

PONTIFÍCIA UNIVERSIDADE CATÓLICA
DO RIO DE JANEIRO



Carlos Eduardo Ferreira de Souza

**Desinformação e regulação da
publicidade personalizada**

Dissertação apresentada como requisito parcial para obtenção do grau de Mestre em Direito pelo Programa de Pós-Graduação em Teoria do Estado e Direito Constitucional do Departamento de Direito da Pontifícia Universidade Católica (PUC-RIO).

Orientador: Prof. Fábio Carvalho Leite

Coorientador: Prof. Ivar Alberto Martins Hartmann

Rio de Janeiro
Maio de 2022

Carlos Eduardo Ferreira de Souza

**Desinformação e regulação da
publicidade personalizada**

Dissertação apresentada como requisito parcial para a obtenção do grau de Mestre em Direito pelo Programa de Pós-Graduação em Direito, do Departamento de Direito da PUC-Rio.

Aprovada pela Comissão Examinadora abaixo:

Prof. Fábio Carvalho Leite

Orientador

Departamento de Direito – PUC-Rio

Prof. Prof. Ivar Alberto Martins Hartmann

Coorientador

Inspere – Instituto de Ensino e Pesquisa

Prof. Clara Iglesias Keller

Pesquisadora autônoma

Prof. Florian Fabian Hoffmann

Departamento de Direito – PUC-Rio

Rio de Janeiro, 30 de maio de 2022

Todos os direitos reservados. É proibida a reprodução total ou parcial do trabalho sem autorização da autora, do orientador e da universidade.

Carlos Eduardo Ferreira de Souza

Advogado de privacidade e proteção de dados pessoais graduado em Direito pela Faculdade Nacional de Direito da Universidade Federal do Rio de Janeiro (UFRJ). Pesquisador do Grupo de Pesquisa sobre Liberdade de Expressão no Brasil (PLEB) do Núcleo de Estudos Constitucionais da Pontifícia Universidade Católica do Rio de Janeiro. Possui interesse temático nas áreas de Direito Constitucional, Direito Civil, Novas Tecnologias, Regulação, Desinformação, Privacidade e Proteção de Dados Pessoais.

Ficha Catalográfica

Souza, Carlos Eduardo Ferreira de

Desinformação e regulação da publicidade personalizada / Carlos Eduardo Ferreira de Souza ; orientador: Fábio Carvalho Leite ; coorientador: Ivar Alberto Martins Hartmann. – 2022.

118 f. ; 30 cm

Dissertação (mestrado)–Pontifícia Universidade Católica do Rio de Janeiro, Departamento de Direito, 2022.

Inclui bibliografia

1. Direito – Teses. 2. Desinformação. 3. Publicidade personalizada. 4. Proteção de dados pessoais. 5. Liberdade de expressão. 6. Regulação. I. Leite, Fábio Carvalho. II. Hartmann, Ivar Alberto Martins. III. Pontifícia Universidade Católica do Rio de Janeiro. Departamento de Direito. IV. Título.

CDD: 340

Agradecimentos

Com pleno respeito a toda fé ou ausência dela, a Deus por haver me permitido cursar o Mestrado em uma instituição de excelência, que me permitiu adquirir conhecimento, desenvolver esta pesquisa e, acima de tudo, conhecer pessoas incríveis.

Agradeço aos professores Fábio Carvalho Leite e Ivar Alberto Martins Hartmann pela atenciosa, próxima e paciente orientação, fundamental para a construção deste trabalho e para o amadurecimento da proposta inicial, moldada a várias mãos. Aproveito para agradecer à professora Clara Iglesias Keller pelos necessários e essenciais conselhos dados em banca de qualificação.

À minha esposa Adriana Ribeirinha, pela companhia e apoio na vida em todos os momentos, com paciência, carinho e muitos incentivos. Aos meus pais, Soraya e Paulo, a minha avó Juracy e a minha irmã Milla por constituírem minha base e suporte desde os primeiros momentos de vida até esta etapa de conclusão.

Aos professores que foram fundamentais para minha caminhada na pesquisa. Por serem muitos, me permito agradecer na figura de alguns especialmente próximos. Além dos mencionados e essenciais orientadores no Mestrado, agradeço à professora Daniela Barcellos, minha orientadora na graduação e querida amiga nessa trajetória, à professora Cintia Konder pela carta de referência para ingresso no programa e gentis orientações na vida acadêmica e à professora Caitlin Mulholland por me apresentar o mundo das novas tecnologias e pela parceria na produção de artigos.

Aos amigos queridos que conheci na vida e na academia. Represento-os nas figuras do Frederico Boghossian, de quem me aproximei no início do curso e que foi o responsável por me inserir na advocacia de privacidade e proteção de dados, que transformou minha trajetória profissional, e da Gabriela Gattulli, que me convenceu de que era o momento certo para iniciar o Mestrado e me ajudou imensamente ao longo do processo seletivo.

Aos amigos que fiz na advocacia em proteção de dados pessoais e regulação de novas tecnologias: os grandes responsáveis por meu desenvolvimento nessa área, Daniel Becker e Beatriz Haikal, às companheiras indispensáveis, Gabriela Sotomayor e Maria Eduarda Sampaio. Aos queridos parceiros que passaram por mim nesta trajetória: Horrara Silva e Pedro Gueiros.

Ao Grupo de Pesquisa em Liberdade de Expressão no Brasil (PLEB), por me proporcionar debates e trocas, me fazendo sentir um gosto de convívio diário com amigos da PUC-RIO mesmo fora do campus.

À CAPES e à PUC-Rio, pelos auxílios concedidos, sem os quais este trabalho não poderia ter sido realizado.

Resumo

Souza, Carlos Eduardo Ferreira; Leite, Fábio Carvalho. **Desinformação e regulação da publicidade personalizada**. Rio de Janeiro, 2022. 118p. Dissertação de Mestrado – Departamento de Direito, Pontifícia Universidade Católica do Rio de Janeiro.

O presente trabalho pretende analisar como a desinformação é monetizada no ambiente virtual e compreender aspectos regulatórios estruturais e concretos para reduzir os efeitos nocivos desta prática. Assim, será demonstrado o conceito de desinformação e de publicidade personalizada, além da relação que possuem entre si. Em virtude dos diversos benefícios gerados por este tipo de publicidade e dos riscos para a liberdade de expressão que podem advir da regulação focada em conteúdo, são apresentadas soluções centradas na arquitetura da plataforma e na proteção de dados pessoais. Como proposta, se apresenta uma regulação multiparticipativa, com amplitude de instrumentos e com a mescla de conceitos mais precisos e mais vagos, buscando segurança jurídica sem descuidar da necessária elasticidade diante da dinâmica que envolve novas tecnologias. Por fim, são apresentadas medidas concretas voltadas para (i) transparência e empoderamento do usuário; (ii) transparência e controle para o anunciante; (iii) *accountability* e dados pessoais.

Palavras-chave

Desinformação; publicidade personalizada; proteção de dados pessoais; liberdade de expressão; regulação.

Abstract

Souza, Carlos Eduardo Ferreira; Leite, Fábio Carvalho (advisor). **Disinformation and regulation of programmatic advertising**. Rio de Janeiro, 2022. 118p. Dissertação de Mestrado – Departamento de Direito, Pontifícia Universidade Católica do Rio de Janeiro.

The present work intends to analyze how disinformation is monetized on the virtual environment and comprehend the concrete and structural regulatory aspects to reduce the damaging effects of said practice. Thus, the concept of disinformation and programmatic advertising will be shown, as well as the link between them. By virtue of many benefits generated by this kind of advertising and the risks to the freedom of speech that can come from regulation focussed on content, solutions based on the architecture of the platform and personal data privacy protection are presented. As a proposal, a multi-stakeholder regulation is presented with the amplitude of mechanisms and with the mix of the most accurate and vague concepts looking for legal security without neglecting the elasticity there is required in view of the dynamics that involves new technologies. Finally, concrete measures designed for (i) transparency and user empowerment are presented; (ii) transparency and control for the advertiser; (iii) accountability and personal data.

Keywords

Disinformation; programmatic advertising; personal data protection; freedom of speech; regulation

Sumário

1. Introdução.....	9
2. Desinformação e a Publicidade Personalizada: o potencial lucrativo	14
2.1. Desinformação, <i>Fake News</i> , <i>Misinformation</i> ou <i>Propaganda</i>	14
2.2. Publicidade personalizada e tratamento de dados pessoais.....	21
2.3. Desinformação monetizada.....	32
3. Aspectos estruturais da regulação da publicidade personalizada	43
3.1. Regulação e liberdade de expressão	43
3.2. O que é regulação e quem pode regular.....	56
3.3. Como regular: importância dos princípios e conceitos vagos	66
3.3.1. <i>Accountability</i>	75
3.3.2. Transparência.....	80
4. Práticas de transparência e <i>accountability</i> ligadas a estrutura e proteção de dados pessoais	84
4.1. Transparência e empoderamento do usuário.....	84
4.2. Transparência e controle para o anunciante	91
4.3. <i>Accountability</i> e dados pessoais.....	98
5. Conclusão	105
REFERÊNCIAS.....	108

1

Introdução

A produção de conteúdo intencionalmente falso disfarçado sob uma ardilosa aparência de veracidade e credibilidade não surge com o advento da internet. Da mesma forma, a utilização daquele tipo de conteúdo para obtenção de vantagens econômicas, políticas ou sociais também não integram história recente. Talvez a mentira, a fraude, a traição, a ilusão e a astúcia tenham acompanhado a humanidade desde suas origens.

De maneira mais específica, a criação de notícias enganosas baseadas em indícios descontextualizados, inexistentes, fabricados ou exagerados com o objetivo de derrotar um adversário político, cobrir um “furo jornalístico” ou simplesmente vender mais edições ou atrair maior audiência é questão antiga na sociedade e nos meios de comunicação tradicionais – não apenas na televisão, mas também em rádios, jornais, revistas, folhetins e tantos outros.

Contudo, nos últimos anos vem se acentuando a preocupação da academia, do poder público e da sociedade com o tema da desinformação. Não há pretensão de ser taxativo quanto aos assuntos afetados pela produção de conteúdo nocivo ou de baixa qualidade, mas a desinformação tem influenciado de maneira particular processos eleitorais, decisões importantes sobre o rumo de países e, mais recentemente, a adoção ou negação de medidas sanitárias recomendadas por profissionais de saúde e organizações internacionais, sobretudo no contexto da pandemia da COVID-19.

Uma das hipóteses é de que mudanças no ambiente virtual e o advento de novas tecnologias tem contribuído para a potencialização da criação e disseminação de conteúdo falso. De maneira mais específica, a presente dissertação focará no estudo da desinformação produzida com objetivo de obter lucro que advém de receitas geradas a partir da chamada publicidade personalizada e analisará aspectos regulatórios estruturais e medidas concretas para mitigar os riscos e danos advindos da prática.

Preliminarmente, cabe fixar um conceito breve de desinformação, aqui entendido como conteúdo falso, com aparência de veracidade e que objetiva enganar o leitor, podendo se dirigir à obtenção de vantagem pessoal, política,

econômica ou social¹. Tal definição será melhor desenvolvida nos capítulos deste trabalho.

Já a publicidade personalizada pode ser definida como a exibição de anúncios direcionados e que focam no perfil do usuário, moldado a partir de amplo tratamento de dados pessoais. Assim, são apresentados anúncios personalizados, com objetivo de ampliar vendas, contratações ou acesso de maneira assertiva e exibida para o usuário mais adequado e propenso à aquisição². Tais anúncios são alocados por grandes empresas, como o Google e a Meta, e outros intermediários em espaços disponibilizados por sites que buscam obter receita que é gerada a partir do clique dos usuários daquelas plataformas. Exemplificativamente, se alguém pesquisa passagens aéreas no Google e, em seguida, clica em um desses sites parceiros que ofereçam matérias jornalísticas – e, portanto, não vendem passagem aérea – anúncios de companhias podem ser exibidos nos displays disponíveis.

Ainda que a prática necessite de melhor desenvolvimento – o que será realizado ao longo deste trabalho – é possível antecipar duas importantes vantagens: (i) os anúncios ficam mais baratos para o anunciante, sobretudo aqueles de pequeno e médio portes que dificilmente teriam condições de anunciar em veículos tradicionais; (ii) os veículos de comunicação passam a ser mais variados e plurais, diante da maior facilidade de obtenção de receitas oriundas de publicidade, o que dependia de grandes esforços ou da decisão de editores em veículos tradicionais. Assim, a publicidade personalizada é construída para gerar lucro para empresas de tecnologia, mas também para facilitar ações de marketing de negócios de todos os tamanhos, de maneira mais barata e assertiva, ao mesmo tempo que possibilita o financiamento de veículos de comunicação de diferentes tamanhos e, muitos deles, de qualidade respeitável.

De outro lado, canais, páginas e usuários mal-intencionados têm se valido do mecanismo para criar desinformação, fomentar o tráfego e, a partir daí, gerar receitas oriundas de publicidade³. Tal situação ocorre porque a publicidade

¹ ALLCOTT, Hunt; GENTZKOW, Matthew. Social Media and Fake News in the 2016 Election. **Journal of Economic Perspectives**, v. 31, n. 2, Spring 2017, pp. 211-236. Disponível em: <https://pubs.aeaweb.org/doi/pdfplus/10.1257/jep.31.2.211>.

² MALTHOUSE, Edward; MASLOWSKA, Ewa; FRANKS, Judy. The role of Big Data in Programmatic TV Advertising. In: CAUBERGHE, Verolien; HUDDERS, Liselot; EISEND, Martin (eds.). **Advances in Advertising Research IX: power to consumers**. European Advertising Academy: Springer Gabler, 2018, pp. 32-33.

³ MILLS, Adam; PITT, Christine; FERGUSON, Sarah. **The Relationship between Fake News And Advertising: Brand Management in the Era Of Programmatic Advertising and Prolific Falsehood**. *Journal of Advertising Research*, 59 (1), pp. 4-5.

personalizada é mais focada no usuário que no conteúdo ao lado do qual o anúncio será exibido, ao contrário do que ocorria em veículos tradicionais, quando o anunciante precisava escolher, por exemplo, o programa, o canal, a estação, a página, o caderno, dentre outros.

Portanto, há um problema a ser solucionado: a monetização da desinformação. Contudo, tal solução não se dirige necessariamente à extinção da publicidade personalizada. Além disso, propostas que se dirigem ao controle do conteúdo, conquanto defendido por parcela considerável, será evitado neste trabalho para proteção de liberdades fundamentais, sobretudo a liberdade de expressão, a liberdade de imprensa e a liberdade religiosa.

O trabalho ora desenvolvido focará em regulação por estrutura e proteção de dados⁴ e não propriamente no controle de conteúdo que, sendo admitido, deve garantir a transparência, o devido processo e o controle pelos afetados. Além disso, devem ser assegurados mecanismos que coloquem os usuários no centro das decisões. Não de maneira meramente formal, mas por meios que atribuam melhores condições para que haja o controle do conteúdo por aquele que o acessará. Deve ser dispensada a definição, por qualquer ator social, de um conceito de verdade ou mentira, prática que tem sido abusiva e indevidamente utilizada por regimes de viés mais autoritários.

Com esse objetivo, foi utilizada a metodologia de pesquisa exploratória feita a partir da análise do estado da arte, pesquisa bibliográfica e documental. O foco da análise foi a doutrina e a legislação brasileira, europeia e norte-americana. No tocante aos aspectos regulatórios, a presença maior de autores e diplomas legais brasileiros e europeus se justificam em razão das peculiaridades ligadas à adoção de políticas públicas e regulamentação específica para privacidade e proteção de dados, bem como para o combate à desinformação e discurso de ódio, com busca da transparência e responsabilidade nas redes. Alguns autores frequentemente citados são Hartmann, Keller, Leonardi, Magrani, Baldwin, Gunningham, Sinclair, além de Benkler, Faris e Roberts.

No desenvolvimento, o capítulo 2 desta dissertação apresenta o conceito de desinformação e relaciona a temática com a publicidade personalizada. No subcapítulo 2.1, será abordada a definição de desinformação e a comparação com termos comumente utilizados para tratar de assuntos que possuem alguma

⁴ O autor deste trabalho reconhece a existência de outros focos da regulação, tendo realizado escolha por motivos que serão expostos no desenvolvimento.

similaridade, mas que não se confundem com a desinformação, tais como *Fake News*, *Misinformation* e *Propaganda*. Já no subcapítulo 2.2, serão expostos o funcionamento da publicidade personalizada – que pode receber outros nomes – e como o tratamento de dados pessoais em larga escala é fundamental para a garantia da assertividade da operação, destacando a importância dela para o desenvolvimento econômico e para a liberdade de expressão. Encerrando o capítulo, o tópico 2.3 demonstra a maneira pela qual os criadores de desinformação, que objetivam lucrar com suas publicações, utilizam a publicidade personalizada para atrair receitas consideráveis para seus canais. É reconhecida a dificuldade enfrentada pelo poder público, pelas empresas de tecnologia e pelos usuários no combate à desinformação sem ameaçar de forma desproporcional a liberdade de expressão, valor inerente a Estados democráticos.

No capítulo 3, são explorados aspectos regulatórios de caráter geral e estrutural, a partir da análise doutrinária e com apontamento de legislação vigente no Brasil que trata do tema, sobretudo a Lei Geral de Proteção de Dados (“LGPD”) e o Projeto de Lei 2.630/2020 (“PL 2630/2020”). A primeira parte (3.1) trata da importância de uma regulação focada na estrutura da plataforma e na proteção de dados pessoais de usuários, em detrimento de alternativas que foquem no conteúdo, com definição de verdade ou mentira, que seria inevitavelmente impactada pela subjetiva interpretação feita pelo agente regulador. No tópico 3.2, será buscada a resposta para duas questões: o que é regulação e quem pode regular. As novas tecnologias que operam no ambiente virtual se modificam com rapidez e frequência e envolvem múltiplos interesses de atores sociais distintos. Logo, parece que a regulação mais adequada deve ser multinível, ampla e com admissão de variados instrumentos. O subcapítulo 3.3 versará sobre a importância dos princípios e conceitos vagos para criar uma regulação que se adeque às rápidas transformações sociais e tecnológicas, sem desproteger o núcleo das disposições. Ressalte-se, desde já, que o presente trabalho não atuará com a dicotomia “regra x princípio”, mas com a variação em um *continuum*⁵ que possui como extremos a vagueza e a precisão, de tal sorte que a regulação deve perseguir diversas nuances, ora se aproximando de um extremo ora se aproximando do outro. A maior vagueza reduz a segurança jurídica, mas amplia a elasticidade necessária para adaptação no espaço e tempo, enquanto a maior precisão amplia a segurança na regulação presente, mas arrisca a obsolescência

⁵ SCHAUER, Frederick. **Thinking like a lawyer: a new introduction to legal reasoning**. Harvard University Press, 2009, pp. 188-202.

com velocidade superior a mudanças legislativas e regulatórias. Ainda naquele subcapítulo, serão destacadas a *accountability* e a transparência como importantes princípios inseridos em matérias que tratam de novas tecnologias em variados lugares do mundo, notadamente no Brasil e no contexto europeu, conforme se desenvolverá.

Por fim, o último capítulo se dedica a apresentar medidas concretas que vêm sendo adotadas nos cenários brasileiros e europeu. Este trabalho não se refere à Europa como um bloco uniforme, indissociável e que ignora as diferenças entre os países que a integram, razão pela qual é destacado, no desenvolvimento, a que práticas internas se refere no caso a caso. Contudo, a menção se dá em razão de normas comuns, tais como o *General Data Protection Regulation (GDPR)*. O subcapítulo 4.1 se refere a mecanismos que garantam maior transparência e confirmem maior empoderamento ao usuário das novas tecnologias que serão apresentadas. Por usuário, se entende tanto o leitor quanto produtores de conteúdo. A diferença é feita em relação ao tópico 4.2, que se dirige a apresentar instrumentos de transparência e controle que se voltem para o anunciante. É necessário destacar que não há impossibilidade de que mecanismos que foquem no usuário sejam úteis para dar maior transparência ao anunciante e vice-versa e a separação foi feita a partir do foco principal de cada análise. Por fim, o tópico 4.3 apresenta instrumental de *accountability*, que tem particular importância nas práticas empresariais hodiernas e cuja efetividade pode ser aproveitada e ampliada para aumentar a proteção de direitos e liberdades fundamentais no ambiente virtual, a partir da adequação de empresas de tecnologia que atuam com publicidade personalizada.

2

Desinformação e a Publicidade Personalizada: o potencial lucrativo

2.1.

Desinformação, *Fake News*, *Misinformation* ou *Propaganda*

O termo desinformação é frequentemente posicionado ao lado de outras expressões que guardam similaridade inicial, mas que se referem a conceitos distintos. Considerando a atualidade do tema e a possibilidade de confusão entre os termos, o presente capítulo busca estabelecer distinções e criar linguagem comum a ser utilizada ao longo desta dissertação.

Assim, o espaço é dedicado à comparação entre a desinformação e os termos *fake news*, *misinformation* e *propaganda*.

Inicialmente, será feita a distinção entre desinformação e *fake news*. A escolha não é ocasional, pois as expressões já possuíam mesmo significado. Conforme se demonstrará, ambas são notícias com conteúdo falso ou enganoso, produzidas de maneira intencional, com objetivo de enganar o leitor. Entretanto, o termo *fake news* perdeu a tecnicidade e assumiu duplo sentido, ao ser utilizado por figuras políticas que buscavam deturpar o discurso da imprensa e de adversários.

Em artigo publicado no início de 2017, Allcott e Gentzkow⁶ traziam a definição de *Fake News* como notícias intencionalmente falsas, criadas com intuito de enganar o leitor e cuja falsidade pode ser objetivamente verificada. O conceito já delimitava seu alcance, ao salvaguardar o erro não-intencional, conteúdos humorísticos e sátiras, bem como rumores que não tivessem origem em notícias e reportagens.

Do ponto de vista da popularização do termo, é possível afirmar que o uso de *fake news* para se referir ao fenômeno ganha força nas eleições presidenciais de 2016, quando Silverman⁷ demonstrou a influência que tais práticas tiveram no pleito que elegeu Donald Trump Presidente dos EUA.

⁶ ALLCOTT; GENTZKOW.

⁷ SILVERMAN, Craig. This Analysis Shows How Viral Fake Election News Stories Outperformed Real News On Facebook. **BuzzFeed**, Canada, 16 nov. 2016. Disponível em:

Contudo, o uso indevido do termo por determinadas figuras políticas levou autoridades públicas e acadêmicos a recomendarem a não utilização da expressão *fake news*. Por óbvio, tal recomendação não desabona a utilização ocorrida em períodos anteriores, como foi o caso da matéria produzida por Silverman e pelo trabalho bastante citado de Allcott e Gentzkow, tampouco impede a menção a tão importantes referências. Neste trabalho, porém, a utilização da expressão será evitada, principalmente em razão de atestada controvérsia.

Ilustrativamente, desde o início de sua atuação na Casa Branca, Trump passou a utilizar sem pudores o termo *fake news* para se referir aos veículos e membros da imprensa que o criticavam, chegando mesmo a criar o “*Fake News Awards*”, destinado a atacar a imprensa e escolher aqueles que seriam chamados por ele de “maiores propagadores de *fake news*”, a despeito da inexistência de notícias comprovadamente falsas. Na ocasião, chegou a atacar importantes veículos, como a *CNN*, o *New York Times* e o *Washington Post*⁸. Evidentemente, o significado de *fake news* atribuído por Trump difere absolutamente daquele delineado por Allcott e Gentzkow ou mesmo utilizado por Silverman.

Donald Trump não foi o único a utilizar a expressão *fake news* para atacar a livre atuação da imprensa, cujos veículos atuavam no contexto da liberdade de expressão, sobretudo da liberdade de imprensa e do direito à informação. Outros personagens que se valeram de campanha agressiva, com uso de conteúdo falso e criado com intenção de enganar o eleitor para obter êxito nas eleições de seus países, também utilizaram o termo *fake news* em larga escala.

Observando o caso brasileiro, é possível afirmar que estratégia semelhante foi utilizada por Jair Bolsonaro, cuja campanha de desinformação já foi massivamente denunciada por diversos veículos e obras, nacionais e estrangeiras⁹. Com objetivo de comprovar o que se afirma, a Agência Lupa

<<https://www.buzzfeednews.com/article/craigsilverman/viral-fake-election-news-outperformed-real-news-on-facebook>>. Acesso em 25 set. 2021.

⁸ LEE, Yen Nee. Trump and GOP attack CNN, New York Times and Washington Post in ‘fake news awards’. **CNBC**, 17 jan., 2018. Disponível em: <https://www.cnbc.com/2018/01/17/fake-news-awards-by-donald-trump-gop-cnn-new-york-times-washington-post.html>. Acesso em 25 set. 2021.

⁹ Vide por todos: CAMPOS MELLO, Patrícia. **A máquina do ódio: notas de uma repórter sobre Fake News e violência digital**. Rio de Janeiro: Companhia das Letras, 2020; DA EMPOLI, Giuliano. **Os Engenheiros do Caos**. Minas Gerais: Autêntica, 2019. HOFFMANN, Stacie; TAYLOR, Emily; BRADSHAW, Samantha. **The Market of Disinformation**. Oxford Technology & Elections Commission. October, 2019, 42 pp. Disponível em: <https://oxtec.oii.ox.ac.uk/wp-content/uploads/sites/115/2019/10/OxTEC-The-Market-of-Disinformation.pdf>. Acesso em 25 set. 2021. GIANIRACUSA, Noah. **How Algorithms Create and Prevent Fake News**. Massachusetts: Apress, 202.

demonstrou que Jair Bolsonaro realizou trinta e uma manifestações nas redes sociais em 2019, contendo os termos *fake news* ou *fake*. Tais manifestações foram, 64,5% das vezes, direcionadas para ataques à imprensa brasileira, tendo sido a Folha de S. Paulo o veículo mais citado, ao lado de O Globo, Globo News, Estado de S. Paulo e Revista Veja, nesta ordem decrescente¹⁰.

No Reino Unido, a *House of Commons*, no âmbito da Comissão para assuntos ligados à mídia, cultura e meios digitais, elaborou um relatório que inicia com a observação de que não seria utilizado o termo *fake news*, pela possibilidade de induzir o leitor a erro e descontentamento, já que o termo poderia ser confundido com o *Fake News Award*, criado por Trump em sua conta no Twitter. A Comissão esclareceu, ainda, que o termo desinformação seria mais adequado e significaria criar e compartilhar notícia deliberadamente falsa com intuito de enganar a audiência, causar danos ou obter ganhos políticos, pessoais ou financeiros¹¹.

A UNESCO, com objetivo de orientar professores e alunos de jornalismo em questões associadas à desinformação, destaca que o termo *fake news* passou a significar mais que um rótulo para informação falsa ou errônea, sendo carregada de conteúdo emocional e utilizado como arma por figuras poderosas para desacreditar a mídia¹².

O próprio Silverman, que contribuiu para a popularização do termo, já publicou matéria no *Buzzfeed*, demonstrando que sente vergonha ou arrepio de ouvir a expressão, que havia sido usurpada por Trump e seus apoiadores¹³.

Benkler, Faris e Roberts¹⁴ também reconhecem a similaridade e justificam a escolha pelo termo desinformação para se referir à disseminação de informação

¹⁰ AFONSO, Nathália. 64,5% das vezes em que Bolsonaro fala em 'fake news' são ataques à imprensa. **Agência Lupa, UOL**, 23 dez. 2019. Disponível em: <https://piaui.folha.uol.com.br/lupa/2019/12/23/bolsonaro-fake-news-imprensa/>. Acesso em 25 set. 2021.

¹¹ REINO UNIDO. House of Commons. Digital, Culture, Media and Sport Committee. **Disinformation and 'fake news': Final Report, 18 fev. 2019**, pp. 7-8. Disponível em: <https://publications.parliament.uk/pa/cm201719/cmselect/cmcmds/1791/1791.pdf>. Acesso em 25 set. 2021.

¹² IRETON, Cheryl; POSETTI, Julie. Journalism, 'Fake News' & Disinformation: handbook for journalism education and training. UNESCO, 2018, pp. 9-19. Disponível em: <https://unesdoc.unesco.org/ark:/48223/pf0000265552>. Acesso em 25 set. 2021.

¹³ SILVERMAN, Craig. I Helped Popularize The Term "Fake News" And Now I Cringe Every Time I Hear It. **BuzzFeed**, Canada, 31 dez. 2017. Disponível em: <https://www.buzzfeednews.com/article/craigsilverman/i-helped-popularize-the-term-fake-news-and-now-i-kringe>. Acesso em 25 set. 2021.

¹⁴ BENKLER, Yochai; FARIS, Robert; ROBERTS, Hal. **Network Propaganda: manipulation, disinformation, and radicalization in american politics**. New York: Oxford University Press, 2018. pp. 24-32.

claramente falsa com intuito de enganar o público. Os autores esclarecem que não utilizam o termo *fake news* por duas principais razões: (i) se tornou um termo vago enquanto categoria de análise; (ii) foi indevidamente apropriado por propagadores de desinformação, como Donald Trump¹⁵.

Portanto, o presente trabalho optará pelo uso do termo desinformação, fazendo menção a *fake news* apenas quando houver transcrição literal de algum trecho que assim proceda.

A segunda distinção trata dos termos desinformação e *misinformation*¹⁶. Aqui, ocorre uma relação de continente e conteúdo, sendo certo que a *misinformation* seria mais ampla e a desinformação seria mais restrita, com possibilidade mesmo de dizer que toda desinformação é uma *misinformation* qualificada pelo elemento intencional, mas nem toda *misinformation* é uma desinformação. A premissa para ambos os termos é a existência de conteúdo falso, verificável e com aspecto de notícia verídica. Não há, portanto, conteúdo verdadeiro nestas definições. Entretanto, as expressões não tratam de objetos idênticos, justamente pela presença, ou não, da vontade.

O elemento que distingue os dois conceitos é anímico, ligado à intenção daquele que produz o conteúdo falso. Na desinformação, seria necessária a intenção de enganar o leitor ou a audiência, enquanto na *misinformation* o erro pode ser inocente ou desprezioso, ou melhor, pode se tratar do erro sem intenção. Portanto, todo conteúdo falso, errôneo ou enganoso com aparência de veracidade seria uma *misinformation*, mas se produzido de maneira intencional deverá ser chamado desinformação.

Segundo Guess e Lyons¹⁷, a desinformação constituiria uma categoria de *misinformation*, se diferenciando em razão do elemento intencional. Assim, ambas seriam conteúdos falsos, mas a desinformação seria intencionalmente enganosa, enquanto a *misinformation* poderia ocorrer de maneira inadvertida ou inintencional.

¹⁵ Ibid., pp. 9, 183-187.

¹⁶ O termo não será traduzido, por falta de consenso na tradução ou mesmo de hábito da literatura em fazê-lo. A escolha se deve ao fato de que essa introdução conceitual busca aclarar os pontos, reduzindo as dúvidas que possam surgir.

¹⁷ GUESS, Andrew M.; LYONS, Benjamin A. Misinformation, Disinformation, and Online Propaganda. In: PERSILY, Nathaniel; TUCKER, Joshua (Ed.). **Social Media and Democracy**. New York: Cambridge University Press, 2020 (ebook).

Para Hoffmann, Taylor e Bradshaw¹⁸, *misinformation* seria a disseminação de informação mal acurada, ou seja, a disseminação de notícia falsa em razão da falta de diligência para confirmação efetiva dos fatos. Enquanto isso, desinformação seria a *misinformation* que é divulgada com intenção de enganar, razão pela qual concluem que toda desinformação é *misinformation*, enquanto nem toda *misinformation* é desinformação, justamente em razão do elemento intencional que existiria nesta última¹⁹.

Benkler, Faris e Roberts destacam que o volume de *misinformation* também se encontra em expansão, dada a variedade de concorrentes e a velocidade com a qual a informação tem sido prestada, o que acaba ampliando equívocos por falta de aferição adequada em um mundo caótico²⁰.

É certo que o uso da internet para fins pessoais e profissionais, com edição de páginas e blogs e, mais especificamente, a popularização do uso das redes sociais, trouxe muitas vantagens ao ampliar a voz de muitos e multiplicar os canais de comunicação. Entretanto, como efeito colateral, também expandiu a busca incessante pelo inédito ou pelo furo jornalístico, já que passou a existir maior número de concorrentes. Tais aspectos contribuíram para a redução de cautela e de investigação da notícia, em certa medida. Paiero, Santoro e Santos elucidam a questão sob o ponto de vista do jornalismo e da comunicação social²¹:

A informação equivocada, conhecida no jargão jornalístico como “barriga”, relaciona-se, ainda que não de forma direta, à busca incessante pelo “furo”, outro jargão que indica o fato apresentado em primeira mão (antes da concorrência, portanto) por algum veículo.

[...]

Imperícia do jornalista, imprudência, busca irresponsável pelo “furo”, pesquisa insuficiente e checagens inapropriadas (ou inexistentes) de dados fornecidos por entrevistados são alguns deles. E todos convergem, obviamente, para problemas relacionados ao exercício inadequado da profissão. Mas, como também já foi salientado, as “barrigas” jornalísticas não devem ser confundidas com a fabricação deliberada de informações. **As notícias falsas distinguem-se dos erros acidentais justamente por sua natureza de origem fraudulenta.** (Grifo nosso)

Wardle¹ já tratava da dificuldade de trabalhar com o termo *fake news* em meio à guerra de informações e desinformações vivida, sobretudo após as eleições de 2016. Com intuito de buscar um substitutivo, realiza a classificação de

¹⁸ HOFFMANN; TAYLOR; BRADSHAW, pp. 37-38.

¹⁹ Em sentido semelhante, BARRETO JUNIOR, Irineu Francisco. Fake News e discurso de ódio: estratégia de guerra permanente em grupos de Whatsapp. In: RAIS, Diogo (Coord.). Fake News: a conexão entre a desinformação e o direito. 2 ed., São Paulo: Thomson Reuters Brasil, 2020. Versão Kindle, pos. 2936.

²⁰ BENKLER, FARIS, ROBERTS, 2018, p. 37.

²¹ Rais, Pos. 3432-3455

desinformação e *misinformation* em sete categorias, que distribui ao longo de uma reta que possui como extremos, de um lado, a falta de intenção de enganar ou prejudicar e, de outro, o deliberado objetivo de ludibriar o leitor. Assim, iria da sátira ou paródia, que é criada sem qualquer intenção de enganar ou prejudicar, até o conteúdo fabricado intencionalmente, que é feito com o objetivo específico e principal, senão exclusivo, de enganar o leitor ou a audiência.

Entre os dois extremos da reta estão outras categorias, nesta ordem: (i) a falsa conexão entre mensagem e autor; (ii) conteúdo enganoso que busca enquadrar o leitor; (iii) inserção de conteúdo verídico em um contexto falso; (iv) conteúdo impostor, que mente acerca da fonte; (v) conteúdo manipulado.

