# Rastreabilidade, metadados e direitos fundamentais:

## Nota técnica sobre o Projeto de Lei 2630/2020

DataPrivacyBR
*Research*

## Ficha técnica

O **Data Privacy Brasil** é um espaço de intersecção entre a escola Data Privacy Ensino e a entidade civil Associação Data Privacy Brasil de Pesquisa. Este relatório foi produzido exclusivamente pela Associação. A Associação Data Privacy Brasil de Pesquisa é uma entidade civil sem fins lucrativos sediada em São Paulo. A organização dedica-se à interface entre proteção de dados pessoais, tecnologia e direitos fundamentais, produzindo pesquisas e ações de incidência perante o sistema de Justiça, órgãos legislativos e governo. A partir de uma Política de Financiamento Ético e Transparência, a associação desenvolve projetos estratégicos de pesquisa em proteção de dados pessoais, mobilizando conhecimentos que podem ajudar reguladores, juízes e profissionais do direito a lidar com questões complexas que exigem conhecimento profundo sobre como tecnologias e sistemas sócio-técnicos afetam os direitos fundamentais. A Associação possui financiamento de filantropias internacionais como Ford Foundation, Open Society Foundations e AccessNow. Para mais informações, visite www.dataprivacybr.org.


**Diretores**
Bruno Bioni e Rafael Zanatta

**Coordenadora Geral de Projetos**
Mariana Rielli

**Líder Geral de Projetos**
Marina Meira

**Coordenadores**
Daniela Dora Eilberg e Helena Secaf

**Analista de Incidência**
Vinícius Silva

**Pesquisadores**
Brenda Cunha, Gabriela Vergili, Hana Mesquita, Jaqueline Pigatto, Júlia Mendonça, Marina Garrote, Mikael Servilha, Nathan Paschoalini, Pedro Saliba e Thaís Aguiar

**Administrativo e Comunicação**
Erika Jardim, Fabrício Sanchez, Gustavo Reis, João Paulo Vicente, Júlio Araújo, Rafael Guimarães, Roberto Júnior e Victor Scarlato

**Imprensa**
Para esclarecimentos sobre o documento e entrevistas, entrar em contato com a Associação pelo e-mail imprensa@dataprivacybr.org

**Como citar este documento**
AGUIAR, Thaís; BIONI, Bruno; FAVARO, Iasmine; KITAYAMA, Marina; RIELLI, Mariana; VERGILI, Gabriela; ZANATTA, Rafael. Rastreabilidade, metadados e direitos fundamentais: nota técnica sobre o Projeto de Lei 2360/2020. São Paulo: Data Privacy Brasil, 2021. Edição revisada e ampliada por AGUIAR, Thaís; BIONI, Bruno; MESQUITA, Hana; PIGATTO, Jaqueline; VERGILI, Gabriela.



**Licença**
Creative Commons
É livre a utilização, circulação, ampliação e produção de documentos derivados desde que citada a fonte original e para finalidades não comerciais.

# Rastreabilidade, metadados e direitos fundamentais: Nota técnica sobre o Projeto de Lei 2630/2020

Primeira versão: 24 de julho de 2020
Segunda versão: 05 de outubro de 2021

## Sumário Executivo

A presente nota técnica da Associação Data Privacy Brasil de Pesquisa analisa os riscos para liberdades civis e direitos fundamentais oriundos do Projeto de Lei 2630/2020, chamada de "Lei Brasileira de Liberdade, Responsabilidade e Transparência na Internet", aprovada no Senado Federal e atualmente em discussão na Câmara dos Deputados.

A nota técnica analisa em detalhes a solução de rastreabilidade de encaminhamentos de mensagens em aplicações de internet (e.g. Whatsapp, Telegram e Signal). A perspectiva adotada centra-se no exame de proporcionalidade da medida para direitos fundamentais, considerando seu objetivo de assegurar a integridade do ambiente informacional, ao mesmo tempo em que promove retenção de uma quantidade massiva de dados pessoais.

No arranjo proposto pelo Senado Federal, se uma mesma mensagem for compartilhada de forma idêntica por mais de cinco pessoas e atingir mais de mil pessoas em um aplicativo com mais de 2 milhões de usuários, deve-se reter as informações de data, hora, endereço I.P. (Internet Protocol), bem como a identificação dos que transmitiram a mensagem e o número de pessoas impactadas. Os defensores argumentam que essa é uma medida necessária para viabilizar investigações criminais. Críticos apontam que a medida carece de eficácia, aumenta o vigilantismo e viola direitos constitucionais.

A partir de uma análise aprofundada da literatura, do debate sobre o projeto de lei na mídia especializada e dos novos parâmetros constitucionais de proteção de dados pessoais no Brasil, a presente nota técnica defende que:

- A retenção preventiva indiscriminada e generalizante de metadados flexibiliza garantias constitucionais ao considerar toda a população como suspeita e, portanto, entra em rota de colisão com o princípio da presunção de inocência;

- O aumento do dever de retenção de metadados, em especial a tentativa de obtenção de dados da porta lógica, não é tecnologicamente neutro e colide com as garantias asseguradas no Marco Civil da Internet;

- A ideia de identificar quem é o autor de um "conteúdo ilícito" que circula em uma plataforma ignora o fato de que muitas vezes os conteúdos são compartilhados entre plataformas (vídeos do Youtube são compartilhados no Whatsapp, do mesmo modo que prints de Twitter são compartilhados no Facebook), por vezes eliminando a possibilidade de identificação precisa de autoria de conteúdo;

