material depicting, promoting, inciting or instructing in abhorrent violent conduct for time-limited periods in crisis situations". Conferir também, Social Media (Anti-Trolling) Bill 2022, ainda em tramitação: "Summary: Establishes a framework relating to potentially defamatory content posted on social media by: deeming a person who administers or maintains a social media page not to be a publisher of third-party material; deeming a social media service provider to be the publisher of material that is published on their service if it is posted in Australia; creating a conditional defence for social media service providers in defamation proceedings relating to material on their service that is posted in Australia if the provider meets certain conditions; empowering courts to issue end-user information disclosure orders to require providers of social media services to give the applicant relevant contact details and country location data in certain circumstances; requiring social media companies to have a nominated entity incorporated in Australia able to discharge certain key obligations; and enabling the Attorney-General to intervene in defamation proceedings on behalf of the Commonwealth and authorise a grant of legal assistance".

[45] Cabe referir previsão legislativa de Hong Kong: "the Personal Data (Privacy) Ordinance (Cap. 486) (PDPO)".

[46] Vale conferir a legislação californiana sobre o tema: California Penal Code, Section 653.2.

[47] Verificar as normativas do estado de Oregon: HB22-1041, aprovada em 24 de março de 2022: "The bill adds child representatives, code enforcement officers, health-care workers, mortgage servicers, and office of the respondent parents' counsel staff members and contractors to the list of

As referidas leis apresentam, principalmente, três abordagens de categorização, a primeira pela criminalização da conduta, a segunda pela proteção de certos grupos na sociedade, a exemplo dos profissionais de saúde, e a terceira pela responsabilidade civil dos agentes que praticam *doxxing*.

Apesar da escassez de trabalhos científicos sobre a delimitação conceitual e enquadramento tipológico formal e material da prática da conduta descrita como *doxxing*, alguns esforços já são notados. Os limites de significados atribuídos à expressão permitem que tal crime seja categorizado, principalmente, como uma violação de privacidade[51], ou forma técnica de prática de violência[52], embora os estudos divirjam quanto às possibilidades de tutela em casos de prática do *cyber-bullying*.

David M. Douglas[53] afirma que o meio não deve ser interpretado e confundido como a própria finalidade da conduta. *Doxxing,* portanto, não é sinônimo de chantagem, difamação ou extorsão, e pode apenas representar a técnica utilizada para essa finalidade.

Todavia, McIntyre diverge sobre a categorização do *doxxing* apenas como um meio de violência contra a vítima. No contexto norte-americano, a autora critica

---

protected ersons whose personal information may be withheld from the internet if the protected person believes dissemination of such information poses an imminent and serious threat to the protected person or the safety of the protected person's immediate family. The bill adds a protected person's full name and home address to the list of personal information that the protected person's written request for removal must include. The bill authorizes access to records maintained by a county recorder, county assessor, or county treasurer for certain individuals if such access is related to a real estate matter".

[48] Ainda em relação à Oregon, ver: House Bill 3047. "Establishes civil cause of action for improper disclosure of personal information".

[49] No tocante ao estado de Connecticut, conferir: Substitute for Raised S.B. No. 989: "An Act Concerning Online Harassment. To combat online harassment, including that motivated by hate, by (1) extending the crime of stalking in the first degree to specifically include certain hate-based motivations, (2) extending the crime of second-degree stalking to include certain electronic disclosures of personal identifiable information without consent and establishing a civil action for victims of such crime, and (3) extending the crime of second-degree harassment to include more electronic forms of communication".

[50] Sobre a atividade legislativa no estado de Nevada, ver: AB296: "Summary: establishes a civil cause of action for the dissemination of personal identifying information or sensitive information under certain circumstances. (BDR 3-121)".

[51] A. Corbridge. *Responding to doxing in Australia* cit. (nt. 4), p. 21.

[52] Victoria. McIntyre. *Do (x) you really want to hurt me: Adapting IIED as a solution to doxing by reshaping intente*, "Tulane Journal of Technology & Intellectual Property", XIX, 2016, pp. 111-134, p. 124-125.

[53] David M Douglas. *Doxing*, cit. (nt. 35), p. 202.

o entendimento de que a conduta só pode ser punida como uma forma de facilitação da perseguição (*stalking*), que, em alguns estados, apenas é punida quando cometida diretamente contra a vítima, e que muitos precedentes ainda dão prevalência ao direito à liberdade de expressão, quando do cotejo analítico.

Ela ainda sustenta que, apesar da perturbação ser, historicamente, um evento que afeta diretamente a vítima, o *doxxing* é caracterizado por ser uma lesão que afeta direta e tacitamente, por combinar riscos atuais e futuros de violação da privacidade. Diante disso, McIntyre[54] propõe uma crítica ao sistema de responsabilidades e tutelas jurídicas sobre a necessária diferenciação dos danos *offline* e *online*.