O elemento intencional, do ponto de vista probatório, é uma dificuldade enfrentada por diversas áreas do Direito. Contudo, para os fins da desinformação, é possível pressupor a intencionalidade em alguns campos, sobretudo no campo político, porque é recurso comumente utilizado para enfraquecer argumentos de opositores e fortalecer o ponto de vista defendido. Sem generalizar, é interessante a entrevista dada por Arthur Finkelstein sobre o *modus operandi* de muitas campanhas. Finkelstein é consultor do Partido Republicano e responsável pela campanha de diversos candidatos de direita em vários países do mundo de maneira bem-sucedida, notadamente Benjamin Netanyahu e Viktor Orban²²:

A coisa mais importante é que ninguém sabe nada. Em política, o que você percebe como verdade é que é a verdade. Se eu digo a vocês que é um prazer estar aqui, porque deixei Boston, onde estava nevando e agora estou em Praga, onde o sol brilha, vocês vão acreditar. Porque vocês sabem que hoje, aqui, está fazendo um dia bonito. Se, ao contrário, eu digo que estou triste de estar aqui porque deixei Boston sob sol forte e em Praga está nevando, vocês não vão acreditar, porque basta olhar pela janela e acreditar que está nevando em Boston porque eu menti a vocês sobre Praga. É isto: um bom político é um sujeito que vai dizer uma série de coisas verdadeiras antes de começar a dizer uma série de coisas falsas, porque assim vocês vão acreditar em tudo o que ele diz, verdades ou mentiras.

Atento aos objetivos desta dissertação, tanto a desinformação quanto a *misinformation* são consideradas importantes, nada obstante o foco maior seja o uso de desinformação para obtenção de lucro.

Quanto à distinção entre desinformação e propaganda, se localiza na necessidade de o conteúdo utilizado ser falso ou não. Na desinformação, o

²² DA EMPOLI, pp. 86-87.

conteúdo precisa ser falso, com aparência de veracidade e intenção de enganar o receptor da mensagem. De outro lado, na *propaganda* o conteúdo pode ser falso, mas também é possível que seja verídico, posto que a falsidade não é elemento necessário. Assim, para caracterizar a propaganda, basta a existência de dois requisitos: (i) a necessária segmentação dos indivíduos; (ii) a criação de conteúdo para induzi-los a determinado fim.

Conforme Benkler, Faris e Roberts, propaganda seria uma espécie de comunicação delineada para manipular uma população segmentada, afetando suas crenças, atitudes e preferências, com intuito de obter uma postura condizente com objetivos políticos pretendidos²³. Comparativamente, afirmam que a desinformação seria nada mais que um subconjunto dentro da propaganda, ou seja, seria um instrumento para manipular a população pela emissão de conteúdo explicitamente falso, com elemento intencional claramente exposto pela própria definição²⁴.

Em sentido semelhante, Guess e Lyons tratam a propaganda como conteúdo que pode ser verdadeiro ou falso, mas que possui o objetivo de desacreditar o ponto de vista do adversário político²⁵. O elemento essencial da propaganda seria manipular indivíduos previamente segmentados, seja com a mentira ou com a verdade.

Para os fins buscados neste trabalho, serão analisados diversos pontos que podem ser caracterizados como propaganda. Entretanto, será restringida apenas à propaganda que utiliza o artifício da desinformação, buscando compreender como o conteúdo falso se expande no ambiente virtual, razão pela qual se fará pouco uso do termo propaganda em si, apesar da referência a ele nos momentos em que a desinformação busque manipular a população segmentada, com fins políticos.

Cabe ressalva de que em hipótese alguma o termo propaganda será utilizado como sinônimo de publicidade, que constitui foco principal do subcapítulo seguinte.

Por fim, há trabalhos acadêmicos sobre a temática que precisam considerar as expressões como sinônimas, já que eventuais agentes estudados podem fazer a confusão entre os termos, razão pela qual a definição prévia se torna

²³ BENKLER; FARIS; ROBERTS, 2018, p. 29-30.

²⁴ Ibid, p. 32.

²⁵ GUESS; LYONS, 2020, p. 11.

dispensável. Exemplificativamente, Brandshaw, Neudert e Howard, ao analisarem as respostas de governos ao uso maléfico das mídias sociais, tomando como amostragem os 100 países com maior número de usuários em 2016 e última atualização em 2018, precisaram utilizar termos como *fake news*, *propaganda* computacional ou online, *misinformation* e desinformação, dentre outros, para identificar como os governos de diversos países agiam, já que tais instituições podem não ter fidelidade à tecnicidade²⁶. Por exemplo, é possível que, buscando se referir ao mesmo objeto, determinado país crie uma Lei das *Fake News* e outro uma Lei de Combate à Desinformação. Evidentemente, até analisando outros trabalhos desenvolvidos, é possível perceber que os autores conheciam a distinção, mas precisaram superá-la temporariamente para atingir o objetivo da pesquisa e não limitar seu alcance em ato que poderia ser prejudicial.

2.2.

Publicidade personalizada e tratamento de dados pessoais

Neste tópico da dissertação, será tratado o conceito de publicidade personalizada, que pode ser conhecida por outros termos²⁷. A ideia é compreender o seu funcionamento, bem como os problemas e os benefícios atrelados a esta forma de geração de receitas para grandes empresas de tecnologia, mas também para canais de produção de conteúdo e anunciantes de pequeno, médio e grande portes.

A publicidade personalizada se constitui como um dos principais fatores de monetização ou lucratividade do ambiente virtual, inclusive para criadores de conteúdo, desde plataformas criadas por grupos que detinham controle sobre meios tradicionais de informação até pequenas agências e pessoas físicas, que elaboram conteúdo por meio de suas páginas, blogs, perfis ou canais.

De maneira simplificada, a publicidade personalizada é aquela que permite que usuários diferentes tenham acesso a anúncios distintos, ainda que estejam na mesma página e no mesmo momento²⁸. Assim, fica evidente que o foco do

²⁶ HOFFMANN; TAYLOR; BRADSHAW, 2019.

²⁷ Exemplos de termos alternativos para se referir a publicidade personalizada, frequentemente utilizados nas referências que respaldam nossa exposição: publicidade dirigida por algoritmos, anúncios algorítmicos, publicidade programática, publicidade direcionada, publicidade baseada em interesses ou publicidade comportamental.

²⁸ LEONARDI, Marcel. **Parecer sobre implicações da LGPD na publicidade personalizada**. IAB Brasil, 2021. Disponível em: https://iabbrasil.com.br/wp-content/uploads/2021/08/IAB-BRASIL_PARECER-JURIDICO_LGPD-E-PUBLICIDADE-PERSONALIZADA_MARCEL-LEONARDI.pdf. Acesso em 10 dez. 2021.

anúncio é o usuário (potencial consumidor) e não propriamente a página ou o conteúdo exibido.

Para Malthouse e Franks, trata-se de um modelo de compra de ambientes para exibição de anúncios personalizados para o público ideal, por meio do qual determinada mensagem chegará apenas àquele perfil de usuário que aparenta ser mais propenso a determinada ação em momento específico, conclusão a que se chega por análise de seu comportamento na rede²⁹.

Já para Busch³⁰, é uma forma de publicidade que se baseia em granularidade (personalização), negociação, atualização e criação em tempo real, além da automação. Tais fatores geram anúncios altamente direcionados, com base em impressões tiradas a partir da utilização da internet pelo usuário individualmente considerado. Trata-se de sistemas de leilões que negociam espaços publicitários disponíveis em sites de empresas de publicidade ou, sobretudo, em sites de terceiros. Tais negociações – ou leilões – ocorrem em milissegundos e o anunciante paga mais a partir do aumento de interação, enquanto o fornecedor do espaço recebe por isso. Há, portanto, incentivo para que grandes empresas de tecnologia ampliem a personalização para aumentar a receita. De outro lado, há incentivo para que os sites terceiros ampliem o tráfego e o engajamento em sua página para gerar interesse e converter a atenção em remuneração.

Boerman, Kruijemeier e Borgesi³¹ decantam o conceito de publicidade comportamental em dois elementos: o monitoramento do comportamento online e a segmentação, a partir do tratamento de dados pessoais, para exibição de anúncios altamente personalizados. Os dados utilizados para segmentação podem variar, mas possuem como marca comum o acompanhamento das atividades do usuário na internet, indo desde os dados de navegação, histórico de pesquisa, dados de consumo, vídeos assistidos, compras, e-mails e postagens em sites.

Para ilustrar, é por meio deste tipo de publicidade que um usuário que utiliza o buscador do Google ou do Facebook para procurar um tênis esportivo passa a

²⁹ MALTHOUSE; MASLOWSKA; FRANKS, pp. 32-33.

³⁰ BUSCH, Oliver. The programmatic advertising principle. In: BUSCH, Oliver (Ed.). **Programmatic advertising: the successful transformation to automated, data-driven marketing in real-time**. Springer: 2016. pp. 3-16.

³¹ BOERMAN, Sophie; KRUIKEMEIER, Sanne; BORGESIUS, Frederick. Online Behavioral Advertising: A Literature Review and Research Agenda. *Journal of Advertising*, 46 (3), 2017, ISSN: 0091-3367 print / 1557-7805 online DOI: 10.1080/00913367.2017.1339368, pp. 363-376.

ser exposto a anúncios sobre tênis e outros materiais esportivos durante a utilização de suas redes sociais ou ao acessar páginas de notícias, entretenimento e mesmo de compras.

Segundo Thomas³², os serviços direcionados produzem três vantagens principais: (i) anúncios baseados em históricos individuais são mais assertivos, se dirigindo ao consumidor que tem interesse relevante e atual; (ii) o custo é proporcional aos efeitos gerados; (iii) o resultado pode ser mensurado de maneira mais adequada.

Mills, Pitt e Ferguson³³ destacam que um comercial exibido na televisão possui valor muito mais alto e se baseia em um estudo aproximado acerca do público e do volume de audiência que determinado programa possui. Entretanto, a publicidade feita em meio digital traz uma lógica diversa: por um custo mais baixo, é possível atingir uma parcela demográfica melhor delineada, com maior personalização e grau de certeza. Assim, há redução de custos e riscos em troca do aumento de resultados para o anunciante.

A publicidade personalizada exige, portanto, o conhecimento acerca do perfil do usuário, com objetivo de transmitir a mensagem ao destinatário certo e no momento em que se encontra mais propício a realizar a ação: comprar, acessar, interagir e outras atividades. Para isso, são analisadas as interações de usuários com as diversas plataformas, informações dos dispositivos que utilizam e informações que fornecem diretamente³⁴.

Por meio da coleta dos mencionados dados pessoais, é possível traçar o perfil do usuário e categorizá-lo para viabilizar e aumentar a eficácia da publicidade personalizada. Segundo Busch³⁵, tal tipo de publicidade é marcada

³² THOMAS, Julian. **Programming, filtering, adblocking: advertising and media automation.** Media International Australia, 2018, p. 2-3.

³³ MILLS; PITT; FERGUSON, pp. 4-5.

³⁴ OS dados mencionados tornam o usuário identificado (ex. nome, CPF, documento de identidade) ou permite sua identificação indireta (ex. hobbies, sites que acessa, tempo em que passa conectado, IP). Assim, podem ser definidos como dados pessoais, nos termos mencionados pelo art. 5º, I da Lei Geral de Proteção de Dados (LGPD) e pelo art. 4º (1) do *General Data Protection Regulation* (GDPR):

Art. 5º, I da LGPD:

“Art. 5º Para os fins desta Lei, considera-se:

I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;”

Art. 4º (1) do GDPR:

“For the purposes of this Regulation:

(1) ‘personal data’ means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;”

³⁵ BUSCH, pp. 7-8

pela consideração de cada usuário individualmente, com processo automatizado de escolha, permitindo que oportunidades sejam selecionadas, avaliadas e precificadas em nível sem precedentes. O autor chega a considerar a granularidade (usuário individualmente considerado) e a automação como princípios da publicidade personalizada.

De fato, parece que a segmentação manual seria inviável para os anúncios direcionados³⁶. As técnicas utilizadas se enquadram na definição de perfilamento ou *profiling*, segundo Doneda³⁷, consistindo na utilização de algoritmos e de novas técnicas para elaboração de perfis, previsão de comportamentos e definição de preferências de usuários, com finalidades diversas, dentre as quais é citado o envio seletivo de mensagens publicitárias.

Portanto, há dois mecanismos essenciais para a publicidade personalizada: a utilização de algoritmos e um amplo banco de dados (*big data*).

Os algoritmos passam as ferramentas operadas pelas plataformas que atuam como intermediários: eles são programados para, a partir de critérios específicos, estabelecer onde determinado anúncio será exibido, focando no usuário e no momento mais favorável para exibição. A atuação algorítmica gera uma dificuldade em termos de transparência, controle e responsabilização. O debate ético que gira em torno da atuação algorítmica é complexo e merece ser ampliado, o que não se fará neste trabalho³⁸.

Ainda, de acordo com Gillespie³⁹, algoritmos são procedimentos que transformam dados coletados em uma resposta supostamente desejada, por meio de cálculos específicos, ou seja, transformam alguns dados reais em previsões que resultam de fórmulas matemáticas especificamente inseridas. Logo, os algoritmos podem ser utilizados para finalidades diversas, desde a previsão do comportamento de corpos celestes à antecipação do comportamento humano. Conforme o autor, seis pontos merecem atenção na análise de algoritmos. São eles:

³⁶ MILLS; PITT; FERGUSON, pp. 4-5.

³⁷ DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. São Paulo: Thomson Reuters, 2019, pp. 151-152.

³⁸ ROMANINI, Anderson Vinícius; MIELLI, Renata. A comunicação dominada pelas “big techs” digitais: superabundância informativa, espetáculo, alienação e fabricação de sentido no mundo algorítmico. *Revista Eptic*, v. 23, n. 1, jan-abr. 2021, ISSN 1518-2487, pp. 142-161.

³⁹ GILLESPIE, Tarleton. The Relevance of Algorithms. In: GILLESPIE, Tarleton; BOCZKOWSKI, Pablo; FOOT, Kirsten (ed.). **Media Technologies: essas on communication, materiality, and society**. Massachusetts: MIT Press, 2014. pp. 168-170.

a) Padrões de inclusão: são as escolhas feitas por trás da programação, ou seja, o que se determina na criação do algoritmo acerca do que deve ser buscado, considerado ou ignorado.

b) Ciclos de antecipação: as implicações geradas pelas tentativas de predição e a importância das conclusões obtidas pelos criadores dos algoritmos.

c) Avaliação de relevância: os critérios utilizados para análise de relevância.

d) Promessa de objetividade algorítmica: o uso da tecnicidade para dar uma aparência neutra, objetiva e não enviesada ao algoritmo.

e) Enredamento com a prática: como os usuários podem reconfigurar suas práticas e tornar os algoritmos lugares de confrontos políticos.

f) Produção de públicos previsíveis ou calculados: como a apresentação dos algoritmos contribuem para moldar a noção do público em si mesmo.

No caso da publicidade personalizada, o algoritmo possuiria duas principais funções: (i) identificar o perfil e as preferências do usuário e; (ii) definir onde serão exibidos anúncios para atingir o usuário certo e no momento mais favorável.

O primeiro ponto será melhor analisado adiante neste capítulo. Quanto ao segundo ponto, a alocação de verbas da publicidade que persegue o usuário ao invés de selecionar o meio em que serão exibidos os anúncios traz um problema, segundo Hartmann⁴⁰: “as empresas anunciantes recebem uma oferta de grupos demográficos cuidadosamente demarcados e tomam decisões baseadas em quem atingir com a propaganda”, ou seja, os anunciantes deixam de verificar se o site é confiável e se o conteúdo é de qualidade, mirando no usuário, onde quer que ele esteja e deixando a critério de algoritmos criados por grandes companhias as decisões sobre alocação de anúncios focados no usuário. Contornar efetivamente o problema demanda um estudo multidisciplinar do tema e outro foro de debates que foge ao escopo desta dissertação, que buscará formas de mitigá-lo.

Há, portanto, uma alienação entre o anunciante e o local onde seu anúncio é exibido. A partir do momento em que, por exemplo, uma determinada marca opta por ter sua produção publicitária exibida para mulheres jovens, entre 20 e 30 anos, de determinada região do planeta, não é esclarecido o critério que será

⁴⁰ HARTMANN, Ivar Alberto. Combinando Bibliotecas de Anúncios com Checagem de Fatos para Aumentar a Transparência sobre a Desinformação. *Direito Público*, [S.l.], v. 18, n. 99, out. 2021. ISSN 2236-1766. Disponível em: <https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/5741>. Acesso em 16 dez. 2021.

utilizado para atingir esse perfil de usuário. Se esta jovem frequenta sites com conteúdo saudável ou com conteúdo nocivo, o algoritmo – novo intermediário – a acompanhará e remunerará a página que houver exibido o anúncio. De maneira simples: a meta é atingir o usuário e convertê-lo em consumidor, independentemente da publicação que figurará ao lado do anúncio, salvo exceções.

Assim, retomando o exemplo do tênis esportivo, se determinado usuário realiza a busca no Google, os anúncios direcionados podem ser exibidos tanto em sites confiáveis, quanto em páginas de reputação e conteúdo duvidoso, o que ocorre sem intervenção humana e, muitas vezes, à revelia do consumidor e do anunciante, além da ausência de intenção da empresa de tecnologia que cria o algoritmo.

Pariser destaca que o Google e o Facebook⁴¹ são dois gigantes da publicidade direcionada que é feita no meio digital, em disputa direta neste mercado⁴². Graham demonstra que o Google obtém quase 90%⁴³ de sua receita a partir da publicidade, sendo o restante relegado à ampla variedade de serviços prestados⁴⁴. Zuboff discorre sobre a decisão do Google acerca da adoção de anúncios direcionados como forma de salvar a companhia e gerar lucro a partir daquela invenção que, inicialmente, objetivava exclusivamente ser o melhor e maior buscador do mundo⁴⁵. Para Busch, Facebook e Google foram os primeiros a adotar sistemas capazes de fornecer publicidade automatizada e movida a dados em tempo real⁴⁶.

Nesse sentido, o Google pode ser considerado a maior empresa de publicidade do mundo, especialmente publicidade personalizada. Por meio de acesso a informações do *Google Ads*, é possível se deparar com a seguinte mensagem⁴⁷:

⁴¹ No dia 28/10/2021, o Facebook Inc. anunciou sua substituição pela Meta Inc., que passou a figurar como controladora do conglomerado. Entretanto, foi mantido o termo “Facebook” pelos seguintes motivos: (i) o trabalho vinha sendo desenvolvido antes da data apontada; (ii) a alteração do termo não trouxe impactos substanciais para as controladas e para os objetivos deste trabalho e; (iii) as principais referências deste trabalho utilizam o termo “Facebook”.

⁴² PARISER, Eli. **O filtro invisível**. Rio de Janeiro: Zahar, 2012, p. 41.

⁴³ Pesquisas que adotam metodologias distintas tendem a variar o percentual, que gira em torno dos 90% apontados, ora para mais ora para menos.

⁴⁴ Graham, R. Google and advertising: digital capitalism in the context of Post-Fordism, the reification of language, and the rise of fake news. *Palgrave Commun* 3, 45 (2017). <https://doi.org/10.1057/s41599-017-0021-4>.

⁴⁵ ZUBOFF, Shoshana. **A era do capitalismo de vigilância**. Rio de Janeiro: Intrínseca, 2020. p. 103.

⁴⁶ BUSCH, p. 19.

⁴⁷ FAQ GOOGLE ADS. **Como o Google Ads Funciona?** Disponível em https://ads.google.com/intl/pt-BR_br/home/faq/. Acesso em 28 dez. 2021.

O *Google Ads* exibe seu anúncio quando as pessoas pesquisam on-line os produtos ou serviços que você oferece. Com uma tecnologia inteligente, o *Google Ads* exibe seus anúncios aos clientes em potencial no momento certo, quando eles estão prontos para realizar uma ação.

[...]

Quando o anúncio for aprovado, ele será exibido sempre que usuários na área de segmentação pesquisarem um produto ou serviço como o seu. Você só paga se os usuários interagem com o anúncio, por exemplo, quando clicam nele ou ligam para a empresa.

Da mesma forma, outras áreas do site demonstram que os anúncios são exibidos não apenas em sites do Google, como Youtube, Gmail ou Maps, mas também em milhões de outros meios, o que inclui páginas de notícias, aplicativos, dispositivos móveis e blogs⁴⁸. Assim, a personalização consegue não apenas delimitar quem é o usuário ideal, mas definir quando é o momento em que está mais propício para receber a mensagem direcionada.

A exibição de anúncios em sites do Google ou de terceiros, ocorrendo de forma apartada de interação direta do usuário, se chama campanhas da rede de display, que interage com ampla rede de páginas e blogs.

Para desativar a personalização, o usuário deve acessar sua conta, ir ao painel de navegação (dados e privacidade), selecionar a opção “suas atividades e os lugares em que esteve” e desativar a personalização dos anúncios. Imediatamente, o Google informa que encerrar a personalização não encerra a exibição de publicidade, mas pode torná-la menos útil e cômoda para o próprio usuário e que, de qualquer forma, continuará utilizando alguns dados pessoais, como localização e horário de navegação⁴⁹.

O Facebook, da mesma forma, promove seus serviços de publicidade com a seguinte mensagem: “Mais de 2 bilhões de pessoas usam o Facebook todo mês. Por isso, não importa qual tipo de público deseja alcançar, você o encontrará aqui”. Em suas orientações, o anunciante deve selecionar o público desejado (ex. faixa etária, gênero e localização), podendo oferecer um vasto detalhamento do usuário alvo para, em seguida, escolher onde deseja veicular o anúncio. Contudo, a escolha que cabe ao usuário é entre integrantes do grupo: se o anúncio será

⁴⁸ GOOGLE ADS. **Campanhas da Rede de Display**. Disponível em https://ads.google.com/intl/pt-BR_br/home/campaigns/display-ads/. Acesso em 28 dez. 2021.

⁴⁹ SUPPORT GOOGLE. Controlar os anúncios que você vê. Disponível em <https://support.google.com/ads/answer/2662856?hl=pt-BR&co=GENIE.Platform%3DAndroid>. Acesso em 20 dez. 2021.

exibido no Facebook, Instagram ou outros, já que a escolha da página e do perfil fica por conta da empresa de tecnologia⁵⁰.

Não é por coincidência que as duas gigantes lideram o mercado de publicidade personalizada. Zuboff destaca que os anúncios direcionados, localizados em site de terceiros, inclusive, trouxe ao Google o pioneirismo de sucesso financeiro⁵¹. Apesar de ter iniciado com estratégia distinta, o Facebook, que mirava em relações entre pessoas e não em pesquisas, também percebeu que a publicidade era capaz de mover altos montantes de dinheiro⁵².

Além disso, as empresas perceberam que aquele que obtivesse maior quantidade de dados pessoais poderia oferecer maior personalização e, portanto, obter maiores lucros, conforme se percebe em ilustração feita por Zuboff⁵³. Segundo a autora, se tratasse de uma fábrica, os dados pessoais seriam matéria-prima extraída de suas fontes – os usuários – enquanto os algoritmos funcionariam como máquinas que produziram produtos (predição e *profiling*) para serem vendidos aos verdadeiros clientes – os anunciantes.

A coleta de dados pessoais, por sua vez, nem sempre é muito clara ou tem sua finalidade elucidada. Rodotà⁵⁴ tratava das novas mídias com distintas funcionalidades, mas com exigência de fornecimento de dados pessoais para utilização de serviços relevantes aos usuários. Contudo, já alertava para a possibilidade de usos secundários altamente lucrativos. Assim, o usuário poderia fornecer informações acreditando possuir uma finalidade, sendo certo que tais informações poderiam ser utilizadas para objetivos diversos.

Como exemplo desta funcionalidade, basta citar o consumo de música em determinados aplicativos ou sites. De um lado, tal informação pode ser utilizada para sugerir ao usuário músicas similares e tornar sua vida mais prática em meio ao excesso de informação. De outro lado, tal dado pode ser utilizado para decifrar emoções, sentimentos e o momento vivido pelo usuário, facilitando o envio de publicidade personalizada, por exemplo.

Tal constatação fica mais clara quando são observados os meios criados pelo Google e Facebook para obtenção de alguns desses dados pessoais. O

⁵⁰ META FOR BUSINESS. **Anúncios do Facebook**. Disponível em <https://www.facebook.com/business/ads>. Acesso em 28 dez. 2021.

⁵¹ ZUBOFF, 2020, p. 83.

⁵² PARISER, pp. 40-42.

⁵³ ZUBOFF, 2020, pp. 85-88.

⁵⁴ RODOTÀ, Stefano. **A vida na sociedade da vigilância**: a privacidade hoje. Rio de Janeiro: Renovar, 2008, p. 46.

Google, por exemplo, ao perceber que precisaria de informações mais detalhadas e dados mais íntimos do usuário, passa a disponibilizar ampla gama de aplicativos e funcionalidades, muitas vezes sem custo para o usuário, tais como o Gmail e os Google Apps⁵⁵.

A empresa e o Facebook iniciam uma corrida para se tornarem onipresentes, adquirindo startups que não geravam lucro aparente, mas que traziam consigo fonte de informações. Foi o caso, por exemplo, da aquisição do YouTube pelo Google ou do WhatsApp e Instagram pelo Facebook. Apesar do prejuízo ou alto índice de processos envolvendo as empresas adquiridas, a quantidade de dados pessoais envolvidos era no mínimo considerável⁵⁶.

Apenas para ilustrar a ampliação da coleta de dados pessoais, a sociedade estaria rodeada por mecanismos com essa aptidão, a partir de recursos que circundam o cotidiano do usuário: transações econômicas e sociais mediadas por computadores e smartphones, dispositivos diversos, que variam de drones, carros automatizados, aparelhos para monitoramento de casa, dados ligados ao governo, instituições financeiras, planos de saúde, companhias aéreas, seguradoras, bem como atividades não mercantis, que incluem relações entre amigos e familiares, trocas de e-mail, publicação de fotografias e filmagens ou seleção de músicas⁵⁷. Sem mencionar, é claro, os produtos que são utilizados com frequência cada vez maior e se ligam à chamada internet das coisas (*IoT* ou *Internet of Things*), que são “um mundo onde objetos e pessoas, assim como dados e ambientes virtuais, interagem uns com os outros no espaço e no tempo” e que coletam uma quantidade grande de dados pessoais no dia a dia⁵⁸. Aqui, os exemplos variam bastante, indo desde assistentes virtuais, como a *Alexa*, televisores, lâmpadas, geladeiras, torradeiras, ar-condicionado, aspirador de pó, cafeteira e muitos outros objetos que devolvem funcionalidade ao titular de dados, mas que ampliam o consumo de informações por empresas de tecnologia.

Magrani destaca que tais mecanismos criam dossiês de informações que podem ser particularmente perigosos para a privacidade e proteção de dados pessoais de indivíduos e da coletividade⁵⁹.

⁵⁵ PARISER, p. 35.

⁵⁶ ZUBOFF, 2020, p. 123-125

⁵⁷ ZUBOFF, Shoshana. Big Other: capitalismo de vigilância e perspectivas para uma civilização de informação. In: BRUNO, Fernanda et. al. **Tecnopolíticas da Vigilância: perspectivas da margem**. São Paulo: Boitempo, 2018. pp. 26-33.

⁵⁸ MAGRANI, Eduardo. **A internet das coisas**. Rio de Janeiro: FGV Editora, 2018, p. 44.

⁵⁹ Ibid., p. 98.

Sintetizando, a publicidade personalizada envolve a coleta de dados pessoais para criação de perfis de usuários com objetivo de vender espaços de anúncios para empresas de portes variados a custos menos elevados que os veículos tradicionais, com a promessa de atingir audiência qualificada, no momento mais favorável e com maior possibilidade de controle.

Alguns pontos, contudo, requerem maior atenção: (i) falta transparência acerca dos critérios de escolhas, em relação ao anunciante; (ii) falta clareza quanto à finalidade do tratamento de dados pessoais dos usuários mirados por anúncios; (iii) os algoritmos tendem a ignorar a qualidade do conteúdo, apesar de fazerem distinções em relação a conteúdos mais explicitamente ilícitos, como pedofilia, violência ou tráfico de entorpecentes; (iv) similarmente, existe alta lucratividade a partir do público atingido, independentemente da qualidade do conteúdo publicado: o foco é o usuário e não a mensagem.

Nada obstante as considerações apontadas, a publicidade personalizada tem grande importância no ambiente virtual, viabilizando o crescimento de pequenos negócios e a manutenção de páginas menores que produzem conteúdo de alta qualidade, o que justifica que a resposta para os contratemplos sinalizados não seja o simples encerramento da prática, tampouco a criação de óbices que impeçam o avanço econômico e tecnológico ou mesmo a proteção da liberdade de expressão.

Conforme destacado por Anderson⁶⁰, o Google presta serviços de publicidade personalizada para as maiores empresas do mundo, mas também para pequenos anunciantes que nunca haviam anunciado qualquer produto ou serviço em outros meios – de páginas amarelas a canais de televisão. Além disso, parte expressiva de sua receita não vem de grandes marcas, mas daqueles pequenos anunciantes que, em conjunto, ultrapassam de forma considerável a receita de grandes players dos mercados.

Da mesma forma, os pequenos editores de conteúdo online passam a ser remunerados sem necessidade de possuir força própria de venda de espaços publicitários, detidos anteriormente por grandes veículos de imprensa, por exemplo. Qualquer blog ou página pode oferecer seu espaço para o Google, que

⁶⁰ ANDERSON, Cris. **The Long Tail: Why the future of business is selling less of more**. Hyperion Books, 2008, pp. 24, 210-216.

aloca o anúncio no espaço disponível e remunera o anfitrião (ex. página de notícias) por cliques.

Assim, conhecendo o usuário, é expandido o resultado para o anunciante e a receita para o produtor de conteúdo. Delegando a função a algoritmos ou softwares, era possível facilitar a mensuração e reduzir os custos de anúncios, sem mencionar a melhoria de resultados. Além disso, seria possível atender desde grandes companhias, passando por médios anunciantes e chegando a pessoas físicas – o Google aproveitou essa análise e criou instrumentais para cada categoria.

Em parecer para o IAB Brasil (*Interactive Advertising Bureau*)⁶¹, Leonardi destaca os benefícios da publicidade direcionada sob diversas perspectivas: do consumidor, dos anunciantes e da sociedade. Ao tratar dos anunciantes, expõe que a atividade publicitária “viabiliza que pequenos negócios façam publicidade de modo acessível e a custos baixos, alcançando consumidores que de outra forma dificilmente saberiam da existência de seus produtos ou serviços”. Sobre o ganho para a sociedade, trata de diversos pontos, sobretudo o fortalecimento de um jornalismo independente que pode ter seus gastos custeados por anúncios de maneira facilitada, bem como a democratização do conteúdo na internet.

A mudança no estilo de financiamento deve ser pensada para proteger o titular, gerar maior segurança ao anunciante – principalmente o de médio e pequeno portes, mas preservando um modelo que permita assegurar os demais direitos e vantagens apontados. Restrições exacerbadas e desproporcionais poderiam representar riscos a pequenos sites de notícias ou páginas de pessoas físicas que possuam compromisso com o leitor e produzam conteúdo de qualidade e bem apurado⁶².

Para Thomas⁶³, o sucesso do jornalismo futuro depende da compreensão de como funciona a propaganda no ambiente virtual, especialmente quanto à personalização, já que seria fonte de renda para os veículos de comunicação. Do lado do anunciante, seria um tempo em que, pela primeira vez, pequenos e médios anunciantes teriam a oportunidade de realizar anúncios que se assemelhavam a grandes players do mercado. Simplificando: a um custo baixo, o anunciante insere o anúncio publicitário para obter efeitos, o que remunera os veículos de

⁶¹ LEONARDI, pp. 2-4.

⁶² BRAUN, Joshua; EKLUND, Jessica. Fake News, Real Money: Ad Tech Platforms, Profit-Driven Hoaxes, and the Business of Journalism, 7(1) **Digital Journalism** 1 (2019).

⁶³ THOMAS, pp. 3-4.

comunicação e gera lucros, também e sobretudo, para grandes empresas de tecnologia, como o Google e o Facebook.

A presente dissertação busca contribuir com o debate, analisando medidas que podem mitigar ou instigar a reflexão acerca dos problemas apontados, sem descuidar da necessária tutela dos benefícios aventados.

2.3.

Desinformação monetizada

O estudo da publicidade personalizada é fundamental para compreender a particular lucratividade gerada para sites que se dedicam a desinformar o usuário. A desinformação pode ser produzida por fatores ideológicos, sobretudo no contexto político e por alas mais radicais da sociedade e talvez seja essa a face mais visível no dia a dia, seja por notícias dadas pela grande mídia, seja por interação em canais menores e até nas redes sociais.

Contudo, conforme se verá, outro fator que contribui para a produção e disseminação de conteúdo intencionalmente falso é a lucratividade a que se vincula, ou seja, há páginas, blogs, sites e veículos de comunicação com tamanhos variados que produzem desinformação com objetivo estrito de obter altos montantes de lucros oriundos de publicidade e obtêm êxito na empreitada. Por tais razões, é relevante analisar os fatores que viabilizam a monetização deste tipo de conteúdo nocivo.

É difícil imaginar que, salvo exceções, empresas de portes variados tenham a mínima intenção de vincular sua marca, produto ou serviço a notícias falsas, sobretudo aquelas que trazem perigo ao leitor ou que agredem determinado indivíduo ou coletividade.

De acordo com a pesquisa realizada, parece que a publicidade personalizada, orientada por dados pessoais e dirigida por algoritmos, possui relevante papel na alocação de recursos em páginas que se dedicam à reiterada produção de conteúdo intencionalmente falso. Assim, haveria indicação de que, sem negar a existência de alguma inércia, nem anunciantes nem a audiência nem as empresas de tecnologia buscariam fomentar a desinformação de maneira voluntária, o que parece um fator relevante na busca de incentivos para redução do problema.

Segundo Mills, Pitt e Ferguson⁶⁴, existem três principais tipos de desinformação: a desinformação inadvertida, a desinformação ideológica e a *exploitative disinformation*.

A primeira, conforme visto no início deste trabalho, é aquela que tem sido chamada pela literatura de *misinformation*, que é a notícia falsa que não se reveste de intencionalidade do autor. Nela, ainda que não tenham sido adotados os padrões de uma imprensa profissional para minar tais ocorrências, não há produção deliberada de conteúdo falso, se confundindo com o erro jornalístico, que não é o alvo deste trabalho. A segunda é a desinformação que pode ser enquadrada como propaganda, ou seja, aquela usada por indivíduos ou organização para desacreditar adversários e alterar comportamentos da audiência. A terceira, que é o objeto principal deste trabalho, é a desinformação que persegue o lucro. Aqui, não importa a ideologia defendida – se direita ou esquerda, progressista ou conservadora – o objetivo é criar e distribuir conteúdo falso com intuito de ganhar dinheiro com essa prática. Como analisamos em tópico anterior, atrair a atenção do usuário é fundamental no empreendimento de obter receita a partir de publicidade direcionada.

