JULHO, 2021

Proteção de Dados e Transparência em Moderação de Conteúdo na Europa, Reino Unido e Brasil

AUTOR
João Victor Archegas

ASSISTENTE DE PESQUISA
Mariana Haddad Vilhena

EDITORAÇÃO E REVISÃO
Celina Bottino
Christian Perrone
Mariana Haddad Vilhena

GREAT for PARTNERSHIP
BRITAIN & NORTHERN IRELAND

ITS
Instituto de Tecnologia & Sociedade do Rio

SUMÁRIO

RESUMO EXECUTIVO

Para viabilizar a moderação de conteúdo na Internet, as plataformas digitais precisam tratar uma considerável quantidade de dados pessoais de seus usuários. Muitos destes dados são sensíveis e revelam informações sobre posicionamento político, orientação sexual, dentre outros. Assim, existem diversos pontos de contato entre o processo de moderação e a proteção de dados pessoais.

Buscando explorar justamente essa área de investigação, o **objetivo** deste relatório de boas práticas é analisar a imposição de obrigações de transparência em moderação de conteúdo às plataformas digitais no Reino Unido, União Europeia e Brasil e sua relação com a privacidade e proteção de dados pessoais.

Para tal, são estudados **três arranjos regulatórios** ainda em discussão no Parlamento Inglês, no Parlamento Europeu e no Congresso Nacional para determinar quais são os mecanismos de proteção de dados vinculados a estas obrigações de transparência.

Embora existam outros mecanismos de transparência em moderação de conteúdo, este documento se dedica ao estudo dos chamados **relatórios de transparência** que, caso os referidos arranjos sejam aprovados, deverão ser publicados periodicamente por diversas plataformas digitais, incluindo redes sociais.

Em termos de metodologia, busca-se analisar cada projeto individualmente em seu estágio atual, focando na obrigação de publicação de relatórios de transparência e no **sistema de freios e contrapesos** previsto por cada projeto para resguardar a privacidade e a proteção de dados dos usuários das plataformas.

A partir de algumas conclusões deduzidas dos casos do Reino Unido e da União Europeia, o relatório faz algumas **considerações e sugestões** sobre o que deve mudar no caso brasileiro para melhor alinhar os mecanismos de transparência em moderação de conteúdo com a disciplina da proteção de dados no país.

INTRODUÇÃO E ESTRUTURA DO RELATÓRIO

A moderação de conteúdo em redes sociais, bem como em outras plataformas digitais, ganha cada vez mais espaço no debate sobre governança e regulação da Internet no Brasil e no mundo. O tema vem crescendo em importância conforme cidadãos e reguladores se dão conta da dimensão e extensão dos impactos do discurso online para diversos aspectos da vida em sociedade, em especial para as interações político-partidárias entre usuários de aplicações na era digital.

Muito se fala, por exemplo, no uso das redes sociais para a disseminação de desinformação ou *fake news* e também nos danos causados por alguns conteúdos compartilhados (*online harms*). Por outro lado, tentativas de tornar a moderação mais transparente podem colocar em cheque a privacidade e a proteção de dados pessoais dos usuários destes serviços online.

Como será abordado ao longo deste estudo, a moderação de conteúdo em plataformas digitais pressupõe o tratamento de grandes quantidades de dados pessoais dos usuários, muitos deles sensíveis. Assim, obrigações de transparência nessa área devem ser cuidadosamente consideradas para evitar a exposição indevida dessas informações.

Estes e outros desafios oferecem um ponto focal para novas políticas públicas que buscam impor obrigações e deveres às plataformas digitais. No presente estudo do Instituto de Tecnologia e Sociedade do Rio de Janeiro (ITS Rio), serão analisadas três propostas regulatórias que ainda estão sob discussão parlamentar e que prometem diretrizes inovadoras de governança digital:

- A *Proposal for a Regulation on a Single Market for Digital Services (Digital Services Act - DSA)* do Parlamento Europeu e do Conselho da Europa;
- O *Online Safety Bill* (anteriormente conhecido como *Online Harms White Paper*) do Parlamento do Reino Unido e, por fim;
- O PL n.º 2.630/2020 que busca instituir a Lei Brasileira de Liberdade, Responsabilidade e Transparência na Internet (também conhecida como Lei das *Fake News*) do Congresso Nacional.

Embora estes documentos tratem sobre diferentes aspectos regulatórios, o foco do relatório será a análise dos mecanismos de transparência por eles previstos. Um dos eixos estruturantes dos três arranjos é o que podemos chamar de "relatórios de transparência", ou seja, a obrigação de que diferentes plataformas digitais, incluindo redes sociais, publiquem periodicamente dados a respeito de suas práticas de moderação de conteúdo.

Entretanto, a imposição da transparência, ainda que desejável, deve ser avaliada com cautela. A obrigação de transparência está longe de ser uma solução para todos os desafios apresentados pela moderação de conteúdo em platafor-

mas digitais. Neste relatório, assim, enfrentamos alguns dos limites associados ao dever de transparência, dando destaque à tensão que existe entre, de um lado, o princípio transparência e, do outro, privacidade e proteção de dados.

Nosso objetivo, portanto, é descobrir se os arranjos dão conta de harmonizar as duas disciplinas de forma que a prevalência de uma não importe na violação da esfera de proteção da outra. Cumpre destacar, desde já, que a transparência não é um valor absoluto, tampouco uma solução generalizante para os problemas da moderação de conteúdo.

Pesquisadores costumam citar uma frase de Louis D. Brandeis, ex-Justice ("Ministro") da Suprema Corte dos Estados Unidos, para ilustrar a importância do tema: "*sunlight is said to be the best of disinfectants*"[1] (em tradução livre, "acredita-se que a luz do sol é o melhor dos desinfetantes").

É curioso notar que Brandeis faz tal afirmação não em um contexto de exercício do poder público, mas sim do setor privado. Ou seja, indo além da tradição iluminista de que a transparência seria um importante mecanismo de prestação de contas (*accountability*) para o Estado, Brandeis defende que a transparência "também pode servir como um freio para o [abuso do] poder privado"[2].

Nesse sentido, Brandeis inaugura uma nova tradição intelectual nos EUA que pensa em mecanismos de transparência também para atividades do setor privado que, de uma forma ou de outra, são permeadas pelo interesse público. É justamente essa linha investigativa - sobre transparência no setor privado - que dá origem às obrigações de publicidade e transparência para plataformas digitais.

Ainda que sejam criadas, operadas e administradas por empresas privadas, estas plataformas moldam diversos aspectos da vida em sociedade na era digital, desde como consumimos bens e serviços até como nos relacionamos enquanto atores de transformação política. Consequentemente, é inevitável (e até certa medida desejável) que diferentes reguladores encarem a transparência como uma esteira de condução de valores públicos para dentro da casa de máquinas da moderação de conteúdo. Afinal, só se pode governar aquilo que se conhece.

De outra sorte, vale lembrar que o próprio Brandeis não via na transparência uma solução generalizável ou totalizante. Anos antes, em dezembro de 1890, ao lado de Samuel D. Warren, Brandeis publicou na Harvard Law Review o seminal artigo "*The Right to Privacy*", onde defendeu de forma pioneira a necessidade de tutela jurídica da privacidade[3].

No texto, Warren e Brandeis identificam no então "direito a ser deixado em paz" (*right to be let alone*) uma crucial manifestação jurídica da privacidade. Os autores estão preocupados, principalmente, com o impacto de novas tecnologias como as fotografias instantâneas que, em suas palavras, "invadiram o recinto sagrado da vida privada e doméstica"[4].

Assim, a própria trajetória acadêmica de Brandeis, um dos precursores da

criação de mecanismos de transparência para a governança do espaço privado, ilustra bem a tensão que existe entre, de um lado, "a luz do sol como desinfetante" e, do outro, a proteção da esfera privada das pessoas diante da emergência de novas tecnologias.

É preciso se certificar, assim, de que novos arranjos regulatórios que apostam na transparência como um dos pilares da governança de plataformas digitais estão de acordo com as regras e os princípios da disciplina de proteção de dados pessoais.

Isso não significa, entretanto, que este relatório parte do pressuposto de que os arranjos regulatórios aqui analisados violam a privacidade e a proteção de dados, mas tão somente que, ao analisá-los, esta é justamente uma das lentes que não podemos perder de vista para evitar atritos e incompatibilidades. Trata-se, portanto, de garantir a manutenção do equilíbrio entre essas duas áreas.

Some-se a isso o fato de que o Brasil atravessa um momento delicado do processo de consolidação e fortalecimento da disciplina de privacidade e proteção de dados no território nacional, especialmente vis-à-vis as melhores práticas e padrões internacionais. Tendo em vista este cenário particular, quando o PL n.º 2.630/2020 busca instituir um "dever de transparência dos provedores de aplicação" é preciso que se levante algumas considerações a respeito de como essa obrigação pode (ou não) ser compatibilizada com a Lei Geral de Proteção de Dados (LGPD).

Felizmente, esse não é um desafio exclusivo do Brasil e, por isso, podemos deduzir ensinamentos (e até mesmo soluções) das experiências no Reino Unido e na União Europeia para melhor conduzir o debate no país. Esse é justamente o objetivo deste relatório que busca apresentar boas práticas.

De outra sorte, é importante que se considere não apenas o aspecto negativo do debate - ou seja, a tensão entre privacidade e transparência -, mas também o seu aspecto positivo; em outras palavras, quando há compatibilidade entre as duas esferas de proteção, uma pode reforçar a outra dentro de um ciclo de suporte mútuo.