Seus limites são necessários para que, numa sociedade democrática, preserve-se a segurança pública, integridade territorial, defesa da ordem, prevenção do crime, proteção da saúde ou da moral, e proteção da honra ou dos direitos de outrem, no intuito de impedir a divulgação de informações confidenciais ou para garantir a autoridade e imparcialidade do poder judicial.

A categorização do *doxxing* demanda a exata compreensão do espaço em que os problemas que envolvem a privacidade virtual ocorrem, já que os perfis virtuais devem ser tratados essencialmente como ambientes privados, ou, ao menos, esferas de acesso limitado[55]. Sendo, portanto, a sua invasão considerada causa para as ações inibitórias, reparatórias e compensatórias de danos decorrentes da violação de privacidade. O *cyberbullying* praticado por meio da divulgação de informações pessoais tem, no *doxxing*, a oportunidade de revisão dos conceitos e definições tradicionais de violação de direitos de privacidade, liberdade e da consolidação do direito à proteção de dados no âmbito subjetivo interrelacional.

A análise do *doxxing,* ademais, também dependerá da classificação da natureza das informações reveladas, se configuram dados sensíveis ou não[56]; do meio pelo qual foram obtidas (ex. *hacking*); dos sujeitos envolvidos; e da existência ou não de interesse público. Por exemplo, de modo abstrato, revelar o endereço eletrônico de alguém não é tão nocivo como revelar seu endereço residencial. Ainda, em algumas jurisdições, revelar as informações pessoais de um funcionário público

---

[54] V. McIntyre. *Do (x) you really want to hurt me,* cit. (nt. 52), p. 125-126.

[55] Nicole.A Moreham. *Beyond information: physical privacy in english law*, "The Cambridge Law Journal", LXXIII-2, 2014, pp. 350-377, p. 374-375.

[56] Por força do artigo 4.º, n.os 13, 14 e 15, artigo 9.º; considerando 51-56 do Regulamento Geral sobre a Proteção de Dados 2016/679: Os seguintes dados pessoais são considerados «sensíveis» e estão sujeitos a condições de tratamento específicas: dados pessoais que revelem a origem racial ou étnica, opiniões políticas e convicções religiosas ou filosóficas; filiação sindical; dados genéticos, dados biométricos tratados simplesmente para identificar um ser humano; dados relacionados com a saúde; dados relativos à vida sexual ou orientação sexual da pessoa.

se enquadra dentro das leis federais de conspiração e é visto como uma ofensa nacional.

Há uma terceira corrente doutrinária que entende que não se trata exclusivamente de uma violação de privacidade, tampouco unicamente de um meio técnico para causar danos, e defende que o que ocorre é a combinação de ambos. Tal prática pode ser tipologicamente qualificada como uma forma de violência facilitada pela tecnologia (*technology-facilitated violence* – TFV), tendo a pesquisa identificado sete – mutualmente não-excludentes – motivações para a prática de *doxxing*: não intencional, extorsão, ameaça, vingança, *stalking,* construção de reputação e por interesse coletivo[57].

Diante da dualidade, dependendo do arcabouço normativo, da jurisdição e do referencial teórico prevalente na categorização, principalmente nos casos das espécies de desanonimização e de desmoralização, o *doxxing* pode ser combatido com a aplicação das leis criadas contra *stalking*, assédio, ameaça e violação do direito da personalidade à privacidade, à honra e à liberdade, na medida em que a internet pode ser compreendida como um meio para a prática da conduta ilícita.

Todavia, quando percebida como espécie de violência típica do ambiente virtual, principalmente nos casos de *doxxing* por segmentação, as condutas podem ser consideradas como fonte material do direito, o que justifica a atividade legislativa específica de delimitação do conteúdo jurídico, ou a aplicação de normas de integração para suprir eventuais lacunas.

Devido à natureza relativamente recente do *doxxing*, as respectivas leis estão em constante evolução e nem sempre são claras ou adequadas a complexidade conceitual do termo, que abrange três espécies e duas possíveis categorias jurídicas. Todavia, é fato que as condutas abrangidas objetivamente são vistas como antiéticas, geralmente praticadas com intenção de intimidar, chantagear e controlar pessoas, além de poderem gerar danos existenciais significativos.

Outrossim, a partir da noção de *doxxing* como uma forma de violência facilitada pela tecnologia, verifica-se a necessidade de estudos científicos específicos destinados a promover a redução de riscos de danos às vítimas, para que haja uma maior compreensão das possibilidades de desenvolvimento de programas de prevenção.

---

[57] Briony Anderson / Mark A. Wood. *Harm Imbrication and Virtualised Violence: Reconceptualising the Harms of Doxxing*. "International Journal for Crime, Justice and Social Democracy", XI-1, 2022, pp.196-209, p. 197. Disponível em https://doi.org/10.5204/, Consulta feita em: 13/07/2022.