Wardle⁶⁵ destaca quatro principais motivações para a desordem informacional: financeira, política, social e psicológica. Para este trabalho, importa a motivação financeira que, segundo a autora, é aquela que gera a desinformação com intuito lucrativo por meio de receitas advindas de publicidade. Trata-se de uma verdadeira indústria, criada para fabricar notícias falsas e gerar lucros por meio dessa criação, o que é possível apenas em razão da lógica de remuneração via publicidade personalizada, destacando a atuação do Google e do Facebook naquela seara. Essa lógica precisa ser combatida de forma conjunta, tanto pelas empresas de publicidade quanto por anunciantes⁶⁶.

Para Benkler, Faris e Roberts⁶⁷, uma rede de estudantes que criava *clickbait*s e desinformação para atrair atenção de usuários convertiam tal atenção em receita: “os empreendedores que criaram esses sites [...] desviaram a atenção e os dólares de publicidade da mídia “legítima”, manipularam o algoritmo do

⁶⁴ MILLS; PITT; FERGUSON, p. 4.

⁶⁵ WARDLE, Claire; DERAKHSHAN, Hossein. **Information Disorder: Toward an interdisciplinary framework for research and policy making**. Council of Europe, 2017, pp. 25, 34-35.

⁶⁶ *Ibid.*, p. 80.

⁶⁷ BENKLER; FARIS; ROBERTS, p. 9, original: “the social media entrepreneurs who created these sites [...] diverted attention and advertising dollars from “legitimate” media, they manipulated Facebook’s algorithm, they were mostly foreign in these stories, and they were purely in it for the money”

Facebook e estavam nessa apenas pelo dinheiro". Neste momento, o presente trabalho não ingressará no debate sobre o papel decisivo de redes sociais e da mídia tradicional. Os autores admitem que parte considerável da desinformação, da propaganda e de teorias da conspiração surgem no meio digital e são ecoados pela mídia tradicional, denotando a relevância do conteúdo publicado na internet, ainda que coloquem em suspeição a eficácia do ambiente virtual para impactar, sozinho, em pleitos importantes como as eleições.

Syed⁶⁸ já destacava que o ambiente virtual tornava a desinformação particularmente lucrativa, por meio da criação de padrões de propaganda que remuneravam a página exclusivamente pelo clique e por interação, independentemente do conteúdo nela veiculado. O mecanismo é favorecido por dois fatores: de um lado, criação de conteúdo mais barata e, de outro, a possibilidade de tornar o conteúdo falso com aparência de veracidade altamente lucrativo.

O montante global movimentado por essa indústria e os ganhos individuais são relevantes. Citando artigo de Sydel, os autores Braun e Eklund⁶⁹ falavam em ganhos entre 10.000 e 30.000 dólares por produtor ao mês, no auge de seus trabalhos nas eleições norte-americanas de 2016. A CNN Money⁷⁰ demonstrou que, operando na Macedônia, sem qualquer manto de ilegalidade e sob argumento de que não há moralidade na política, pelo menos 100 sites dedicados a desinformação atuaram naquele pleito eleitoral, gerando receitas milionárias para estudantes que aprenderam a tornar virais alguns de seus conteúdos. Segundo Silverman⁷¹, os sites traziam notícias atraentes e com aparência de veracidade e, com isso, atraíam o interesse dos usuários e convertiam essa atenção em dólares oriundos de receita publicitária, com alcances de 3.000 dólares por dia em determinados casos.

⁶⁸ SYED, Nabihah. **Real Talk About Fake News: Towards a Better Theory for Platform Governance**. The Yale Law Journal, v. 127 (2017). Disponível em <http://www.yalelawjournal.org/forum/real-talk-about-fake-news>. Acesso em 03/01/2022.

⁶⁹ BRAUN; EKLUND, p. 10-15.

⁷⁰ DAVEY-ATTLE, Florence; SOARES, Isa. The Fake News Machine: inside a town gearing up for 2020. **CNN MONEY**, 2020. Disponível em: <https://money.cnn.com/interactive/media/the-macedonia-story/>. Acesso em 03/01/2022.

⁷¹ SILVERMAN, Craig; ALEXANDER, Lawrence. How Teens In The Balkans Are Duping Trump Supporters With Fake News. **BuzzFeed**, 03/11/2016. Disponível em: <https://www.buzzfeednews.com/article/craigsilverman/how-macedonia-became-a-global-hub-for-pro-trump-misinfo>. Acesso em 03/01/2022.

Na mesma linha, Berthon e Pitt⁷² destacam a criação de uma indústria de desinformação construída em alguns países, como é o caso dos mencionados “Meninos da Macedônia”. Toda indústria busca o lucro e, segundo os autores, tal lucro viria do financiamento feito por marcas que patrocinam os portais que se dedicam a disseminar desinformação. Nem sempre de maneira direta, mas justamente em razão da automação na escolha de plataforma, perseguindo o usuário e não a confiabilidade do conteúdo. Por meio da alienação entre o dono da marca e o local de anúncio, cria-se o ambiente propício para a lucratividade oriunda da desinformação.

É claro que algumas medidas acabam sendo adotadas, como a comparação do site com plataformas que integram uma espécie de *blacklist*, para evitar que as marcas figurem ao lado de tráfico de entorpecentes, pornografia, pedofilia e outras atividades que não se coadunam com aquilo que é enunciado. Entretanto, a desinformação não é tão simples de ser descoberta. Em primeiro lugar, em razão da similaridade que é conferida e que torna dificultosa a distinção entre desinformação e notícia verdadeira. Em segundo lugar, porque a instantaneidade e a dinâmica do ambiente virtual exigem produção massiva de conteúdo, o que gera a criação de conteúdo frequentemente mal apurado (*misinformation*), que não desabilitariam o site pela ausência de conduta reiterada ou intencionalidade.

O que as marcas buscam é o resultado. As empresas de publicidade personalizada, por sua vez, recebem maior remuneração com o aprimoramento do resultado oferecido para seus anunciantes. Portanto, quanto maior o fluxo de usuários, sobretudo usuários qualificados e com maior propensão a consumir determinado produto ou serviço, melhor é o ambiente para exibição de anúncios, o que acaba deixando o tema da desinformação como secundário.

O anúncio persegue o usuário e muitos usuários tendem a acessar sites que contenham desinformação. Segundo Vosoughi, Roy e Aral⁷³, a desinformação alcança amplas audiências.

Trata-se, portanto, de mais um incentivo para a criação de desinformação com objetivo exclusivo de obtenção do lucro: afastado de ideologia e de moralidade, a criação seria mais apta a atrair cliques e compartilhamentos,

⁷² BERTHON, P. R.; PITT, L. F. (2018). **Brands, Truthiness and Post-Fact**. *Journal of Macromarketing*, 38(2), 218–227. doi:10.1177/0276146718755869.

⁷³ VOSOUGHI, Soroush; ROY, Deb; ARAL, Sinan. **The Spread of True And False News Online**. MIT Initiative on the digital economy research brief, 2018.

gerando maior tráfego de usuários e, conseqüentemente, receita oriunda de publicidade, não importando seu conteúdo.

Hartmann⁷⁴ sustenta que “o sistema de anúncios algorítmicos recompensa editores cujas publicações são pensadas dentro da lógica de maximizar atenção – e nada mais”. Se trata da lógica de geração de capital, atingindo o usuário e remunerando aquele que melhor atrai sua atenção, seja ele produtor de desinformação ou não.

A escolha algorítmica aliena o anunciante do local onde o anúncio é exibido. Os mecanismos de impulsionamento criados pela publicidade direcionada contribuem para o surgimento de indústrias de desinformação que, como tais, se especializam na criação e disseminação de conteúdo nocivo com intuito exclusivo de lucro⁷⁵.

Por meio da coleta massiva de dados pessoais e construção de perfis que permitem o direcionamento de anúncios, empresas de publicidade como Google, Facebook e outras passaram a ocupar o privilegiado espaço que existe entre o anunciante, o produtor de conteúdo e a audiência. Não há exata transparência para qualquer das partes⁷⁶.

Não há, portanto, inserção voluntária de anúncios publicitários ao lado da desinformação, pelo menos não como regra. Os instrumentos de escolha são opacos e performáticos, ou seja, não há clareza de critérios e há uma transformação por meio de aprendizado de máquina.

Braun e Eklund⁷⁷ explicam como funciona a engenharia utilizada por editores de conteúdo que criam desinformação com objetivo de lucro e justificam por que anunciantes e empresas de tecnologia que operam a publicidade personalizada tolerarem a desinformação, de forma não proposital.

Do ponto de vista do anunciante, o principal incentivo é o barateamento da publicidade em páginas de menor renome, mas que acabam gerando resultado satisfatório, pois é possível atingir o público segmentado mesmo em páginas

⁷⁴ HARTMANN, p. 466.

⁷⁵ WESTRUP, Ana Carolina. Para além da aparência: saídas amplas e democráticas. In: MARTINS, Helena (org.). **Desinformação: crise política e saídas democráticas para as Fake News**. São Paulo: Veneta, 2020.

⁷⁶ PASQUALE, Frank. *The Black Box Society. The Secret Algorithms That Control Money and Information*. Harvard University Press, 2015. pp. 69-72.

⁷⁷ BRAUN; EKLUND, p. 10-26.

menores, menos conhecidas e com conteúdo suspeito, criado com o simples objetivo de atrair esse tipo de receita.

Do ponto de vista das empresas de tecnologia, há uma exacerbada dificuldade de identificação da desinformação, sobretudo quando se compara com outros tipos de conteúdo nocivo: a pornografia, a pedofilia, o tráfico de entorpecentes e outras questões são de mais fácil detecção. Até mesmo o discurso de ódio é de mais fácil rastreio. A desinformação, por sua vez, é criada para se assemelhar a conteúdo legítimo, o que dificulta a seleção algorítmica. A criação de listas também não parece atender suficientemente aos objetivos de combate à desinformação: o *blacklisting ban* gera o banimento de páginas que propagam conteúdo nocivo, inclusive desinformação. Contudo, o surgimento diário de milhares de páginas torna o mecanismo insuficiente. O mesmo cenário ocorre com o *whitelisting*, que é a criação de um rol de sites confiáveis. Aqui existem dois problemas: a seleção é difícil e pode gerar a não recomendação de sites com conteúdo de qualidade, por mera falha de escolha em meio a milhares de páginas. Por fim, eventual gradação de níveis de editores, mais ou menos confiáveis, com espaços publicitários mais ou menos caros a depender do grau atribuído, tornaria a seleção um produto premium e marginalizaria anunciantes de menor porte, ou seja, apenas grandes empresas conseguiriam anunciar em sites confiáveis, enquanto pequenos negócios ficariam com os sites com conteúdo suspeito ou, alternativamente, acabariam quebrando seus empreendimentos em razão do alto investimento necessário para driblar a desinformação – a solução não satisfaz.

Apesar dos pontos mencionados, o *blacklisting ban* e o *whitelisting* não devem ser descartados de plano, já que oferecem vantagens para o anunciante que refletem na sociedade, a partir do momento em que reduzem a monetização da desinformação. Tais aspectos serão desenvolvidos na última parte deste trabalho, que versará sobre instrumentos concretos que podem contribuir para o combate à desinformação por meio do redirecionamento de receitas oriundas da publicidade personalizada.

De maneira sintética, o artigo expõe que a transparência é fundamental para solucionar a questão. O afastamento entre o anunciante e o local de anúncio, bem como a presença de número alto de intermediários, contribuiriam para o que chamou de ecossistema nocivo de publicidade direcionadas.

O tema ganha importância e sofre influência do impacto causado pelo movimento *Sleeping Giants*, que se autodefine como “uma campanha pela responsabilidade da mídia, da publicidade e de plataformas digitais”⁷⁸, com equivalente brasileiro denominado *Sleeping Giants Brasil*, descrito como “um movimento de consumidores contra o financiamento do discurso de ódio e da desinformação”⁷⁹.

Tal movimento tem aparecido em notícias como responsável pela mudança de comportamento de algumas empresas e marcas e pela redução milionária de publicidade que custeava a desinformação e o discurso de ódio.

Bezerra e Borges⁸⁰ analisaram o movimento e definiram sua tática como tentativa de desmonetizar um ecossistema nocivo, que inclui a desinformação. Com isso, o movimento *Sleeping Giants* levaria ao conhecimento de marcas e empresas a existência de anúncios de sua autoria em sites com conteúdo falso intencionalmente criado para enganar o leitor. Tais empresas não tinham conhecimento do fato e, não raramente, retiraram seus aportes publicitários, retirando a lucratividade das páginas. O objetivo do grupo, portanto, não é boicotar tais empresas, que desconhecem o teor daquilo que financiam, mas alertá-las com objetivo de desmonetizar a desinformação:

A despeito do desconforto de uma notificação pública nas redes sociais, *Sleeping Giants* não pode ser acusado de assédio às marcas ao flagrá-las financiando discursos de ódio. Na verdade, *Sleeping Giants* acaba por prestar um serviço às empresas, prevenindo-as de prejuízos à imagem de suas marcas e colaborando para que sejam mais vigilantes sobre onde estão posicionando seus anúncios na internet.

Segundo notícia do El País⁸¹, o movimento levou 4.500 anunciantes a retirarem seus anúncios do Breitbart News, que teve prejuízo de US\$ 50.700.000,00 (cinquenta milhões e setecentos mil dólares). Com objetivo de informar empresas sobre o patrocínio que suas marcas faziam ao site de conteúdo nocivo, o movimento printava telas e divulgava nas redes sociais dos próprios anunciantes.

⁷⁸ Twitter. **Sleeping Giants**. Disponível em https://twitter.com/slpng_giants. Acesso em 12/01/2022.

⁷⁹ Instagram. **Sleeping Giants Brasil**. Disponível em https://www.instagram.com/slpng_giants_pt/?hl=pt-br. Acesso em 12/01/2022.

⁸⁰ BEZERRA, Arthur Coelho. **Sleeping Giants: a ofensiva moral dos gigantes adormecidos contra o novo regime de desinformação**. Revista Eptic, v. 23, n. 1, jan-abr, 2021. ISSN 1518-2487.

⁸¹ QUEIMALIÑOS, Rebeca. **O homem que arruinou a extrema direita nos EUA**. El País. 17 de maio de 2020. Disponível em <https://brasil.elpais.com/icon/2020-05-17/o-homem-que-arruinou-a-extrema-direita-nos-eua.html>. Acesso em 12/01/2022.

Segundo Benkler, Faris e Roberts⁸², o Breitbart News atuou como ponto central na campanha de Donald Trump, servindo como veículo de extrema direita que utilizava desinformação como propaganda, voltada a atacar não apenas democratas, mas também republicanos que teriam disputado as prévias com Trump ou que, posteriormente, fizeram oposição ao candidato. O canal teria feito, ainda, campanhas anti-imigração e *anti-mulçumana*.

O que impressiona é o fato de que essas marcas desconheciam tal realidade, ou seja, financiavam a desinformação e o ódio em montantes significativos e não tinham noção de que isso ocorria. Tal relato corrobora o fato de que o ecossistema da publicidade personalizada mira no usuário, onde quer que esteja, não importando se consome conteúdo de qualidade ou se é levado pelas criações do Breitbart News e que, por sua vez, o anunciante – que paga a conta – não teria o conhecimento de tais fatos.

No Brasil, o movimento também produziu efeitos. De acordo com O Globo⁸³, *Sleeping Giants* teria evitado que mais de R\$ 14.000.000,00 (quatorze milhões de reais) patrocinassem a desinformação, com apenas um ano de funcionamento. A supressão dos valores inclui a evasão de pequenos anunciantes, mas também de grandes marcas, como Bradesco, Adidas, Ford, Fiat, Uber e Amazon, que aportavam valores sem saber que suas marcas, já consolidadas, figuravam ao lado de desinformação, o que reitera o mecanismo narrado, causador de alienação entre o anunciante e o local de publicação. O que reforça o desconhecimento é a imagem negativa que transmitem, prejudicando o sucesso já consolidado.

No Senado, o Movimento inspirou a proposta de Emenda 39 ao Projeto de Lei nº 2.630 (“PL das Fake News”), cujo teor é idêntico ao do Projeto de Lei nº 2.922/2020⁸⁴, e propunha responsabilizar empresas de tecnologia que atuavam com publicidade personalizada pela veiculação de anúncios ao lado de conteúdo desinformativo ou discurso de ódio. Segundo a justificativa, a ideia era isentar

⁸² Network Propaganda, pp. 54-60.

⁸³ SONAR. **Em um ano Sleeping Giants Brasil evitou mais de R\$ 14 milhões em publicidade a sites de fake news, calculam os fundadores**. Publicado em 26 de maio de 2021. Disponível em: <https://blogs.oglobo.globo.com/sonar-a-escuta-das-redes/post/em-um-ano-sleeping-giants-brasil-evitou-mais-de-r-14-milhoes-em-publicidade-sites-desinformativos-calculam-fundadores.html>. Acesso em 04/01/2022.

⁸⁴ BRASIL. Senado Federal. Emenda ao Projeto de Lei nº 2.630 de 2020. Inclui a disposição “Art. As empresas, nacionais e estrangeiras, que forneçam serviços de mídia programática não poderão veicular anúncios em páginas da internet que contenham desinformação. Brasília: Senado Federal, 2020. Disponível em <https://legis.senado.leg.br/sdleg-getter/documento?dm=8117340&disposition=inline>. Acesso em 04/01/2022.

anunciantes, já que não possuíam controle e conhecimento sobre o local onde seus anúncios eram exibidos. A Emenda foi rejeitada, porque o termo desinformação não seria mencionado diretamente no PL 2.630, restando a proposta prejudicada, ou seja, rejeitada sem análise do mérito⁸⁵.

De fato, a proposta parecia vaga, simplista e não apontava para soluções concretas, seguindo o caminho de estabelecer responsabilidades em detrimento de obrigações que possam gerar efetivos acertos pelo poder público, com reflexo na atuação de empresas privadas.

Contudo, o caminho regulatório que aponte para soluções que desmonetizem a desinformação é desejável, restando debater temas como o arranjo institucional, a forma e a abrangência. Mais do que estabelecer responsabilização posterior, concentrar esforços na prevenção de riscos e danos e desmonetizar retira o estímulo para produção de parcela relevante da desinformação – aquela que se baseia em obtenção de receitas oriundas de publicidade.

Nada obstante a importância de movimentos e iniciativas como do *Sleeping Giant*, eles ainda são insuficientes diante da magnitude de receita publicitária arrecadada pelas duas maiores empresas de publicidade do mundo: o Google e o Facebook, que vêm alterando suas políticas e normas internas para se prevenir a ocorrência de danos ligados à desinformação.

Segundo Rivitz, criador do *Sleeping Giants* “esse tipo de publicidade é uma farsa. Os anunciantes precisam de ferramentas que forneçam transparência para encontrar conteúdos de qualidade”⁸⁶. A análise apontada ratifica isso. Quando informados acerca da alocação de seus anúncios, parte considerável das empresas notificadas retiraram, voluntária e preventivamente, seu dinheiro de tais plataformas, o que denota que mecanismos que facilitassem a identificação poderiam ser eficazes aliados da desestruturação dos criados de desinformação.

Portanto, parece existir um interesse conjunto da sociedade civil no debate do tema, o que engloba o poder público, o usuário da internet, os editores que atuam na mídia legítima, os anunciantes e as próprias empresas de tecnologia.

⁸⁵ BRASIL. Senado Federal. Parecer do Relator no Projeto de Lei 2.630 de 2020. Brasília: Senado Federal, 2020. Disponível em: <https://legis.senado.leg.br/sdleg-getter/documento?dm=8127630&ts=1630418520274&disposition=inline>. Acesso em 04/01/2021.

⁸⁶ QUEIMALIÑOS, Rebeca. EL PAÍS.

Assim, os movimentos devem ser incentivados, inclusive pelo poder público, mas deve ser buscada uma solução mais eficiente, simultaneamente. Tal solução não deve apontar apenas para os sintomas ou as consequências, mas para a causa, que reside na lógica de funcionamento da publicidade direcionada: baseada no usuário, com alienação entre o anunciante e o espaço publicitário e a falta de transparência, tanto para o titular quanto para as empresas que realizam publicidade.

Borges e Bezerra⁸⁷ destacam que o movimento é limitado pela estrutura de vigilância de dados pessoais, sobre a qual é construída a lógica de publicidade personalizada em ambientes informatizados. Neste sentido, o fundador do *Sleeping Giants* também afirma que, apesar de haver causado prejuízo financeiro a produtores de desinformação, ainda não se alcançou uma mudança sistêmica, relevante e necessária.

O presente trabalho busca apresentar propostas de regulação que possam contribuir para o debate a respeito de possíveis soluções. A princípio, parece que o combate incidental à desinformação é bastante relevante, mas que a mudança estrutural é fundamental para subtrair o potencial lucrativo da desinformação, o que dificilmente ocorrerá de maneira apartada do tema da privacidade e proteção de dados pessoais. A transparência também parece ter papel relevante: de um lado, diante do usuário e, de outro, perante o anunciante que precisa conhecer onde seus anúncios serão exibidos. Outro princípio importante é o da *accountability*, que impõe maior responsabilidade e incentiva a cooperação das empresas de tecnologia no combate à desinformação.

Nesse sentido, a última parte desta dissertação conterá propostas e sugestões que possam mitigar as causas que tornam a desinformação altamente lucrativa. Algumas medidas constantes da última versão do PL 2.630/2020⁸⁸ serão analisadas, tais como a biblioteca de anúncios e outras disposições ligadas à transparência e à criação de instrumentos de *accountability*. A redação atual contém problemas graves que podem afastar a cooperação de importantes setores da sociedade, especialmente as empresas de tecnologia, principais detentoras da expertise sobre publicidade personalizada. O objetivo é propor uma

⁸⁷ BORGES E BEZERRA.

⁸⁸ BRASIL. Câmara dos Deputados. Complementação de voto do relator. Deputado Orlando Silva. Disponível em https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=2115425. Acesso em 08.03.2022.

solução integrada, que não relegue o tema apenas ao mercado, mas que também não o aliene da questão tratada.

Outros instrumentos regulatórios que serão trabalhados no último capítulo estão presentes na Lei Geral de Proteção de Dados (“LGPD”), que tem como objetivo “proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural”. A norma traz importantes fundamentos, conceitos e princípios que podem contribuir com o combate à lucratividade da desinformação por meio da publicidade personalizada, sobretudo pela previsão da transparência, responsabilidade, prestação de contas e da possibilidade de tratamento de dados pessoais com base no legítimo interesse, como ocorre no caso da publicidade personalizada. Tal hipótese exige a elaboração de documentos que permitem o conhecimento detalhado da operação, a previsão de riscos e a adoção de medidas para mitigá-los. Se trata de previsões que já estão em vigor e vêm sendo praticadas por empresas de diversos ramos de atuação, o que contribui para o direcionamento mais célere para o combate à desinformação.

3

Aspectos estruturais da regulação da publicidade personalizada

3.1.

Regulação e desinformação

O tema da regulação de novas tecnologias frequentemente esbarra na preocupação com cerceamento de direitos fundamentais, em especial a liberdade de expressão. O conflito é apontado em trabalhos acadêmicos, debates políticos e publicações feitas por veículos de comunicação e grandes empresas de tecnologia. Quando tal regulação é associada ao combate à desinformação, a preocupação tende a aumentar, haja vista as variadas tentativas, bem-intencionadas ou não, de intervenção direta no conteúdo e no discurso.

Conforme destacado por Karanicolas, uma tendência mundial agravada pela pandemia da COVID-19 é o surgimento de legislações que criminalizam o discurso, trazem um conceito próprio de verdade (o conceito estabelecido por quem detém o poder) e provêm instrumentos de perseguição da imprensa e da oposição política, a pretexto do legítimo combate à desinformação e à *misinformation*⁸⁹.

De outro lado, a ausência absoluta de regulação multinível não tem sido o melhor caminho para a liberdade de expressão, sobretudo no ambiente virtual, intermediado por grandes empresas de tecnologia que atuam em escala global, com regras que frequentemente derivavam de autorregulação sem intervenção externa relevante. Pasquale⁹⁰ denuncia que poderosas empresas de tecnologia vêm censurando o discurso e reprimindo a fala ocorrida na internet ao redor do mundo, por meio de políticas, procedimentos e algoritmos muitas vezes obscuros e com poucas oportunidades de auditoria. Nesse contexto, menciona o caso de uma antiga vice-conselheira do Google, que figurava como a pessoa mais poderosa do mundo para determinar quem poderia falar, qual seria o conteúdo e quem poderia ser ouvido no ambiente virtual, o que ocorria por meio de critérios

⁸⁹ KARANICOLAS, Michael. Introduction – Understanding the Challenge. In: KARANICOLAS, Michael (Ed.). *Tackling the “Fake” Without Harming the “News”*. New Haven: Yale Law School, 2021, p.3-9.

⁹⁰ PASQUALE, Frank. *Platform Neutrality: Enhancing Freedom of Expression in Spheres of Private Power*. University of Maryland Legal Studies Research Paper, n. 2016-24, 29p.

opacos de remoção de conteúdo ou desindexação. No caso mencionado, o poder que cercearia a liberdade de expressão seria oriundo de uma empresa privada ou, mais especificamente, de um número restrito de funcionários que estabeleceriam critérios e que não teriam balizas externas relevantes para atuação. O que gera a concentração de poderes para moderar o discurso é justamente a presença de um número restrito de intermediários que atuam em escala global e dominam a tecnologia onde parte considera daqueles discursos ocorre, como é o caso do Facebook, Instagram e WhatsApp (Meta), Google, Twitter, Telegram e outras plataformas. Por tais razões, o autor defende que a tentativa de regulação para restringir a atuação de tais intermediários e torná-los mais responsáveis não seria necessariamente lesiva à liberdade de expressão, mas, pelo contrário, figuraria como um aliado em seu fortalecimento.

O ideal é que a eventual moderação de conteúdo ocorra de maneira transparente, moderada e com possibilidade de controle externo, tanto pelo usuário quanto pelo poder público. Além disso, a regulação deve se ligar a aspectos estruturais, em detrimento de regulação de conteúdo em si.

É importante lembrar que importantes empresas de tecnologia já obstruíram diversas tentativas ilegítimas de interferência que são feitas por determinados governos autoritários, que buscam derrubar canais, conteúdos, desmonetizá-los ou desindexá-los, mas que têm os intentos frustrados pela atuação daquelas plataformas que atuam como intermediárias⁹¹. Portanto, a regulação deve ser menos focada no conteúdo e não deve colocar o poder exclusivamente nas mãos de qualquer parte, seja do poder público ou de empresas privadas.

Keller⁹² propõe medidas de maior alcance e que possuam eficácia mais ampla, considerando que parte relevante das questões envolvendo desinformação estão ligadas à transformação digital, ao surgimento de novos canais de comunicação e à interposição de intermediários nos meios de comunicação, reconhecendo que se tais fatores não forem considerados e tratados como políticas públicas, pouco adiantará o debate sobre a verdade ou mentira. Outro ponto relevante trazido é a importância de uma regulação

⁹¹ ROSEN, Jeffrey. **The Deciders: The Future of Privacy and Free Speech in the Age of Facebook and Google**. 80 Fordham L. Rev., v 80 (4), 1525 (2012). Available at: <https://ir.lawnet.fordham.edu/flr/vol80/iss4/1>

⁹² KELLER, Clara Iglesias. Don't Shoot the Message: Regulating Disinformation Beyond Content. **Direito Público**, [S.l.], v. 18, n. 99, out. 2021, ISSN 2236-1766. Disponível em: <<https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/6057>>.

multinível, sem descuidar da regulação estatal direta como fator considerável de regulação.

Adentrando as propostas concretas, a autora destaca três categorias de estratégia regulatória, que variam conforme a centralidade em: (i) conteúdo; (ii) dados ou; (iii) estrutura. Antes de detalhar cada uma delas, é importante trazer a ressalva contida no trabalho de que nenhuma dessas categorias é estática ou destinada a apenas um alvo, mas que, de maneira geral, as estratégias focadas em conteúdo costumam vincular mais o usuário enquanto as estratégias focadas em dados e estrutura tendem a vincular mais as plataformas que atuam como intermediárias.

Resumidamente, a regulação focada no conteúdo precisaria definir o que é verdade e o que é mentira. Além disso, teria foco na ilicitude de determinados discursos e consequente derrubada ou desindexação, o que cria um aparato considerável de instrumentos de ofensa à liberdade de expressão. De maneira exemplificativa, traz a legislação de diversos países que optaram por focar na criminalização ou exacerbação de penas para condutas ligadas diretamente ao conteúdo ou que, focando no intermediário, se ligavam mais ao conteúdo que dados e estrutura, criando a obrigação de moderação em prazos estreitos e com responsabilidades gravosas, o que prejudicava a moderação e trazia riscos à liberdade de expressão.

As políticas que focam nos dados pessoais costumam constituir marcos legais que regulam o tratamento das informações que tornam o indivíduo identificado ou identificável. Para o contexto da desinformação, Keller aponta que a importância é predominantemente ligada à técnica de *microtargeting* para fins políticos, ainda que reconheça a possibilidade de utilização em outros contextos, o que envolve a coleta e análise de dados pessoais para perfilamento e encaminhamento de mensagens específicas a um destinatário mais propício a recebê-la. No âmbito desta dissertação, o tratamento de dados pessoais também é fundamental para o perfilamento e direcionamento de mensagens a usuários mais propensos a recebê-las, com possibilidade de geração de lucros a canais de comunicação que se dedicam à criação de desinformação.

Em terceiro lugar, a autora trata da regulação que foca em aspectos estruturais, ou seja, que prevê mecanismos destinados a impor ou incentivar a mudança de operações realizada pelas plataformas, o que pode se dar pela imposição de responsabilidades estabelecidas pelos governos, criação de códigos

de ética e conduta pela própria plataforma ou alteração de procedimentos e mecanismos, o que abrange várias finalidades, inclusive o combate à desinformação.

Por fim, Keller defende que a estratégia relacionada ao conteúdo é a que traz maiores riscos à liberdade de expressão, pois se apoia em necessário entendimento sobre o que é a verdade, que inevitavelmente será estabelecida a partir de conceitos subjetivos do aplicador. Além de trazer maiores ameaças, carrega o ônus de propiciar a menor eficácia e amplitude, já que pouco enfrenta a questão das transformações digitais e do surgimento de intermediários relevantes. Por sua vez, regulações focadas em dados pessoais e na estrutura teriam maior aptidão para coibir a criação ou reduzir a circulação de desinformação, com menores danos e riscos à liberdade de expressão.

Medidas que se direcionam ao incentivo ou obrigatoriedade da moderação de conteúdo devem ser tratadas como excepcionais, já que existem diversos outros meios que devem ser previamente considerados para um combate que seja mais eficaz e que evite a atribuição do papel de censor a um ente, seja público ou privado. Exemplificativamente, são mencionados o bloqueio de *bots* não identificados, a vedação de contas falsas, o ajuste de critérios algorítmicos de priorização de exibição das páginas e a implementação de mecanismos que aumentem a transparência⁹³.

A regulação deve se dirigir a mudanças estruturais feitas pelas empresas de tecnologia que atuam como intermediárias como forma mais eficaz de tratar a questão da desinformação, o que se sobrepõe a medidas de responsabilização civil ou criminal que se destinam individualmente ao usuário⁹⁴. Para Balkin, a maneira menos eficiente de solucionar o problema da desinformação é a partir da perseguição ou responsabilização de autores ou organizações que produzem o conteúdo nocivo, sobretudo porque muitos atuam no anonimato, por meio de robôs ou fora do país. Assim, a regulação deveria se dirigir a grandes empresas de tecnologia, com imposição de deveres ligados a criação de novos procedimentos, programas, critérios de algoritmo e políticas internas.

⁹³ KAYE, David. **Speech Police: the global struggle to govern the Internet**, Columbia Global Reports, 2019.

⁹⁴ BALKIN, Jack. **Free Speech in the Algorithmic Society: Big Data, Private Governance, and New School Speech Regulation**. University of California, 2018, v. 51, pp. 1149-1210.

Hartmann⁹⁵ demonstra que as grandes empresas de tecnologia não possuem estrutura para avaliar individualmente o conteúdo postado por cada usuário, o que ocorre em grande volume e a todo momento. Traçando uma comparação entre os veículos tradicionais de comunicação de massa e a atual lógica de discurso contida na internet, demonstra que o cenário atual, conquanto passível de críticas, se tornou mais democrático que antes. Se, de um lado, ainda há concentração de decisão sobre o conteúdo que será exibido ou removido, de outro, há maior número de veículos de comunicação e meios para resposta e esclarecimento dos fatos. Se ainda há um número restrito de pessoas que tomam decisões sobre critérios de moderação (integrantes das empresas de tecnologia), atualmente há um número relevante de pessoas que tomam decisões sobre o compartilhamento ou a criação desses conteúdos, o que é feito de forma individual e ocorre em grandes quantidades diárias. Como não possuem estrutura para tomar tais decisões individuais de moderação de conteúdo, não deveriam gozar de legitimidade para tanto ou, pelo menos, não deveriam ter legitimidade para usar como primeiro e principal recurso.

Distintamente, as plataformas possuem ampla capacidade de adoção de medidas que se ligam a suas arquiteturas. São soluções que não operam necessariamente em modo binário, ou seja, com escolha entre exclusão e manutenção de conteúdo, forma e apresentação. Por exemplo, uma postagem nociva ou inadequada ou, pelo menos, duvidosa, poderia ser marcada com uma bandeira vermelha que sinaliza seu status ao usuário sem que sejam adotadas medidas de remoção ou mesmo redução de visibilidade. Uma das vantagens é que a sinalização figura na notícia original e não depende de outra publicação para remediação – como ocorreria no jornal impresso, em que um direito de resposta somente poderia figurar em edição posterior. Outra hipótese é a redução de alcance a partir de perfis demográficos: determinado conteúdo apareceria com certa frequência a determinado tipo de usuário, enquanto apareceria com frequência distinta a indivíduos com características diferentes.

Tais considerações apontam na direção de mudanças estruturais, promovidas principalmente por empresas de tecnologia que atuam como intermediários, seja de maneira imposta, estimulada ou voluntária, em oposição a regulações que focam no conteúdo, especialmente o conteúdo individualmente analisado. Uma regulação focada na estrutura não precisaria definir o que é

⁹⁵ HARTMANN, Ivar. **A new framework for online content moderation** (2020), 36 Computer Law & Security Review.

verdade e o que é mentira, tampouco determinar prazos escassos e sanções elevadas que pressionem a moderação excessiva de conteúdo pelas plataformas. Ainda, dispensaria a imposição de responsabilidade civil ou criminal voltadas para a esfera individual, sobretudo mirando no usuário ou no veículo de comunicação⁹⁶.