Veja-se, por exemplo, o direito à autodeterminação informativa que é um dos pilares da LGPD. Para que o titular dos dados exerça esse direito em sua plenitude, é indispensável que os controladores de dados (a exemplo de plataformas digitais) sejam transparentes a respeito de suas atividades de processamento. Só assim o titular pode tomar conhecimento de eventuais violações ou ilegalidade e agir para remediá-las. Assim, aspectos da transparência são indispensáveis para garantir a eficiência da proteção de dados.

Em termos de estrutura do relatório, no primeiro capítulo serão apresentados os mecanismos de transparência propostos pelo *Online Safety Bill ("OSB")* no Reino Unido e pelo *Digital Services Act ("DSA")* na União Europeia e a correlação

com a disciplina de privacidade e proteção de dados. Na sequência, na primeira subseção, será feita uma análise crítica sobre o tipo de transparência que pode emergir da aplicação desses mecanismos e sua harmonização com a proteção de dados pessoais. Na segunda subseção, então, avalia-se com maior profundidade a relação entre transparência e privacidade na moderação de conteúdo à luz dos ensinamentos deduzidos da análise do DSA e do *Online Safety Bill*.

Já no segundo capítulo faremos uma discussão mais aprofundada do PL das fake news e sua relação com a LGPD. Na primeira subseção será feita uma análise crítica sobre o tipo de transparência que se encontra no projeto, Já na segunda subseção avaliar-se-á os ensinamentos trazidos pela perspectiva internacional, o grau de alinhamento entre o projeto brasileiro e os arranjos do Reino Unido e da União Europeia em termos de privacidade e proteção de dados pessoais e eventuais reformas que podem ser adotadas pelo legislador brasileiro.

1. MECANISMOS DE TRANSPARÊNCIA EM MODERAÇÃO DE CONTEÚDO NA UNIÃO EUROPEIA E NO REINO UNIDO

1.1. *Online Safety Bill* no Reino Unido

No Reino Unido, o *Online Safety Bill*, ao propor um novo marco regulatório para proteger a segurança dos cidadãos britânicos na Internet e combater diferentes categorias de *online harms* - como conteúdos de cunho terrorista, campanhas de desinformação, conteúdos que violem direitos de crianças, etc. - adota como um de seus pilares o desenvolvimento de uma cultura de transparência, confiança e prestação de contas (*accountability*).

Um dos instrumentos que garantiria este desenvolvimento seria a publicação de "relatórios de transparência" (*transparency reports*), nos quais as empresas que estejam dentro do escopo da nova regulamentação deveriam prestar contas sobre os tipos de *online harms*[5] que estão enfrentando e quais foram as medidas implementadas para combatê-los.

O objetivo do relatório anual não é apenas a prestação de contas entre a empresa e o governo do Reino Unido, mas também a construção de uma relação de confiança entre a empresa e seus usuários. A aposta do novo marco regulatório é que, ao saber quais são os *online harms* que prevalecem num dado serviço e quais são os passos concretos tomados para para neutralizá-los, os clientes se sentirão mais seguros ao longo de suas interações online e terão mais confiança no trabalho desenvolvido por uma determinada plataforma digital, além, é claro, de contarem com mais informações para que possam cobrar soluções e monitorar seu desempenho.

O centro gravitacional desse novo esquema regulatório é a criação de um dever de cuidado (*duty of care*) que deverá guiar as ações de plataformas digitais.

O projeto faz uma distinção entre *user-to-user service* (que inclui redes sociais, onde os conteúdos são criados e compartilhados entre usuários) e *search service* (que inclui buscadores como Google e Bing). A implementação desse novo dever será garantida através da atuação de um regulador independente para assuntos de segurança online[6].

O regulador eleito pelo *Online Safety Bill* é o *Office of Communications* (OFCOM), uma entidade do governo britânico fundada em 2003 e responsável por regular diferentes setores de comunicações e telecomunicações, como serviços postais, rádio e televisão. Segundo o texto da legislação proposta, o OFCOM ganharia uma nova esfera de competências e passaria a regular também provedores de aplicações da Internet (serviços *user-to-user* e de busca) com o objetivo específico de proteger cidadãos dos riscos de dano envolvidos no uso dessas plataformas.

1.2. *Digital Services Act* na União Europeia

De outra sorte, o *Digital Services Act* foi apresentado pela primeira vez pela Comissão Europeia em dezembro de 2020 e consiste em uma proposta de regulação pelo Parlamento Europeu e o Conselho da Europa para criar um mercado único para serviços digitais dentro dos limites da União Europeia. Se aprovado, o DSA vai emendar e atualizar a famosa diretiva de *e-commerce* da União Europeia (Diretiva 2000/31/EC).

Segundo a própria justificativa da proposta, seu objetivo é "garantir as melhores condições para a prestação de serviços digitais inovadores no mercado interno, contribuir com a segurança online e a proteção de direitos fundamentais, e consolidar uma estrutura de governança robusta e durável para a efetiva supervisão dos provedores de serviços intermediários"[7] (tradução livre). Tal como o *Online Safety Bill* no Reino Unido, o DSA busca proteger os usuários de plataformas digitais a partir da imposição de uma série de deveres a estes intermediários.

Nesse sentido, o DSA também aposta em princípios como *accountability* e transparência para melhor possibilitar o monitoramento desses serviços pelas autoridades públicas da União Europeia. Para garantir a implementação dessa moldura regulatória, o DSA prevê a criação de um *Digital Services Coordinator* (Coordenador de Serviços Digitais) para cada Estado-membro e um *European Board for Digital Services* (Conselho Europeu de Serviços Digitais) que dará suporte para a atuação dos coordenadores nacionais.

Assim como a proposta do Reino Unido, o DSA também aposta na concretização de um dever de transparência por parte das plataformas digitais que se traduz na publicação de relatórios de transparência (*transparency reports*). Nas palavras da proposta elaborada pela Comissão Europeia, "para garantir um nível adequado de transparência e *accountability*, provedores de serviços interme-

diários devem reportar anualmente [...] dados de suas práticas de moderação de conteúdo, incluindo as medidas adotadas como consequência da aplicação e imposição de seus termos e condições"[8] (tradução livre).

Como afirmam Aline Blankertz e Julian Jauch, o objetivo do texto é estabelecer um nível mínimo de transparência para plataformas digitais que já existem em outros setores da economia há décadas. Em outras palavras, não se trataria de uma tentativa de substituir o modelo de autorregulação das plataformas por um modelo de regulação estatal, mas apenas de impor alguns parâmetros básicos de transparência que, por sua vez, irão garantir de uma forma mais eficiente a proteção do interesse público dentro da esfera digital, hoje com um espaço mais amplo de controle por parte das empresas privadas[9].

1.3. Uma análise dos mecanismos de transparência no *Online Safety Bill* e no *Digital Services Act* à luz da Proteção de Dados e da Privacidade

Antes de analisar as nuances dos mecanismos de transparência propostos pelo *Online Safety Bill* e pelo DSA - especialmente à luz da disciplina de proteção de dados pessoais e privacidade -, cumpre contextualizar essas iniciativas dentro de um quadro mais amplo de regulação e governança das práticas de moderação de conteúdo pelas plataformas digitais.

Segundo os professores John Bowers e Jonathan Zittrain, a governança dessas plataformas se dividiu até o momento em três grandes eras que eles denominam de (a) **era dos direitos** (*era of Rights*), que se estende dos anos 90 até 2010, (b) **era do bem-estar público**[10] (*era of Public Health*), que se estende de 2010 até o presente, e (c) **era do processo** (*era of Process*), que está apenas começando a emergir.[11]

O trabalho de Bowers e Zittrain foi escolhido por ser um importante referencial para compreender o contexto no qual os arranjos regulatórios aqui discutidos estão inseridos. Sua classificação tripartite nos permite avaliar a tensão entre as duas primeiras fases regulatórias - quais sejam, a era dos direitos e a era do bem-estar público - e, assim, avaliar quais são as inovações e soluções propostas pela terceira fase regulatória - qual seja, a era do processo.

O grande marco da era dos direitos é a aprovação da seção 230 do *Communications Decency Act* (CDA) dos Estados Unidos, a qual concede uma ampla proteção legal às plataformas digitais contra a responsabilização pelo conteúdo de terceiros, especialmente os usuários dessas aplicações. Nas palavras de Bowers e Zittrain, esse período é marcado pela preocupação compartilhada entre diferentes reguladores de proteger "uma esfera de discurso online ainda em maturação contra coerções externas, sejam empresariais ou governamentais"[12] (tradução livre).

Em outras palavras, regimes de responsabilização de intermediários como a seção 230 do CDA - que encontra paralelos também no artigo 19 do Marco Civil da Internet no Brasil e na diretiva de *e-commerce* da União Europeia -, conferiram (e ainda conferem) um amplo espaço de proteção às plataformas de forma a promover a inovação na Internet e evitar interferências deletérias sobre o discurso dos usuários.

A era dos direitos, então, consolidou uma esfera de autorregulação das plataformas digitais, a qual se traduz na estipulação de termos de uso e padrões da comunidade que guiam a atividade de moderação de conteúdo em serviços como buscadores e redes sociais.

Como constatou um relatório do ITS Rio sobre o assunto, "desde a década de 90 [...] as diversas plataformas digitais passaram a atuar dentro de um paradigma de autorregulação" e, portanto, "estabelecem regras internas, [...] contratam moderadores de conteúdo, desenvolvem algoritmos de moderação e removem publicações que não estão de acordo com suas propostas de comunidade"[13].

Em segundo lugar, a era do bem-estar público emerge principalmente diante da crescente preocupação de atores políticos com os danos gerados pelo discurso de usuários nas redes sociais. Um importante exemplo é o fenômeno da desinformação e manipulação política nas plataformas, que se tornou latente principalmente após o escândalo envolvendo o Facebook e a Cambridge Analytica [14]e a interferência russa nas eleições presidenciais dos EUA em 2016 a partir do prédio da *Internet Research Agency* em São Petersburgo[15].