7. Conclusões

A partir da análise da tríade conceitual *bullying,* cibercultura e *cyberbullying*, verificou-se ser possível a identificação de fenômenos sociais típicos do ambiente virtual, como o *doxxing*, a conduta de divulgar no ambiente virtual dados referentes à determinada pessoa sem o seu consentimento, o que geralmente ocorre com a intenção maliciosa de causar algum dano. O ponto central da análise abordou a possibilidade de a conduta de *doxxing* ser configurada como espécie autônoma de *cyberbullying*, ou apenas meio, do qual decorre a conduta de atentar contra a personalidade.

Sobre a hipótese de o *doxxing* ser tratado apenas como meio para a prática de violência, a conclusão é a de que o ambiente virtual e suas especificidades devem ser considerados como circunstâncias judiciais no momento da aplicação das sanções ao caso concreto.

Sob um outro prisma, adotada a categorização da espécie como tipo autônomo de violência, há de se reconhecer a fonte material, que inova o ordenamento jurídico, e reclama tratamento legislativo específico, sobretudo na seara do direito penal, em razão da segurança jurídica advinda da observância de seus princípios gerais.

Após análise tipológica e categorização dos fenômenos descritos como *doxxing*, constatou-se, na revisão bibliográfica, três correntes sobre sua natureza jurídica, que são: a) um meio de se praticar a violência na internet, que não pode ser confundido com a própria finalidade do agente; b) um tipo específico de violência praticado contra a vítima, em razão das especificidades dos danos praticados no ambiente virtual; e, c) a teoria dualista, combinando as duas matizes, defendendo tratar-se ora de uma forma, ora de uma espécie de violência facilitada pela tecnologia, com sua categorização dependendo, efetivamente, do cotejo analítico dos fatos.

Foram identificadas três espécies ou modalidades de prática do *doxxing:* de desanonimização, de segmentação e difamatório, cada uma definida de acordo com o principal bem jurídico lesado, quais sejam: o anonimato, o "direito a ser deixado de lado" e a honra, respectivamente. Fica demonstrado que a análise e enquadramento jurídico em categorias dependerá, igualmente, do contexto da divulgação, da natureza das informações reveladas em questão, do meio pelo qual foram obtidas, dos sujeitos envolvidos e da existência ou não de interesse público.

A hipótese do *doxxing* enquanto tipo autônomo de violência facilitada pela tecnologia é confirmada, principalmente, na sua espécie de segmentação, em razão da classificação da conduta como de perigo abstrato. As demais formas, desanonimização e difamatório, enquadram-se propriamente na hipótese de ser o *doxxing* percebido como um meio para a prática de violências já combatidas tradicionalmente na sociedade, por meio da tipificação das condutas que ofendem os direitos da pessoa humana.

O *doxxing* comprovou-se como uma expressão muito abrangente, que comporta condutas classificadas em três conjuntos heterogêneos. Não se deve esquecer que apesar de, em algumas circunstâncias, as ações serem mutuamente não excludentes, elas guardam características que permitem, a depender do caso, configurar uma violência tipológica autônoma, ou apenas o meio para perpetrar o *cyberbullying*.

É possível concluir, portanto, que a teoria dualista é a mais adequada ao enfrentamento da hipótese, e deve ser empregada nas funções jurídicas de integração, criação e decisão; nas definições de políticas públicas; pesquisas científicas e programas de prevenção e de enfrentamento ao *cyberbullying*.

Ademais, a construção democrática dos processos de cidadania e de promoção dos direitos humanos em relação ao ambiente virtual depende diretamente da sustentação formal e funcional dos direitos da proteção de dados pessoais, como forma de defesa e de prevenção dos perigos da perpetuação de estigmas sociais, violências e abusos registrados nas representações sociais estratificadas.

É certo que a importância desse debate não se circunscreve somente nas camadas sociais que lutam pelo reconhecimento identitário. Nesse sentido, é possível asseverar que a defesa de fundamentos axiológico-normativos dos direitos da pessoa humana, especialmente daqueles que tangem a privacidade informacional, representa no mundo virtualizado a pedra angular para as estratégias de desenvolvimento dos valores e do progresso social.

Desta feita, com a retomada dos três panoramas normativos do direito à proteção de dados que foram descritos – direito fundamental positivado na constituição; derivado da teoria estruturante do direito fundamental à liberdade; ou decorrente da mesma teoria estruturante só que aplicada à intimidade – constata-se que cabe ao Estado, por força de seus deveres de proteção, garantir a privacidade e a autodeterminação informacional. Consequentemente, a tutela da intimidade, da honra, da integridade, e de tantos outros direitos da personalidade; por conseguinte, resguardam a dignidade da pessoa humana.

Para tanto, é dever do Estado zelar pela consistência constitucional dos marcos normativos infraconstitucionais que tratam da proteção de dados pessoais no ambiente virtual; e, principalmente, promover a integração e harmonização produtiva dos diplomas legais isoladamente considerados, para superar eventuais contradições e assegurar ao direito fundamental à proteção de dados a sua máxima eficácia e efetividade. Por fim, ressalta-se haver a pertinência na criação de leis específicas de combate à prática do *doxxing* nos países em que ainda não há disciplina determinada, como Brasil e Portugal.