Aderindo à ideia de que o tema da desinformação deve seguir a regulação de dados pessoais e de estrutura das plataformas, é possível analisar o caso específico da legislação brasileira. No caso da regulação com foco nos dados pessoais, a Lei Geral de Proteção de Dados (“LGPD” ou Lei nº 13.709/2018) deve ser o marco regulatório que rege a matéria, por divesas razões. Tepedino explica que as mudanças sociais, políticas e econômicas impuseram uma alteração na postura legislativa, que passa a regular uma gama de relações ligadas a vários ramos do direito:

Cuida-se de leis que regulamentam exaustivamente extensas matérias, e passam a ser designadas como estatutos, veiculando não apenas normas de direito material, mas também processuais, de direito administrativo, regras interpretativas e mesmo de direito penal. Anuncia-se, em doutrina, a era dos estatutos.

[...]

Em relação a estes [estatutos] o Código Civil perdeu qualquer capacidade de influência normativa, configurando-se um polissistema, caracterizado por um conjunto crescente de leis tidas como centros de gravidade autônomos e chamados, por conhecida corrente doutrinária, de microssistemas.

Nesse contexto, tal como o Código de Defesa do Consumidor se apresenta para as relações de consumo, a LGPD deve servir para o tratamento de dados pessoais. Além disso, é importante considerar que a Lei chega em um momento em que não há consolidada cultura de privacidade e proteção de dados pessoais e que o Congresso Nacional se manifestou sobre a necessidade de uniformizar o regramento e conferir maior segurança jurídica quando da aprovação da EC 115/2022, que tornou a proteção de dados pessoais um direito fundamental e assegurou competência privativa da União para legislar sobre o tema⁹⁷. Assim, alterações em diploma legal tão recente e que ainda está em fase de conhecimento pela sociedade brasileira pode não ser desejável, sob risco de redução da eficácia e lesão a direitos tão importantes.

⁹⁶ Tal hipótese não deve ser descartada para solução de casos concretos que cheguem ao Poder Judiciário e envolvam corporações ou indivíduos diretamente mencionados ou que tenham produzido o conteúdo. Contudo, a análise dessa pertinência não será feita neste trabalho, que mira em soluções de amplo alcance e que sejam encaradas como políticas públicas.

⁹⁷ BRASIL. Senado Federal. Parecer da Relatora na PEC 17/2019, que resultou na EC 115/2022. Brasília: Senado Federal, 2019. Disponível em: <https://legis.senado.leg.br/sdleg-getter/documento?dm=7954439&ts=1647518557730&disposition=inline>. Acesso em 02/04/2022.

Por tais razões, o presente trabalho antecipa críticas sobre as disposições do PL 2630/2020 que versem sobre dados pessoais. Neste momento, eventuais transformações seriam prejudiciais por gerar incertezas ainda maiores sobre o tema. Referência especial é feita ao art. 7º, §1º do PL 2630/2020, que cria óbices excessivos à realização de publicidade direcionada e dificulta a utilização dos chamados cookies de terceiros sem atribuir-lhe um substituto viável, desafio reconhecido por instituições internacionais e por autoridades de proteção de dados pessoais na Europa⁹⁸⁹⁹.

O PL 2630/2020, a despeito das críticas, é o veículo que traz uma proposta de alterações estruturais e de arquitetura fundamentais para combate à desinformação, em detrimento de uma proposta focada no conteúdo, o que é desejável. Ainda, aponta para grandes empresas de tecnologia que atuam como intermediárias, ao invés de estabelecer o usuário como alvo principal. O projeto propõe medidas que parecem mais efetivas que a responsabilização individual ou a imposição de moderação de conteúdo com mecanismos de quase coação de plataformas para tomada de decisões apressadas.

É importante salientar que o caminho adotado não é trivial e que dezenas de propostas legislativas foram apresentadas nos últimos anos, sobretudo após as eleições de 2018 e da ocorrência da pandemia da COVID-19. Em 01/06/2020, já tramitavam na Câmara dos Deputados mais de 50 projetos de lei tratando de desinformação¹⁰⁰. Sem pretensão de análise de todas as propostas ou agrupamento em categorias, é possível mencionar diversas tentativas de criminalização ou responsabilização individual, sem qualquer outra medida agregada, ou seja, miravam no conteúdo e na responsabilidade individual sem focar em medidas de alcance amplificado e efetivo. O PL 2389/2020¹⁰¹ propunha alteração do Código Penal, para punir quem cria, divulga ou dissemina informações falsas acerca da pandemia no ambiente virtual, com hipóteses de

⁹⁸ REINO UNIDO. Information Commissioner's Office. **How do we comply with the cookie rules?** Disponível em <https://ico.org.uk/for-organisations/guide-to-pecr/guidance-on-the-use-of-cookies-and-similar-technologies/how-do-we-comply-with-the-cookie-rules/#comply14>. Acesso em 03.04.2022.

⁹⁹ IAB Brasil. **Um guia para a Era Pós-Cookies de Terceiros.** Disponível em <https://iabbrasil.com.br/wp-content/uploads/2021/11/guia-para-era-sem-cookies-final-V2.pdf>. Acesso em 02/04/2022.

¹⁰⁰ BRASIL. Câmara dos Deputados. **Combate a fake news é tema de 50 propostas na Câmara dos Deputados.** Disponível neste link. Acesso em 03.04.2022.

¹⁰¹ BRASIL. Câmara dos Deputados. Projeto de Lei 2.389, de 2020. **Dispõe sobre a tipificação do crime de criação e divulgação de notícias falsas – Fake News sobre a pandemia do Coronavírus – Covid – 19 acrescentando o art. 140-A ao do Decreto-Lei nº 2.848, de 7 de dezembro de 1940, Código Penal e dá outras providências.** Deputada Federal Rejane Dias. Disponível neste link. Acesso em 03.04.2022.

aumento de pena para líderes e coordenadores de esquemas de desinformação. Os PLs 1258/2020¹⁰² e 2601/2019¹⁰³ traziam, respectivamente, (i) previsão de responsabilidade criminal para quem divulgasse desinformação em tempos de calamidade pública ou de crises constitucionais (intervenção federal, estado de defesa e estado de sítio) e; (ii) obrigação para que provedores de aplicações indisponibilizassem notícias falsas, tão logo fossem notificados extrajudicialmente pelo usuário que se considerasse ofendido, sob pena de responsabilidade solidária e das sanções previstas no art. 12 do Marco Civil da Internet, que varia desde advertência até multa de 10% sobre faturamento e proibição de exercício de atividades.

Distintas são as propostas feitas pelo PL 2630/2020. O primeiro ponto fundamental é que, ao longo da tramitação, o projeto abdicou da tentativa de definir desinformação, o que demonstra a ausência de pretensão de fixar o que é verdade e o que é mentira. O texto inicial afirmava que desinformação seria o conteúdo “inequivocamente falso ou enganoso, passível de verificação, colocado fora de contexto, manipulado ou forjado, com potencial de causar danos individuais ou coletivos, ressalvado o ânimo humorístico ou de paródia”¹⁰⁴. Ocorre que a análise do que seria “inequivocamente falso ou enganoso” não é tão simples, razão pela qual o parecer do relator no Senado (casa iniciadora) foi taxativo ao descartar a tentativa de definição. Neste sentido, esclareceu que o combate à desinformação é um objetivo claro das instituições, mas que a implementação prática imporia desafios maiores e que a tentativa de conceituar pela via legislativa poderia gerar prejuízos à liberdade de expressão, de opinião e religiosa:

A definição adotada, aparentemente, volta-se especificamente para conteúdo que reporte fatos que possam ser verificados [...] verifico que existe uma zona perigosa, não muito clara, que pode representar conflito entre a proposição e as garantias constitucionais ao livre pensamento e expressão.

Ainda que se tente dizer categoricamente que manifestação de pensamento, de crença ou de opinião não são passíveis de classificação como desinformação, resta

¹⁰² BRASIL. Câmara dos Deputados. Projeto de Lei 1.258, de 2020. **Tipifica a divulgação de notícias falsas durante o período de calamidade pública, estado de defesa, estado sítio ou intervenção, tratando ainda do indiciamento e da indenização em tais casos, alterando o Decreto-Lei nº 2.848, de 7 de dezembro de 1940, Código Penal.** Deputado Federal Luis Miranda. Disponível neste link. Acesso em 03.04.2022.

¹⁰³ BRASIL. Câmara dos Deputados. Projeto de Lei 2.601, de 2019. **Altera a Lei nº 12.965, de 23 de abril de 2014, para criar obrigação de indisponibilização de notícias falsas por provedores de aplicações de internet e dá outras providências.** Deputado Federal Luis Miranda. Disponível neste link. Acesso em 03.04.2022.

¹⁰⁴ BRASIL. Câmara dos Deputados. Complementação de voto do relator. Deputado Orlando Silva. Disponível em https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=2115425. Acesso em 08.03.2022.

uma gama de manifestações que, por sua própria natureza, permitem avaliações distintas, dependendo do olhar de quem avalia.

Aliás, esse é um ponto importantíssimo: a atividade de rotular determinada informação como falsa é, em si, uma manifestação de opinião – a opinião do verificador.

Atualmente, o Comitê Gestor da Internet (CGI)¹⁰⁵ é o órgão ao qual se atribuiu a competência para promover estudos e debates com intuito de aprofundar o entendimento sobre a definição do termo desinformação, bem como os respectivos mecanismos de combate, o que contribui com o amadurecimento do tema e com transformações nos meios de comunicação¹⁰⁶.

Além disso, o PL 2630/2020 não se aplica a todas as empresas de tecnologia que possibilitam o uso de redes sociais, buscas ou mensageria instantânea, se limitando aos provedores que tenham mais de 10.000.000 (dez milhões) de usuários registrados no país, o que abarca boa parte dos aplicativos utilizados no dia a dia (Facebook, Instagram, Twitter, WhatsApp, Telegram, Messenger, Google, Yahoo, dentre outros)¹⁰⁷.

Outro ponto interessante se refere ao uso de contas automatizadas (ou *bots*). De maneira correta, o PL 2630/2020 não veda a utilização de tais contas, já que possuem finalidades legítimas variadas, como atender ao usuário, facilitar treinamentos ou mesmo oferecer determinado produto ou serviço de maneira lícita. Contudo, elas precisam ser identificadas, razão pela qual há disposições que impedem o funcionamento de contas automatizadas que não sejam identificadas como tais¹⁰⁸, ou seja, de contas que, apesar de operadas por softwares, fingem se tratar de pessoa real. Como denunciado por Kalil e Santini¹⁰⁹ “as chamadas “tropas cibernéticas” ou exércitos virtuais são comumente utilizados nas redes sociais para ativar a militância online a favor do governo e falsificar a opinião pública”, o que demonstra como contas automatizadas podem ser instrumentalizadas em favor da desinformação.

¹⁰⁵ O texto encaminhado aprovado no Senado Federal previa a criação de um Conselho de Transparência e Responsabilidade na Internet. Contudo, o Grupo de Trabalho que atuou na Câmara dos Deputados atribui a competência ao Comitê Gestor da Internet, por se constituir “um órgão já experiente em questões regulatórias da internet e mais técnico e adequado para lidar com as vicissitudes tecnológicas e a dinamicidade tão próprias da rede mundial de computadores”.

¹⁰⁶ BRASIL. Câmara dos Deputados. Complementação de voto do relator. Deputado Orlando Silva.

¹⁰⁷ Art. 2º do PL

¹⁰⁸ Art. 6º, I do PL

¹⁰⁹ KALIL, I. & SANTINI, R. M. **Coronavírus, Pandemia, Infodemia e Política**. Relatório de pesquisa. Divulgado em 01 de abril de 2020. 21p. São Paulo / Rio de Janeiro: FESPSP / UFRJ. Disponível: https://www.fespssp.org.br/store/file_source/FESPSP/Documentos/Coronavirus-e-infodemia.pdf

Somando-se a tais previsões, os conteúdos publicitários e impulsionados, mediante pagamento ao provedor, devem ser identificados, tanto na publicação original quanto em eventuais compartilhamentos. Tais anúncios e impulsionamentos devem ser acompanhados do contato respectivo do responsável e figurar em históricos semestrais que possibilitem consulta pública¹¹⁰. No contexto eleitoral, a postagem também precisa ser identificada como impulsionada e, quando se referir a candidato, coligação ou partido, será necessária disponibilização de todo conjunto da propaganda realizada, que também deve figurar em lista aberta e de fácil acesso ao público¹¹¹. A preocupação do direcionamento publicitário no contexto político levou a ANPD e o Tribunal Superior Eleitoral (TSE) à elaboração de Guia Orientativo para aplicação da lei geral de proteção de dados pessoais por agentes de tratamento no contexto eleitoral, já que “candidatas, candidatos e partidos políticos querem fazer suas propostas chegar ao eleitorado e, para isso, é muito valioso conhecer seus hábitos e suas opiniões e pretensões”¹¹², com tecnologias altamente modernas e precisas de perfilamento, o que traz especial preocupação. No campo da desinformação, a estratégia de exibição do conjunto da propaganda é relevante. Da Empoli¹¹³ demonstra que, numa campanha, a mensagem enviada é segmentada para atingir um público igualmente segmentado: para uns, mensagens moderadas e, para outras, mensagens mais radicais, defendendo distintos pontos de vistas. Assim, a obrigação de disponibilizar todo conjunto da propaganda se apresenta como importante ferramenta de combate à desinformação, sobretudo aquela ligada à descontextualização.

No campo da transparência, há um extenso rol de requisitos que compõem relatórios semestrais que devem ser elaborados, exibidos de forma pública e submetidos a análises, o que permite, ainda, a avaliação e aprimoramento de mecanismos, seja pelas próprias plataformas ou por órgão externo. Dentre os elementos que devem ser trazidos no relatório, estão os seguintes¹¹⁴: (i) o número de usuários brasileiros ou de conexões situadas no Brasil; (ii) o número de medidas aplicadas a contas e conteúdos em razão de regras próprias; (iii) o número total de pedidos de revisão apresentados por usuários diante das medidas

¹¹⁰ Art. 6º, II e §1º, 16, §único e 18 do PL

¹¹¹ Arts. 17 e 19 do PL

¹¹² BRASIL. Presidência da República. Autoridade Nacional de Proteção de Dados. Tribunal Superior Eleitoral. Guia Orientativo de aplicação da Lei Geral de Proteção de Dados Pessoais por agentes de tratamento no contexto eleitoral. Brasília, 2021.

¹¹³ DA EMPOLI, pp. 81 - 82.

¹¹⁴ Arts. 9º e 10 do PL

citadas; (iv) o número de medidas aplicadas a contas e conteúdos em razão de ordem judicial, com indicação de respectiva base legal; (v) características das equipes envolvidas na atividade de aplicação de políticas de conteúdo, número e detalhamento de medidas de identificação de conteúdo; (vi) informações sobre o alcance de conteúdos identificados como irregulares pelo provedor; (vii) os critérios e metodologias para aferição do alcance de conteúdo impulsionado e de publicidade; (viii) informação sobre emprego e funcionamento de sistemas automatizados na aplicação de regras próprias; (ix) informações sobre atualização de políticas próprias e termos de uso e o número total de medidas aplicadas sobre contas consideradas de interesse público.

Outro grupo de normas se dirige à *accountability* e ao estabelecimento de regras que garantam direitos de acesso, fundamentação, justificativa e possibilidade de revisão de decisões tomadas, por meio automatizado ou não. Por exemplo, deverão ser elaboradas regras próprias que respeitem a liberdade de expressão e a livre concorrência, com exibição de políticas de forma clara, acessível e em português. Além disso, deve haver a limitação de encaminhamento de mensagens ou mídias, nos termos de Código de Conduta e limitação de listas de transmissão apenas para contatos cadastrados, simultaneamente, na lista de remetente e destinatário. Outra medida é o estabelecimento de mecanismos que possibilitem o consentimento prévio do usuário para inclusão em grupos e listas de transmissão e, ainda, a desabilitação, por padrão de autorização para inclusão em grupos. Deve ser estruturado, ainda, um procedimento de identificação de anunciantes, com possibilidade de exigência de documento de identificação.

Quando adotadas ações que impliquem exclusão, indisponibilização, redução de alcance ou sinalização de conteúdos gerados e que tenham sido denunciados ou avaliados, deve ser garantida a notificação do autor, com devida fundamentação e garantia de pedido de revisão. Para facilitar denúncias, deve ser disponibilizado canal próprio, destacado e de fácil acesso.

O art. 31 do PL 2630/2020 prevê penalidades judiciais que podem ser cumuladas com sanções civis, criminais e administrativas, em caso de descumprimento das disposições. Dentre elas se encontram: (i) advertência; (ii) multa de até 10% do faturamento do grupo econômico; (iii) suspensão ou proibição de exercício das atividades.

Outro ponto que chama a atenção é a criação de crime em espécie, trazido pelo art. 36 do PL 2630/2020¹¹⁵:

Art. 36 Promover ou financiar, pessoalmente ou por meio de terceiros, mediante uso de contas automatizadas e outros meios ou expedientes não fornecidos diretamente pelo provedor de aplicações de internet, disseminação em massa de mensagens que contenha fato que sabe inverídico e passíveis de sanção criminal que causem dano à integridade física das pessoas ou sejam capazes de comprometer a higidez do processo eleitoral.

Pena: reclusão, de 1(um) a 3 (três) anos e multa.

Ainda que o aspecto criminal não seja o foco deste trabalho, breves comentários devem ser feitos. O projeto se diferencia daqueles apontados anteriormente, porque não se limita a prever a criação de um crime, causa de aumento ou qualificadora, tampouco exacerba penas ou traz medidas semelhantes sem conexão com políticas mais efetivas. Assim, a despeito de tipificar novo crime em espécie, a disposição surge como um artigo em meio a 42 disposições que versam basicamente sobre estrutura e dados pessoais. Parece, ainda, que a criação ocorre em razão da legalidade penal, que não autorizaria a criação de novo tipo penal por órgãos como o CGI, por exemplo, e que sua aplicabilidade deveria aguardar o debate e consolidação dos estudos trazidos pelo órgão para preenchimento do significado de “fato que sabe inverídico”, sem prejuízo das penalidades para utilização de contas automatizadas de forma ilícita. Por fim, seguindo os princípios do direito penal, a disposição deve ser tomada como *ultima ratio*, o que parece ter sido a intenção do projeto, que trata sobre estrutura e dados ao longo do texto, inserindo tipificação única no penúltimo capítulo, antecedendo apenas às disposições finais. Tal atitude parece apontar para a exposição feita no início deste tópico, acerca da ineficácia e do potencial violador da liberdade de expressão que o tratamento no varejo e focado na responsabilização individual pode gerar.

O último capítulo se destina ao aprofundamento de algumas propostas estruturais relevantes trazidas no projeto e de outras extraídas da análise do estado da arte, com foco na regulação do ambiente virtual para manutenção da publicidade personalizada com extinção ou redução do incentivo financeiro à desinformação. Antes, porém, será dado enfoque em aspectos estruturais que versam sobre regulação multinível e sobre a estrutura principiológica trazida pelo PL 2630/2020, na linha do que faz a LGPD. Importante salientar que os princípios

¹¹⁵ Art. 36 do PL

figuram em meio a outras normas que variam conforme grau de precisão ou vagueza, considerado o *continuum* vagueza-precisão trazido por Schauer. Ao invés de nos preocuparmos em classificar uma norma como regra ou como princípio, deveria ser questionado: quão vaga ou quão precisa é a norma naquele *continuum*? Isso ocorre porque a classificação não é estanque, mas se dá por gradações distintas. Quanto mais próxima uma norma estiver do extremo “regra”, menor será a flexibilidade e maior será a capacidade de reger com precisão o presente. Quanto mais próxima uma norma estiver do extremo “princípio”, maior será a flexibilidade e menor será sua aptidão para reger com precisão o presente, o que ocorre em troca de conferir maior resistência da norma à obsolescência imposta pelo tempo. O autor menciona a importância da flexibilidade justamente para tratar de questões ligadas a novas tecnologias¹¹⁶:

Quanto às rápidas mudanças nas comunicações eletrônicas, por exemplo, qualquer tentativa de se escrever leis específicas neste momento estará tão destinada à obsolescência quanto regras específicas, feitas há uma geração, que não antecipavam o uso generalizado do telefone celular, o desenvolvimento e o domínio da internet, com uma densidade alta de tecnologias de comunicação baseadas em satélite que faz com que comunicações limitadas ao rádio, televisão e cinema pareçam arcaicas.

Portanto, o PL 2630/2020, com ressalva às críticas e imperfeições, caminhou bem ao prever normas mais precisas e normas mais vagas, acomodando a necessidade de controlar determinados aspectos do presente, haja vista o problema da desinformação ser um desafio urgente e atual, com a busca pela manutenção da vida e eficácia da norma independentemente do avanço tecnológico que segue com velocidade muito superior àquela apresentada pelo processo legislativo.

Como exemplos de normas vagas, é possível citar não apenas o rol contido no art. 3º do Projeto, que traz princípios como liberdade de expressão e imprensa, garantia de direitos da personalidade, respeito ao usuário, responsabilidade pela preservação de esfera pública livre, plural e democrática, vedação à discriminação e incentivo à transparência, mas também diversas outras passagens, como o art. 6º que impõe a obrigação de adotar medidas para vedar funcionamento de contas

¹¹⁶ SCHAUER, Frederick. **Thinking like a lawyer: a new introduction to legal reasoning**. Harvard University Press, 2009, pp. 188-202. O trecho foi traduzido do inglês: *With respect to rapid changes in electronic communications, for example, any attempt to write specific laws at this time is as destined to obsolescence as were those specific rules of only a generation ago that did not and could not have anticipated widespread cell phone usage, the development and dominance of the Internet, and a density of satellite-based communication technologies that makes a list of communications media limited to radio, television, and motion pictures seem archaic. So too in many other areas.*

automatizadas não identificadas. Poderia o texto prever os mecanismos precisos para concretizar o intento tão logo a lei passasse a vigorar. Contudo, a evolução da tecnologia certamente traria a rápida obsolescência, sem mencionar outras disposições. De outro lado, ao impor que o PL 2630/2020 trata apenas de provedores que contem com número superior a 10.000.000 (dez milhões) de usuários, há norma mais precisa.

Tal estrutura tem sido adotada de maneira correta por outros diplomas normativos que tratam novas tecnologias, sobretudo aquelas presentes no ambiente virtual. É o caso, por exemplo, do Marco Civil da Internet e da LGPD, esta última aplicável também ao tratamento de dados pessoais realizados em meios físicos, mas cujo impulsionamento por uma legislação de privacidade e proteção de dados se originou do avanço da internet e da circulação de dados pessoais no meio virtual.

3.2.

O que é regulação e quem pode regular

A publicidade personalizada pode trazer riscos desproporcionais para direitos fundamentais, tais como a privacidade, a proteção de dados pessoais e a liberdade de expressão. De outro lado, sua sistemática tem permitido que anunciantes que nunca tiveram a oportunidade de produzir conteúdo publicitário relevante possam exibir seus anúncios para um público ideal a um custo reduzido. Além disso, tal forma de publicidade permite o surgimento e subsistência de maior número de veículos de comunicação no ambiente virtual, tais como blogs, páginas em redes sociais, sites de notícias e tantos outros, contribuindo para o fortalecimento da liberdade de expressão e imprensa.

Portanto, a publicidade personalizada é um elemento do ambiente virtual que traz vantagens sociais, econômicas e tecnológicas, razão pela qual a extinção ou criação de óbices excessivos podem ser tão nocivos quanto a permissão de funcionamento sem estabelecimento de regras e princípios específicos. Com objetivo de contribuir para a solução e a harmonização de direitos, são propostas medidas de regulação que atentem para um modelo regulatório amplo e que permita a participação de múltiplos atores sociais envolvidos na temática.

Dentre os diversos aspectos que costumam ser levantados para tratar de regulação de novas tecnologias, dois serão os pontos fundamentais deste tópico:

o que se entende por regulação (conceito) e quem pode regular (qual é o arranjo institucional). Neste sentido, é importante considerar que o impacto da regulação atinge diferentes áreas, sendo relevante ao poder público, ao mercado, a entes sem fins lucrativos, ao titular de dados pessoais e outros interessados. Todos são potenciais destinatários e podem contribuir de maneiras diversas, sobretudo pela variação da expertise e interesse de cada grupo.

Assim, um conceito amplo e inclusivo de regulação da publicidade personalizada parece o mais adequado. Baldwin, Cave e Lodge¹¹⁷ conceituam regulação da seguinte forma: (i) um modo discreto de atividade governamental; (ii) o controle exercido por um órgão público sobre atividades valorizadas por uma comunidade; (iii) o conjunto específico de regras vinculantes que funcionam como comando para determinado grupo, com aplicação e controle feitos por meio de órgão público criado para tal fim; (iv) qualquer forma de ação estatal que possa influenciar o comportamento social ou empresarial ou; (v) qualquer forma de influência social ou econômica, baseada no Estado ou outras fontes, que tenham potencial de afetar comportamentos.

Os conceitos indicados não são necessariamente contraditórios, podendo haver relação de complementaridade ou de continente-conteúdo. Entretanto, é na última definição que repousará o sentido de regulação tratado neste trabalho. Assim, será possível considerar um amplo rol de atores, formas e estratégias para regulação da publicidade personalizada, pois o significado se sustenta na influência social ou econômica exercida por qualquer ator social que tenha a capacidade de afetar as ações dos entes regulados.

Tal acepção é importante porque retira do Estado o monopólio regulatório, mas não o transfere para o mercado, havendo necessário compartilhamento de funções entre os diversos atores sociais. Conforme visto em subcapítulo anterior, a atribuição de exclusividade ao poder público tem gerado tantas ameaças à liberdade de expressão quanto a absoluta ausência de regras que vinculem as empresas de tecnologia e que, conseqüentemente, releguem a atuação desta apenas a normas próprias.

¹¹⁷ BALDWIN, Robert; CAVE, Martin; LODGE, Martin. **Understanding Regulation: theory, strategy and practice**. 2 ed. Oxford, 2012, pp. 2-3.

Para Binenbojm¹¹⁸, o curso natural da democracia é da desestatização do poder de polícia e descentralização da capacidade normativa, o que não significa a extinção dos poderes regulatórios do Estado, mas sim a quebra do monopólio regulatório para abarcar outros agentes fundamentais. A constatação assume especial relevância no tema das novas tecnologias ligadas ao ambiente virtual.

Neste sentido, apesar da variedade de modelos regulatórios e de arranjos institucionais existentes, a escolha por apenas um deles passa a ter importância reduzida, ou seja, não é necessário escolher apenas um modo de regular ou conceder o monopólio da regulação para uma força social, apenas. Mais do que desnecessárias, as escolhas parecem impossíveis pela própria natureza da regulação e dos problemas que busca solucionar. Entregar o monopólio ao poder público retira a eficácia da regulação, em razão do dinamismo do objeto regulado. Entregar o monopólio ao mercado retira a prioridade na pessoa humana e direitos fundamentais inerentes. Sob a ótica da liberdade de expressão, atribuir capacidade exclusiva para o poder público ou para ente privado acabam desaguando em ameaças para a liberdade de expressão, que se consubstancia na determinação de um censor (ou potencial censor) que não se submete a outras normas ou entes.

Black¹¹⁹ trata da regulação descentralizada, argumentando que a sociedade, sobretudo no contexto da globalização, tem se tornado cada vez mais complexa e que nem o poder público nem o poder privado possuiriam todas as ferramentas para regulação das matérias às quais estão expostos.

A autora menciona sete aspectos sobre os quais a descentralização da regulação se sustenta. O primeiro seria a complexidade dos problemas sociais, que surgem a partir da interação de múltiplos fatores, personagens, objetivos, propósitos, normas e poderes. O segundo, a fragmentação do conhecimento, já que nenhum dos atores envolvidos deteria o monopólio do conhecimento sobre determinada área, o que encerra a antiga afirmação de que apenas o mercado seria suficiente para lidar com todos os pontos (em razão da expertise) ou de que apenas o Estado possuiria essa capacidade (em razão do interesse público e social). O terceiro aspecto seria o exercício do poder e do controle, que deixa de

¹¹⁸ BINENBOJM, Gustavo. **Poder de Polícia, Ordenação, Regulação: transformações político-jurídicas, econômicas e institucionais do direito administrativo ordenador**. Fórum: Belo Horizonte, 2016, pp. 294-296.

¹¹⁹ BLACK, Julia. **Decentring Regulation: Understanding the Role of Regulation and Self-Regulation in a 'Post-Regulatory' World**. *Current Legal Problems*, v. 54, issue 1, 2001, pp. 103-146.

ser um monopólio estatal para ser dividido com os demais atores sociais – “regulation occurs in many location, in many fora” - o que resultaria no quarto aspecto, em que todos os atores sociais gozariam de certa autonomia, o que não se traduz em absoluta ausência de intervenção estatal, mas simplesmente na ideia de que o Estado não possui o monopólio sobre a regulação. Como quinto aspecto, todos os atores sociais envolvidos possuiriam relações interdependentes, o que impõe a necessidade de diálogos e negociações para atingir os melhores fins. O sexto seria o colapso da distinção entre público e privado, em termos do papel formal para regulação, autoridade e governança. Por fim, estaria a recomendação de estratégias regulatórias híbridas, multifacetadas e indiretas – de acordo com esta última, mais do que regular o tema diretamente, seria fundamental regular a forma como esses temas serão regulados.

Sinclair¹²⁰ também defende o uso de instrumentos híbridos que surgem a partir da combinação da regulação estatal e da autorregulação, o que tem sido cada vez mais frequente, tornando difícil a identificação de arranjos institucionais isolados. O autor destaca que não haveria necessária dicotomia entre as alternativas e que os agentes reguladores devem ter foco maior na obtenção de medidas eficazes e eficientes, em detrimento de se prender a escolhas rígidas que costumam ser insuficientes para alcançar os objetivos esperados.

A identificação de arranjos institucionais sob a ótica prescritiva perde a importância e pode ser um mecanismo de enrijecimento que cria obstáculos desnecessários para alcance de regulação efetiva. Sob a ótica descritiva, o tema permanece relevante, já que permite identificar o papel que cada ator social possui em contextos distintos. Assim, não há problemas na análise do arranjo institucional utilizado pelo regulador, mas no estabelecimento prévio de que determinado arranjo deve ser adotado e partir da regulação com foco exclusivo naquele que foi selecionado.

Rodotà¹²¹ menciona que as experiências de regulação estatal direta ou de atribuição regulatória exclusivamente para o mercado se mostraram insuficientes e que a regulação de novas tecnologias e circulação de dados pessoais deveria contar, em breve síntese, com disciplina legislativa que contivesse preponderantemente cláusulas gerais e normas processuais, guardando normas mais específicas apenas para casos mais específicos. Além disso, tal legislação

¹²⁰ SINCLAIR, Darren. Self-Regulation Versus Command and Control: Beyond False Dichotomies. *Law & Policy*, v. 19, n. 4, Oct. 1997, Oxford: Blackwell Publishers, pp. 529-559.

¹²¹ RODOTÀ, pp. 87-88.

deveria prever uma autoridade administrativa independente, com possibilidade de recurso à autoridade judiciária¹²² e a previsão de mecanismos de controle difuso por outros atores sociais.

Os fundamentos apresentados se aproximam da chamada regulação inteligente, trazida por Gunningham e Sinclair¹²³, que defendem um pluralismo regulatório. Tal ideia também abrange a multiplicidade de atores e formas de interferência na atividade regulatória. Quanto aos atores, engloba o Estado, organizações da sociedade civil, empresas que compõem o mercado e outras entidades que podem ser afetadas pela regulação e, portanto, devem ter a capacidade de influenciá-la. Quanto às formas de regulação, variam desde instrumentos tradicionais até mecanismos mais novos e imaginativos apresentados pela pluralidade de atores.

A regulação inteligente surgiu justamente num contexto em que nem a presença exclusiva do Estado nem a delegação absoluta de poderes ao mercado se mostravam como respostas adequadas.

A regulação inteligente estaria calcada em cinco principais fundamentos:

- 1) Preferência de combinações de instrumentos regulatórios em detrimento de instrumento único;
- 2) Possibilidade de ações interventivas por parte do Estado, mas com prioridade de medidas que sejam menos intervencionistas, ou seja, havendo duas ou mais opções de intervenção, deveria ser escolhida a que menos interfere na atividade desempenhada;
- 3) Estabelecimento de resposta em escalada ou pirâmide, ou seja, a fixação de instrumentos mais brandos na base, com possibilidade de evolução para instrumentos mais rígidos, a depender da postura do ente regulado. Portanto, instrumentos mais brandos abrangeriam o maior número de situações;
- 4) Capacitação de entes não-estatais para atuação como reguladores, nos casos em que seja mais interessante ceder o protagonismo estatal;
- 5) Maximização dos resultados oriundos da conformidade a partir de incentivos para que empresas busquem a conformidade com a regulação, de forma voluntária e preventiva. Algumas estratégias têm contribuído para

¹²² No Brasil, tal observação não estaria incorreta, mas pode ser considerada dispensável, em razão da inafastabilidade do controle jurisdicional, prevista no art. 5º, XXXV da CRFB.

¹²³ GUNNINGHAM, Neil; SINCLAIR, Darren. Smart Regulation. In DRAHOS, Peter (ed.); **Regulatory Theory: Foundations and Applications**. ANU Press, 2017, pp. 133–148.

que entes regulados não apenas cumpram a regulação, mas estabeleçam mecanismos que vão além do determinado.

A combinação de distintos arranjos institucionais, cuja prevalência varia de acordo com o contexto, parece ser o melhor caminho para uma regulação eficaz, que acompanhe a dinâmica da publicidade personalizada, mas que tenha como prioridade a privacidade, a proteção de dados pessoais e a liberdade de expressão, ao lado de direitos que já são priorizados, como a função social da empresa, a inovação, o desenvolvimento econômico e a autonomia.

Para compreender os arranjos institucionais que devem ser combinados, é possível estabelecer uma reta imaginária que tenha como um dos extremos a regulação estatal direta e, no outro, a autorregulação, ambas em suas formas mais puras.

Keller¹²⁴ considera que a “regulação direta acontece quando um órgão criado por lei desenvolve, aplica, monitora e fiscaliza um determinado arcabouço regulatório”, ou seja, quando um órgão criado por lei atua em todas as etapas da atividade regulatória. Para Majone¹²⁵, seria a regulação econômica ou social por agências públicas que operam sob supervisão da administração central. Tal atuação requereria um conhecimento detalhado sobre a atividade regulada, o que tem se tornado cada vez mais difícil ao Estado, diante da alta expertise detida por grandes empresas de tecnologia e da rápida transformação tecnológica.

Já a autorregulação em seu estado mais puro implicaria a completa ausência de intervenção estatal e regulação das atividades setoriais exclusivamente por próprios integrantes de determinada parcela do mercado. Por algum tempo, foi a concepção que predominou no ambiente virtual, a partir da aceção teórica *excepcionalista*¹²⁶ que, de forma sintética, pregava que o poder público não teria capacidade de regular o ambiente virtual sem necessariamente deturpar suas características fundamentais. Durante esse período, surgiu uma grande quantidade de instrumentos autorregulatórios que cuidavam das relações estabelecidas na internet, mas que se mostraram insuficientes para tutelar direitos

¹²⁴ KELLER, Clara Iglesias. **Regulação Nacional de Serviços na Internet: exceção, legitimidade e o papel do Estado**. Rio de Janeiro: Lumen Juris, 2019, p. 176.