Mas os danos não se limitam apenas ao mundo das *fake news*. Outras preocupações legítimas envolvem dados pessoais vazados, campanhas de comportamento inautêntico coordenado que inflam a popularidade de conteúdos de forma inorgânica, discurso de ódio, *bullying*, disseminação de pornografia não consensual ou *revenge porn*, violação de direitos autorais, violação da esfera de proteção de crianças e adolescentes, discriminação, dentre outras. A prevalência desses conteúdos na Internet suscitou um importante debate sobre a eficiência do controle desempenhado pelas plataformas digitais num contexto de autorregulação e a segurança dos usuários.

Como explicam Bowers e Zittrain, o foco da era do bem-estar público é enfrentar os efeitos agregados de conteúdos problemáticos. Por exemplo, embora uma postagem que jogue dúvidas infundadas sobre a eficácia da vacina contra COVID-19 não seja um problema em si, uma campanha de desinformação pautada nessa mesma mensagem pode gerar um grande impacto negativo para o bem-estar público em tempos de pandemia.[16]

Nas palavras dos autores, "é feito um pedido para as plataformas para que usem seu chapéu de epidemiologista e atuem para mitigar danos específicos e contextuais [...] que surgem das interações entre usuários numa escala massiva"[17]

(tradução livre). Ou seja, trata-se de garantir a segurança dos usuários e proteger os seus direitos fundamentais durante suas interações nas plataformas.

O problema é que as exigências da era do bem-estar público muitas vezes entram em conflito com as proteções garantidas pelos regimes de responsabilização de intermediários que surgiram na era dos direitos, os quais evitam que plataformas sejam responsabilizadas por conteúdos de terceiros. Veja-se, por exemplo, as inúmeras propostas de reforma da seção 230[18] nos EUA e do Marco Civil na Internet no Brasil, inclusive pela via de ações judiciais[19], com o objetivo de restringir a esfera de autorregulação das plataformas pelos mais variados motivos.

É o caso, por exemplo, da minuta de decreto do governo federal do Brasil que busca regulamentar o Marco Civil da Internet para restringir o escopo da moderação de conteúdo na Internet sob o pretexto de proteger a liberdade de expressão dos brasileiros. Uma vez assinado, o decreto inverteria a lógica da moderação no país; as plataformas só poderiam agir nas hipóteses previstas no ato ou então mediante ordem judicial, o que levanta questionamentos sobre sua legalidade e constitucionalidade[20].

Isso acaba inevitavelmente levando a um debate sobre os valores ideológicos e/ou políticos que devem reger a moderação de conteúdo, paralisando qualquer possibilidade real de mudança diante de severas divergências e clivagens políticas. Vale lembrar que embora exista alguma área de convergência entre atores da direita e da esquerda nessa área, os motivos para reforma ainda são incompatíveis; enquanto a direita quer proteger posições conservadoras nas redes contra supostos atos de censura, a esquerda tende a favorecer regulações mais severas de combate à desinformação.[21]

Mas existe uma terceira via que passa pelo que Bowers e Zittrain identificam como a era do processo. A ideia é compatibilizar o modelo de autorregulação com a proteção do interesse público com base na estruturação de um modelo de co-regulação. Ou seja, alguns aspectos da moderação de conteúdo que precisam ser informados pela perspectiva da proteção de direitos fundamentais deve se dar fora das estruturas dessas plataformas por uma organização independente.[22]

Essa organização independente não teria o papel de tomar decisões de moderação de conteúdo no lugar das plataformas, mas sim de monitorar a aplicação de certas obrigações procedimentais que buscam promover valores como transparência e *accountability*. A ideia é criar legitimidade em torno da moderação de conteúdo e superar o impasse criado pelo choque de posições antagônicas do espectro político.[23]

É justamente nessa terceira fase da governança de plataformas que se inserem as propostas hoje debatidas na União Europeia e no Reino Unido. A partir da atribuição de competências a uma organização independente, esses novos arranjos regulatórios buscam garantir a prevalência do interesse público na Internet sem que isso signifique o fim da autorregulação de plataformas.

Embora existam diferentes mecanismos que se encaixem na proposta "da era do processo", neste relatório, como mencionado anteriormente, o foco será na análise dos relatórios de transparência mencionados pelo *Online Safety Bill* e DSA. Isso se deve a dois principais motivos:

- Primeiro, os relatórios de transparência são exemplos claros de **mecanismos procedimentais** que objetivam dar mais legitimidade ao processo de moderação de conteúdo buscando não ameaçar a esfera de autorregulação das plataformas;
- Segundo, estes relatórios envolvem a **publicação de dados**, o que permite uma análise mais detida sobre pontos de tensão entre novos arranjos regulatórios inseridos na "era do processo" e a disciplina de proteção de dados pessoais e privacidade.

1.3.1. Relatórios de Transparência no *Online Safety Bill*

A minuta do *Online Safety Bill* do Reino Unido menciona em sua subseção 49(1) que todos os provedores de serviços regulados (serviços *user-to-user* e de busca)[24] devem produzir um relatório anual, denominado "relatório de transparência" (*transparency report*), que contará com as informações descritas pelo *Office of Communications* (OFCOM) em uma notificação encaminhada ao próprio provedor.

Adiante, na subseção 49(4), a minuta estipula que o OFCOM deverá descrever exatamente quais informações devem estar presentes nos relatórios anuais e lista treze gêneros de informações que podem ser solicitadas pela autoridade. Essa lista propõe-se a ser exaustiva e qualquer informação que não se encaixe em uma das treze hipóteses não poderia ser legitimamente requisitada pelo OFCOM.

Dentre os diferentes gêneros, cumpre destacar os seguintes "clusters" de dados que podem estar presentes nos relatórios de transparência que serão preparados anualmente pelos provedores:

Dados sobre a incidência de conteúdo ilegal e conteúdo considerado danoso para adultos ou crianças nas plataformas e sobre quantos usuários foram potencialmente expostos a esses conteúdos;

Dados sobre a maneira como esses conteúdos são disseminados e distribuídos na plataforma;

Dados sobre a maneira como os termos de uso da plataforma são aplicados para lidar com esses conteúdos;

- Dados sobre os sistemas e processos disponibilizados aos usuários para que reportem tais conteúdos à plataforma;
- Dados sobre as formas de cooperação entre as plataformas e diferentes órgãos públicos, como representantes do governo e autoridades regulatórias;
- Dados sobre os sistemas e processos implementados pelas plataformas para mensurar o risco de dano representado pela presença desses conteúdos;
- Dados sobre as medidas adotadas pela plataforma para garantir uma esfera de proteção mais robusta às crianças que usam seus serviços;
- Dados sobre as medidas adotadas pela plataforma para melhorar a educação midiática (media literacy) de seus usuários.

1.3.2. Proteção de Dados Transparência no *Online Safety Bill*

A partir de uma análise meramente textual da subseção 49(4) da minuta do *Online Safety Bill*, pode-se dizer que nenhuma das categorias que podem estar presentes nos relatórios anuais de transparência deve representar, por si só, uma ameaça direta à esfera de proteção de dados pessoais. As exigências não se direcionam a identificar individualmente os usuários, mas tão somente dados estatísticos e que dizem respeito à própria atuação das plataformas em sentido amplo.

Em outras palavras, seria possível que as plataformas cumprissem todos os requisitos postos na notificação do OFCOM apenas com base na apresentação de dados anonimizados[25], o que seria o ideal em se tratando de privacidade e proteção de dados pessoais. Esta anonimização deve ser feita corretamente e seguindo os padrões técnicos vigentes, caso contrário o que se verifica é a entrega, ainda que involuntária ou inadvertida, de dados pessoais. É de se destacar, entretanto, que as plataformas não devem usar essa requisição para obrigatoriamente tratar mais dados do que o necessário.

Ademais, é importante que existam mecanismos que limitem tentativas do OFCOM de extrapolar seu mandato legal. Isso pode acontecer, por exemplo, com base na última hipótese elencada na subseção 49(4), qual seja, a determinação de publicação de "informações sobre outros passos que o provedor esteja dando que se relacionam a questões de segurança online"[26] (tradução livre). Por se tratar de uma espécie de cláusula de abertura - afinal, não há nenhuma definição sobre quais seriam os "outros passos" -, essa hipótese dá mais flexibilidade ao OFCOM, que, por sua vez, poderá requerer a disponibilização de dados pessoais e até mesmo sensíveis.

Mesmo nesse cenário, o *Online Safety Bill* oferece três importantes salvaguardas que se alinham com a disciplina da proteção de dados pessoais. Em primeiro lugar, dentre os deveres que são atribuídos aos próprios provedores de serviços na Internet (serviços *user-to-user* e buscadores) está a obrigação de "proteger os usuários de infrações injustificadas de sua privacidade"[27], nos termos da subseção 12(3).

Ou seja, ainda que durante sua operação o OFCOM decida usar a última hipótese da subseção 49(4) para determinar a disponibilização de dados pessoais como parte da publicação anual de relatórios de transparência, as próprias plataformas terão a oportunidade de se opor à determinação com base no seu dever de proteção da privacidade dos usuários que está disposto no próprio *Online Safety Bill*.

Em segundo lugar, a seção 50 da minuta determina que o OFCOM deverá publicar um guia para auxiliar as plataformas na elaboração dos relatórios de transparência. Ainda, nos termos da subseção 50(2), antes da criação do guia, o OFCOM deverá se consultar com diferentes *stakeholders* e, dentre eles, "pessoas que o OFCOM considera ter expertise em questões de igualdade e direitos humanos, em especial [...] o direito de respeitar a vida privada e familiar"[28] (tradução livre). Isso permite, portanto, que o guia seja informado pelos valores da privacidade e da proteção de dados, o que impacta diretamente na maneira como os relatórios serão redigidos,

Por fim, em terceiro lugar, a minuta confere ao Secretário de Estado do Reino Unido a competência para revisar a implementação do arranjo regulatório, nos termos da seção 115. Nesse sentido, uma das atribuições do Secretário será considerar a eficiência da operacionalização do *Online Safety Bill*, garantindo, dentre outros aspectos, que os usuários de serviços digitais estão sendo devidamente protegidos de violações à privacidade.

Portanto, é possível dizer que a minuta propõe um arranjo que visa evitar a violação da privacidade e da esfera de proteção de dados pessoais no que diz respeito à implementação dos relatórios anuais de transparência. Ainda que existam cláusulas de abertura como a da subseção 49(4), diversos mecanismos de defesa - verdadeiros *checks and balances* - estão previstos no *Online Safety*

Bill para corrigir eventuais distorções durante a operação do OFCOM.

O *Online Safety Bill* se propõe, aparentemente, a buscar uma relação harmônica e equilibrada entre, de um lado, o dever de cuidado materializado nas obrigações de transparência e, de outro, a proteção de dados no sentido de, sempre que possível e dentro de um mínimo necessário, tratar apenas dados anonimizados (e estatísticos). As estratégias de proteção de dados na minuta parecem gerar salvaguardas suficientes, ainda que existam lacunas que dependem de limitações externas.

1.3.3. Relatórios de Transparência no DSA

A minuta do *Digital Services Act*, por sua vez, oferece um arranjo de obrigações de transparência consideravelmente mais complexa e com três diferentes espécies de relatórios de transparência que oferecem deveres cumulativos a depender da natureza do provedor de serviços e do seu tamanho, evitando certos ônus regulatórios que podem atrasar a inovação tecnológica no setor.

Como a própria minuta assevera, isso é uma decorrência do princípio da proporcionalidade que deve guiar a estruturação e operacionalização da nova regulação. Em suas palavras, "certas obrigações substanciais são limitadas apenas para plataformas digitais muito grandes [*very large*], as quais, devido ao seu alcance, possuem um papel sistemático e central em facilitar o debate público e as transações econômicas"[29] (tradução livre).

Para o DSA, plataformas 'muito grandes' são aquelas com pelo menos 45 milhões de usuários ativos, o que representa 10% da população da União Europeia. A regulação implementa, assim, uma série de obrigações especiais quando se trata dessas empresas, justamente porque a minuta parte do pressuposto de que os riscos envolvidos em suas operações são mais salientes e podem impactar desproporcionalmente a população da região.[30]

Ainda, mesmo os requisitos mínimos de transparência não afetam provedores de serviços que se encaixam nas categorias de micro ou pequena empresa nos termos da Recomendação da Comissão Europeia 2003/361/EC.[31] Enquanto o *Online Safety Bill* delega ao OFCOM a responsabilidade de estabelecer gradações na prática, o DSA já incorpora (e concretiza) o princípio da proporcionalidade no próprio texto da proposta de regulação.

A primeira espécie de relatório de transparência está disposta no artigo 13 do DSA e se aplica a todos os provedores de serviços intermediários na Internet, independente do tamanho. Segundo a disposição, essas empresas devem publicar, pelo menos uma vez por ano, relatórios sobre suas atividades de moderação de conteúdo, incluindo:

- O número de ordens recebidas de autoridades governamentais de membros da União Europeia e o tempo que decorreu entre o seu recebimento e a tomada de uma decisão;

- O número de notificações recebidas por indivíduos ou entidades externas e as ações correspondentes que foram tomadas, inclusive informando se a decisão se baseou na lei ou nos seus termos de uso;

- Dados sobre a atividade de moderação de iniciativa própria do provedor, incluindo as medidas de restrição adotadas e quais foram as razões e as bases para tomar tais decisões;

- O número de notificações recebidas a partir de mecanismos internos de reclamação, incluindo informações sobre os motivos das reclamações e a quantidade de casos onde ocorreu a reversão da decisão original do provedor.

Já a segunda espécie de relatório de transparência está disposta no artigo 23 do DSA e se aplica às plataformas digitais que, além de elaborar relatórios com as informações acima, também devem levantar as seguintes informações:

- O número de disputas que foram submetidas às entidades externas de resolução de disputas[58] e o resultado desses casos;

- O número de suspensões aplicadas pelas plataformas no caso de usuários que compartilham frequentemente conteúdos manifestamente ilegais e de usuários que apresentam reiteradamente notificações ou reclamações sem fundamento;

- Dados sobre o uso de mecanismos automatizados de moderação de conteúdo, incluindo indicadores de acurácia desses algoritmos e medidas de salvaguarda implementadas pela plataforma.

Por fim, em terceiro lugar, o DSA prevê a publicação de uma terceira espécie de relatório de transparência por aquelas plataformas que são consideradas 'muito grandes' pela proposta de regulação. Essas empresas devem publicar seus relatórios semestralmente (e não anualmente) e, além das informações acima, incluir:

- Um relatório de análise de riscos sistêmicos na plataforma, incluindo a disseminação de conteúdo ilegal, efeitos negativos ao exercício de direitos fundamentais e manipulação intencional do serviço (como, por exemplo, a prevalência de comportamento inautêntico ou automatizado);
- As medidas de mitigação de riscos que foram identificadas pelo relatório acima e quais foram implementadas pela plataforma;
- Um relatório de auditoria que deve ser contratada pela própria plataforma pelo menos uma vez ao ano e conduzida por uma organização independente para verificar se a plataforma está de acordo com as obrigações do DSA;
- Um relatório de implementação das sugestões feitas a partir da auditoria, as quais devem ser implementadas até um mês depois de serem recebidas pela plataforma.

1.3.4. Proteção de Dados e Transparência no DSA

Em comparação com o *Online Safety Bill*, as informações que devem estar presentes nos relatórios de transparência do DSA são mais abrangentes e muitas vezes tocam em questões muito específicas da moderação de conteúdo, como a motivação da adoção de uma determinada medida de restrição de conteúdo ou então a suspensão de usuários pelo compartilhamento reiterado de conteúdo "manifestamente ilegal".

Em se tratando dos relatórios de transparência que devem ser publicados por plataformas em geral, a subseção 23(4) do DSA afirma que "a Comissão [Europeia] poderá adotar atos de implementação para apresentar modelos [*templates*] com a forma, conteúdo e outros detalhes"[32] que devem estar nos relatórios

(tradução livre). Nada obstante, enquanto tais diretrizes não forem publicadas, existe um risco de que os relatórios exponham dados pessoais de usuários em detrimento à proteção de dados.

Por exemplo, para que um provedor possa apresentar dados sobre o que motivou uma determinada ação de restrição de conteúdo é necessário que certos dados contextuais também sejam disponibilizados, como o teor da publicação, a cláusula dos termos de uso que foi violada, o risco envolvido, etc. Caso não exista uma preocupação com a completa anonimização das informações em questão, esses dados podem acabar levando à identificação do usuário e expor até mesmo dados sensíveis como orientação sexual e posição político-partidária.

Ainda assim, o DSA oferece alguns mecanismos que podem mitigar riscos de violação da privacidade dos usuários quando da publicação dos relatórios. Em primeiro lugar, em relação às grandes plataformas, a subseção 33(3) permite que as empresas se abstenham, de forma justificada, de publicar informações confidenciais ou que possam causar danos aos usuários. Ou seja, o DSA delega às plataformas a responsabilidade de zelar pela privacidade dos usuários.

Em segundo lugar, a própria seção de justificativa da proposta fala sobre a necessidade de compatibilizar o novo arranjo regulatório com o *General Data Protection Regulation* (GDPR). A justificativa inclusive exalta o aspecto positivo da transparência para a proteção de dados, afirmando que as informações que serão publicadas pelas plataformas "vão auxiliar as pessoas a exercerem seus direitos enquanto titulares de dados"[33] (tradução livre).

Mais adiante, o documento afirma que "todas as medidas contidas na proposta estão completamente alinhadas com os exigentes requisitos da proteção de dados e da privacidade"[34] (tradução livre). É evidente que apenas uma manifestação genérica não basta para proteger a privacidade dos usuários, mas ao menos isso demonstra que os reguladores estão preocupados com os eventuais pontos de contato (e de tensão) entre o DSA e a disciplina de proteção de dados pessoais.

Em terceiro lugar, a proposta prevê a possibilidade do *Board for Digital Services* - órgão vinculado à União Europeia e responsável por monitorar as atividades dos coordenadores nacionais - cooperar com outros órgãos governamentais e organizações da sociedade civil, mencionando expressamente "grupos de aconselhamento com responsabilidades em campos como [...] o da proteção de dados"[35] (tradução livre). Essa abertura torna o sistema estruturado pelo DSA mais sensível às demandas de especialistas da privacidade de dados.

Por fim, em quarto lugar, a subseção 41(6) da minuta do DSA garante aos Estados o poder de monitorar a ação dos *Digital Services Coordinators* - autoridades independentes nomeadas pelos Estados para supervisionar os serviços abrangidos pelo DSA em uma determinada jurisdição -, especialmente para garan-

tir que sua competência só seja exercida "de acordo com o direito de respeito à vida privada"[36] (tradução livre).

Ou seja, tal como no *Online Safety Bill* do Reino Unido, o DSA busca oferecer um sistema robusto de *checks and balances* para lidar com a tensão entre transparência e proteção de dados durante a operacionalização da regulação, em especial no que diz respeito à formulação e publicação de relatórios de transparência.

1.4. Proteção de dados, moderação de conteúdo e relatórios de transparência

Em sua reunião plenária em março de 2021, o *Steering Committee for Media and Information Society* (Comitê de Direcionamento para Assuntos de Mídia e Sociedade da Informação) do Conselho da Europa adotou um relatório de boas práticas para a estruturação de modelos de auto e co-regulação na área de moderação de conteúdo na Internet. Nas palavras do relatório, "transparência é o elemento mais importante para atingir uma moderação de conteúdo eficiente"[37] (tradução livre).