¹²⁵ MAJONE, Giandomenico. **The rise of the regulatory state in Europe**. West European Politics, 17(3), pp. 77–101. doi:10.1080/01402389408425031.

¹²⁶ O excepcionalismo não se trata de um período na história, mas de uma concepção teórica que conta com adeptos até os dias atuais. A comparação é feita exclusivamente com um período em que tal corrente era majoritária.

fundamentais, sobretudo a privacidade, a proteção de dados pessoais e a liberdade de expressão¹²⁷.

Entre os extremos daquela reta, existem variações que atribuem diferentes papéis ao mercado e ao Estado. Dentre elas, é possível destacar a autorregulação regulada e a correção¹²⁸.

Para Maranhão e Campos¹²⁹, a autorregulação regulada seria capaz de conciliar a regulação por terceiros (normalmente o Estado) e a autorregulação, já que o setor público conseguiria induzir o setor privado a assegurar direitos e liberdades fundamentais, sendo possível utilizar meios coercitivos para concretizar a indução. Por meio da autorregulação regulada, o Estado iria prever a autorregulação e estabelecer parâmetros, limites e consequências do descumprimento.

Já foi visto ao longo desta dissertação que a regulação de entes privados e do poder público, simultânea e conjuntamente, é capaz de conferir nuances que impeçam a figura de um censor. Além disso, estimulam a busca por soluções alternativas que possuem maior eficácia e trazem menores riscos à liberdade de expressão, notadamente a regulação da estrutura, em detrimento da regulação do conteúdo.

Finck¹³⁰ trata a correção como uma complexa interação entre normas emanadas do poder público e normas emanadas de um órgão autorregulador, ou seja, seriam arranjos híbridos que conjugariam a regulação estatal direta e a autorregulação privada, o que combina a expertise e o interesse público e social. Como pode ser observado, são conceitos muito próximos e que não raramente se confundem na prática.

Para aclarar a diferença, Keller¹³¹ trata a correção e a autorregulação regulada como arranjos que se assemelham em alguma medida, mas se diferenciam no grau de participação do poder público: na correção, haveria

¹²⁷ KELLER, 2019, pp. 183-188.

¹²⁸ Para os fins desta dissertação, foram escolhidas as formas mais utilizadas e que se mostram suficientes para os fins buscados, o que não implica na negativa de existência de ampla variação de arranjos institucionais. Exemplificativamente, é possível mencionar outros arranjos institucionais, tais como a meta-regulação e a *quasi* regulação.

¹²⁹ MARANHÃO, Juliano; CAMPOS, Ricardo. Fake News e autorregulação regulada das redes sociais no Brasil: fundamentos constitucionais. In: ABOUD, George; NERY JR, Nelson; CAMPOS Ricardo. **Fake News e Regulação**. São Paulo: Thomson Reuters Brasil, 2021, pp. 341-346.

¹³⁰ Finck, Michèle, **Digital Co-Regulation: Designing a Supranational Legal Framework for the Platform Economy** (June 20, 2017). European Law Review (2018 Forthcoming), LSE Legal Studies Working Paper No. 15/2017, Available at SSRN: <http://dx.doi.org/10.2139/ssrn.2990043>.

¹³¹ KELLER, pp. 179-180.

um equilíbrio de participação, enquanto na autorregulação regulada prevaleceria a atuação de entidades privadas.

Tais combinações têm sido comuns em diplomas legais que tratam de novas tecnologias no ambiente virtual.

No Brasil, o Comitê Gestor da Internet (CGI) foi criado pelo Decreto nº 4.829/2003 e possui atribuições amplas ligadas ao uso e desenvolvimento da Internet no Brasil. Em razão de sua expertise, suas competências já haviam sido ampliadas pelo Marco Civil da Internet.

O PL 2630/2020¹³² reforça a importância do CGI, que deverá acompanhar as medidas implementadas pelo Projeto. O critério para atribuição se originou no Grupo de Trabalho da Câmara, que entendeu que o CGI constitui um órgão já experiente em questões regulatórias da internet, sendo mais técnico e adequado para lidar com as vicissitudes tecnológicas e a dinamicidade tão próprias da rede mundial de computadores. Dentre as atribuições, se encontram a apresentação de “diretrizes para a elaboração de Código de Conduta para provedores, aplicável enquanto mecanismo corregulatório” e promover estudos para aprofundar o entendimento sobre desinformação e respectivo combate, o que demonstra a necessidade de amadurecer o tema.

Nesse último ponto, o PL 2630/2020 demonstra a responsabilidade em não definir o que é verdade ou mentira, mas promover debates amplos e democráticos que contem com a atuação multissetorial do CGI, que é constituído por múltiplos atores sociais, que incluem representantes¹³³: (i) do Ministério da Ciência e Tecnologia; (ii) da Casa Civil; (iii) do Ministério das Comunicações; (iv) do Ministério da Defesa; (v) do Ministério do Desenvolvimento, Indústria e Comércio Exterior¹³⁴; (vi) do Ministério do Planejamento, Orçamento e Gestão; (vii) da ANATEL; (viii) do Conselho Nacional de Desenvolvimento Científico; (ix) do Fórum Nacional de Secretários Estaduais para Assuntos de Ciência e Tecnologia; (x) de notório saber em assuntos de internet; (xi) do setor empresarial; (xii) do terceiro setor; (xiii) da comunidade científica e tecnológica.

¹³² Inicialmente criavam o Conselho de Transparência, mas o Grupo de Trabalho criado na Câmara dos Deputados optou por atribuir ao CGI, em razão da estrutura criada e da expertise para tratar de temas relevantes ligados à internet.

¹³³ BRASIL. Presidência da República. Decreto nº 4.829, de 03 de setembro de 2003. **Dispõe sobre a criação do Comitê Gestor da Internet no Brasil - CGIbr, sobre o modelo de governança da Internet no Brasil, e dá outras providências.** Disponível em: http://www.planalto.gov.br/ccivil_03/decreto/2003/d4829.htm. Publicação em DOU de 04.09.2003.

¹³⁴ A Medida Provisória nº 870/2019 tornou o Ministério do Desenvolvimento, Indústria e Comércio Exterior um integrante da estrutura do Ministério da Economia.)

Além disso, a última versão do PL 2.630/2020 traz expressa a autorregulação regulada, com objetivo de “combinar a regulação estatal e a autorregulação do setor”¹³⁵. Na proposta aprovada pelo Senado, foi facultada a criação de instituição de autorregulação pelos provedores de redes sociais e serviços. Na Câmara dos Deputados, houve alteração para impor a criação de instituição de autorregulação, deixando de ser uma faculdade para se tornar um dever¹³⁶. Além disso, foram realizados ajustes para estabelecer atribuições amplas ao setor privado, como de criação de procedimentos de recebimento de denúncias, tomadas de decisões e respectivos processos de revisão, além da obrigação da duração razoável da apuração de denúncias, desenvolvimento de boas práticas para suspensão de contas inautênticas, criação de código de conduta, resoluções e súmulas interpretativas, bem como divulgação em sítio na internet¹³⁷.

Wimmer e Pieranti¹³⁸ afirmam que formas de regulação que eram pouco adotadas passam a ser mais consideradas na legislação recente, colocando a maior parte das situações sob a autorregulação, autorregulação regulada e correção, mas sem descuidar da possibilidade de sanções e medidas mais severas pela atuação estatal direta. Traçando um paralelo com a pirâmide defendida pela regulação inteligente, os autores falam que as formas regulatórias que inserem o privado como agente regulador estariam na base e a regulação estatal direta estaria no topo. Ao tratarem do tema, destacam que essa formatação é fundamental para garantir que o regulado atenda bem aos objetivos econômicos e sociais:

A adoção voluntária de mecanismos autorregulatórios pode ter por objetivo afastar a regulação mais intensa ou mais hostil por parte do Estado ou, ainda, evitar a incidência de normas equivocadas ou insensíveis às necessidades da indústria. Há benefícios de imagem, para as empresas, em atuarem como bons cidadãos; assim como podem também existir vantagens competitivas em tais condutas. Para o próprio poder público, a autorregulação pode representar uma alternativa interessante, por conferir maior abrangência e profundidade à atuação regulatória,

¹³⁵BRASIL. Senado Federal. Projeto de Lei 2.630, de 2020. **Institui a Lei Brasileira de Liberdade, Responsabilidade e Transparência na Internet**. Relatório. Senador Ângelo Coronel. Disponível neste link. Acesso em 15.02.2022.

¹³⁶ BRASIL. Câmara dos Deputados. Projeto de Lei 2.630, de 2020. **Institui a Lei Brasileira de Liberdade, Responsabilidade e Transparência na Internet**. Relatório do Grupo de Trabalho Aperfeiçoamento da Legislação Brasileira - Internet. Deputado Federal Orlando Silva. Disponível neste link. Acesso em 15.02.2022.

¹³⁷ Ibid.

¹³⁸ WIMMER, Miriam; PIERANTI, Octavio Penna. Programas de compliance e a LGPD: a interação entre autorregulação e a regulação estatal. In: FRAZÃO, Ana; VILLAS BÔAS CUEVA, Ricardo. **Compliance e políticas de proteção de dados**. São Paulo: Thomson Reuters Brasil, 2021, pp. 205-221.

por viabilizar a atuação com maiores níveis de expertise e conhecimento técnico e por aliviar a pressão sobre recursos orçamentários e humanos escassos.

Os autores citam exemplos concretos presentes no art. 50 da LGPD. O dispositivo determina que os agentes de tratamento de dados pessoais podem formular amplas regras de boas práticas e governança para suas respectivas organizações, o que na prática implica no estabelecimento de preceitos que vinculam seus próprios integrantes. Tal atribuição englobaria desde o cotidiano da organização até procedimentos de respostas a direitos dos titulares, normas de segurança, ações educativas e mecanismos de supervisão interna.

A despeito da liberdade estabelecida, ela deve ser exercida dentro de parâmetros previstos no parágrafo segundo daquele dispositivo e o resultado deve ser publicado e atualizado com frequência, com possibilidade de análise da suficiência pela Autoridade Nacional de Proteção de Dados (ANPD).

De outro lado, é importante verificar o amplo poder regulatório, fiscalizatório e sancionatório conferido à ANPD, órgão da Administração Pública Federal que integra a Presidência da República. Alguns exemplos podem ser trazidos, como os arts. 52 e 55-J da LGPD. O primeiro estabelece sanções que variam de uma simples advertência, com a possibilidade de evoluir para multas que podem chegar a R\$ 50.000.000,00 (cinquenta milhões de reais) e mesmo a proibição total de atividades relacionadas a tratamento de dados pessoais. O segundo determina que a ANPD é responsável por zelar pela proteção de dados, apreciar petições do titular contra o controlador e dispor sobre uma série de questões, tais como relatórios de impacto, diretrizes de segurança da informação e publicidade das operações.

Outra demonstração da participação de múltiplos atores sociais é a composição do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade (CNPDP), que compõe a ANPD¹³⁹. De acordo com a previsão da LGPD, o CNPD é composto por 23 representantes dos seguintes órgãos¹⁴⁰: (i) Poder Executivo Federal; (ii) Senado Federal; (iii) Câmara dos Deputados; (iv) Conselho Nacional de Justiça; (v) Conselho Nacional do Ministério Público; (vi) Comitê Gestor da Internet¹⁴¹; (vii) entidades da sociedade civil com atuação relacionada à

¹³⁹ LGPD, Art. 55-C.

¹⁴⁰ LGPD, Art. 58-A.

¹⁴¹ O CGI foi instituído pelo Decreto nº 4.829, de 03 de setembro de 2003. Segundo a plataforma, "O Comitê Gestor da Internet no Brasil tem a atribuição de estabelecer diretrizes estratégicas relacionadas ao uso e desenvolvimento da Internet no Brasil e diretrizes para a execução do registro

proteção de dados; (viii) instituições científicas, tecnológicas e de inovação; (ix) confederações sindicais representativas das categorias econômicas do setor produtivo; (x) entidades representativas do setor empresarial relacionado à área de tratamento de dados pessoais; (xi) entidades representativas do setor laboral. Em síntese, seriam representantes do setor público, representantes de entidades da sociedade civil, representantes empresariais e representantes laborais.

É possível concluir que a regulação precisa ser efetiva e conciliar interesses sociais que eventualmente possam conflitar, sem descuidar do principal objetivo do ordenamento jurídico, que é a proteção da pessoa humana. Tais objetivos exigem a participação de múltiplos atores sociais, conforme mencionado.

3.3.

Como regular: importância dos princípios e conceitos vagos

O tema da publicidade personalizada como instrumento de monetização da desinformação traz outro desafio: como prever normas que possam ter aplicação imediata, com segurança jurídica e sem correr o risco de se tornarem obsoletas em pouco tempo? Consoante exposto, as normas variam em um *continuum* que tem como extremos a vagueza e precisão. Assim, ora são mais vagas, ora mais precisas, o que confere maior ou menor flexibilidade e maior ou menor segurança jurídica, que se constituem grandezas inversamente proporcionais¹⁴². Tal preocupação é ampliada no cenário atual, em que mudanças sociais, políticas, econômicas e tecnológicas ocorrem em uma velocidade sem precedentes registrados.

Logo, para tratar o atual e urgente tema de combate à desinformação por meio da adequação da publicidade personalizada, que deve ajustar o fluxo de suas receitas para veículos de comunicação legítima, que não se dedicam a disseminar conteúdo nocivo, é necessária a previsão de normas que se aproximem da precisão, enquanto a longevidade destas normas depende de conceitos mais vagos, cujo extremo pode ser considerado o princípio.

de Nomes de Domínio, alocação de Endereço IP (Internet Protocol) e administração pertinente ao Domínio de Primeiro Nível ".br". Também promove estudos e recomenda procedimentos para a segurança da Internet e propõe programas de pesquisa e desenvolvimento que permitam a manutenção do nível de qualidade técnica e inovação no uso da Internet.". Disponível em <https://www.cgi.br/>. Acesso em 15.02.2022.

¹⁴² SCHAUER, pp. 188-202.

Prever apenas mecanismos rígidos, fixos e altamente específicos pode ser um caminho arriscado para obter resultados efetivos ou pelo menos duradouros, já que a dinâmica do Direito, mesmo nos arranjos propostos no capítulo anterior, não acompanhará o dinamismo da inovação e das transformações tecnológicas, correndo o risco de a norma se tornar obsoleta mesmo antes de sua entrada em vigor. Tal situação ocorre por haver exigência de diagnóstico, discussões, aprovações de propostas e adaptações das empresas de tecnologia que são alvo da regulação proposta. A presente dissertação busca explorar a adoção de mecanismos maleáveis que possam se adequar a distintas épocas e respectivo desenvolvimento tecnológico, com destaque a importantes princípios e conceitos vagos que têm regido o tema.

Não se trata da negativa de regras precisas, mas da necessária abertura que diversos mandamentos regulatórios possuem. Por exemplo, o PL 2630/2020 determina que, “ao aplicar regras próprias que impliquem a exclusão, indisponibilização, redução de alcance ou sinalização de conteúdos gerados por terceiros ou de suas contas”, os provedores deverão notificar o usuário sobre a medida aplicada, o âmbito territorial, a fundamentação, procedimentos e prazos para revisão. Algumas perguntas poderiam ser feitas, sem pretensão de esgotá-las: (i) qual é a forma de notificação?; (ii) quais meios podem ser utilizados?; (iii) como deve ser feita a comprovação de notificação?; (iv) além dos elementos listados, qual deve ser o integral conteúdo da fundamentação?; (v) qual deve ser o grau de profundidade da fundamentação?; (vi) quais são os procedimentos adequados para exercer o direito de revisão?; (vii) qual é o prazo razoável?; (viii) quem possui legitimidade para exercício do direito de revisão?

Trata-se de norma que possui precisão, devendo ser imediatamente implementada, mas com vários aspectos passíveis de debates. Apesar da ausência de precisão que permita garantir uma régua para análise integral de adequação dos procedimentos à norma, a forma como se estrutura a previsão é fundamental para sua sobrevivência: poderia a lei prever respostas para todos os itens sem torná-las insuficientes ou inadequadas em pouco tempo? Apenas para tratar dos itens (i) e (ii) apontados, seria a norma capaz de prever, alguns anos atrás, a notificação via celular como adequada? E via WhatsApp? E via DocuSign? A resposta é não, em razão da inexistência de algumas dessas tecnologias em um passado recente.

Em vários casos, haverá a utilização de normas muito mais precisas, tais como a fixação do número de 10.000.000 (dez milhões) de usuários como patamar mínimo para incidência do PL 2630/2020 ou a restrição de aplicabilidade da LGPD para proteção apenas de pessoas naturais, que figuram como titular de dados pessoais, mas em tantos outros é muito válida a utilização de princípios e normas vagas.

Nesse sentido, diplomas legais e previsões regulatórias têm adotado a estratégia de utilização de princípios e conceitos vagos para não engessar as disposições e abarcar o maior número de situações, com adequação à variação temporal, espacial e tecnológica. Não por acaso, países distintos têm adotado, em tempos distintos, previsões semelhantes para assuntos ligados a novas tecnologias.

Aqui, não se trata propriamente de regulação por princípios, exclusivamente, mas da utilização de princípios e conceitos vagos como elementos que tornam a regulação tecnológica mais adequada, sendo certo que o grau de vagueza varia conforme a disposição.

Uma legislação que utilize a técnica de regulação por princípios possui maior abertura e flexibilidade, o que torna mais fácil a atualização regulatória, evita sobrecarregar e impedir tecnologias inovadoras e amplia o espaço de atuação das companhias privadas, que possuirão maior facilidade para encontrar determinadas soluções¹⁴³. Contudo, não se nega a possibilidade de adaptação de tal técnica com outras existentes.

Assim, a abertura inerente aos princípios evitaria a realização de procedimentos formais e normalmente burocráticos para alteração da substância da regulação, além de se adequar melhor a cada tipo de empresa, variando de acordo com o negócio desenvolvido, o volume de tratamento de dados pessoais e os riscos inerentes à atividade. Por fim, traria especial contribuição para que os diversos atores sociais apontados neste trabalho possam contribuir com a regulação. A estratégia contribui para maior proteção de direitos fundamentais, ao mesmo tempo em que torna menos burocráticos a inovação e o desenvolvimento econômico e tecnológico.

¹⁴³ KELLER, 202-204.

Gunningham e Sinclair¹⁴⁴ falam que uma regulação rígida, sólida e determinante pode não produzir soluções satisfatórias quando lida com circunstâncias que podem se alterar com frequência. Assim, o ideal seria estabelecer princípios que balizam as decisões adotadas por formuladores de políticas. Na ocasião, os autores tratavam da regulação ambiental, mas a constatação é perfeitamente cabível para as tecnologias desenvolvidas no contexto do ambiente virtual, também consideradas maleáveis. Os mesmos autores reiteram a concepção em trabalho posterior, com preferência pela adoção de princípios na regulação, com objetivo de gerar maiores benefícios e efetividade¹⁴⁵.

A publicidade personalizada pode ser regulada de maneira distinta para empresas e produtores de conteúdo que possuam características distintas. Da mesma forma, a evolução tecnológica pode impor decisões regulatórias que demandem agilidade, que estaria impedida por normas absolutamente rígidas. Por exemplo, o regulador pode prever a obrigação de garantia da transparência sem aprofundar os mecanismos que devem ser utilizados, já que tais mecanismos são periodicamente modificados pela própria evolução tecnológica ou, ainda, prever disposições normativas que possuam balizas mínimas, mas que garantam ao intérprete margem de vagueza que deverá ser preenchida a partir dos princípios estabelecidos.

Exemplificativamente, o PL 2630/2020 determina aos provedores de aplicações a criação de instituição de autorregulação voltada à transparência e à responsabilidade no uso da internet que, dentre outras coisas, deverá “desenvolver, em articulação com as empresas de telefonia móvel, boas práticas para suspensão das contas de usuários cuja autenticidade for questionada ou cuja inautenticidade for estabelecida”. As “boas práticas” mencionadas geram uma ampla variedade de normas e mecanismos que podem atender ao mandamento legal, tornando difícil definir o que o legislador quis dizer especificamente. Para isso, um bom norteador são os princípios fixados. Assim, por exemplo, as boas práticas devem atentar para a proteção da liberdade de expressão, da transparência, da não discriminação, da responsabilidade, dos direitos da personalidade, dentre outros.

¹⁴⁴ GUNNINGHAM, Neil; SINCLAIR, Darren. **Designing Smart Regulation (2004)**.

¹⁴⁵ GUNNINGHAM; SINCLAIR, 2017, pp. 133-134.

Doneda¹⁴⁶ trata o cenário tecnológico, sobretudo no contexto da internet, como um espaço fortemente dinâmico que necessita regular o presente, mas também prever as possibilidades futuras trazidas pelo que chamou de “concretude do mundo”. O autor ressalta, contudo, que a regulação não pode ser confundida com futurologia e que instrumentos já existentes e aplicados pelo direito civil podem ser utilizados para conformação daquele mundo concreto ao mundo jurídico, privilegiando aquela que deve ser a maior preocupação do direito: a pessoa humana. Nessa tarefa, destaca a utilização de instrumentos de *soft law* e dos princípios: “nesse sentido, o recurso a técnicas como a utilização de *soft law* ou de cláusulas gerais, aliadas a um trabalho conjunto com outros setores do ordenamento, podem ser alguns dos caminhos a seguir”.

Rodotà¹⁴⁷ também trata da necessidade de previsão de conceitos abertos ou de cláusulas gerais, bem como o estabelecimento de princípios para que a norma não se torne obsoleta com o transcurso do tempo. Contudo, o autor vai além e defende a utilização dos recursos mencionados para garantir que as normas sejam eficazes para destinatários e situações diferentes que convivam no mesmo tempo, transcendendo a lógica diacrônica e alcançando o que chamou de dimensão sincrônica:

A questão da flexibilidade não é nova. Historicamente, porém, ela se referia ao fato de que o passar do tempo criava uma distância entre as normas jurídicas e a transformação da realidade. [...] Isso quer dizer que se levava em consideração a dimensão diacrônica, introduzindo na legislação uma série de fórmulas, ‘cláusulas gerais’ ou ‘conceitos elásticos’, capazes de determinar uma adaptação automática do sistema jurídico à transformação social, sem necessidade de contínuas intervenções legislativas.

Hoje, porém, junta-se à dimensão diacrônica outra dita sincrônica, no sentido de que a adaptação diz respeito também a situações diversas, mas coexistentes em um mesmo momento. [...]

Assim, a lei não é mais vista como um instrumento rígido, e sim flexível; sua concreta atuação impõe um trabalho de adaptação atribuído a outros sujeitos, que não o legislador¹⁴⁸.

De maneira sintética, Rodotà não apenas se preocupa que determinada norma criada hoje deixe de ser eficaz no próximo mês ou ano, mas que normas criadas hoje sejam possíveis, eficientes e suficientes para uns e não para outros.

¹⁴⁶ DONEDA, 2019, pp. 62-70.

¹⁴⁷ RODOTÀ, 2008, pp. 85-88.

¹⁴⁸ Quando trata de outros sujeitos, que não o legislador, Rodotà não se refere apenas ao mercado ou empresas de tecnologias, mas também ao Poder Judiciário, organizações da sociedade civil e atores sociais, mais ou menos formalizados.

Exemplificativamente, mecanismos de *compliance* rigidamente estabelecidos podem ser absolutamente executáveis para uns e inviáveis para outros.

Mulholland e Gomes¹⁴⁹ destacam a importância dos princípios no campo da inteligência artificial e da proteção de dados pessoais, dois importantes temas que se ligam às novas tecnologias. Neste sentido, os autores destacam a estrutura principiológica da LGPD, sobretudo pela previsão trazida pelo art. 6º da Lei. Tal previsão permite abarcar situações presentes e futuras, com possibilidade de adequação concreta para distintos atores que operam no mesmo lapso temporal.

De acordo com os autores, a estrutura axiológica pode ser eficaz para a proteção de dados pessoais, justamente por se amoldar a situações distintas. Além disso, princípios éticos e guias deontológicos e de boas práticas poderiam proteger o titular de dados pessoais, mas com aprimoramento tecnológico benéfico para os próprios desenvolvedores.

Neste sentido, cabe destacar que o ajuste da empresa de tecnologia a boas práticas traz diversos benefícios, como o aumento da confiança do usuário e de investidores, além de evitar sanções administrativas e judiciais.

Magrani e Guedes¹⁵⁰ também defendem princípios éticos como forma de aumentar os benefícios ligados a novas tecnologias, reduzindo os riscos inerentes. Para corroborar a constatação, citam o mapeamento de pelo menos 84 (oitenta e quatro) iniciativas regulatórias de definição de princípios éticos na área de tecnologias desenvolvidas no ambiente virtual. Dentre os princípios mais mencionados, estão os seguintes, em ordem decrescente: transparência, justiça, não maleficência, responsabilidade (*accountability*), privacidade, beneficência, liberdade e autonomia, confiança, sustentabilidade, dignidade e solidariedade.

No Brasil, tem se tornado frequente a utilização dos princípios mencionados para a regulação de novas tecnologias, inclusive ligadas a publicidade personalizada. Exemplificando, é possível mencionar a LGPD e o PL 2630/2020.

¹⁴⁹ MULHOLLAND, Caitlin; GOMES, Rodrigo Dias de Pinho. Inteligência artificial e seus principais desafios para os programas de compliance e as políticas de proteção de dados. In: FRAZÃO, Ana; CUEVA, Ricardo Villas Bôas. **Compliance e políticas de proteção de dados**. São Paulo: Thomson Reuters Brasil, 2021, pp. 161-184.

¹⁵⁰ MAGRANI, Eduardo; GUEDES, Paula. Inteligência artificial: desafios éticos e jurídicos. In: FRAZÃO, Ana; CUEVA, Ricardo Villas Bôas. **Compliance e políticas de proteção de dados**. São Paulo: Thomson Reuters Brasil, 2021, pp. 161-184.

Na LGPD, é possível observar a utilização de princípios e conceitos abertos tanto na apresentação dos fundamentos quanto na lista de princípios, previstos nos arts. 2º e 6º do diploma legal, respectivamente.

São previstos como fundamentos da disciplina de proteção de dados pessoais o respeito à privacidade, a autodeterminação informativa, a liberdade de expressão, de informação, de comunicação e de opinião, a inviolabilidade da intimidade, da honra e da imagem, o desenvolvimento econômico, tecnológico e a inovação, além da livre iniciativa, livre concorrência, a defesa do consumidor, os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais¹⁵¹. De outro lado, são onze princípios trazidos pelo art. 6º da LGPD: finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação, responsabilização e prestação de contas.

No campo dos conceitos abertos relevantes para a publicidade personalizada, é possível citar a base legal do interesse legítimo do controlador, prevista no art. 7º, IX da LGPD, que fundamenta o tratamento de dados pessoais para casos não previstos expressamente nas demais bases legais¹⁵².

Toda operação de tratamento de dados pessoais deve se basear em pelo menos uma das hipóteses previstas nos arts. 7º ou 11 da LGPD, também chamadas de bases legais. Assim, qualquer operação que não encontre justificativas nas situações listadas é considerada ilegítima. Dentre as bases legais listadas, se inclui o interesse legítimo do controlador, um conceito aberto que pode ser utilizado como fundamento para o tratamento de dados pessoais que não esteja justificado nas demais hipóteses.

Tal base legal é historicamente flexível, tendo surgido no contexto europeu e, posteriormente, sido transposta para o ordenamento brasileiro. Segundo Bioni¹⁵³:

o legítimo interesse tem sido encarado como a mais flexível das bases legais de tratamento de dados no regime do direito comunitário europeu. Ainda que sob o mesmo nível hierárquico, o legítimo interesse serviria como uma válvula de escape para que as demais bases legais não fossem “sobrecarregadas”. De um lado, sob o ponto de vista de que quatro das bases legais seriam aplicáveis em situações específicas, como a execução de um contrato, de uma obrigação legal

¹⁵¹ Art. 2º LGPD

¹⁵² LEONARDI, Marcel. Legítimo Interesse. Revista do Advogado, v. 39, n. 144 nov, 2019, pp. 67-73.

¹⁵³ BIONI, 2019, pp. 313-338.

e de um interesse público, bem como para a proteção de interesses vitais do titular dos dados. De outro lado, porque, em muitas situações, seria: a) desnecessário coletar novo consentimento para outros usos (implícitos) dentro de uma relação já preestabelecida com o titular; ou b) quando terceiros: b.1) não tivessem meios para obter tal tipo de autorização; ou b.2) esse tipo de interação inviabilizaria o próprio tratamento dos dados.

Outro ponto importante é a ausência de hierarquia entre as bases legais. Assim, nem sempre o consentimento se apresenta como base legal adequada ao tratamento de dados pessoais e esse é o caso da publicidade personalizada, em que a exigência de coleta inviabilizaria o processo ou o tornaria extremamente oneroso, deturpando as finalidades da publicidade realizada¹⁵⁴. Aliás, Bioni se refere à utilização do interesse legítimo para fins publicitários como “um dos principais gargalos”, pois a “principal engrenagem do formato atual da economia são os dados pessoais para personalizar a oferta e o próprio bem de consumo”¹⁵⁵.

Assim, o legítimo interesse seria um importante fator de conciliação entre os dois grandes grupos de fundamentos trazidos pela LGPD: aquele que se liga à proteção de dados pessoais e aquele que se refere ao desenvolvimento econômico e tecnológico, sobretudo por fundamentar o uso secundário de dados pessoais, que ocorreria quando um dado é coletado para determinada finalidade, mas passa a servir a finalidade distinta, por ordem do controlador, desde que haja respeito aos princípios estabelecidos na legislação vigente que trata de privacidade e proteção de dados pessoais e haja o enquadramento adequado na base legal do legítimo interesse¹⁵⁶.

De fato, a União Europeia enfrentou problemas com a criação do legítimo interesse, já que a ausência de balizas enfraqueciam a efetividade da proteção de dados pessoais, mas tal situação tem sido corrigida com algumas medidas, dentre as quais se destacam o desenvolvimento de Relatórios de Impacto à Proteção de Dados Pessoais (*Data Protection Impact Assessment* ou *DPIA*) e do chamado Teste de Legítimo Interesse (*Legitimate Interests Assessment* ou *LIA*), que tornaram a aplicação da base ainda mais adequada e permitiram ao agente de tratamento conhecer a operação detalhadamente, justificando a utilização do legítimo interesse, identificando riscos inerentes e adotando salvaguardas.

¹⁵⁴ LEONARDI, 2019, pp. 67-73.

¹⁵⁵ BIONI, 2019, pp. 334.

¹⁵⁶ PARENTONI, Leonardo. **Compartilhamento de dados pessoais e a figura do controlador**. In: FRAZÃO, Ana; CUEVA, Ricardo Villas Bôas. **Compliance e políticas de proteção de dados**. São Paulo: Thomson Reuters Brasil, 2021, pp. 161-184.

A dissertação desenvolvida não irá explorar a polêmica atribuição de bases legais para a publicidade personalizada, ainda que aposte, inicialmente, na utilização do legítimo interesse.

Contudo, independentemente do legítimo interesse ser atribuído ou não, é possível exigir a elaboração de relatório de impacto à proteção de dados pessoais em razão da larga escala de tratamento de dados pessoais, utilização de tecnologia inovadora e outros critérios que serão vistos em capítulo próprio.

O PL 2630/2020, seguindo a tendência de regulação de novas tecnologias, inicia suas previsões com uma série de princípios (art. 3º), tais como: (i) liberdade de expressão e de imprensa; (ii) garantia dos direitos de personalidade, da dignidade, da honra e da privacidade do indivíduo; (iii) respeito ao usuário em sua livre formação de preferências políticas de uma visão de mundo pessoal; (iv) responsabilidade compartilhada pela preservação de uma esfera pública, livre, plural e democrática; (v) garantia de confiabilidade e da integridade dos sistemas informacionais; (vi) vedação à discriminação ilícita ou abusiva dos usuários aos serviços dos provedores de aplicações de que trata esta lei, inclusive a dados atualizados e a não restrição técnica de funcionalidades; (vii) acesso amplo e universal aos meios de comunicação e à informação; (viii) proteção dos consumidores; (ix) transparência e isonomia nas regras, como a veiculação de anúncios e conteúdos pagos; (x) proteção a saúde pública. A tais princípios, são acrescentados aqueles previstos em outros diplomas legais, como a própria LGPD, que tem disposições referenciadas em diversas passagens do projeto¹⁵⁷.

É importante notar que tanto a LGPD quanto o PL 2630/2020 trazem a transparência e a responsabilidade (*accountability*) como princípios norteadores que impõem deveres tanto em relação ao tratamento de dados pessoais quanto em relação à liberdade, transparência e responsabilidade na internet. Por serem princípios tão mencionados por legislações – no Brasil e no mundo – e por se apresentarem como importantes aliados do combate à monetização da desinformação por meio da publicidade personalizada, serão destacados a seguir, não como substitutos absolutos de regras e normas próximas do extremo da precisão, mas como institutos que auxiliam na interpretação e conferem flexibilidade às demais disposições.

¹⁵⁷ BRASIL. Câmara dos Deputados. Complementação de voto do relator. Deputado Orlando Silva.

3.3.1.

Accountability

O princípio da *accountability* estimula o cumprimento das disposições regulatórias de maneira preventiva e voluntária, bem como a eventual demonstração posterior daquele cumprimento com objetivo de reduzir sanções e responsabilidades, em caso de incidentes ou situações que gerem risco ou dano desproporcional ao titular de direitos.

No presente trabalho, o desenvolvimento do conceito de *accountability* assume especial relevância, sobretudo na área de proteção de dados pessoais. A importância foi brevemente justificada no subcapítulo 3.1 deste trabalho. Ao focar em regulação de dados pessoais e de estrutura, a tendência é a geração de resultados mais efetivos e com menores riscos à liberdade de expressão que a regulação focada no conteúdo. Conforme observado, não se objetiva a vedação ao recurso da moderação de conteúdo em si, mas não há estímulo para que ela seja feita e, quando for o caso, devem ser adotadas cautelas que mitiguem os riscos gerados por técnicas moderadoras. Na LGPD e no PL 2630/2020, há estímulos para a *accountability*, não apenas pela menção ao instituto, mas também pela inspiração para regulação que fomente a atuação preventiva e a possibilidade de utilização desta atuação para redução de riscos, danos e consequências negativas subsequentes, traduzidas em normas mais precisas que a previsão expressa do princípio em si.

Segundo a *Information Commissioner's Office (ICO)*¹⁵⁸, que é a autoridade de proteção de dados do Reino Unido, a *accountability* é um dos princípios-chave das leis de proteção de dados e funciona de duas maneiras: (i) para incentivar o cumprimento voluntário da legislação; (ii) se necessário, demonstrar a conformidade em momento posterior. De acordo com os padrões estabelecidos, a *accountability* traz a oportunidade para definição de altos padrões internos e de liderança pelo exemplo, o que contribui não apenas para proteger o negócio e o titular, mas para reduzir riscos de sanções e ampliar a confiança de parceiros de negócios e investidores. A autoridade lista algumas medidas de *accountability*:

1. Criar um programa abrangente de gerenciamento de privacidade;
2. Verificar as próprias práticas existentes em relação às expectativas da legislação e de regulação específica;

¹⁵⁸ REINO UNIDO. Information Commissioner's Office. **Accountability Framework** Disponível em <https://ico.org.uk/for-organisations/accountability-framework/>. Acesso em 25.02.2022.