O Comitê demonstra, acertadamente, que modelos de autorregulação e co-regulação possuem um ônus intrínseco: uma queda em *accountability* e legitimidade democrática no processo de moderação. De outra sorte, o Comitê também entende que estes modelos são importantes e necessários para garantir mais flexibilidade às plataformas e abrir espaço para a inovação tecnológica.[38] É justamente essa tensão que deve ser enfrentada por novos modelos regulatórios.

Assim, como uma forma de equilibrar esses dois fatores, a transparência deve ser usada para garantir acesso aos dados que permitem avaliar se há previsibilidade, necessidade e proporcionalidade nas decisões de moderação de conteúdo. Nas palavras do Comitê, "sem transparência efetiva não é possível identificar e avaliar mudanças ou fazer os ajustes necessários. Assim, sem transparência, a sociedade perde o benefício da auto e co-regulação"[39] (tradução livre).

Ainda assim, o relatório em questão reconhece que outros valores, como o direito à privacidade e à liberdade de expressão, também devem informar a extensão e a aplicação de mecanismos de transparência na área de moderação de conteúdo. Em outras palavras, ainda que a transparência apresente benefícios imprescindíveis ao interesse público, é preciso ter cautela para evitar que a sua prevalência acabe levando à violação de outros direitos e princípios.

Em relação a proteção de dados, o Comitê destaca o fato de que as plataformas precisam tratar diversos dados pessoais para operacionalizar suas atividades de moderação de conteúdo. Ademais, o relatório assevera que "o tratamento desses dados pode incluir categorias especiais de dados como opiniões políticas, associação à sindicatos, crenças religiosas e outras crenças em geral"[40] (tradução livre).

Portanto, a moderação de conteúdo não pode ser dissociada de tratamento de dados pessoais. Ademais, levando em consideração que os usuários de plataformas digitais usam os seus serviços como um importante instrumento de exercício da liberdade de expressão, muitos desses dados acabam revelando características sensíveis desses indivíduos.

Levando em consideração esse contexto, é indispensável que o dever de transparência seja moldado a partir de uma perspectiva de proteção de dados pessoais e de salvaguarda da privacidade dos usuários de plataformas digitais. Ou seja, como o tratamento de dados pessoais (inclusive sensíveis) é um componente inerente da moderação de conteúdo, o avanço da transparência não pode significar um retrocesso em termos de proteção de dados.

Segundo os professores Mike Annany e Kate Crawford, muito se fala em imposição de deveres de transparência enquanto poucos reguladores realmente refletem sobre qual tipo de transparência é desejável diante de um determinado contexto. Ainda, nas palavras dos autores, "este ideal de transparência - enquanto um método para observar, compreender e governar sistemas complexos dentro de um tempo razoável - é limitado de diferentes formas"[41] (tradução livre).

Dentre as diferentes limitações identificadas pelos autores está justamente o fato de que a transparência pode causar danos às pessoas. Como argumentam Ananny e Crawford, "se implementada sem uma noção do motivo pelo qual determinada parte de um sistema deve ser revelada, a transparência pode ameaçar a privacidade e inibir conversas francas"[42] por expor pessoas vulneráveis (tradução livre).

À luz dos deveres de transparência contidos no *Online Safety Bill* e no DSA, é possível afirmar que os reguladores envolvidos na elaboração destas duas propostas buscaram criar certos freios e contrapesos para evitar que o ideal de transparência ameace a privacidade dos usuários.

A transparência no contexto da moderação de conteúdo tem como objetivo garantir valores como *accountability* e confiança além da previsibilidade, necessidade e proporcionalidade das decisões tomadas pelas plataformas. Como ficou demonstrado pelas discussões acima sobre os relatórios de transparência, deve-se buscar dentro do possível determinar a publicação de dados que nos aproximam desses valores sem comprometer a privacidade dos usuários atingidos pela moderação.

Isso não significa, entretanto, que os relatórios de transparência são uma completa novidade. A Access Now mantém um índice de relatórios de transparência publicados por mais de setenta empresas de tecnologia ao redor do mundo desde 2010, quando a Google publicou o seu primeiro relatório[43]. Ainda assim, como notam Daphne Keller e Paddy Leerssen, estes relatórios possuem diversas limitações. Dentre elas estão o fato de que os relatórios apresentam

apenas a perspectiva das próprias plataformas e contam com diferentes categorias de dados, o que dificulta comparações entre os documentos de diferentes empresas[44].

2. DEVER DE TRANSPARÊNCIA NO PL DAS FAKE NEWS

Tal como a União Europeia e o Reino Unido, atualmente o Congresso Nacional no Brasil também debate uma proposta de legislação que busca instituir mecanismos de transparência para plataformas digitais, especialmente provedores de redes sociais e serviços de mensageria privada como WhatsApp[45] e Telegram[46], duas aplicações muito populares no país.

Trata-se da Lei Brasileira de Liberdade, Responsabilidade e Transparência na Internet, popularmente conhecida como 'Lei ou PL das Fake News'[47]. O projeto foi apresentado pelo Senador Alessandro Vieira em maio de 2020 e já sofreu diversas modificações desde que começou a tramitar. No dia 30 de junho de 2021 o PL foi aprovado pelo Senado e encaminhado para a Câmara dos Deputados, onde agora segue em tramitação[48].

É imperioso ressaltar, desde já, que o presente documento irá focar apenas nos relatórios de transparência previstos pelo projeto. Ou seja, a análise a seguir não compreende outros pontos de tensão que existem entre o PL das Fake News e a proteção de dados pessoais e não deve ser lido como um endosso ao projeto como um todo.

Alguns pontos da minuta são incompatíveis com os princípios da LGPD e do Marco Civil da Internet e devem ser devidamente enfrentados pelo Congresso Nacional. Por exemplo, o Art. 7º da minuta permite que plataformas solicitem a apresentação de documento de identidade válido para a autenticação de contas, o que gera preocupações em termos de tratamento de dados desnecessários, vigilantismo na Internet e discriminação[49].

Ainda, outro ponto que merece destaque é o Art. 10º da minuta, que prevê que serviços de mensageria privada devem guardar os registros de mensagens veiculadas em encaminhamentos em massa pelo prazo de três meses. Há aqui, novamente, um ponto de atenção a respeito da proteção de dados pessoais dos usuários destes serviços à luz da LGPD.

Outras críticas ao PL podem ser encontradas nas notas técnicas do ITS Rio[50] e da Coalizão Direitos na Rede (CDR)[51]. Desde então, alguns dos pontos levantados pelo instituto e outras organizações já foram solucionados ou parcialmente endereçados, mas outros merecem mais atenção até hoje, como críticas ao processo legislativo opaco e apressado, impactos negativos à inovação tecnológica, isolamento do Brasil dentro do cenário internacional, imprecisões conceituais, definição problemática de 'conta inautêntica', estímulo à censura, etc.

Feitas estas ressalvas, este relatório seguirá com uma análise tópica e específica de uma das dimensões do PL das Fake News. Dentre os diferentes objetivos que a proposta pretende alcançar está "a busca por maior transparência das práticas de moderação de conteúdos postados por terceiros em redes sociais, com a garantia do contraditório e da ampla defesa" (Art. 4º, inciso III).

Tal como o *Digital Services Act* e o *Online Safety Bill*, o PL das Fake News aposta na publicação de relatórios de transparência pelas plataformas digitais, os quais devem ser escritos em português e "informar os procedimentos e as decisões de tratamento de conteúdos gerados por terceiros no Brasil" (Art. 13).

Ademais, um outro elemento importante da proposta é a previsão de criação, por ato próprio do Congresso Nacional, de um Conselho de Transparência e Responsabilidade na Internet que será responsável por monitorar a implementação da lei no território nacional. Dentre suas atribuições específicas estão a de analisar os relatórios de transparência publicados pelas plataformas e sugerir diretrizes para a moderação de conteúdo.

Veja-se, portanto, que o PL das Fake News guarda paralelos com as duas minutas analisadas anteriormente; de um lado, a proposta brasileira busca concretizar o princípio da transparência com base na publicação de relatórios pelas plataformas com dados sobre moderação de conteúdo enquanto, de outro lado, procura garantir o funcionamento do novo arranjo regulatório ao instituir uma nova entidade responsável por monitorá-lo.

Com base nas conclusões deduzidas da análise do texto do DSA e do *Online Safety Bill*, nas próximas duas subseções serão tecidas algumas considerações sobre os dados que devem ser disponibilizados pelos provedores de redes sociais no Brasil nos termos do PL das Fake News. Ademais, seguindo a metodologia acima, busca-se verificar se há compatibilidade entre a proposta e a disciplina de proteção de dados, especialmente à luz da Lei Geral de Proteção de Dados (Lei n.º 13.709 de 2018).

2.1. Uma análise dos dados que devem ser disponibilizados pelos provedores de redes sociais

Em primeiro lugar, seguindo o princípio da proporcionalidade que emerge de forma mais evidente no DSA europeu, o PL das Fake News estipula em seu Art. 1º, § 1º que as disposições da lei, incluindo a publicações de relatórios de transparência, não se aplicam às plataformas que tenham menos de 2 milhões de usuários brasileiros registrados[52].