3. Aprimorar as práticas internas existentes, ainda que restrito a áreas específicas;
4. Estabelecer maneiras de demonstrar conformidade;
5. Registrar, acompanhar e relatar o progresso;
6. Aumentar o envolvimento da alta administração e a conscientização sobre privacidade em toda a organização.

Trata-se, portanto, de estímulo ao cumprimento voluntário da legislação vigente e da regulação específica, por meio de mecanismos internos que independem da ação de agentes que não integram a companhia, tais como órgãos jurisdicionais ou autoridades administrativas.

Rosenvald e Faleiros Júnior¹⁵⁹ destacam que a *accountability* pode ser traduzida para a língua portuguesa como responsabilidade, da mesma forma que os termos *responsibility* e *answerability*, mas que os verdadeiros sentidos diferem em substância. Como ponto em comum, os três termos transcenderiam o desfazimento judicial de prejuízos e trariam maior capacidade de resposta para questões mais complexas, como é o caso de novas tecnologias e da internet. Além disso, as medidas seriam mais adequadas à velocidade de transformação social e tecnológica atual.

Contudo, existem diferenças entre os conceitos. *Responsibility* seria a responsabilidade como conceito moral, nunca imposto juridicamente, tendo dois âmbitos de incidência: para o agente de tratamento, como incorporação de valores éticos em suas atividades e, para o titular, como educação digital. *Answerability* seria um procedimento recíproco de justificação de escolhas, possibilitando a compreensão do cenário pelo agente e pelo titular, como ocorre na possibilidade de revisão de decisões tomadas exclusivamente com base em tratamento automatizado de dados pessoais.

Accountability, por sua vez, seria a ampliação do espectro da responsabilidade, por meio da inclusão de aparato regulatório preventivo que possui função *ex ante* ou *ex post*. No plano *ex ante*, a *accountability* funciona como um guia de posturas, conduta e ética que deve ser adotado pelos agentes de tratamento de dados pessoais – no caso deste trabalho, seriam as próprias empresas de tecnologia que realizam o tratamento de dados pessoais para

¹⁵⁹ ROSENVALD, Nelson; FALEIROS JÚNIOR, José Luiz de Moura. **Accountability e mitigação da responsabilidade civil na Lei Geral de Proteção de Dados Pessoais**. In: FRAZÃO, Ana; CUEVA, Ricardo Villas Bôas. **Compliance e políticas de proteção de dados**. São Paulo: Thomson Reuters Brasil, 2021, pp. 771-808.

viabilizar a publicidade personalizada. De outro lado, no plano *ex post*, serviria para demonstrar alguns pontos relevantes ao magistrado e autoridades administrativas, tais como: (i) a suficiência e razoabilidade daqueles guias elaborados; (ii) a adoção efetiva daquele guia; (iii) a efetividade e eficiência das medidas adotadas; (iv) parâmetros para o estabelecimento mais acertado de sanções, seja na seara judicial ou administrativa.

Bennett e Raab¹⁶⁰ tratam da *accountability* como um dos principais instrumentos globais utilizados para regulação da privacidade e proteção de dados pessoais, impulsionada pela evolução tecnológica e comunicacional, sendo tomada como filosofia e técnica tanto pela regulação estatal quanto pela autorregulação. Segundo os autores, há uma aposta na estratégia para estabelecer maior autonomia aos agentes de tratamento para criação de códigos de condutas e respectiva adesão interna, que pode incluir questões como a forma de notificação, a gestão de incidentes de segurança da informação, o estabelecimento de diretrizes voltadas à privacidade e à proteção de dados pessoais e outras questões.

Combinando os conceitos expostos, na *accountability* seria possível estabelecer para empresas que lidam com publicidade personalizada a atribuição para criação de normas técnicas, procedimentos, códigos de conduta e ética e outros padrões para reduzir o impacto da publicidade personalizada como fomento à desinformação. Desta forma, a atuação cotidiana, que exige expertise e dinamismo ficaria a cargo das empresas de tecnologia. Contudo, diante da já mencionada insuficiência da autorregulação, haveria sempre a possibilidade de fiscalização e análise por autoridades administrativas e judiciais acerca da adequação das normas e seu fiel cumprimento, funcionando não apenas como parâmetros sancionatórios, mas também como uma espécie de prêmio para aquelas empresas que adotam medidas eficazes para solução do problema apresentado.

Para Mendes e Fonseca¹⁶¹, tais mecanismos seriam importantes, pois a previsão de direitos não seria suficiente sem meios de efetivação. Neste sentido, seriam necessárias condições institucionais para garantir a proteção de direitos

¹⁶⁰ BENNETT, Colin; RAAB, Chales. **Revisiting the governance of privacy: contemporary policy instruments in global perspective**. Regulation & Governance, 2018, doi:10.1111/rego.12222.

¹⁶¹ MENDES, Laura Schertel; FONSECA, Gabriel Campos Soares. **Proteção de dados para além do consentimento: tendências de materialização**. In: MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JR., Otavio Luiz (Coords.). **Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: Forense, 2021, pp. 135-167.

como a liberdade de expressão e a privacidade, com condições institucionais para participação de múltiplos atores, sobretudo porque a adoção de determinadas medidas demandaria a participação direta dos agentes responsáveis pelo tratamento.

No Brasil, a LGPD traz diversas previsões que apontam para a *accountability* como um importante fator a ser observado por agentes de tratamento de dados pessoais, a iniciar pelo rol principiológico do art. 6º, especificamente no inciso X, que prevê que as atividades de tratamento de dados devem observar a boa-fé, a responsabilização e a prestação de contas, que seria a “demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas”¹⁶².

O grau de discricionariedade do agente se encontra em algumas disposições da Lei, dentre as quais podemos destacar o art. 52, §1º da LGPD, que traz diversos parâmetros e critérios para aplicação de sanções administrativas, dentre os quais: (i) a cooperação do infrator; (ii) a adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano, voltados ao tratamento seguro e adequado de dados; (iii) a adoção de política de boas práticas e governança; (iv) a pronta adoção de medidas corretivas¹⁶³.

Ao longo da LGPD, raramente se estabelece o grau preciso de segurança e os mecanismos que devem ser utilizados, se valendo de expressões como “medidas de segurança, técnicas ou administrativas aptas a proteger os dados pessoais”¹⁶⁴. A ideia desta previsão é possibilitar que os agentes de tratamento se adequem de acordo com a estrutura, o volume de dados, a relevância, o serviço prestado, a sensibilidade de dados tratados, dentre outros, já que a LGPD se aplica de pequenos negócios a grandes empresas de tecnologia que tratam volume massivo de dados pessoais e utilizam técnicas de *profiling*, de tal sorte que a Lei provavelmente falharia ao tentar prever medidas concretas para todos os níveis.

Sem dúvidas, a LGPD se apresenta como aliada na regulação de publicidade personalizada como forma de regulação da desinformação pela proteção de dados pessoais, em detrimento de uma regulação focada no conteúdo

¹⁶² LGPD, Art. 6º, X.

¹⁶³ LGPD, Art. 52, §1º.

¹⁶⁴ LGPD, Art. 46.

que traga ameaças à liberdade de expressão. Fortalecer a LGPD como centro gravitacional da proteção de dados e como efetivação do agora expresso direito fundamental à proteção de dados é importante para coibir o tratamento irregular de dados pessoais que estimule a produção de desinformação feita com objetivos meramente lucrativos.

Nesse aspecto, cabem dois comentários: (i) a LGPD prevê a base legal do interesse legítimo do controlador, que exige a elaboração de dois documentos muito ligados à *accountability*, que são o DPIA e LIA, que contribuem para detalhamento e identificação da operação, riscos e medidas de salvaguarda. Assim, o objetivo é verificar os riscos inerentes à operação e respectivos instrumentos de mitigação, o que deverá incluir potenciais violações oriundas de desinformação e mecanismos de redução do fluxo de receitas de publicidade para veículos que se dedicam à produção de conteúdo nocivo; (ii) nesse momento, não devem ser estimuladas disposições externas à LGPD que intervenham no tema de dados pessoais diretamente, como faz o art. 7º, §1º do PL 2630/2020, que veda “a combinação do tratamento de dados pessoais dos serviços essenciais dos provedores com os de serviços prestados por terceiros, quando tiverem como objetivo exclusivo a exploração [...] no mercado”. Os motivos da crítica já foram expostos em momento anterior.

Diversos pontos do PL 2630/2020 preveem a efetivação da *accountability* para os provedores. Em primeiro lugar, no art. 3º, IV e V está prevista a responsabilidade compartilhada pela preservação de uma esfera pública livre, plural e democrática, além da garantia de confiabilidade e da integridade de sistemas informacionais. Em segundo lugar porque o parágrafo primeiro do mesmo artigo prevê a expressa aplicabilidade da mencionada LGPD. Em terceiro lugar, porque existem disposições que permitem ao provedor agir com certo grau de discricionariedade, de maneira preventiva, mas com necessidade de comprovação da efetividade em caso de riscos ou danos causados. Exemplo disso é a previsão do art. 7º, *caput*, que determina a criação de regras próprias para atender aos objetivos trazidos no PL, de maneira a assegurar o respeito à legislação vigente e a direitos fundamentais. Outro exemplo é a previsão de disponibilização de informações claras, públicas e objetivas que conduzam ao cumprimento do dever de transparência. Trata-se de previsões que determinam a criação de regras e mecanismos sob discricionariedade do provedor, mas cuja eficácia deve ser buscada em razão da possibilidade de controle posterior.

Há medidas concretas – que serão vistas em capítulo seguinte – que podem contribuir para a implementação de mecanismos efetivos para minimização dos danos causados pela desinformação, sobretudo no campo preventivo, que se baseia no desestímulo à criação do conteúdo desinformativo por simples esvaziamento de receitas destinadas a sites que se dedicam a espalhar o conteúdo falso com deliberada intenção de enganar o usuário.

3.3.2.

Transparência

Além da mencionada *accountability*, há outro princípio importante para o tema da regulação de novas tecnologias e da publicidade personalizada: o princípio da transparência, que contribui para a regulação focada em dados pessoais e na estrutura dos provedores, em detrimento da regulação focada em moderação do conteúdo. Mais do que isso: o princípio - e mesmo as normas mais precisas que buscam atender parâmetros de transparência – é capaz de estabelecer instrumentos de controle e autodeterminação inclusive na hipótese de moderação do conteúdo, conforme será observado.

De acordo com a ICO, a transparência é outro princípio-chave estabelecido para o tema da privacidade e proteção de dados, que facilita a concepção de privacidade *by design* e *by default*. Tal princípio possui sentido amplo. No âmbito do GDPR e da LGPD, é tratado como garantia de informações claras, precisas e facilmente acessíveis pelo titular acerca do tratamento de seus dados pessoais.

Previsto no art. 6º, VI da LGPD, a transparência também figura como ponto fundamental quando da utilização do interesse legítimo do controlador como base legal, consoante art. 10, §2º, que sobressalta a já imperiosa transparência que deve acompanhar qualquer operação de tratamento de dados pessoais. Além disso, os agentes de tratamento podem implementar programa de governança que tenha como objetivo aumentar a confiança do titular, por meio de atuação transparente. De acordo com Frazão¹⁶⁵, “é fundamental que a relação entre a empresa e os titulares de dados seja facilitada, aberta, transparente e se realize em um ambiente dialógico e transparente”.

¹⁶⁵ FRAZÃO, Ana. **Propósitos, desafios e parâmetros gerais dos programas de compliance**. In: FRAZÃO, Ana; CUEVA, Ricardo Villas Bôas. **Compliance e políticas de proteção de dados**. São Paulo: Thomson Reuters Brasil, 2021, pp. 33-64.

De acordo com pesquisa apresentada pela SproutSocial¹⁶⁶, o crescimento do uso de mídias sociais e o aprofundamento da relação entre marcas e consumidores, aliados a outros fatores inerentes ao ambiente virtual, têm contribuído para o surgimento de uma “Era da desconfiança”, que impõe o alargamento da transparência. Segundo levantamento feito, o maior número de pessoas considerou como transparente o negócio tido como “aberto, claro e honesto”, em detrimento de outras características utilizadas na pesquisa, tais como integridade, comunicação e autenticidade. Além disso, o público entrevistado depositava maior expectativa na transparência de negócios, acima de qualquer outra categoria, como de políticos e organizações sem fins lucrativos, respectivamente em segundo e terceiro lugares.

No PL 2630/2020, há diversas previsões acerca da transparência, que é um dos três pilares do projeto, ao lado da liberdade e da *accountability*. A seção II do Capítulo II trata exclusivamente dos deveres de transparência, com divisão em subseções que tratam, respectivamente, de: (i) Deveres de Transparência das Redes Sociais e dos Serviços de Mensageria Instantânea e (ii) Deveres de Transparência das Ferramentas de Busca. O capítulo III trata especificamente da transparência em relação a impulsionamentos e publicidade, prevendo o dever de identificação de conteúdo impulsionado e publicitário, além da disponibilização facilitada de todos os conteúdos de propaganda eleitoral impulsionada, dentre outras previsões, passíveis de elogios e críticas¹⁶⁷.

Dentre os dispositivos, estão consolidadas normas mais precisas e outras normas mais vagas, o que confere um grau de certeza mínimo para aplicação atual, mas sem impor parâmetros extremamente rígidos que atraiam a obsolescência prematura da norma.

Por exemplo, os arts. 9º e 10 do PL 2630/2020 impõem a elaboração de relatórios semestrais de transparência que devem ser disponibilizados ao público em até 30 (trinta) dias após o término do semestre. Se trata de parâmetros fixos: (i) há obrigação de produzir um relatório; (ii) o relatório precisa ser semestral; (iii) o prazo para disponibilização ao público é de 30 (trinta) dias após o respectivo

¹⁶⁶ Sprout Social. **From risk to responsibility: social media & the Evolution of transparency.** Disponível em: <https://media.sproutsocial.com/uploads/2019/04/Sprout-Social-Brands-Get-Real-Evolution-of-Transparency.pdf>.

¹⁶⁷ Dentre os exemplos, é possível citar o recente “Manifesto Conjunto: PL das Fake News é Retrocesso Digital”, assinado por diversas associações, tais como a Fecomercio/SP, o IAB Brasil e a Asociación Latinoamericana de internet. O documento destacava 9 pontos de atenção, dentre os quais o risco de proibir a publicidade personalizada e, de forma mais grave, obstar a publicidade online, cuja importância para anunciantes e produtores de conteúdo de portes variados já foi demonstrada nesse trabalho.

semestre. De outro lado, a forma e a estrutura de disponibilização não são rígidas, bem como os “padrões tecnológicos abertos” não são absolutamente fixos, sobretudo porque os veículos e estrutura de apresentação podem variar de acordo com o tempo. Qual seria o balizador da parte vaga da norma, que se apresenta ao lado de estrutura mais precisa? Sem dúvidas, é a busca pela transparência, que imporá sempre a escolha pelo mecanismo mais adequado para atendê-la, em detrimento de mecanismos que tragam menos transparência.

A moderação de conteúdo não é um foco do PL 2630/2020, mas também não é considerada ilícita, já que existem situações que exigirão a prática. Contudo, o PL é muito focado em tornar os mecanismos mais transparentes e promover aos atores envolvidos a possibilidade de analisar como a moderação tem ocorrido e propor ou impor melhorias, a depender da posição ocupada. Tal pretensão é expressa em algumas passagens, tais como os arts. 9º, §1º e 10, §1º, que impõem a elaboração de relatórios que contenham quantidade de conteúdo moderado, a identificação de fundamentos em regras próprias ou em determinações judiciais, o número de pedidos de revisão pelo autor do conteúdo, as características gerais das equipes que estabelecem os parâmetros e/ou realiza avaliação, o total de conteúdos identificados, removidos, suspensos ou considerados irregulares pelo provedor.

No tocante à transparência voltada para impulsionamentos e publicidade, também há variação no *continuum* vagueza-precisão, mais do que divisões binárias entre regras/princípios ou conceitos vagos/conceitos determinados. Assim, o art. 16 do PL 2630/2020 estabelece que provedores de redes sociais e mensageria instantânea identifiquem conteúdos impulsionados e publicitários com menção à conta que promove tal conteúdo. Além disso, os provedores devem disponibilizar a visualização do conjunto da propaganda eleitoral realizada (art. 17) e “histórico dos conteúdos impulsionados e publicitários com os quais a conta teve contato nos últimos 6 (seis) meses, detalhando informações a respeito dos critérios e procedimentos utilizados”, dentre outras disposições.

O princípio pode assumir diversas acepções no âmbito das novas tecnologias. Neste sentido, pode se dirigir ao consumidor, ao cidadão, a agentes reguladores, a autoridades administrativas ou judiciais. Da mesma forma, a transparência pode se dirigir aos anunciantes e marcas, que não querem figurar ao lado de conteúdo nocivo, como é o caso da desinformação, o que acaba ocorrendo frequentemente por falta de transparência.

Hartmann propõe uma resposta regulatória que busque ampliar a transparência¹⁶⁸:

Uma resposta regulatória que criasse mais transparência para os anúncios algorítmicos, assim realinhando os incentivos dos anunciantes, negaria receita de propaganda a publicadores de desinformação prejudicial. A melhor forma de alcançar esse objetivo é fornecer às empresas anunciantes e ao público em geral um conjunto de dados detalhados em larga escala sobre gastos com propaganda que seja cruzado com bases de dados de checagem de fatos.

Nesse sentido, propostas variadas podem ser apresentadas, tais como a constante do trabalho citado, que defende a combinação de bibliotecas de anúncios e agência de checagem dos fatos.

Além disso, há a possibilidade de criação de termos de uso¹⁶⁹ e políticas de privacidade¹⁷⁰ que contemplem de maneira clara, completa e objetiva as hipóteses de tratamento e alocação dos anúncios, sempre atenta aos segredos comercial e industrial.

O capítulo seguinte trará medidas concretas que busquem atender à *accountability* e à transparência com objetivo de regular a publicidade personalizada e sua relação com a desinformação sob o viés da regulação focada em dados pessoais e na estrutura, reduzindo os riscos trazidos por uma regulação focada em conteúdo e definição subjetiva da verdade e da mentira.

¹⁶⁸ HARTMANN, Ivar Alberto. **Combinando Bibliotecas de Anúncios com Checagem de Fatos para Aumentar a Transparência sobre a Desinformação**. Direito Público, [S.l.], v. 18, n. 99, out. 2021. ISSN 2236-1766.

¹⁶⁹ WIELSCH, Dan. Os ordenamentos das redes: termos e condições de uso – Código – Padrões de Comunidade. In: ABOUD, Georges; NERY JR., Nelson; CAMPOS, Ricardo (Orgs.). **Fake News e regulação**. São Paulo: Thomson Reuters, pp. 135-162.

¹⁷⁰ TZIRULNIK, Ernesto; DE ALMEIDA, Gustavo Palheiros. **Recomendações gerais para o desenvolvimento de programas de privacidade e proteção de dados no setor de seguros**. In: FRAZÃO, Ana; CUEVA, Ricardo Villas Bôas. **Compliance e políticas de proteção de dados**. São Paulo: Thomson Reuters Brasil, 2021, pp. 915-935.

4

Práticas de transparência e *accountability* ligadas a estrutura e proteção de dados pessoais

4.1.

Transparência e empoderamento do usuário

A desinformação é um problema que prospera com maior facilidade no ambiente virtual, sobretudo quando motivada pela finalidade lucrativa, com receitas oriundas da publicidade personalizada que é capaz de remunerar veículos de comunicação sem analisar o conteúdo, mas com base no perfil do usuário que acessa determinado canal. Além disso, foi demonstrado que o combate a tais fatores deve perpassar o caminho da regulação, o que não se dá de maneira necessariamente trivial e intuitiva. A moderação de conteúdo pode parecer a solução ideal, porque o conteúdo falso deve ser combatido, afirmação que não está em discussão. Contudo, a definição de desinformação para fins de análise do caso concreto não é precisamente definida e traz concepções controversas que podem violar discursos legítimos, demandando propostas que corrijam ou mitiguem os riscos e danos oriundos da desinformação, mas sem violar a liberdade de expressão de maneira desproporcional.

Por tais razões, foram apresentadas algumas diretrizes, como a busca de regulação por meio de aspectos estruturais e de proteção de dados, com garantia de participação de múltiplos atores sociais e com suporte de importantes princípios e conceitos que se aproximam do extremo da vagueza no *continuum* estabelecido, como a transparência e a *accountability*, sem prejuízo de disposições mais precisas.

Contudo, tratar de regulação com foco na transparência estabelece um norte que deve ser perseguido, mas não resolve o problema de maneira imediata. Ainda que as normas sobre o ambiente virtual devam ser interpretadas com a lente da transparência, o rol de possibilidades regulatórias permanece amplo.

O objetivo deste tópico é tratar medidas concretas relevantes, por meio da análise de trabalhos acadêmicos e propostas legislativas, inclusive no Brasil

Dentre elas, é necessário destacar a busca pelo devido processo legal¹⁷¹, que fornece maiores garantias ao criador do conteúdo, como a possibilidade de conhecer os fundamentos da decisão que derrubou o conteúdo ou sua conta ou que limitou o alcance de seu discurso, além de poder contestar o resultado e recorrer da decisão.

De acordo com o *Office of the United Nations High Commissioner for Human Rights (OHCHR)*¹⁷², a moderação de conteúdo ocorreria quando a plataforma define o discurso que pode ser exibido, mantido e/ou disponibilizado. Além disso, reconhece que a prática era mais simples de ser implementada e operada quando se limitava a direitos autorais ou conteúdo que envolvia abuso sexual infantil, por exemplo. Contudo, o escopo se expandiu para questões mais complexas, como a moderação de discurso de ódio e desinformação, que provocaram legislações que cometeram alguns erros comuns: (i) definição imprecisa de “desinformação”, “notícia falsa” e “discurso nocivo”, por exemplo; (ii) atribuição de monopólio regulatório para as plataformas ou, pelo menos, de amplos poderes regulatórios para tais empresas; (iii) priorização de moderação de conteúdo como solução e fixação de prazos irrealistas, que levam à coação por remoção e; (iv) utilização excessiva de inteligência artificial, que reproduz e amplifica preconceitos existentes.

De outro lado, medidas que se ancoram em direitos humanos e que focam no processo e não no conteúdo seriam muito mais eficientes. Tais regulações devem se preocupar menos em estabelecer um conceito rígido de verdade ou mentira (frequentemente chamada de desinformação, *fake news*, conteúdo falso ou semelhantes). O foco, portanto, deveria ser a garantia de maior transparência e empoderamento do usuário, que teria como um dos principais e mais modernos mecanismos o devido processo.

Hartmann¹⁷³ defende que o poder público deveria se concentrar em alternativas que trouxessem maiores garantias, poderes e liberdades ao usuário,

¹⁷¹ Alguns autores chamam de *private due process* ou devido processo legal privado (tradução livre), com objetivo de se referir a um devido processo ou um caminho a ser percorrido por plataformas privadas. Vide LLANSÓ, Emma et. al. **Artificial intelligence, content moderation, and Freedom of Expression**. Transatlantic Working Group on Content Moderation Online and Freedom of Expression, 2020.

¹⁷²¹⁷² United Nations Human Rights. **Regulating online content – the way forward**. Digital Spaces, 2020. Disponível aqui.

¹⁷³ HARTMANN, Ivar Alberto; MONTEIRO, Julia lunes. Fake News no Contexto de Pandemia e Emergência Social: os Deveres e Responsabilidades das Plataformas de Redes Sociais na Moderação de Conteúdo Online: entre a Teoria e as Proposições Legislativas. **Direito Público**, [S.l.], v. 17, n. 94, jul/ago. 2020, pp. 388-414.

o que incluiria o devido processo legal. Aliás, a defesa é de que o principal papel do poder público seria garantir o adequado funcionamento desta estrutura para que houvesse possibilidade real e mais equilibrada de o usuário ser o verdadeiro moderador do conteúdo. Assim, o Poder Legislativo deveria inserir a previsão em lei ou as plataformas poderiam trazer procedimentos próprios ligados à garantia do devido processo, enquanto o Poder Judiciário teria como principal atribuição “avaliar elementos procedimentais dos sistemas de moderação de conteúdo criados e administrados pelas plataformas. Isto é, verificar se o esquema de moderação estabelecido pela plataforma respeita regras mínimas de devido processo”¹⁷⁴. O papel do Poder Executivo seria de atuar como um intermediário, capaz de se especializar e auditar os sistemas, códigos e arquitetura implementados. Todos os atores mencionados deveriam trabalhar para estabelecer mecanismos intuitivos e orientações claras e acessíveis acerca do procedimento de moderação. Nesse contexto, o principal agente de controle do discurso seria o usuário¹⁷⁵:

Quem deveria então realizar a análise de mérito de cada caso de fake news em particular? Em razão também do volume das manifestações que precisam ser submetidas a algum crivo, este trabalho é o novo papel para os usuários. Os usuários devem ser os filtros (Hartmann, 2017) pelo fato de que a vasta maioria dos discursos flui entre agentes que não possuem uma capacidade comunicativa especialmente dominante, como a de grandes jornais, em comparação com pessoas comuns.

O legislador, portanto, deveria se abster de impor obrigações que levam à moderação de conteúdo com prazos que inviabilizam uma atuação de qualidade, buscando estabelecer salvaguardas que incluem diretamente o devido processo. Tal preocupação se expande no ambiente virtual que impõe a necessidade de decisões automatizadas e operadas por algoritmos, aumentando a preocupação com cerceamento à liberdade de expressão e o anseio por instrumentos e procedimentos mais adequados de reclamação e resolução de disputas na moderação de conteúdo online¹⁷⁶.

¹⁷⁴ Ibid.

¹⁷⁵ Ibid

¹⁷⁶ LLANSÓ, Emma et. al. **Artificial intelligence, content moderation and Freedom of Expression**. Transatlantic Working Group on Content Moderation Online and Freedom of Expression, 2020.

Keller¹⁷⁷ demonstra que não foi esse o caminho trilhado pelo Marco Civil da Internet, sobretudo a partir da análise dos arts. 19 a 21, porque os dispositivos facultam a moderação de conteúdo, mas não a impõem ou criam balizas precisas de atuação, respondendo o intermediário apenas em caso de descumprimento de ordem judicial de remoção de conteúdo, salvo raríssimas exceções que não abrangem a desinformação (publicação de nudez ou ato sexual de caráter privado e questões ligadas a direitos autorais). Com isso, basicamente não são previstos instrumentos adequados de notificação e salvaguarda, deixando a regulação sob a guarda das plataformas privadas e como único escrutínio público o Poder Judiciário, que é limitado por uma série de questões, como a incapacidade de lidar com todos os casos de desinformação ocorridos no ambiente virtual e a necessidade de ser provocado para agir, limitações que fomentam abusos ou inércias, por parte do intermediário, que não são passíveis de sanções.

Para Sander¹⁷⁸, a busca por uma regulação baseada em direitos humanos, o que inclui a liberdade de expressão, deve necessariamente assegurar o devido processo legal, seja no ambiente virtual ou fora dele. Contudo, resta a pergunta: o que seria devido processo legal online? O autor responde que todo processo legal somente será devido por meio de análise contextual. No ambiente virtual, demandaria a garantia mínima de notificação e apelação a todos os usuários cujos conteúdos tenham sido removidos, suspensos ou restringidos. Além disso, a notificação deveria conter, no mínimo: (i) linguagem compreensível; (ii) identificação do conteúdo removido (iii) os dispositivos legais ou de políticas próprias que tenham sido violados; (iv) indicação dos mecanismos de contestação e revisão; (v) o modo pelo qual o conteúdo foi detectado e punido e; (vi) prazos para recursos e decisões. Quanto à apelação, deveria ser garantida, pelo menos, a possibilidade de revisão por pessoa ou junta de pessoas que não tenham se envolvido na decisão inicial.

O PL 2630/2020 traz disposições que versam exclusivamente sobre procedimentos de devido processo (Seção IV). O art. 15, I determina que, no caso de a aplicação das normas pela plataforma implicar “exclusão, indisponibilização, redução de alcance ou sinalização de conteúdos gerados por terceiros ou de suas contas”, deve ser analisado o procedimento de notificação, que deve conter

¹⁷⁷ KELLER, Clara Iglesias. Policy by judicialisation: the institutional framework for intermediary liability in Brazil. **International Review of Law, Computers & Technology**, 35:3, 185-203, DOI: 10.1080/13600869.2020.1792035.

¹⁷⁸ SANDER, Barrie. Freedom of Expression in the Age of Online Platforms: the Promise and Pitfalls of a Human Rightsbased Approach to Content Moderation. **Fordham International Law Journal**. v.43:4, pp. 939-1006.

natureza da medida, âmbito geográfico de aplicação, a fundamentação e prazos para revisão, inclusive quando adotada exclusivamente por meio automatizado. A última previsão observará o art. 20, §1º da LGPD, que trata da revisão de decisão tomada unicamente com base em tratamento automatizado de dados pessoais. Ao exposto, acrescente-se a necessidade de análise de pedidos de revisão, com resposta fundamentada. Se for o caso de reforma da decisão “os provedores de redes sociais ou mensageria instantânea devem, no âmbito e nos limites técnicos de seus serviços, informar os usuários sobre seu erro, na mesma proporção de alcance do conteúdo”¹⁷⁹.

Desta forma, caso haja descumprimento, o Poder Judiciário deveria ser legitimado não para avaliar o conteúdo da postagem, mas para verificar o respeito ao devido processo, além de outros aspectos formais, não devendo interferir, como regra, no conteúdo da publicação.

Além dos pressupostos acima, caberia ao Estado-juiz a análise de outras questões formais, como as características das equipes que procedem criação e aplicação dos critérios de moderação de conteúdo, nos termos do art. 9º, V e 10, VI do PL 2630/2020. Tal papel é fundamental, por razões que se somam à constatação feita por Hartmann¹⁸⁰: “as pessoas contratadas indiretamente pelas plataformas para [...] visualizar centenas de posts diariamente para decidir se constituem violação dos ‘termos de serviço’ sofrem com condições de trabalho precarizadas e falta de garantias”.

Para fins de publicidade personalizada, o devido processo também é absolutamente importante, pois permite que o usuário exerça todas as possibilidades de revisão de decisões que levem à desmonetização ou perda de receitas oriundas de anúncios publicitários. Conforme exposto, um dos maiores benefícios da publicidade personalizada para a liberdade de expressão é a possibilidade de ampliação do número de veículos de comunicação que passam a ter uma fonte de patrocínio de suas atividades de maneira muito mais fácil e democrática do que ocorria nos veículos tradicionais.

Tais medidas são fundamentais para o combate à desinformação (já que permite eventual moderação de conteúdo), mas traz salvaguardas para o autor do

¹⁷⁹ Art. 15, §3º do PL 2.630/2020.

¹⁸⁰ HARTMANN; MONTEIRO, 2020, p. 399.

conteúdo que seria alvo de moderação. Contudo, o devido processo deve ser substancial e não meramente formal.

Outro instrumento de transparência e empoderamento do usuário é a identificação de publicação promovida ou impulsionada. Segundo Hartmann¹⁸¹, tal mecanismo de transparência afeta o comportamento dos leitores, principalmente no contexto político, porque tendem a dar menos credibilidade a anúncios pagos e compartilhá-los com menor frequência. Tal garantia seria importante para aumentar o senso crítico, revelar recursos que se destinam a bancar a desinformação e impactar negativamente as marcas e veículos que se utilizam da estratégia como forma de monetizar o conteúdo nocivo.

Além disso, o rótulo destacado, com indicação de se tratar de conteúdo impulsionado ou publicitário, é capaz de mudar a percepção do usuário e quebrar a automatização da crença naquilo que está acessando, estimulando um senso crítico: “como nós somos, em certo sentido, ‘programados’ para acreditar naquilo que vemos ou ouvimos, temos a tendência de considerar vídeos e áudios como autênticos e incorruptíveis”¹⁸². A fixação do rótulo, longe de deslegitimar a postagem, é capaz de acender sinal de alerta.

Por tais razões, a Resolução nº 23.671/2021 do Tribunal Superior Eleitoral determinava, dentre outras medidas, que os provedores de aplicação deveriam informar os usuários acerca da possibilidade de tratamento de dados pessoais para fins de propaganda eleitoral. Além disso, deveriam garantir a identificação expressa de propaganda política feita por candidatos, partidos, federações e coligações. O Tribunal desenvolveu, ainda, um guia orientativo acerca do tratamento de dados pessoais no contexto eleitoral e determinou que a LGPD fosse observada nos casos de tratamento de dados voltado ao envio de mensagens publicitárias personalizadas: “perfil comportamental, que está na base do microdirecionamento da publicidade on-line, constitui dado pessoal, já que associado a uma pessoa natural identificada, no caso, uma usuária ou um usuário de um provedor de aplicação de internet”.

¹⁸¹ HARTMANN, 2021, p. 466.

¹⁸² MULHOLLAND, Caitlin; OLIVEIRA, Samuel Rodrigues. Uma Nova Cara para a Política? Considerações sobre Deepfakes e Democracia. **Direito Público**, v. 18, n.99, pp. 368-396, jul-set/2021.

Não há qualquer disposição que vede a realização da operação de tratamento ou mesmo o envio de mensagens direcionadas. O que se busca é garantir a transparência por meio de identificação destacada.

Aliás, é o que recomenda o art. 6º, II e §1º do PL 2.630/2020. Segundo o dispositivo¹⁸³:

Art. 6º. Com o objetivo de proteger a liberdade de expressão, o acesso à informação e fomentar o livre fluxo de ideias na internet e resguardar os usuários de práticas fraudulentas, os provedores, no âmbito dos seus serviços, devem adotar medidas para:

[...]

II - identificar todos os conteúdos impulsionados e publicitários cuja distribuição tenha sido realizada mediante pagamento ao provedor, bem como os conteúdos referentes às contas automatizadas;

[...]

§ 1º A identificação de conteúdos impulsionados e publicitários de que trata este artigo deve ser sinalizada de maneira destacada e a sinalização mantida inclusive quando o conteúdo ou mensagem for compartilhado, encaminhado ou repassado de qualquer maneira.

Assim, o que se busca é garantir a liberdade de expressão e o direito à informação, com determinação de que toda distribuição feita mediante pagamento seja identificada de forma destacada, tanto na publicação original quanto em eventual compartilhamento.

Somado a isso, deve ocorrer a identificação do responsável pelo impulsionamento e do anunciante (art. 16) e a disponibilização de meio de fácil acesso para visualização de todos os conteúdos de propaganda eleitoral personalizada (art. 17). Em conjunto com a identificação do impulsionamento, publicidade e autoria, devem figurar uma série de dados previstos no art. 19 do PL 2630/2020.

O PL 2630/2020, por ora, perde oportunidade de empoderar o usuário de maneira mais efetiva, plural e democrática, nada obstante possa fazê-lo ao longo da tramitação. Isso porque deveriam ser utilizados os já existentes mecanismos de perfilamento de publicidade personalizada para escolher usuários de diferentes áreas de formação, classes sociais, matrizes culturais, graus de instrução dentre outros fatores para avaliar a mesma publicidade ou conteúdo, conferindo-lhes maior grau de análise de uma postagem, proporcionando a análise pelo usuário mas reduzindo (senão impedindo) a atuação de grupos que operam em bolha:¹⁸⁴

¹⁸³ Complementação do Voto do Relator. PL 2.630/2020.

¹⁸⁴ HARTMANN; MONTEIRO, p. 400.

As plataformas deveriam, em qualquer caso, buscar por usuários moderadores atuantes com diferentes backgrounds, evitando assim “filtros bolha [...] As iniciativas de publicidade personalizada, já praticadas por essas empresas, permitem, por exemplo, que possam escolher usuários de diferentes áreas de formação – médicos, por exemplo – e inclinações políticas – nem só com valores progressistas e nem só com valores conservadores – para avaliar postagens marcadas como fake news, tanto no intuito de restringir a sua divulgação para uma audiência ampliada quanto no intuito de evitar uma avaliação enviesada sob o ponto de vista cultural.

As propostas apresentadas são capazes de reduzir o impacto da desinformação, senão sua criação e disseminação, por meio de regulação voltada para a estrutura da plataforma e não para o conteúdo ou definição de mentira ou verdade.

4.2.

Transparência e controle para o anunciante

Os anunciantes que pagam os valores que frequentemente financiam a desinformação por meio da publicidade personalizada possuem pouco controle sobre o local em que o anúncio será exibido.

Por tais razões, o presente tópico se debruça sobre formas de conferir maior transparência e controle aos anunciantes, o que precisa ocorrer de forma mais fácil e acessível, já que a empresa ou marca não será necessariamente grande e bem estruturada. Pelo contrário, a maior parte do volume de receitas oriundas de publicidade personalizada advém de pequenos e médios negócios.

O objetivo é contribuir com reflexões já iniciadas ou estruturadas, ainda que o problema não possa ser decidido de plano, já que a atribuição de transparência e total clareza para os anunciantes seria o “Santo Graal”¹⁸⁵ da responsabilidade no setor de publicidade personalizada. Estruturar e operacionalizar mecanismos eficientes não é simples¹⁸⁶.

Sugestões mais genéricas acerca do PL 2630/2020 podem ser realizadas. Um dos pontos seria a inclusão de princípio expresso não apenas de transparência, mas de transparência e controle voltados para o anunciante. De outro lado, poderia ser atribuída ao Comitê Gestor da Internet a busca específica por mecanismos que oferecessem maior controle e transparência ao anunciante

¹⁸⁵ BRAUN; EKLUND, p. 17.

¹⁸⁶ Ibid.

– e não apenas ao usuário. Tal medida poderia contribuir para o combate ao conteúdo de baixa qualidade e à desinformação, por liberalidade do anunciante, que investe em anúncios. Nada obstante a ausência de disposições expressas, é possível atuar, fora do processo legislativo, para a busca de medidas neste sentido, inclusive como obrigação legal imposta de maneira indireta, já que o art. 3º, IX do PL 2630/2020 prevê a transparência, o art. 33 determina a realização de estudos e recomendações sobre responsabilidade e transparência, além de diretrizes voltadas para a elaboração de Código de Conduta para provedores. Outra disposição é aquela que determina o aprofundamento de pesquisas sobre o combate da desinformação na internet e nas redes sociais. O que parece, contudo, é que a ausência de determinação expressa voltada para o aumento de controle pelo anunciante prejudica solução que caminhe neste sentido.

De maneira mais concreta, Hartmann¹⁸⁷ destaca que as bibliotecas de anúncios têm sido os principais e mais efetivos instrumentos de transparência sobre o ecossistema de publicidade personalizada:

Trata-se de repositórios curados por plataformas digitais listando todo o conteúdo promovido e impulsionado, incluindo os metadados relevantes, como o dinheiro pago para aumentar o alcance de um post e a informação básica sobre as pessoas que realmente o visualizaram. Facebook e Instagram lançaram uma biblioteca de anúncios em 2018, seguidos pelo Twitter e então o Google, embora o último apenas incluía na biblioteca anúncios sobre candidatos à eleição.

[...]

As bibliotecas fornecem conhecimento valioso sobre o conteúdo, autores e audiência de *fake news* artificialmente disseminada.

O autor destaca que muitas plataformas que atuam como intermediárias passaram a elaborar bibliotecas de anúncios de maneira voluntária para conferir maior transparência. Além disso, não faltaram iniciativas legislativas que impuseram a ampliação da transparência, sobretudo no contexto das eleições.

Em sentido semelhante, o PL 2630/2020 impõe a criação de algumas bibliotecas de anúncios. Os arts. 17 a 19 determinam que os provedores disponibilizem, por fácil acesso, a visualização de conteúdos e propaganda eleitoral impulsionada, além da disponibilização de histórico de todas as publicações publicitárias ou impulsionadas às quais o usuário teve acesso nos últimos seis meses. Além disso, “provedores que fornecerem impulsionamento de propaganda eleitoral ou de conteúdos que mencionem candidato, coligação ou

¹⁸⁷ HARTMANN, 2020, p. 467.

partido devem disponibilizar ao público todo o conjunto de anúncios impulsionados”, sem prejuízo da inclusão de informações mais específicas listadas no inciso do art. 19.

As bibliotecas de anúncios são capazes de conferir transparência e acesso para diversos atores, dentre os quais se incluem os usuários, pesquisadores e, para nossos fins, o anunciante. Se houvesse maior capacidade de gerenciamento e controle feito pelo anunciante sobre onde os anúncios deveriam ser exibidos, certamente menos dinheiro seria encaminhado para sites de conteúdo nocivo ou de baixa qualidade¹⁸⁸, sobretudo porque os anunciantes atualmente investem valores que se destinam a financiar a desinformação sem que haja intenção de realizar tais investimentos.

Contudo, as bibliotecas voluntárias carecem de arquitetura e de características fundamentais para sua efetividade. Imediatamente, podem ser listados 5 problemas: (i) limitação de escopo, abrangendo apenas anúncios feitos por políticos, partidos e seus representantes; (ii) algumas cobrem apenas o período eleitoral, enquanto a desinformação ocorre em qualquer época do ano; (iii) as condições de acesso e usabilidade são criticáveis, já que apresentam bugs, que a despeito de poderem ser corrigidos em breve, mas que não trazem uma estrutura de dados abertos, requerendo confirmação de identidade, por exemplo; (iv) algumas plataformas limitam as bibliotecas a um espaço geográfico limitado, não sendo universal, normalmente abrangendo apenas países desenvolvidos e; (v) inconsistência de dados catalogados, não exibindo dados essenciais para verificar critérios de direcionamento¹⁸⁹.

Além do aprimoramento destas falhas e a implementação de biblioteca de anúncios que se preocupe em combater a desinformação, uma das medidas fundamentais para este combate seria cruzar essas bases de dados estruturadas, ou seja, a biblioteca que aponta para todos os conteúdos publicitários ou impulsionados, com conteúdo verificado por agências de checagem, cuja importância será vista ao final deste tópico, já que devem figurar como importante filtro para identificar conteúdo absolutamente desinformativo e conteúdo absolutamente verdadeiro, bem como as diversas nuances e rótulos que podem ser criados entre os dois extremos.

¹⁸⁸ HARTMANN, 2020, p. 462.

¹⁸⁹ HARTMANN, 2020, pp. 469-472.

Ressalte-se que não se trata de impor obrigação a tais agências para que chequem todo e qualquer conteúdo, obrigação que seria onerosa e que foi proposta por parlamentares brasileiros no escopo do PL 2630/2020, mas negado a pedido das próprias agências, que afirmaram não possuir estrutura para assumir o ônus e que a imposição de obrigações dessa natureza poderia dificultar ou inviabilizar seus trabalhos.

Nessa linha, mas sob outra ótica, Bozarth e Budak¹⁹⁰ afirmam que os anunciantes possuem a capacidade de definir filtros amplos, como o impedimento de exibição de anúncios em sites que contenham conteúdo pornográfico ou de violência explícita. Contudo, não é admitida a limitação a determinados domínios, tampouco apenas a notícias verídicas, o que se liga diretamente à dificuldade de estabelecer o que seria desinformação ou não.

Assim, os autores defendem a criação de uma *blacklist* ou lista negra, que contenha um rol de canais de comunicação que se dediquem a divulgar, reiteradamente, notícias falsas ou de baixa qualidade, com possibilidade de restrição de alocação de anúncios em tais páginas. Como fundamentos, apresentam que (i) a maior parte da receita obtida por páginas suspeitas advém de anúncios confiáveis e sérios; (ii) os anúncios são alocados por grandes empresas de tecnologia que atuam com publicidade personalizada (são os intermediários, bastante conhecidos); (iii) a criação de uma *blacklist* e vedação de anúncios nessas páginas trariam prejuízos mínimos a essas empresas, em comparação com valores globais recebidos, além de gerar benefícios que abarcam a liberdade de expressão, o direito de informação, a democracia, direitos da personalidade e, conforme demonstrado na pandemia da COVID-19, até mesmo a proteção à saúde e à integridade¹⁹¹.

A regulação que impusesse a criação de uma *blacklist* e disponibilização do filtro para o anunciante seria direcionada ao intermediário, que abarca grande parte do ambiente virtual. Tal regulação, para ser mais viável ou eficaz, poderia perfeitamente mirar apenas as maiores empresas de publicidade personalizada, que ocupam a maior parte do mercado. Conforme demonstrado, diversos direitos fundamentais seriam tutelados sem ameaçar a inovação, o desenvolvimento

¹⁹⁰ BOZARTH, Lia; BUDAK, Ceren. Market Forces: Quantifying the Role of Top Credible Ad Servers in the Fake News Ecosystem. **Association for the Advancement of Artificial Intelligence (2021)**, pp. 83-94.

¹⁹¹ O estudo demonstra que as 10 maiores empresas de publicidade, que obtêm lucros bilionários, teriam gerado algo entre US\$ 985,7 mil e US\$ 1,15 milhão. A interrupção de exibição deste tipo de anúncio geraria, portanto, prejuízo ínfimo, considerando a remota possibilidade deste valor não ser redistribuído para outras páginas de maior confiabilidade.

econômico e a livre iniciativa, fundamentos que abstratamente se opõem à regulação interventiva.

Alternativa seria a criação de uma *whitelist*, que prioriza ou possibilita a exibição de anúncios somente em sites confiáveis e já testados por intermediários que viabilizam a exibição dos anúncios¹⁹². Por essência, é o oposto da *blacklist*: nesta, constariam os sites em que não devem ser exibidos anúncios e, naquelas, estariam os sites que são confiáveis para oferecimento de anúncios com reduzido risco para o anunciante que não deseja figurar ao lado de desinformação, o que impõe um gasto superior, mas possibilita a redução do problema.

As duas soluções já existem, mas a utilização eficaz não é de fácil implementação. Alguns problemas comuns são: (i) o alto volume de sites e páginas que surgem diariamente; (ii) a definição daquilo que deve figurar como conteúdo de qualidade ou não ou, mais ainda, como desinformação ou informação. O primeiro está diretamente ligado à dificuldade de controlar os integrantes da lista, já que surgem centenas ou milhares de domínios por dia, a depender do porte da empresa de publicidade personalizada¹⁹³:

O problema com o *blacklisting*, é claro, é que apenas websites já conhecidos como problemáticos podem ser banidos. Enquanto isso, o grande volume de novos sites criados todos os dias dificulta muitos esforços feitos pelas empresas para proteger os anunciantes. Mesmo uma empresa menor, com menos de 70 colaboradores, relatou receber em média mais de 400 inscrições de criadores de conteúdo por dia. Líderes do setor, como a rede AdSense do Google, colocam na lista negra milhões de novos sites anualmente, bem como centenas de milhares de sites existentes.

A mesma situação afeta a *whitelist*, pois a lista de sites confiáveis é inevitavelmente incompleta, já que o surgimento de sites todos os dias dificulta a gestão. Além disso, a criação de uma lista premium torna os anúncios mais caros para os anunciantes e limita a monetização de veículos de qualidade que sejam relativamente novos¹⁹⁴.

O segundo problema ameaça a liberdade de expressão de maneira mais direta, já que exige inevitável controle sobre o conteúdo postado: quais são os critérios para estabelecimento de conteúdo confiável e quem deve ser responsável pela classificação?

¹⁹² BRAUN, EKLUND.

¹⁹³ Ibid.

¹⁹⁴ Ibid.

Conforme visto, o papel de agente moderador não pode ser concentrado no poder público ou nas grandes empresas de tecnologia, pelos diversos motivos expostos. A função desses atores é prover estrutura que garanta que o conteúdo seja avaliado de forma democrática e com possibilidade de defesa pelo autor do conteúdo, que não pode ser afastado do processo de tomada de decisão.

Neste caso, é importante fortalecer a já mencionada atuação do usuário, além do fomento à atuação de agências de checagem de fatos e de iniciativas como os *Sleeping Giants*. Antes, porém, deve ser feita ressalva de que o fomento se liga ao incentivo de atuação e não à sua imposição, em razão da falta de estrutura para atuar em todo ambiente virtual e diante do desserviço que seria a imposição de obrigações e responsabilidades a tais atores.

As agências de checagem não são uma novidade no mundo, mas vêm crescendo em escopo e número de atores que se dedicam à atividade em razão do largo aumento de desinformação e capacidade de disseminação deste conteúdo nocivo¹⁹⁵.

Além disso, tais agências têm sido vistas de maneira positiva pelo público, sobretudo em razão do investimento que é feito em transparência e credibilidade. Para a liberdade de expressão, outros pontos têm sido relevantes¹⁹⁶:

Todas explicam como chegaram à conclusão sobre a veracidade das informações publicadas, destacando as fontes originais de informação com links e referências. Outro ponto importante para assegurar a qualidade é a busca pela diversidade de personalidades checadas e uma política clara de erros. As agências não checam opiniões e previsões, além de tópicos de pouca relevância para o debate público, como vícios de linguagem, questões de foto íntimo e afins.

No Brasil, por exemplo a Agência Lupa explica sua metodologia¹⁹⁷, com destaque à priorização de conteúdo e afirmações “feitas por personalidades de destaque nacional, a assuntos de interesse público (que afetem o maior número de pessoas possível) e/ou que tenham ganhado destaque na imprensa ou na internet recentemente”. A agência Aos Fatos¹⁹⁸ também seleciona as notícias a

¹⁹⁵ DINIZ, Amanda Tavares de Melo. Fact-checking no ecossistema jornalístico digital: prática, possibilidades e legitimação. **Mediapolis**. n.5 (2017), pp. 23-37.

¹⁹⁶ SPINELLI, Egle Muller; SANTOS, Jéssica de Almeida. Jornalismo na era da pós-verdade: fact-checking como ferramenta de combate às fake news. **Revista Observatório**, v. 4, n. 3, mai/2018. ISSN nº 2447-4266, DOI: <https://doi.org/10.20873/uft.2447-4266.2018v4n3p759>.

¹⁹⁷ Agência Lupa. **Como a Lupa faz suas checagens?** Rio de Janeiro, out. 2015. Disponível em: <https://piaui.folha.uol.com.br/lupa/2015/10/15/como-fazemos-nossas-chechagens/>. Acesso em 12/04/2022.

¹⁹⁸ Aos Fatos. **Nosso Método**. Disponível em: <https://www.aosfatos.org/nosso-m%C3%A9todo/>. Acesso em 12/04/2022.

partir de sua relevância, com dupla checagem e consulta às fontes de origem. Assim, apesar de não haver estrutura ou possibilidade de cobertura integral do que é produzido no ambiente virtual, tais agências de checagem buscam a maior abrangência possível.

Outra questão é que não há remoção de conteúdo imediata, mas disponibilização de rótulos que variam, mas que dificilmente operam no modo binário. A “Fato ou Fake” classifica as notícias como “Fato”, “Fake” ou “Não é bem assim”. A Agência Lupa traz nove rótulos para postagens¹⁹⁹: “Falso”, “Verdadeiro”, “Ainda é Cedo”, “Exagerado”, “Insustentável”, “De Olho”, “Verdadeiro, mas”, “Contraditório” e “Subestimado”. A Aos Fatos traz sete rótulos: “Verdadeiro”, “Impreciso”, “Exagerado”, “Contraditório”, “Insustentável”, “Distorcido” ou “Falso”²⁰⁰.

O conteúdo também não se restringe a política, abrangendo economia, cultura, notícias internacionais e questões como saúde, Black Friday, esportes e outros temas.

Outro aspecto relevante é a institucionalização que vem ocorrendo com as agências de checagem. Segundo Graves e Cherubini²⁰¹, os verificadores tendem a seguir o mesmo modelo de trabalho: escolha de conteúdo relevante, busca por dados confiáveis, profissionais independentes, atribuição de transparência, por meio da exposição de metodologia e declarações de princípios, sem prejuízo de diferenças que não afetam esse quadro geral.

Um dos problemas enfrentados pelas agências de checagem é o alcance do público, ou seja, “a dificuldade de *fact-checkers* em atrair uma audiência mais representativa que acesse esses conteúdos voluntariamente”²⁰². Daí a importância de combinar os dados levantados com bibliotecas de anúncios²⁰³, bem como utilizá-los para a criação de *blacklists*, *whitelists* e *scores* que possam afetar a monetização de maneira ampla.

Já os *Sleeping Giants*, apontados nos tópicos iniciais, trabalham de maneira mais ativa e abordando diretamente anunciantes que eventualmente financiem desinformação ou discurso de ódio. Apesar de operar de forma mais manual e

¹⁹⁹ Agência Lupa. **Entenda as etiquetas da Lupa**. Rio de Janeiro, out. 2015. Disponível em: <https://piaui.folha.uol.com.br/lupa/2015/10/15/entenda-nossos-pinguins/>. Acesso em 12/04/2022.

²⁰⁰ Aos fatos.

²⁰¹ GRAVES, Lucas; CHERUBINI, Federica. The Rise of Fact-Checking sites in Europe. **Digital News Project** (2016).

²⁰² SPINELLI; SANTOS.

²⁰³ HARTMANN, 2020.

menos estrutural, a iniciativa tende a obter resultados mais mensuráveis e imediatos. Conforme demonstrado, os *Sleeping Giants* utilizam imagens de anúncios que figuram ao lado daquele tipo de conteúdo e abordam diretamente a marca ou empresa que patrocina o conteúdo, se valendo do engajamento de seus públicos em redes sociais: além de postar em páginas próprias, o grupo costuma postar nas páginas das empresas que pagam o anúncio. A atuação confere maior transparência aos anunciantes, sem remoção do conteúdo ou proposta similar. O que se clama é pela desmonetização destes canais, sobretudo porque as empresas e marcas frequentemente não patrocinam o conteúdo de forma voluntária.

De toda sorte, devem ser garantidos mecanismos de devido processo legal, conforme visto no tópico anterior. Deve ser garantida a possibilidade do contraditório, da ampla defesa, da concessão de prazos razoáveis para que o autor e/ou o proprietário da página se justifiquem e requeiram pedido de revisão.

4.3.

***Accountability* e dados pessoais**

A regulação do ambiente virtual que foca na estrutura e no tratamento de dados pessoais para combate à desinformação gera menos riscos à liberdade de expressão que a regulação focada no conteúdo, com definição de verdade e mentira, que frequentemente se baseia em parâmetros subjetivos e assume o contorno definido pelo sujeito que cria o conceito.

Nos subcapítulos anteriores, foram listadas maneiras de regular com base na estrutura ou na arquitetura apresentada por intermediários que atuam entre o criador do conteúdo e o leitor e entre o anunciante e o destinatário do anúncio. Neste tópico, serão avaliadas medidas que também se direcionam ao mesmo intermediário, que são as empresas de tecnologia que operam as maiores plataformas de busca, redes sociais e mensageria instantânea.

Contudo, o foco passa a ser a proteção de dados pessoais e instrumentos que já estão disponíveis na legislação nacional e indicados em normas estrangeiras, além de serem recomendadas por órgãos consultivos ou autoridades de proteção de dados pessoais.

O tema da privacidade e proteção de dados pessoais tem ganhado repercussão em diversos países. No Brasil, a LGPD teve forte inspiração no GDPR e outras normas ligadas ao tema que já vigoravam no continente europeu e regia as relações existentes, o que justifica as diversas referências feitas ao ordenamento europeu neste tópico. Não se trata de desenvolvimento de direito comparado, mas de análises pontuais a diretrizes que podem contribuir com o presente estudo.

Conforme visto, um dos princípios estabelecidos pela LGPD é a *accountability*, traduzida como responsabilidade e prestação de contas, que impõe a adoção de medidas eficazes e capazes de fortalecer a proteção de dados pessoais e comprovar a eficácia de tais medidas, com aumento de benefícios para o titular, buscado pelo agente de tratamento²⁰⁴.

Um dos instrumentos de *accountability* que vêm sendo frequentemente adotado por empresas de tecnologia em operações de tratamento de dados pessoais tem sido o Relatório de Impacto à Proteção de Dados (RIPD) ou *Data Protection Impact Assessment (DPIA)*, que tem como objetivo documentar os processos de tratamento de dados que possam maior capacidade de “gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco”²⁰⁵. Hayduk²⁰⁶ reconhece a importância do RIPD como uma ferramenta para equilíbrio entre direitos fundamentais e a inovação, “para o uso ético, transparente e racional dos dados pessoais. Leva em consideração a massificação de técnicas de monitoramento”. O autor menciona pelo menos três motivos para que o controlador se dedique a elaborar documentos de qualidade que gerem consequências úteis e efetivas, são eles: o imperativo ético, a possibilidade de impacto reputacional sobre as marcas e o *enforcement* das leis de proteção de dados e atuação das respectivas autoridades responsáveis pela fiscalização e sanção. Bioni²⁰⁷ ressalta que a previsão de elaboração do RIPD extrai sentido e fundamento justamente da necessidade de adoção de ações que mitiguem riscos para o titular dos dados pessoais. Viola e Teffé destacam que a mitigação dos riscos interessa ao controlador, sobretudo

²⁰⁴ Art. 6º, X da LGPD.

²⁰⁵ Art. 5º, XVII da LGPD

²⁰⁶ HAYDUK, Gabriel. Requisitos do relatório de impacto à proteção de dados pessoais. In: FRAZÃO, Ana; CUEVA, Ricardo Villas Bôas. **Compliance e políticas de proteção de dados**. São Paulo: Thomson Reuters Brasil, 2021, pp. 569-586.

²⁰⁷BIONI, p. 326.

porque se dirige a ambas as partes da relação: ao titular e ao próprio agente de tratamento.

Apesar da obrigação contida na LGPD, a legislação é silente acerca do que significa risco a liberdades e direitos fundamentais. Em outras passagens, é informado que a ANPD poderá solicitar o RIPD (i) em caso de tratamento de dados pessoais feito com base no legítimo interesse do controlador ou de terceiro²⁰⁸; (ii) quando o tratamento for realizado pelo poder público²⁰⁹ e; (iii) nas operações que envolvam dados sensíveis²¹⁰. Além disso, a ANPD deverá “editar regulamentos e procedimentos [...] sobre relatórios de impacto à proteção de dados pessoais para casos em que o tratamento representar alto risco à garantia dos princípios gerais de proteção de dados pessoais”²¹¹.

Tais disposições, conquanto forneçam um norte, não especificam o que seriam esses riscos e ameaças. De outro lado, são disposições que passaram a vigorar em setembro de 2020, de maneira imediata, juntamente com os demais dispositivos, ressalvadas exceções previstas no art. 65, I e II da LGPD, que não afetam a presente análise. Ademais, o documento tem sido utilizado com frequência por empresas de tecnologia, conforme sinalizado.

Por todo exposto, é necessário recorrer a outros parâmetros que não estejam fixados na Lei para saber como o RIPD funciona, quando deve ser elaborado e qual é o seu conteúdo. Ante à ausência de regulação específica, observar diretrizes estrangeiras que têm matrizes semelhantes àquelas que inspiraram parte da legislação brasileira vigente no tocante à privacidade e proteção de dados pessoais parece ser um caminho adequado.

A ICO exige a elaboração de um RIPD/DPIA em diversos casos²¹²: (i) utilização de tecnologia inovadora; (ii) utilização de perfis e categorias para tomada de decisões acerca de acesso a serviços; (iii) perfilamento em larga escala; (iv) processamento de dados genéticos ou biométricos; (v) combinação de dados ou conjuntos de dados que originam de fontes distintas; (vi) coleta de dados pessoais sem fornecimento de um aviso de privacidade ao titular; (vii) geolocalização; (viii) tratamento de dados comportamentais; (ix) perfilamento de

²⁰⁸ Art. 10, §3º da LGPD.

²⁰⁹ Art. 32 da LGPD.

²¹⁰ Art. 38 da LGPD.

²¹¹ Art. 55-J, XIII da LGPD.

²¹² ICO. Data protection impact assessments. Disponível aqui. Acesso em 12/04/2022.

crianças ou publicidade direcionada a elas; (x) processamento de dados que coloquem em risco a saúde ou segurança do indivíduo.

É possível observar que a publicidade personalizada atende a várias hipóteses listadas. Na prática, grandes empresas de tecnologia têm se valido do RIPD para verificar os métodos adotados para tratamento de dados de crianças ou para criação de critérios de combate ao discurso de ódio ou mesmo ligado a questões sensíveis de saúde, como distúrbios alimentares, razão pela qual se confia na elaboração do RIPD também para combater a desinformação, alimentada por publicidade personalizada.

No presente caso, os itens (i), (ii), (iii), (v), (vi), (vii), (viii) e (ix) parecem imediatamente preenchidos pela operação de tratamento de dados pessoais para fins de publicidade personalizada. Especificamente no tema da desinformação, também o item (x) poderia ser potencialmente preenchido, já que têm sido frequentes as notícias de monetização de notícias que prejudicam a saúde e a incolumidade, principalmente no contexto da pandemia da COVID-19.

O *Article 29 Data Protection Working Party* elaborou um documento chamado *Guidelines on DPIA*, com hipóteses similares àquelas apontadas pela ICO²¹³. Dentre os exemplos de operações que exigiam a elaboração de DPIA estava a coleta de dados pessoais por mídias sociais para geração de perfis. A publicidade personalizada consiste justamente em coletar de titulares para criação de perfis e encaminhamento de anúncio ao usuário adequado, quando está mais propenso a comprar ou contratar.

Um dos riscos relevantes da operação é o que tem sido exposto e analisado nesta dissertação, que é o incentivo financeiro que é dado à produção e disseminação de desinformação por meio da alocação de receitas oriundas de publicidade personalizada. Tal risco deve ser levado em consideração e medidas efetivas devem ser adotadas para evitar os danos reputacionais, mas também as sanções administrativas e judiciais que podem advir de documentos meramente formais e apartados da realidade ou da falta de iniciativas para combate ou mitigação razoável de riscos e danos que possam ser gerados pela desinformação.

²¹³ Article 29 Data Protection Working Party. **Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679.** Oct. 2017.

Outro ponto importante gira em torno do conteúdo do RIPD, que também não foi delineado pela Lei ou por regulação específica. O art. 35 (7) do GDPR determina que um RIPD deve conter pelo menos: (i) descrição das operações de tratamento e respectivas finalidades perseguidas, incluindo o interesse legítimo perseguido; (ii) análise da necessidade e proporcionalidade das operações de tratamento; (iii) avaliação dos riscos para os direitos e liberdades dos titulares de dados; (iv) medidas para combater os riscos diagnosticados, o que inclui instrumentos de salvaguardas e mecanismos de segurança que levem em conta os direitos e interesses dos titulares e demais pessoas que podem ser impactadas²¹⁴. Neste caso, também seria interessante a criação de mecanismos que atendam ao art. 35 (9), que trata da possibilidade de o controlador obter a participação e pontos de vistas de titulares, de seus representantes e pessoas interessadas²¹⁵. Aqui, podem ser mencionados os titulares diretamente atingidos pela desinformação, o poder público, os anunciantes e entes que integram a sociedade civil.

A recém-criada ANPD não expediu *template* sobre o tema, mas é possível analisar aqueles criados pela ICO²¹⁶ e pela *Agencia Española de Protección de Datos (AEPD)*²¹⁷. Em comum, estão a exibição dos requisitos a seguir: (i) nome do controlador; (ii) identificação do DPO/Encarregado; (iii) contatos do controlador e do DPO/Encarregado; (iv) identificação da necessidade de elaboração do RIPD; (v) descrição da operação, com indicação de como é coletado, quais são as fontes, se há compartilhamento de dados, qual é a natureza do dado, se existe alguma categoria especial de dados, como o titular é afetado e informações similares; (vi) descrição do contexto da operação e os propósitos do tratamento; (vii) descrição da necessidade do tratamento de dados pessoais, focado na minimização que possibilite tratar o menor volume de dados para obtenção de resultado similar; (viii) análise da proporcionalidade do tratamento, demonstrando as vantagens do tratamento, a relação tratamento x ausência de tratamento, direitos e liberdades fundamentais que podem ser violados, o fundamento legal ou constitucional para tratamento, a legítima expectativa do titular, a demonstração de relação pré-existente; (ix) indicação de riscos para realização da operação; (x) instrumentos de salvaguarda e mitigação de riscos e danos.

²¹⁴ Art. 35 (7) do GDPR.

²¹⁵ Art. 35 (9) do GDPR.

²¹⁶ ICO. **Sample DPIA Template**. Disponível aqui. Acesso em 12/04/2022.

²¹⁷ AEPD. **Template For Data Protection Impact Assessment Report (DPIA) For Private Sector**. Disponível aqui. Acesso em 12/04/2022.

Para Carvalho, Mattiuzzo e Ponce, o documento pode ser exigido a qualquer tempo pela ANPD e será, em grande medida²¹⁸:

um produto do mapeamento e mensuração de riscos realizados na implementação do programa de governança – uma vez que deverá conter descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações, bem como medidas, salvaguardas e mecanismos de mitigação de risco adotados pela organização (art. 38, parágrafo único).

No caso da desinformação, o potencial ofensivo se dirige não apenas ao titular, mas a terceiros, ao poder público e à sociedade. Além disso, o controlador (no caso, as empresas de tecnologia que atuam como intermediário e desenvolvem a publicidade personalizada) não pode ser diretamente responsabilizado pela desinformação – pelo menos em regra – mas deve demonstrar a dedicação e esforços efetivos para desmonetizar a atividade e coibir a criação e disseminação, pelo menos por meio de ajuste da arquitetura e dos métodos de tratamento de dados pessoais. Não há presunção de estabelecer uma solução definitiva e integralmente eficaz, mas a comprovação de que todas as medidas razoáveis e possíveis têm sido adotadas e que a atuação dessas empresas tem caminhado para o combate à desinformação por meio da desmonetização, já que o combate de viés ideológico pode ser um pouco mais complicado.

Neste trabalho, não será possível desenvolver os critérios específicos que devem ser considerados como salvaguardas e medidas eficientes de combate à desinformação, o que não retira a importante contribuição que é a aplicação de instrumento já criado por lei e que tem expectativa de regulação por autoridade de proteção de dados a matéria tão necessária como é o caso da desinformação e de sua desmonetização por meio de instrumentos expostos neste trabalho e em tantos outros.

Se trata de uma forma de engajar voluntariamente as empresas que atuam como intermediárias, sob a possibilidade de supervisão pelo poder público (via Poder Judiciário ou autoridade administrativa) e pelo escrutínio público (via reputação, boicotes e reações negativas).

²¹⁸CARVALHO, Vinícius Marques; MATTIUZZO, Marcela; PONCE, Paula Pedigoni. Boas práticas e governança na LGPD. In: MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JR., Otavio Luiz (Coords.). **Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: Forense, 2021, pp. 571-572

Ademais, se trata de medida que aponta para o tratamento de dados pessoais e para a arquitetura da plataforma, não focando no controle de conteúdo ou no estabelecimento de um conceito rígido do que seria a verdade ou a mentira, o que afasta riscos razoáveis à liberdade de expressão.

5

Conclusão

O presente estudo pretendeu contribuir para a compreensão de como a desinformação pode ser monetizada por criadores de conteúdo que buscam exclusiva ou prevalentemente o lucro oriundo de receitas de publicidade personalizada. Além disso, foram expostos aspectos regulatórios úteis para a mitigação do problema, mas com foco na preservação da liberdade de expressão, que não pode ser atingida sob argumento de combate a determinados discursos. De fato, a desinformação e outras formas de conteúdo nocivo devem ser coibidos, mas a prática tem revelado a dificuldade de estabelecer conceitos de verdade ou mentira, razão pela qual se defendeu a prioridade da regulação por meio da proteção de dados pessoais e de aspectos voltados para arquitetura da plataforma.

Buscando atingir tais objetivos, foi estabelecido o conceito de desinformação, que não se confunde com *Fake News* em razão de uma subtração reprovável deste termo por autoridades públicas responsáveis por acusar falsamente importantes veículos de mídia e opositores políticos, o que levou a recomendações de diversas origens pela não utilização da expressão. O termo também não deve ser confundido com *misinformation*, já que esta independe da intenção e a desinformação é necessariamente intencional. De outro lado, a desinformação também não é *propaganda*. Conquanto possa servir como instrumental desta, não é um elemento constitutivo necessário e a *propaganda* pode, ainda, se valer de conteúdo verídico.

Determinados veículos, com busca exclusiva ou primordial de lucro, passaram a produzir desinformação, aumentando o engajamento e atraindo receitas oriundas de anúncios alocados em suas páginas com foco no perfil de seu usuário que não atentam propriamente para o conteúdo ao lado do qual figuram. A estrutura e o tratamento de dados pessoais em larga escala contribuíram – e contribuem – para o funcionamento de tais engrenagens.

Contudo, foi demonstrada a importância da publicidade personalizada para atingir benefícios que não eram viáveis nos veículos tradicionais, tais como: (i) o anúncio mais barato, assertivo e mensurável por pequenos, médios e grandes

negócios; (ii) a captação de recursos por veículos de comunicação de variados portes que precisam da receita para se manter e produzir conteúdo de qualidade.

Por serem proporcionadas vantagens para todas as partes – plataformas, anunciantes, leitores e produtores de conteúdo – a prática não deve ser abolida, mas aprimorada, razão pela qual se justifica uma regulação que não mire na extinção ou exacerbação desproporcional dos custos da operação, mas na adoção de cautelas para ampliar a proteção de dados pessoais e a arquitetura das plataformas.

Conforme visto, tal regulação não deve estabelecer um conceito de verdade ou mentira, tampouco relegar tal função a um órgão específico, seja público ou privado. Tal ideia reduz os riscos que circundam a liberdade de expressão.