Para as demais plataformas existe a obrigação, nos termos do Art. 13, de publicar a cada trimestre um relatório em português com dados sobre "os procedimentos e as decisões de tratamento de conteúdos gerados por terceiros no Brasil". Segundo o § 1º do referido artigo, os relatórios devem conter no mínimo dez categorias diferentes de dados, incluindo:

- Número de usuários brasileiros que acessam a plataformas e que estão ativos no serviço;
- Número de ‘medidas de moderação’ adotadas com base nos termos de uso da plataforma, no cumprimento da Lei ou no cumprimento de ordem judicial, sempre especificando as motivações para a decisão;
- Número de contas automatizadas e de ‘redes de distribuição artificial’ detectadas no serviço e as medidas adotadas após a detecção;
- Número de decisões de moderação que foram revertidas pela plataforma, incluindo remoção de conteúdo e suspensão de contas;
- Média de tempo entre a detecção de um conteúdo e a adoção das medidas de restrição;
- Dados sobre o engajamento em torno de conteúdos ‘irregulares’ (por exemplo, visualizações, compartilhamentos e alcance geral);
- Informações sobre a atualização dos termos de uso que foram feitas no último trimestre, além das justificativas para cada mudança.

Em geral há diversas áreas de convergência entre as categorias de dados que devem estar nos relatórios de transparência segundo o PL das Fake News e as outras duas propostas analisadas neste relatório. Destaca-se principalmente as estatísticas sobre o processo de moderação de conteúdo, passando também por uma preocupação específica com comportamento inautêntico[53] nas redes e a divulgação das motivações por trás de decisões específicas.

Nada obstante, o projeto também inova em duas ocasiões que merecem mais atenção. Em primeiro lugar, o Art. 13, § 1º, inciso VII determina que os relatórios também devem conter informações sobre “características gerais do setor responsável por políticas aplicáveis a conteúdos gerados por terceiros, incluindo

informações sobre a qualificação, a independência e a integridade das equipes de revisão de conteúdo".

Estes são dados importantes sobre a moderação de conteúdo, principalmente em países do Sul Global que não falam inglês como língua oficial ou costumeira. Há interesse em confirmar, por exemplo, quantos membros deste setor são lusófonos e conhecem o contexto político e social do Brasil. Isso permite que as autoridades públicas verifiquem até que ponto o contexto específico do país está sendo levado em consideração durante o processo de moderação de conteúdo.

Em segundo lugar, o Art. 13, § 1º, inciso X aduz que os relatórios também deverão conter descrições das "atualizações das políticas e termos de uso feitas no trimestre, a data da modificação e a justificativa para a sua adoção".

Considerando, por exemplo, que há plataformas que ainda disponibilizam alguns trechos de seus padrões da comunidade em inglês no Brasil - conforme demonstrou pesquisa anterior do ITS Rio[54] -, a obrigação de publicar estas atualizações em português por meio dos relatórios trimestrais promoverá mais *accountability* e confiança na moderação de conteúdo por parte do público brasileiro.

Ademais, para atuar como órgão de supervisão desta nova regulação, o PL prevê em seu Art. 25 a criação do Conselho de Transparência e Responsabilidade na Internet (CTRI) que, nos termos da proposta, "terá como atribuição a realização de estudos, pareceres e recomendações sobre liberdade, responsabilidade e transparência na internet".

Entre as competências específicas do conselho, o parágrafo único do Art. 25 cita o poder de "avaliar os dados constantes nos relatórios" (inciso III) e "avaliar os procedimentos de moderação adotados pelos provedores de redes sociais, bem como sugerir diretrizes para sua implementação" (inciso VIII). O conselho é um órgão multissetorial composto por 21 conselheiros, incluindo representantes da sociedade civil, da academia, do setor de telecomunicações e outros (Art. 26).

Ainda assim, cumpre destacar que, diferentemente dos órgãos de supervisão previstos pelo *Online Safety Bill* e DSA, o CTRI carece de independência e autonomia. O Conselho será criado pelo próprio Congresso Nacional e todos os seus membros são indicados pelo Poder Legislativo. Ademais, suas despesas estão vinculadas ao orçamento do Senado Federal. Ainda que seja multissetorial em sua composição, a proximidade com o Congresso representa uma limitação à esfera de atuação do Conselho.

Por fim, o PL também prevê a possibilidade das plataformas criarem uma "instituição de autorregulação voltada à transparência" (Art. 30) que seria certificada pelo CTRI (Art. 30, § 1º) e teria a responsabilidade de elaborar e encaminhar ao conselho os relatórios trimestrais de transparência (Art. 30, § 2º), além de aprovar "resoluções e súmulas de modo a regular seus procedimentos de análise" (Art. 30, § 3º).

2.2. Diálogo internacional a respeito da tensão e harmonização entre a implementação de deveres de transparência e a proteção de dados pessoais

Assim como o DSA e o *Online Safety Bill*, o PL das Fake News traz algumas considerações sobre a proteção da privacidade e dados pessoais dentro deste novo arranjo regulatório. Em primeiro lugar, o Art. 2º afirma que a nova lei deve levar em consideração os princípios e as garantias previstas em diplomas como o Marco Civil da Internet e a Lei Geral de Proteção de Dados Pessoais.

Em segundo lugar, o Art. 3º, inciso II diz que a lei deve ser pautada pela "garantia dos direitos da personalidade, da dignidade, da honra e da privacidade do indivíduo". Ou seja, o próprio PL reconhece que suas disposições devem estar alinhadas com os preceitos da disciplina de proteção de dados pessoais, evitando, assim, que o fortalecimento de uma esfera de proteção signifique a violação de outra.

Em terceiro lugar, o Art. 13, § 5º permite que as plataformas se abstenham de disponibilizar certas informações em seus relatórios trimestrais de transparência desde que apresentem "justificativa técnica adequada". O legislador não dá detalhes sobre o que configura ou não uma justificativa técnica, mas é possível que uma plataforma retenha certas informações que podem violar a privacidade de seus usuários com base neste dispositivo. Ainda assim, como argumentado abaixo, seria importante que este dispositivo tivesse um foco mais pontual em proteção de dados.

Em quarto lugar, além de publicar relatórios de transparência, o Art. 13, § 6º prevê que as plataformas devem "facilitar o compartilhamento de dados com instituições de pesquisa acadêmica" mas que, ao assim proceder, precisam resguardar "o respeito à proteção de dados pessoais".

Ainda assim, à luz dos mecanismos analisados anteriormente que fazem parte do DSA - em especial a atuação do *Board for Digital Services* e dos *Digital Services Coordinators* - e do *Online Safety Bill* - em especial a atuação do OFCOM e do Secretário de Estado -, o sistema que visa resguardar a privacidade no PL das Fake News não parece ser robusto o suficiente a ponto de estruturar um verdadeiro modelo de *checks and balances*.

Como demonstram os professores Gorwa e Ash, "a efetiva transparência geralmente precisa ser sustentada por supervisão regulatória"[55] (tradução livre). Ou seja, de nada adianta determinar a publicação de relatórios de transparência se não existirem entidades dedicadas para analisar esses dados, agir de acordo com as evidências e corrigir eventuais distorções para evitar que a operacionalização da transparência viole outros direitos e interesses.

Por exemplo, o *Online Safety Bill* prevê que, no exercício das suas funções, o OFCOM deve consultar especialistas em privacidade e proteção de dados e que

o Secretário de Estado, ao revisar o arranjo regulatório no futuro, deverá avaliar se os usuários estão devidamente protegidos contra violações de sua vida privada.

O DSA, ao seu turno, garante ao *Board for Digital Services* a prerrogativa de cooperar com grupos de aconselhamento sobre questões de proteção de dados pessoais, além de mencionar que os Estados devem monitorar a atuação dos *Digital Services Coordinators* para garantir que suas atribuições sejam exercidas sem implicar na violação do direito à privacidade.

Ainda que o PL das Fake News preveja a criação do Conselho de Transparência e Responsabilidade na Internet e das chamadas 'instituições de autorregulação' pelas plataformas, não há nenhuma garantia direta de que estes órgãos atuarão em defesa da proteção de dados e da privacidade. Faltam, portanto, freios e contrapesos nos moldes das propostas do Reino Unido e da União Europeia.

Para preencher esta lacuna no texto do PL, uma primeira mudança poderia ser feita na composição do CTRI. Atualmente a proposta que está sendo debatida na Câmara dos Deputados prevê a criação de um conselho multissetorial com representantes das seguintes entidades e setores: Senado Federal, Câmara dos Deputados, CNJ, CNMP, CGI.br, sociedade civil, academia e comunidade técnica, provedores de acesso, aplicações e conteúdo da Internet, comunicação social, telecomunicações, Conselho Nacional dos Chefes da Polícia Civil, Departamento da Polícia Federal, Anatel e Conar.

É imprescindível que o Conselho também conte com representantes da sociedade civil (incluindo acadêmicos) que atuem diretamente com proteção de dados pessoais e privacidade, além de representantes da Autoridade Nacional de Proteção de Dados (ANPD). Esse seria um importante passo para garantir que o CTRI vai considerar os impactos à disciplina da proteção de dados quando, por exemplo, analisar os relatórios de transparência e sugerir diretrizes para a moderação de conteúdo de plataformas no Brasil.

Ademais, a própria natureza jurídica do Conselho precisa ser repensada. Atualmente, a previsão legal é que o CTRI seja criado por ato próprio do Congresso Nacional, seus membros indicados exclusivamente pelo Poder Legislativo e suas despesas atreladas ao orçamento do Senado Federal. Isso diminui consideravelmente a autonomia e independência do Conselho, duas características que estão presentes na estrutura do OFCOM, do *Board for Digital Services* e dos *Digital Services Coordinators*.

Além disso, uma segunda mudança poderia ser feita no Art. 30 do PL para estipular expressamente que, dentre as diferentes atribuições já previstas pelo artigo, as instituições de autorregulação que podem ser criadas pelos provedores de redes sociais também devem prezar pela privacidade e proteção de dados pessoais dos usuários quando da elaboração dos relatórios de transparência, especialmente os dados sensíveis, optando, sempre que possível, pela anoni-

mização dos dados em conformidade com a LGPD[56] e as futuras regulações da ANPD[57]. Ou seja, as instituições de autorregulação também devem ter como valor cardinal a proteção de dados.