Além disso, foi demonstrada a participação de múltiplos atores sociais no ambiente virtual, seja como anunciante, criador de conteúdo ou leitor. Ainda, as plataformas de tecnologia foram apontadas como detentoras da expertise tecnológica e o poder público como um dos principais interessados na garantia de direitos e liberdades fundamentais, como a liberdade de expressão, a privacidade e a proteção de dados pessoais. Assim, não é recomendada a entrega do papel regulatório para apenas uma das categorias envolvidas, mas para múltiplos agentes, englobando todos os principais interessados na regulamentação do tema. Para facilitar a compreensão e demonstrar a viabilidade, foram apontados órgãos que servem como exemplos, sobretudo os mencionados CGI e CNPD, sendo certo que àquele primeiro o PL 2630/2020 tem atribuído a função regulatória para responsabilidade, liberdade e transparência no uso da internet.

Outro ponto fundamental foi a demonstração da importância de alguns conceitos que tendam para o extremo da precisão, mas, principalmente, outros conceitos que pendam para o extremo da vagueza, permitindo maior elasticidade e longevidade das disposições estabelecidas, notadamente pela exposição de princípios que têm sido frequentemente utilizados para regular novas tecnologias, são eles: a *accountability* e a transparência.

Por fim, foram apresentados instrumentos que se dividem em três categorias: (i) transparência e empoderamento do usuário; (ii) transparência e controle para o anunciante; (iii) *accountability* e dados pessoais. Tais categorias foram capazes de abranger o devido processo legal, a criação de sinalização de conteúdo patrocinado ou impulsionado, a distribuição para diferentes comunidades e bolhas, a criação de bibliotecas de anúncios aprimoradas a partir

do cruzamento da base com agências de checagem dos fatos, *blacklists*, *whitelists* e a utilização do já criado e utilizado RIPD ou DPIA, que vem sendo previsto e aprimorado por legislações recentes sobre privacidade e proteção de dados pessoais, inclusive no Brasil a partir da LGPD.

Não se pretendeu encerrar o debate ou solucionar o problema de maneira definitiva. Conquanto fosse desejada a possibilidade de extinguir a monetização da desinformação e, ainda mais, a própria mentira em si, são dois elementos que possivelmente não encontrarão soluções integrais e definitivas. Assim, se espera que a contribuição tenha colaborado com compreensão do problema e com propostas de melhoria da estrutura das plataformas, de ampliação da proteção de dados pessoais e de melhoria do fluxo de receitas da importante operação de publicidade personalizada.

REFERÊNCIAS

AEPD. **Template For Data Protection Impact Assessment Report (DPIA) For Private Sector**. Disponível aqui. Acesso em 12/04/2022.

AFONSO, Nathália. 64,5% das vezes em que Bolsonaro fala em ‘fake news’ são ataques à imprensa. **Agência Lupa, UOL**, 23 dez. 2019. Disponível em: <https://piaui.folha.uol.com.br/lupa/2019/12/23/bolsonaro-fake-news-imprensa/>. Acesso em 25 set. 2021.

Agência Lupa. **Como a Lupa faz suas checagens?** Rio de Janeiro, out. 2015. Disponível em: <https://piaui.folha.uol.com.br/lupa/2015/10/15/como-fazemos-nossas-checagens/>. Acesso em 12/04/2022.

Agência Lupa. **Entenda as etiquetas da Lupa**. Rio de Janeiro, out. 2015. Disponível em: <https://piaui.folha.uol.com.br/lupa/2015/10/15/entenda-nossos-pinguins/>. Acesso em 12/04/2022.

ALLCOTT, Hunt; MATTHEW Gentzkow. 2017. Social Media and Fake News in the 2016 Election. **Journal of Economic Perspectives**, v. 31, n. 2, Spring 2017, pp. 211-36.

ANDERSON, Cris. **The Long Tail: Why the future of business is selling less of more**. Hyperion Books, 2008, pp. 24, 210-216.

Aos Fatos. **Nosso Método**. Disponível em: <https://www.aosfatos.org/nosso-m%C3%A9todo/>. Acesso em 12/04/2022.

Article 29 Data Protection Working Party. **Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679**. Oct. 2017.

BALDWIN, Robert; CAVE, Martin; LODGE, Martin. **Understanding regulation: theory, strategy, and practice**. 2nd ed. New York: Oxford University Press, 2012.

BALKIN, Jack. **Digital Speech and Democratic Culture: a Theory of Freedom of Expression for the Information Society**. New York University Law Review, Vol. 79, No. 1, 2004, Yale Law School, Public Law Working Paper No. 63.

BALKIN, Jack. **Free Speech in the Algorithmic Society: Big Data, Private Governance, and New School Speech Regulation**. University of California, 2018, v. 51, pp. 1149-1210.

BALKIN, Jack. **Old-School/New-School Speech Regulation**. Harvard Law Review, 2014, pp. 2296-2342.

BARBERÁ, Pablo. Social Media, Echo Chambers, and Political Polarization. In: PERSILY, Nathaniel; TUCKER, Joshua A. (Orgs.). **Social media and democracy: the state of the field, prospects for reform**. Cambridge New York Port Melbourne New Delhi Singapore: Cambridge University Press, 2020, p. 345.

BARRETO JUNIOR, Irineu Francisco. *Fake News e discurso de ódio: estratégia de guerra permanente em grupos de Whatsapp*. In: RAIS, Diogo (Coord.). **Fake News: a conexão entre a desinformação e o direito**. 2 ed., São Paulo: Thomson Reuters Brasil, 2020. Versão Kindle, pos. 2936.

BENKLER, Yochai; FARIS, Robert; ROBERTS, Hal. **Network Propaganda: manipulation, disinformation, and radicalization in american politics**. New York: Oxford University Press, 2018.

BENNET, Colin J.; ODURO-MARFO, Smith. **Privacy, Voter Surveillance and Democratic Engagement: Challenges for Data Protection Authorities**. [s.l.]: University of Victoria, 2019.

BENNETT, Colin J.; LYON, David. **Data-driven elections: implications and challenges for democratic societies**. *Internet Policy Review*, v. 8, n. 4, 2019. Disponível em: <https://policyreview.info/node/1433>. Acesso em: 10 out. 2021.

BENNETT, Colin; RAAB, Chales. **Revisiting the governance of privacy: contemporary policy instruments in global perspective**. *Regulation & Governance*, 2018, doi:10.1111/rego.12222.

BERTHON, P. R.; PITT, L. F. (2018). **Brands, Truthiness and Post-Fact**. *Journal of Macromarketing*, 38(2), 218–227. doi:10.1177/0276146718755869.

BEZERRA, Arthur Coelho. **Sleeping Giants: a ofensiva moral dos gigantes adormecidos contra o novo regime de desinformação**. *Revista Eptic*, v. 23, n. 1, jan-abr, 2021. ISSN 1518-2487.

BINENBOJM, Gustavo. **Poder de polícia, ordenação, regulação: transformações político-jurídicas, econômicas e institucionais do direito administrativo ordenador**. Belo Horizonte: Fórum, 2016.

BLACK, Julia. **Decentring Regulation: Understanding the Role of Regulation and Self-Regulation in a ‘Post-Regulatory’ World**. *Current Legal Problems*, v. 54, issue 1, 2001, pp. 103-146.

BOERMAN, Sophie; KRUIKEMEIER, Sanne; BORGESIUUS, Frederick. **Online Behavioral Advertising: A Literature Review and Research Agenda**. *Journal of Advertising*, 46 (3), 2017, ISSN: 0091-3367 print / 1557-7805 online DOI: 10.1080/00913367.2017.1339368, pp. 363-376.

BOZARTH, Lia; BUDAK, Ceren. **Market Forces: Quantifying the Role of Top Credible Ad Servers in the Fake News Ecosystem**. *Association for the Advancement of Artificial Intelligence (2021)*, pp. 83-94.

BRAGA, Renê Moraes da Costa. **A indústria das fake news e o discurso de ódio**. In: PEREIRA, Rodolfo Viana (Org.). *Direitos políticos, liberdade de expressão e discurso de ódio: volume I*. Belo Horizonte: Instituto para o Desenvolvimento Democrático, 2018, p. 207.

BRASIL. Câmara dos Deputados. **Combate a fake news é tema de 50 propostas na Câmara dos Deputados**. Disponível neste link. Acesso em 03.04.2022.

BRASIL. Câmara dos Deputados. Projeto de Lei 2.389, de 2020. **Dispõe sobre a tipificação do crime de criação e divulgação de notícias falsas – Fake News sobre a pandemia do Coronavírus – Covid – 19 acrescentando o art. 140-A ao do Decreto-Lei nº 2.848, de 7 de dezembro de 1940, Código Penal e dá outras providências**. Deputada Federal Rejane Dias. Disponível neste link. Acesso em 03.04.2022.

BRASIL. Câmara dos Deputados. Projeto de Lei 1.258, de 2020. **Tipifica a divulgação de notícias falsas durante o período de calamidade pública, estado de defesa, estado sítio ou intervenção, tratando ainda do indiciamento e da indenização em tais casos, alterando o Decreto-Lei nº 2.848, de 7 de dezembro de 1940, Código Penal.** Deputado Federal Luis Miranda. Disponível neste link. Acesso em 03.04.2022.

BRASIL. Câmara dos Deputados. Projeto de Lei 2.601, de 2019. **Altera a Lei nº 12.965, de 23 de abril de 2014, para criar obrigação de indisponibilização de notícias falsas por provedores de aplicações de internet e dá outras providências.** Deputado Federal Luis Miranda. Disponível neste link. Acesso em 03.04.2022.

BRASIL. Câmara dos Deputados. Projeto de Lei 2.630, de 2020. **Institui a Lei Brasileira de Liberdade, Responsabilidade e Transparência na Internet.** Relatório do Grupo de Trabalho Aperfeiçoamento da Legislação Brasileira - Internet. Deputado Federal Orlando Silva. Disponível neste link. Acesso em 15.02.2022.

BRASIL. Presidência da República. Autoridade Nacional de Proteção de Dados. Tribunal Superior Eleitoral. **Guia Orientativo de aplicação da Lei Geral de Proteção de Dados Pessoais por agentes de tratamento no contexto eleitoral.** Brasília, 2021

BRASIL. Presidência da República. Decreto nº 4.829, de 03 de setembro de 2003. **Dispõe sobre a criação do Comitê Gestor da Internet no Brasil - Cgilbr, sobre o modelo de governança da Internet no Brasil, e dá outras providências.** Disponível em: http://www.planalto.gov.br/ccivil_03/decreto/2003/d4829.htm. Publicação em DOU de 04.09.2003

BRASIL. Senado Federal. **Emenda ao Projeto de Lei nº 2.630 de 2020.** Inclui a disposição “Art. As empresas, nacionais e estrangeiras, que forneçam serviços de mídia programática não poderão veicular anúncios em páginas da internet que contenham desinformação. Brasília: Senado Federal, 2020. Disponível em <https://legis.senado.leg.br/sdleg-getter/documento?dm=8117340&disposition=inline>. Acesso em 04/01/2022.

BRASIL. Senado Federal. **Parecer da Relatora na PEC 17/2019,** que resultou na EC 115/2022. Brasília: Senado Federal, 2019. Disponível em: <https://legis.senado.leg.br/sdleg-getter/documento?dm=7954439&ts=1647518557730&disposition=inline> . Acesso em 02/04/2022.

BRASIL. Senado Federal. Parecer do Relator no Projeto de Lei 2.630 de 2020. Brasília: Senado Federal, 2020. Disponível em: <https://legis.senado.leg.br/sdleg-getter/documento?dm=8127630&ts=1630418520274&disposition=inline>. Acesso em 04/01/2021.

BRAUN, Joshua A.; COAKLEY, John D.; WEST, Emily. **Activism, advertising, and far-right media: the case of Sleeping Giants.** Media and Communication, v. 7, n. 4, 2019.

BRAUN, Joshua A.; EKLUND, Jessica L. **Fake news, real money: ad tech platforms, profit-driven hoaxes, and the business of journalism**. Digital Journalism, v. 7, n. 1, 2019.

BUSCH, Oliver. The programmatic advertising principle. In: BUSCH, Oliver (Ed.). **Programmatic advertising: the successful transformation to automated, data-driven marketing in real-time**. Springer: 2016. pp. 3-16.

CAMPOS MELLO, Patrícia. **A máquina do ódio: notas de uma repórter sobre Fake News e violência digital**. Rio de Janeiro: Companhia das Letras, 2020.

CARVALHO, Vinícius Marques; MATTIUZZO, Marcela; PONCE, Paula Pedigoni. Boas práticas e governança na LGPD. In: MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JR., Otavio Luiz (Coords.). **Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: Forense, 2021, pp. 571-572

CRUZ, Francisco Brito. **Novo jogo, velhas regras: democracia e direito na era da nova propaganda política e das fake news**. Belo Horizonte, MG: Grupo Editorial Letramento, Casa do Direito, 2020.

DA EMPOLI, Giuliano. **Os Engenheiros do Caos**. Minas Gerais: Autêntica, 2019.

DAVEY-ATTLE, Florence; SOARES, Isa. The Fake News Machine: inside a town gearing up for 2020. **CNN MONEY**, 2020. Disponível em: <https://money.cnn.com/interactive/media/the-macedonia-story/>. Acesso em 03/01/2022.

DINIZ, Amanda Tavares de Melo. Fact-checking no ecossistema jornalístico digital: prática, possibilidades e legitimação. **Mediapolis. n.5 (2017)**, pp. 23-37.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. São Paulo: Thomson Reuters Brasil, 2019.

FAQ GOOGLE ADS. **Como o Google Ads Funciona?** Disponível em https://ads.google.com/intl/pt-BR_br/home/faq/. Acesso em 28 dez. 2021.

FARIS, Robert M.; ROBERTS, Hal; ETLING, Bruce; et al. Partisanship, Propaganda, and Disinformation: Online Media and the 2016 U.S. Presidential Election. Cambridge, U.S.: Berkman Klein Center for Internet & Society at Harvard University, 2017. Disponível em: <http://nrs.harvard.edu/urn-3:HUL.InstRepos:33759251>.

FENWICK, Mark D.; KAAL, Wulf A.; VERMEULEN, Erik P. M. Regulation tomorrow: what happens when technology is faster than the law? *American University Business Law Review*, v. 6, n. 3, 2017.

FINCK, Michèle, **Digital Co-Regulation: Designing a Supranational Legal Framework for the Platform Economy** (June 20, 2017). *European Law Review* (2018 Forthcoming), LSE Legal Studies Working Paper No. 15/2017, Available at SSRN: <http://dx.doi.org/10.2139/ssrn.2990043>.

FRAZÃO, Ana. **Propósitos, desafios e parâmetros gerais dos programas de compliance**. In: FRAZÃO, Ana; CUEVA, Ricardo Villas Bôas. **Compliance e**

políticas de proteção de dados. São Paulo: Thomson Reuters Brasil, 2021, pp. 33-64.

FRIDKIN, Kim; KENNEY, Patrick J.; WINTERSIECK, Amanda. Liar, liar, pants on fire: how fact-checking influences citizens' reactions to negative advertising. *Political Communication*, v. 32, n. 1, 2015.

GAUR, Akriti. Towards Policy and Regulatory Approaches for Combating Misinformation in India. In: KARANICOLAS, Michael (Ed.). **Tackling the "Fake" Without Harming the "News"**. New Haven: Yale Law School, 2021, p.30-49.

GIANSIRACUSA, Noah. **How Algorithms Create and Prevent Fake News.** Massachusetts: Apress, 2021, p. 152.

GILLESPIE, Tarleton. The Relevance of Algorithms. In: GILLESPIE, Tarleton; BOCZKOWSKI, Pablo; FOOT, Kirsten (ed.). **Media Technologies: essays on communication, materiality, and society.** Massachusetts: MIT Press, 2014. pp. 168-170.

GOOGLE ADS. **Campanhas da Rede de Display.** Disponível em https://ads.google.com/intl/pt-BR_br/home/campaigns/display-ads/. Acesso em 28 dez. 2021.

GORWA, Robert. The platform governance triangle: conceptualising the informal regulation of online content. **Internet Policy Review**, v. 8, n. 2, 2019.

GRAHAM, Rachie. Google and advertising: digital capitalism in the context of Post-Fordism, the reification of language, and the rise of fake news. **Palgrave Commun** 3, 45 (2017). DOI: <https://doi.org/10.1057/s41599-017-0021-4>.

GRAVES, Lucas; CHERUBINI, Federica. The Rise of Fact-Checking sites in Europe. **Digital News Project** (2016).

GUESS, Andrew M. (Almost) Everything in Moderation: New Evidence on Americans' Online Media Diets. **American Journal of Political Science**, Feb. 2021.

GUESS, Andrew M.; LYONS, Benjamin A. Misinformation, Disinformation, and Online Propaganda. **Journal of Quantitative Description: Digital Media**, Apr. 2021.

GUESS, Andrew et al. Cracking Open the News Feed: Exploring What U.S. Facebook Users See and Share with Large-Scale Platform Data. In: PERSILY, Nathaniel; TUCKER, Joshua (Ed.). **Social Media and Democracy.** New York: Cambridge University Press, 2020 (*ebook*).

GUNNINGHAM, Neil; SINCLAIR, Darren. **Designing Smart Regulation (2004).**

GUNNINGHAM, Neil; SINCLAIR, Darren. Smart Regulation. In DRAHOS, Peter (ed.); **Regulatory Theory: Foundations and Applications.** ANU Press, 2017, pp. 133–148.

HARTMANN, Ivar. A new framework for online content moderation. **Computer Law & Security Review**, v. 36, 2020.

HARTMANN, Ivar Alberto. Combinando Bibliotecas de Anúncios com Checagem de Fatos para Aumentar a Transparência sobre a Desinformação. **Direito Público**, [S.l.], v. 18, n. 99, out. 2021. ISSN 2236-1766. Disponível em: <https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/5741>. Acesso em 16 dez. 2021.

HARTMANN, Ivar. Combining Ad Libraries with Fact Checking to Increase Transparency of Misinformation. In: KARANICOLAS, Michael (Ed.). **Tackling the “Fake” Without Harming the “News”**. New Haven: Yale Law School, 2021, p.67-84.

HARTMANN, Ivar Alberto; MONTEIRO, Julia Iunes. Fake News no Contexto de Pandemia e Emergência Social: os Deveres e Responsabilidades das Plataformas de Redes Sociais na Moderação de Conteúdo Online: entre a Teoria e as Proposições Legislativas. **Direito Público**, [S.l.], v. 17, n. 94, jul/ago. 2020, pp. 388-414.

HAYDUK, Gabriel. Requisitos do relatório de impacto à proteção de dados pessoais. In: FRAZÃO, Ana; CUEVA, Ricardo Villas Bôas. **Compliance e políticas de proteção de dados**. São Paulo: Thomson Reuters Brasil, 2021, pp. 569-586.

HOFFMANN, Stacie; TAYLOR, Emily; BRADSHAW, Samantha. The Market of Disinformation. **Oxford Technology & Elections Commission**. October, 2019, 42 pp. Disponível em: <https://oxtec.oii.ox.ac.uk/wp-content/uploads/sites/115/2019/10/OxTEC-The-Market-of-Disinformation.pdf>. Acesso em 25 set. 2021.

IAB Brasil. **Um guia para a Era Pós-Cookies de Terceiros**. Disponível em <https://iabbrasil.com.br/wp-content/uploads/2021/11/guia-para-era-sem-cookies-final-V2.pdf>. Acesso em 02/04/2022.

ICO. **Data protection impact assessments**. Disponível aqui. Acesso em 12/04/2022.

ICO. **Sample DPIA Template**. Disponível aqui. Acesso em 12/04/2022.

Instagram. **Sleeping Giants Brasil**. Disponível em https://www.instagram.com/slpng_giants_pt/?hl=pt-br. Acesso em 12/01/2022

IRETON, Cheryl; POSETTI, Julie. **Journalism, ‘Fake News’ & Disinformation: handbook for journalism education and training**. UNESCO, 2018, 128 pp. Disponível em: <https://unesdoc.unesco.org/ark:/48223/pf0000265552>. Acesso em 25 set. 2021.

KALIL, I. & SANTINI, R. M. **Coronavírus, Pandemia, Infodemia e Política**. Relatório de pesquisa. Divulgado em 01 de abril de 2020. 21p. São Paulo / Rio de Janeiro: FESPSP / UFRJ. Disponível: https://www.fespsp.org.br/store/file_source/FESPSP/Documentos/Coronavirus-e-infodemia.pdf

KARANICOLAS, Michael. Introduction – Understanding the Challenge. In: KARANICOLAS, Michael (Ed.). **Tackling the “Fake” Without Harming the “News”**. New Haven: Yale Law School, 2021, p.3-9.

KAYE, David. **Speech Police: the global struggle to govern the Internet**, Columbia Global Reports, 2019.

KELLER, Clara Iglesias. **Regulação nacional de serviços na internet: exceção, legitimidade e o papel do Estado**. Rio de Janeiro: Lumen Juris, 2019. 360 p.

KELLER, Clara Iglesias. Don't Shoot the Message: Regulating Disinformation Beyond Content. **Direito Público**, [S.l.], v. 18, n. 99, out. 2021, ISSN 2236-1766. Disponível em: <<https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/6057>>. Acesso em: 25 nov. 2021.

KELLER, Clara Iglesias. Policy by judicialisation: the institutional framework for intermediary liability in Brazil. **International Review of Law, Computers & Technology**, 35:3, 185-203, DOI: 10.1080/13600869.2020.1792035.

LAZER, David et al.. The science of fake news. **Science**, pp. 1094–1096. doi:10.1126/science.aao2998.

LEE, Yen Nee. Trump and GOP attack CNN, New York Times and Washington Post in 'fake news awards'. **CNBC**, 17 jan., 2018. Disponível em: <https://www.cnbc.com/2018/01/17/fake-news-awards-by-donald-trump-gop-cnn-new-york-times-washington-post.html>. Acesso em 25 set. 2021.

LEONARDI, Marcel. **Legítimo Interesse**. Revista do Advogado, v. 39, n. 144 nov, 2019, pp. 67-73.

LEONARDI, Marcel. **Parecer sobre implicações da LGPD na publicidade personalizada**. IAB Brasil, 2021. Disponível em: https://iabbrasil.com.br/wp-content/uploads/2021/08/IAB-BRASIL_PARECER-JURIDICO_LGPD-E-PUBLICIDADE-PERSONALIZADA_MARCEL-LEONARDI.pdf

LEVINSON, Sanford; BALKIN, Jack M. **Democracy and Dysfunction**. The University of Chicago Press, 2019. 217 p.

LLANSÓ, Emma et. al. **Artificial intelligence, content moderation, and Freedom of Expression**. Transatlantic Working Group on Content Moderation Online and Freedom of Expression, 2020.

MAGRANI, Eduardo. **A internet das coisas**. Rio de Janeiro: FGV Editora, 2018, p. 98.

MAGRANI, Eduardo. **Democracia conectada: a internet como ferramenta de engajamento político-democrático**. Curitiba: Juruá, 2014.

MAGRANI, Eduardo; GUEDES, Paula. Inteligência artificial: desafios éticos e jurídicos. In: FRAZÃO, Ana; CUEVA, Ricardo Villas Bôas. **Compliance e políticas de proteção de dados**. São Paulo: Thomson Reuters Brasil, 2021, pp. 161-184.

MAJONE, Giandomenico. **The rise of the regulatory state in Europe**. West European Politics, 17(3), pp. 77–101. doi:10.1080/01402389408425031.

MALTHOUSE, Edward; MASLOWSKA, Ewa; FRANKS, Judy. The role of Big Data in Programmatic TV Advertising. In: CAUBERGHE, Verolien; HUDDERS, Liselot;

EISEND, Martin (eds.). **Advances in Advertising Research IX: power to consumers**. European Advertising Academy: Springer Gabler, 2018, pp. 32-33.

MARANHÃO, Juliano; CAMPOS, Ricardo. Fake News e autorregulação regulada das redes sociais no Brasil: fundamentos constitucionais. In: ABOUD, George; NERY JR, Nelson; CAMPOS Ricardo. **Fake News e Regulação**. São Paulo: Thomson Reuters Brasil, 2021, pp. 341-346.

MARÉCHAL, Nathalie; RENIERIS, Elizabeth; RYDZAK, Jan. Better Processes Lead to Better Outcomes: Corporate Governance as a Tool to Address Misinformation. In: KARANICOLAS, Michael (Ed.). **Tackling the “Fake” Without Harming the “News”**. New Haven: Yale Law School, 2021, p.10-29.

MENDES, Laura Schertel. **O Supremo Tribunal Federal e a proteção constitucional dos dados pessoais: rumo a um direito fundamental autônomo**. In: MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JR., Otavio Luiz (Coords.). **Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: Forense, 2021, pp. .

MENDES, Laura Schertel; FONSECA, Gabriel Campos Soares. **Proteção de dados para além do consentimento: tendências de materialização**. In: MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JR., Otavio Luiz (Coords.). **Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: Forense, 2021, pp. 135-167.

META FOR BUSINESS. **Anúncios do Facebook**. Disponível em <https://www.facebook.com/business/ads>. Acesso em 28 dez. 2021.

MILLS, Adam; PITT, Christine; FERGUSON, Sarah. The Relationship between Fake News And Advertising: Brand Management in the Era Of Programmatic Advertising and Prolific Falsehood. **Journal of Advertising Research**, 59 (1), p. 5.

MULHOLLAND, Caitlin; GOMES, Rodrigo Dias de Pinho. Inteligência artificial e seus principais desafios para os programas de compliance e as políticas de proteção de dados. In: FRAZÃO, Ana; CUEVA, Ricardo Villas Bôas. **Compliance e políticas de proteção de dados**. São Paulo: Thomson Reuters Brasil, 2021, pp. 161-184.

MULHOLLAND, Caitlin; OLIVEIRA, Samuel Rodrigues. Uma Nova Cara para a Política? Considerações sobre Deepfakes e Democracia. **Direito Público**, v. 18, n.99, pp. 368-396, jul-set/2021.

PARENTONI, Leonardo. **Compartilhamento de dados pessoais e a figura do controlador**. In: FRAZÃO, Ana; CUEVA, Ricardo Villas Bôas. **Compliance e políticas de proteção de dados**. São Paulo: Thomson Reuters Brasil, 2021, pp. 161-184.

PARISER, Eli. **O filtro invisível: o que a internet está escondendo de você?** Rio de Janeiro: Zahar, 2012.

PASQUALE, Frank. **Platform Neutrality: Enhancing Freedom of Expression in Spheres of Private Power**. University of Maryland Legal Studies Research Paper, n. 2016-24, 29p.

PASQUALE, Frank. *The Black Box Society. The Secret Algorithms That Control Money and Information*. Harvard University Press, 2015. pp. 69-72.

QUEIMALIÑOS, Rebeca. **O homem que arruinou a extrema direita nos EUA**. *El País*. 17 de maio de 2020. Disponível em <https://brasil.elpais.com/icon/2020-05-17/o-homem-que-arruinou-a-extrema-direita-nos-eua.html>. Acesso em 12/01/2022.

REINO UNIDO. House of Commons. Digital, Culture, Media and Sport Committee. **Disinformation and ‘fake news’: Final Report, 18 fev. 2019**, 109 pp. Disponível em: <https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/1791/1791.pdf>. Acesso em 25 set. 2021.

REINO UNIDO. Information Commissioner’s Office. **Accountability Framework** Disponível em <https://ico.org.uk/for-organisations/accountability-framework/>. Acesso em 25.02.2022.

REINO UNIDO. Information Commissioner’s Office. **How do we comply with the cookie rules?** Disponível em <https://ico.org.uk/for-organisations/guide-to-pecr/guidance-on-the-use-of-cookies-and-similar-technologies/how-do-we-comply-with-the-cookie-rules/#comply14>. Acesso em 03.04.2022.

RODOTÀ, Stefano. **A vida na sociedade da vigilância: a privacidade hoje**. Organização, seleção e apresentação: DE MORAES, Maria Celina Bodin. Rio de Janeiro: Renovar, 2008.

ROMANINI, Anderson Vinícius; MIELLI, Renata. A comunicação dominada pelas “big techs” digitais: superabundância informativa, espetáculo, alienação e fabricação de sentido no mundo algorítmico. *Revista Eptic*, v. 23, n. 1, jan-abr. 2021, ISSN 1518-2487, pp. 142-161.

ROSEN, Jeffrey. **The Deciders: The Future of Privacy and Free Speech in the Age of Facebook and Google**. 80 *Fordham L. Rev.*, v 80 (4), 1525 (2012). Available at: <https://ir.lawnet.fordham.edu/flr/vol80/iss4/1>

ROSENVALD, Nelson; FALEIROS JÚNIOR, José Luiz de Moura. **Accountability e mitigação da responsabilidade civil na Lei Geral de Proteção de Dados Pessoais**. In: FRAZÃO, Ana; CUEVA, Ricardo Villas Bôas. **Compliance e políticas de proteção de dados**. São Paulo: Thomson Reuters Brasil, 2021, pp. 771-808.

SANDER, Barrie. Freedom of Expression in the Age of Online Platforms: the Promise and Pitfalls of a Human Rightsbased Approach to Content Moderation. **Fordham International Law Journal**. v.43:4, pp. 939-1006.

SARLET, Ingo Wolfgang. Fundamentos Constitucionais: o direito fundamental à proteção de dados. In: MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JR., Otavio Luiz (Coords.). **Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: Forense, 2021, pp..

SCHAUER, Frederick. **Thinking like a lawyer: a new introduction to legal reasoning**. Harvard University Press, 2009, pp. 188-202.

SCHULZ, Wolfgang. Regulating Intermediaries to Protect Privacy Online – the Case of the -German NetzDG, **HIIG Discussion Paper Series**, 01-2018. pp. 1-14.

SILVERMAN, Craig; ALEXANDER, Lawrence. How Teens In The Balkans Are Duping Trump Supporters With Fake News. **BuzzFeed**, 03/11/2016. Disponível em: <https://www.buzzfeednews.com/article/craigsilverman/how-macedonia-became-a-global-hub-for-pro-trump-misinfo>. Acesso em 03/01/2022.

SILVERMAN, Craig. I Helped Popularize The Term “Fake News” And Now I Cringe Every Time I Hear It. **BuzzFeed**, Canada, 31 dez. 2017. Disponível em: <https://www.buzzfeednews.com/article/craigsilverman/i-helped-popularize-the-term-fake-news-and-now-i-criinge>>. Acesso em 25 set. 2021.

SILVERMAN, Craig. **This Analysis Shows How Viral Fake Election News Stories Outperformed Real News On Facebook**. BuzzFeed, Canada, 16 nov. 2016. Disponível em: <https://www.buzzfeednews.com/article/craigsilverman/viral-fake-election-news-outperformed-real-news-on-facebook>>. Acesso em 21 ago. 2021.

SINCLAIR, Darren. Self-Regulation Versus Command and Control: Beyond False Dichotomies. **Law & Policy**, v. 19, n. 4, Oct. 1997, Oxford: Blackwell Publishers, pp. 529-559.

SONAR. **Em um ano Sleeping Giants Brasil evitou mais de R\$ 14 milhões em publicidade a sites de fake news, calculam os fundadores**. Publicado em 26 de maio de 2021. Disponível em: <https://blogs.oglobo.globo.com/sonar-a-escutas-das-redes/post/em-um-ano-sleeping-giants-brasil-evitou-mais-de-r-14-milhoes-em-publicidade-sites-desinformativos-calculam-fundadores.html>. Acesso em 04/01/2022.

SPINDLER, Gerald. Internet Intermediary Liability Reloaded The New German Act on Responsibility of Social Networks and its (In-) Compatibility with European Law. JIPITEC, n. 8, 2017.

SPINELLI, Egle Muller; SANTOS, Jéssica de Almeida. Jornalismo na era da pós-verdade: fact-checking como ferramenta de combate às fake news. **Revista Observatório**, v. 4, n. 3, mai/2018. ISSN nº 2447-4266, DOI: <https://doi.org/10.20873/uft.2447-4266.2018v4n3p759>.

Sprout Social. **From risk to responsibility: social media & the Evolution of transparency**. Disponível em: <https://media.sproutsocial.com/uploads/2019/04/Sprout-Social-Brands-Get-Real-Evolution-of-Transparency.pdf>.

SUNSTEIN, Cass. **Liars: Falsehoods and Free Speech in an Age of Deception**. Oxford University Press, 2021.

SUPPORT GOOGLE. Controlar os anúncios que você vê. Disponível em <https://support.google.com/ads/answer/2662856?hl=pt-BR&co=GENIE.Platform%3DAndroid>. Acesso em 20 dez. 2021.

SYED, Nabiha. Real Talk About Fake News: Towards a Better Theory for Platform Governance. **Online Platforms and Free Speech: Regulating Fake News**. New Haven: Yale Law School, 2018, p.337-357.

TARGETT, Simon; BUTMAN, John. **Facebook got clobbered Thursday. Why Mark Zuckerberg won't care.** *The Washington Post*, Made by History. Disponível em <https://www.washingtonpost.com/news/made-by-history/wp/2018/07/27/facebook-got-clobbered-on-thursday-why-mark-zuckerberg-wont-care/>, publicação em 27.07.2018.

THOMAS, Julian. Programming, filtering, adblocking: advertising and media automation. *Media International Australia*, 2018, p. 35.

TUFEKCI, Zeynep. Algorithmic harms beyond Facebook and Google: emergent challenges of computational agency. *Colorado Technology Law Review*, n. 13, 2015.

Twitter. **Sleeping Giants**. Disponível em https://twitter.com/slpng_giants. Acesso em 12/01/2022.

United Nations Human Rights. **Regulating online content – the way forward.** Digital Spaces, 2020. Disponível aqui.

VOSOUGHI, Soroush; ROY, Deb; ARAL, Sinan. **The Spread of True And False News Online.** MIT Initiative on the digital economy research brief, 2018.

WARDLE, Claire; DERAKHSHAN, Hossein. **Information Disorder: Toward an interdisciplinary framework for research and policy making.** Council of Europe, 2017, pp. 25, 34-35.

WESTRUP, Ana Carolina. Para além da aparência: saídas amplas e democráticas. In: MARTINS, Helena (org.). **Desinformação: crise política e saídas democráticas para as Fake News.** São Paulo: Veneta, 2020.

WIMMER, Miriam; PIERANTI, Octavio Penna. Programas de compliance e a LGPD: a interação entre autorregulação e a regulação estatal. In: FRAZÃO, Ana; VILLAS BÔAS CUEVA, Ricardo. **Compliance e políticas de proteção de dados.** São Paulo: Thomson Reuters Brasil, 2021, pp. 205-221.

ZUBOFF, Shoshana. **A Era do Capitalismo de Vigilância: a luta por um futuro humano na nova fronteira do poder.** Rio de Janeiro: Intrínseca, 2020.

ZUBOFF, Shoshana. Big Other: capitalismo de vigilância e perspectivas para uma civilização de informação. In: BRUNO, Fernanda et. al. **Tecnopolíticas da Vigilância: perspectivas da margem.** São Paulo: Boitempo, 2018. pp. 26-33.

ZUBOFF, Shoshana. Big Other: Surveillance Capitalism and the Prospects of an Information Civilization. *Journal of Information Technology*, v. 30, Apr. 2015, pp. 75-89.