Por fim, uma terceira mudança poderia ser feita no Art. 13 do PL para reservar às plataformas o direito de não disponibilizar, sempre mediante justificativa, dados em desacordo com os princípios e regras da LGPD. Afinal, na qualidade de agentes de tratamento de dados pessoais, muitos deles sensíveis, as plataformas também possuem a obrigação legal de zelar pelos direitos dos titulares de dados no Brasil. Isso pode ser feito através da interpretação de que a "justificativa técnica" mencionada pelo Art. 13, § 5º compreende violações à privacidade.

CONSIDERAÇÕES FINAIS

Este relatório se ateve a uma análise dos relatórios de transparência que podem ser instituídos no Brasil, na União Europeia e no Reino Unido caso, respectivamente, o PL das Fake News, o *Digital Services Act* e o *Online Safety Bill* sejam aprovados e entrem em vigor num futuro próximo. Trata-se, portanto, de um debate dinâmico e que ainda está se desenrolando em diferentes jurisdições ao redor do globo.

Assim, o atual cenário oferece uma oportunidade singular de avaliar as nuances dessas obrigações de transparência em moderação de conteúdo a partir de uma visão comparativa. O diálogo entre os diferentes arranjos regulatórios é essencial para avaliar quais salvaguardas devem ser instituídas para evitar tensões negativas entre a transparência enquanto mecanismo de *accountability* em plataformas digitais e outras esferas de proteção de direitos.

Dentre as diferentes dimensões presentes neste debate, o relatório focou no possível atrito entre os relatórios de transparência e a esfera da privacidade e proteção de dados pessoais. Em suma, partindo do pressuposto de que a moderação de conteúdo na Internet envolve o tratamento de diversos dados pessoais dos usuários - incluindo dados sensíveis -, a transparência emerge como um mecanismo que, sem freios ou limites pré-estabelecidos, pode violar a privacidade destes mesmos usuários.

Foi notado, entretanto, que a transparência também pode reforçar a proteção de dados ao oferecer informações às quais o titular de dados não teria acesso antes. Nesse sentido, determinados aspectos da transparência dão sustentação ao fundamental direito à autodeterminação informativa. Essa constatação apenas reforça a necessidade de instituir um sistema de freios e contrapesos que evite a violação da privacidade pela transparência; ao neutralizar esse perigo, o legislador pode garantir a prevalência do referido benefício.

Após a análise do DSA e do *Online Safety Bill*, é possível perceber que os dois projetos apostam em um sistema de *checks and balances* que envolve a participação de diversos atores independentes entre si - alguns cuja criação é prevista pelo próprio texto. Estas entidades devem prezar pela privacidade e proteção de dados pessoais durante o exercício de suas atividades, inclusive a partir de consultas com especialistas.

É difícil antecipar como essa arquitetura regulatória funcionará na prática e se os mecanismos já previstos serão suficientes para evitar impactos negativos sobre a proteção de dados na União Europeia e no Reino Unido. Ainda assim, uma análise preliminar permite concluir que reguladores levaram esse ponto em consideração e buscaram inserir instrumentos de proteção no texto das propostas.

De outra sorte, ao olhar para o PL das Fake News com este contexto em mente, este relatório constatou que o projeto brasileiro carece de alguns desses

instrumentos. Três principais mudanças precisam ser implementadas para que o PL atinja níveis semelhantes de proteção da privacidade e dados pessoais como aqueles vistos no DSA e no *Online Safety Bill*. São elas:

- Modificar a estrutura do Conselho de Transparência e Responsabilidade na Internet para que ele seja mais responsivo às demandas da proteção de dados pessoais, além de repensar sua criação para reforçar sua autonomia e independência;

- Atribuir às instituições de autorregulação, quando da elaboração dos relatórios de transparência, a obrigação de antecipar possíveis consequências negativas à proteção de dados e proteger a privacidade dos usuários, optando sempre que possível pela anonimização dos dados;

- Reservar às plataformas o direito de não disponibilizar, sempre mediante justificativa, dados em desacordo com os princípios e regras da LGPD.

Isso não significa, entretanto, que, uma vez adotadas essas medidas, o mecanismo de transparência proposto pelo PL se tornaria compatível com a LGPD ou poderia ser considerado a solução ideal para o contexto brasileiro. O presente estudo se limitou tão somente a uma discussão sobre os relatórios de transparência previstos pelo projeto. Outras preocupações permanecem e devem ser enfrentadas pelo Congresso Nacional, como a apresentação de documento de identidade válido para a autenticação de contas e a guarda de registros de mensagens veiculadas em encaminhamentos em massa, entre outros já mencionados em outros momentos e remarcados por outras organizações da sociedade civil.

ANEXO - TABELA COMPARATIVA DAS CATEGORIAS DE DADOS PRESENTES NOS RELATÓRIOS DE TRANSPARÊNCIA

RELATÓRIOS DE TRANSPARÊNCIA	ONLINE SAFETY BILL	DIGITAL SERVICES ACT	PL FAKE NEWS
Conteúdos ilegais identificados nas plataformas	√	√	√
Casos de comportamento automatizado detectados no serviço		√	√
Ordens recebidas de autoridades governamentais e cooperação com órgãos públicos	√	√	
Medidas de moderação adotadas com base nos termos de uso das plataformas	√	√	√
Medidas adotadas pelas plataformas a respeito de proteção das crianças	√		
Notificações recebidas a partir de mecanismos internos de reclamação	√	√	
Notificações recebidas por indivíduos ou entidades externas		√	
Medidas de educação midiática (media literacy) dos usuários	√		
Atividades de moderação de iniciativa própria das plataformas		√	
Suspensões aplicadas pelas plataformas		√	√
Usuários ativos nas plataformas		√	√
Atualização dos termos de uso no último trimestre			√
Disputas submetidas às entidades externas de resolução de disputas		√	
Disseminação, distribuição e engajamento com conteúdos irregulares e/ou ilegais	√		√
Sistemas de denúncia disponibilizados aos usuários	√	√	
Uso de mecanismos automatizados de moderação de conteúdo		√	
Medidas de mitigação de riscos adotadas pelas plataformas	√	√	
Auditoria contratada pelas próprias plataformas		√	
Análise de riscos sistêmicos na plataforma	√	√	
Decisões de moderação que foram revertidas pelas plataformas		√	√
Média de tempo entre a detecção de um conteúdo e a adoção das medidas de restrição			√

NOTAS

1. . BRANDEIS, Louis D. What Publicity Can Do. Harper's Weekly, 20 de dezembro de 1913. Disponível em <https://bit.ly/2RDPC66>

2. . GORWA, Robert; ASH, Timothy Garton. Democratic Transparency in the Platform Society. In PERSILY, Nathaniel; TUCKER, Joshua A. Social Media and Democracy: The State of the Field, Prospects for Reform. Cambridge: Cambridge University Press, 2020, 286-312, 290.

3. . WARREN, Samuel D. BRANDEIS, Louis D. The Right to Privacy. Harvard Law Review, v. 4, n. 5, 1890, 193-220.

4. . .Ibid., p. 195-96.

5. . O Online Safety Bill foca em dois tipos de danos que são genericamente definidos em suas seções 45 e 46 como, respectivamente, "conteúdo danoso para crianças" e "conteúdo danoso para adultos". Isso inclui, portanto, as mais variadas categorias de danos que podem ocorrer no ambiente digital, como exploração e abuso de crianças, conteúdo e atividade terrorista, pornografia não consensual, crimes de ódio, cyberbullying, desinformação, dentre outros. Para uma lista de possíveis online harms ver Minister of State for Digital and Culture. Online Harms White Paper. Londres, 2019, pp. 30-2. Disponível em <https://bit.ly/2UPdmW1>

6. . O termo "segurança online" deve ser interpretado de forma ampla e não se restringe a conceitos como segurança da informação, segurança cibernética ou segurança pública.

7. . Comissão Europeia. Proposal for a Regulation of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act) and amending Directive 2000/31/EC. Bruxelas, 2020, p. 2. Disponível em <https://bit.ly/3gWQqvj>.

8. . Ibid., p. 26.

9. . BLANKERTZ, Aline; JAURSCH, Julian. What the European DMA and DSA Proposals Mean for Online Platforms. Brookings Tech Stream, 14 de Janeiro, 2021. Disponível em <https://brook.gs/3gQCynw>.

10. . Os autores utilizam originalmente o termo "Public Health", que em português poderia ser traduzido para "Saúde Pública". Nada obstante, buscando uma maior clareza conceitual, optamos por traduzir para "Bem-Estar Público". Em inglês o termo se refere à saúde em sentido amplo, abrangendo diversos riscos que estão associados ao uso de plataformas digitais, como desinformação, bullying, assédio, dentre outros. Assim, a ideia de bem-estar em português parece refletir com mais exatidão o objetivo dos autores.

11. . BOWERS, John; ZITTRAIN, Jonathan. Answering Impossible Questions: Content Governance in an Age of Disinformation. The Harvard Kennedy School Misinformation Review, v. 1, n. 1, 2020.

12. .Ibid., p. 2.

13. . ESTARQUE, Marina; ARCHEGAS, João Victor. Redes Sociais e Moderação de Conteúdo: Criando regras para o debate público a partir da esfera privada. Instituto de Tecnologia e Sociedade do Rio de Janeiro, 2020, p. 19.

14. . CADWALLADR, Carole; GRAHAM-HARRISON, Emma. Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. The Guardian, 17 de março, 2018. Disponível em <https://bit.ly/3qknEsQ>.

15. . CHEN, Adrian. The Agency. The New York Times Magazine, 2 de junho, 2015. Disponível em <https://nyti.ms/3gV5vxC>.

16. BOWERS, John; ZITTRAIN, Jonathan. Answering Impossible Questions: Content Governance in an Age of Disinformation. The Harvard Kennedy School Misinformation Review, v. 1, n. 1, 2020, p. 4.

17. Ibid., p. 5.

18. JEEVANJEE, Kiran et al. All the Ways Congress Wants to Change Section 230. Slate, 23 de março, 2021. Disponível em <https://bit.ly/2UraCOd>.

19. LAUX, Francisco de Mesquita. O Supremo Tribunal Federal debate o artigo 19 d

20. SOUZA, Carlos Affonso. Decreto de Bolsonaro inverte lógica ao impedir moderação de contas e criar index do que pode ser removido na Internet. Folha de S.Paulo, 20 de maio de 2021. Disponível em <https://bit.ly/3r55s77>.

21. SHIELDS, Todd; BRODY, Ben. Washington's Knives Are Out for Big Tech's Social Media Shield. Bloomberg, 11 de agosto, 2020. Disponível em <https://bloom.bg/3vVxti2>.

22. BOWERS, John; ZITTRAIN, Jonathan. Answering Impossible Questions: Content Governance in an Age of Disinformation. The Harvard Kennedy School Misinformation Review, v. 1, n. 1, 2020, p. 5.

23. Ibid., pp. 5-6.

24. O Online Safety Bill traz em sua "Schedule 1" alguns serviços que estão fora do escopo da regulação e, por isso, são considerados isentos, como os serviços user-to-user onde os únicos conteúdos compartilhados pelos usuários são e-mails ou mensagens SMS.

25. Dado anonimizado é aquele que, embora diga respeito a um titular de dados pessoais, não permite a identificação do sujeito com base na instrumentalização dos meios técnicos que estão disponíveis no momento do tratamento. Em outras palavras, trata-se do dado pessoal que se tornou anônimo e, portanto, deixa de se relacionar a uma pessoa identificada ou identificável.

26. Minister of State for Digital and Culture. Draft Online Safety Bill. Londres, 2021, pp. 44-5. Disponível em <https://bit.ly/3h0LxBj>.

27. Ibid., p. 11.

28. Ibid., p. 101.

29. Comissão Europeia. Proposal for a Regulation of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act) and amending Directive 2000/31/EC. Bruxelas, 2020, p. 6. Disponível em <https://bit.ly/3gWQqvj>.

30. Ibid., p. 31.

31. Ibid, p. 26.

32. Comissão Europeia. Proposal for a Regulation of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act) and amending Directive 2000/31/EC. Bruxelas, 2020, p. 58. Disponível em <https://bit.ly/3gWQqvj>.

33. Ibid., p. 5.

34. Ibid., p. 13.

35. Ibid., p. 40.

36. Ibid., p. 71.

37. Conselho da Europa. Content Moderation: Best practices towards effective legal and procedural frameworks for self-regulatory and co-regulatory mechanisms of content moderation. Bruxelas, Junho de 2021, p. 46. Disponível em <https://bit.ly/3zUUAwi>.

38. Ibid., pp. 42-3.

39. Ibid., p. 43.

40. Ibid., p. 30.

41. ANANNY, Mike; CRAWFORD, Kate. Seeing without knowing: Limitations of the transparency ideal and its application to algorithmic accountability. New Media & Society, v. 20, n. 3, 2018, p. 977.

42. Ibid., p. 978.

43. Access Now. Transparency Reporting Index. Disponível em <https://bit.ly/3xrKVM9>.

44. KELLER, Daphne; LEERSSEN, Pady. Facts and Where to Find Them: Empirical Research on Internet Platforms and Content Moderation. In PERSILY, Nathaniel; TUCKER, Joshua A. Social Media and Democracy: The State of the Field, Prospects for Reform. Cambridge: Cambridge University Press, 2020, 220-251, 228-9.

45. Segundo dados de 2020, o WhatsApp está instalado em 99% dos celulares no Brasil e 93% dos brasileiros usam o aplicativo todos os dias. VENTURA, Felipe. WhatsApp chega a 99% dos celulares do Brasil; Telegram cresce. Tecnoblog, 27 de fevereiro de 2020. Disponível em <https://bit.ly/3dfVjhV>.

46. Segundo dados de 2021, o Telegram está presente em 45%

dos celulares brasileiros. FABRO, Clara. Telegram cresce e está em 45% dos celulares de brasileiros, diz pesquisa. TechTudo, 08 de março de 2021. Disponível em <https://glo.bo/3y7kb3J>.

47. A versão atualizada do PL que serviu de base para este relatório durante sua escrita em julho de 2021 pode ser acessada em <https://bit.ly/3halnMR>.

48. CRUZ, Bruna Souza. PL das Fake News: Aprovado no Senado, entenda o que pode mudar. Tilt UOL, 30 de junho de 2021. Disponível em <https://bit.ly/3xUEy40>.

49. Embora o projeto já tenha sofrido alterações desde então, algumas das críticas apresentadas por Carlos Affonso Souza em 2020 ainda merecem destaque. SOUZA, Carlos Affonso. PL das Fake News vai impedir 1 em cada 5 brasileiros de usar redes sociais. Tilt UOL, 25 de junho de 2020. Disponível em <https://bit.ly/3h3vnIH>.

50. A Nota Técnica sobre os Projetos de Lei nº 2927/2020 (Câmara) e nº 2630/2020 (Senado) do ITS Rio pode ser acessada em <https://bit.ly/2Ta3ZzT>.

51. A Nota Técnica da CDR sobre o Projeto de Lei nº 2630/2020 (Senado) intitulada “Combater desinformação assegurando liberdade de expressão e privacidade” pode ser acessada em <https://bit.ly/3hnjRrR>.

52. É de se questionar, entretanto, o real impacto desse recorte regulatório. Afinal, nenhuma plataforma é criada para ser pequena; seus fundadores estão sempre atrás de novos usuários. Com o tempo, as obrigações contidas no DSA passarão a abranger uma considerável parte das plataformas digitais.

53. Segundo os padrões da comunidade do Facebook, comportamento inautêntico nas redes consiste em usar ativos, como contas e páginas, para enganar outros usuários e a própria plataforma sobre sua identidade, a popularidade de um conteúdo, seu objetivo, a fonte ou a origem de um conteúdo e para evitar a aplicação das políticas da empresa. Os padrões da comunidade podem ser acessados em <https://bit.ly/35ZQg1b>.

54. ESTARQUE, Marina; ARCHEGAS, João Victor. Redes Sociais e Moderação de Conteúdo: Criando regras para o debate público a partir da esfera privada. Instituto de Tecnologia e Sociedade do Rio de Janeiro, 2020.

55. GORWA, Robert; ASH, Timothy Garton. Democratic Transparency in the Platform Society. In PERSILY, Nathaniel; TUCKER, Joshua A. Social Media and Democracy: The State of the Field, Prospects for Reform. Cambridge: Cambridge University Press, 2020, 286-312, 291.

56. Segundo o Art. 5º, inciso XI da LGPD, a anonimização consiste na “utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo” e é um direito do titular de dados nos termos do Art. 18, inciso IV do mesmo diploma legal.

57. Segundo o Art. 12, § 3º da LGPD, “a autoridade nacional poderá dispor sobre padrões e técnicas utilizados em processos de anonimização e realizar verificações acerca de sua segurança, ouvido o Conselho Nacional de Proteção de Dados Pessoais”.

58. Em seu artigo 18, o DSA prevê que os Estados-membro deverão estabelecer ou certificar a atuação de out-of-court dispute settlement bodies que terão a competência de julgar disputas entre as plataformas e seus usuários no contexto da moderação de conteúdo na hipóteses desses casos não serem resolvidos in-house.

SOBRE OS AUTORES

João Victor Archegas

Mestre em direito constitucional comparado pela Universidade de Harvard. Foi Gammon Fellow por mérito acadêmico na Harvard Law School. Ex-aluno do Columbia Summer Program in American Law na Universidade de Leiden. É pesquisador da área de Direito e Tecnologia do Instituto de Tecnologia e Sociedade do Rio de Janeiro (ITS Rio).

Celina Bottino

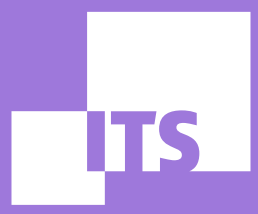
Mestre em direitos humanos pela Universidade de Harvard. Foi pesquisadora da Human Rights Watch em Nova York. Supervisora da Clínica de Direitos Humanos da FGV Direito-Rio. Foi consultora da Clínica de Direitos Humanos de Harvard e pesquisadora do ISER. Diretora de projetos do Instituto de Tecnologia e Sociedade do Rio de Janeiro (ITS Rio).

Christian Perrone

Pesquisador Fulbright (Universidade de Georgetown, EUA). Doutorando em Direito Internacional (UERJ); Mestre em Direito Internacional (L.L.M/Universidade de Cambridge, Reino Unido). Ex-Secretário da Comissão Jurídica Interamericana da OEA. Coordenador da área de Direito e Tecnologia no Instituto de Tecnologia e Sociedade do Rio de Janeiro (ITS Rio).

Mariana Haddad Vilhena

Estudante de Direito na Universidade do Estado do Rio de Janeiro (UERJ); foi integrante da Equipe de Arbitragem da UERJ como oradora em competições internacionais de arbitragem simulada referentes ao Willem C. Vis International Commercial Arbitration Moot; Estagiária na Equipe de Direito e Tecnologia no Instituto de Tecnologia e Sociedade do Rio de Janeiro (ITS Rio).



Esse relatório contou com o generoso apoio financeiro do Reino Unido através de programa *Digital Access*

Acesse nossas redes

itsrio.org