- Ao criar um sistema rígido ou uma padronização para a rastreabilidade de mensagens, é provável que isso abra a oportunidade de técnicas para "enganar o sistema" (*game the system*);

- A análise custo-benefício se mostra frustrada. As vantagens não são grandes o suficiente, considerando os problemas fundamentais de orientação da medida (a expectativa de identificar a autoria não será possível) e o fato de que a rastreabilidade afetará provavelmente um número grande de jornalistas, ativistas e pessoas comuns, ao mesmo tempo em que permitirá que técnicas para burlar o sistema sejam utilizadas por grupos e indivíduos com intenções maliciosas cuja atividade já é profissionalizada;

- O metadado é uma espécie de "envelope" do processo comunicacional e engloba vários tipos de dados (i.e. dados sobre o usuário que realiza a comunicação, localização, tipo de mensagem, a rede utilizada, horário, duração). Por isso, fornece uma alta quantidade e variedade de informações que, quando agregadas e analisadas, podem chegar a permitir um perfilhamento comportamental do indivíduo bastante intrusivo;

- Metadados detêm um certo tipo de valor agregado para fins de vigilância que decorre de sua alta confiabilidade. Isto porque, na medida em que são dados gerados pelo próprio sistema operacional, não são facilmente alteráveis;

- Em suma, medidas que exigem o monitoramento e armazenamento de dados sobre mensagens (metadados) geram mais riscos do que benefícios, ainda que haja critérios para esse rastreamento.

- A última versão desta nota técnica[1] compara 04 (quatro) propostas, que alargam o dever de retenção de dados de forma preventiva e prospectiva de metadados no ordenamento jurídico brasileiro, sob qual é o seu respectivo grau de **interferência em liberdades e direitos fundamentais**:

  I. **Proposta A (altíssima)[2]:** É questionável a eficácia da proposta em vista da série de métodos possíveis que burlariam (gamificariam)[3] a rastreabilidade da cadeia de desinformação. Além disso, o dever de retenção de dados preventivo vai de encontro a uma série de direitos e liberdades fundamentais como da presunção de inocência, liberdade de expressão e direito de reunião de todos os usuários dos serviços de mensageria atingidos pelo dispositivo. Em suma, a análise custo-benefício se mostra frustrada.

  II. **Proposta B (altíssima)[4]**: Esta proposta não traz muitos avanços em termos da proteção dos direitos fundamentais e, em especial, à proteção de dados pessoais, em relação à proposta original. É também questionável a eficácia da proposta em vista da série de métodos possíveis que burlariam (gamificariam) a rastreabilidade da cadeia de desinformação. Além disso, o dever de retenção de dados preventivo vai de encontro a uma série de direitos e liberdades fundamentais como da presunção de inocência, liberdade de expressão e direito de reunião de todos os usuários dos serviços de mensageria atingidos pelo dispositivo. No mais, a proposta falha ao não se basear nos preceitos do Marco Civil da Internet e da Lei Geral de Proteção de Dados Pessoais como a exigência de consentimento informado, livre, inequívoco e expresso, e princípios da proteção de dados como a minimização.

  III. **Proposta C (média)[5]**: frente às duas propostas anteriores, esta está mais alinhada ao princípio da presunção de inocência uma vez que prevê a retenção

**1** Esta nota técnica é uma atualização feita em outubro de 2021, onde o principal objeto foi o quadro comparativo das propostas mencionadas. A primeira versão desta nota data de julho de 2020, e foi ampliada e atualizada por Thaís Aguiar, Bruno Bioni, Hana Mesquita, Jaqueline Pigatto e Gabriela Vergili.

**2** Proposta do art.10 do PL 2630/2020.

**3** Conforme explicação em fóruns técnicos e na Wikipédia: *"Gaming the system (also gaming or bending the rules, or rigging, abusing, cheating, milking, playing, cheating the system, working the system, or breaking the system) can be defined as using the rules and procedures meant to protect a system to, instead, manipulate the system for a desired outcome"*.

**4** A proposta foi apresentada por João Brant. Ver: Aperfeiçoamento de legislação brasileira - Internet. Audiência Pública Extraordinária (Virtual) de 24/08/2021. Câmara dos Deputados. Disponível em: <https://www.camara.leg.br/evento-legislativo/62790> Acesso em: 07 out 2021.

**5** Esta proposta foi elaborada por Flávia Lefèvre e Diego Canabarro, endossada pelo Professor Danilo Doneda. Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/um-novo-caminho-para-investigacoes-em-aplicativos-de-mensagens-05102021>. Acesso em: 20 out 2021.

prospectiva de metadados de alvos específicos e não preventiva da população de forma ampla e geral[6]. No entanto, é problemática por permitir que a preservação dos registros das interações ocorra mediante simples pedido administrativo, sem ordem judicial. Além disso, a proposta peca ao não precisar quais seriam os metadados passíveis de serem disponibilizados de acordo com requisição de autoridade judicial, o que fere o princípio (da reserva) da legalidade haja vista que qualquer limitação a direito fundamental deve ser estabelecida por lei e não ser objeto de delegação ao judiciário;

IV. **Proposta D (baixa)[7]**: o Poder Judiciário atua no primeiro plano de salvaguardas, impedindo que haja o alargamento da retenção massiva de metadados mediante mero pedido administrativo. Comparativamente à proposta C, o texto sugerido pela proposta D é mais cuidadoso e preocupado com o ciclo de vida dos dados pessoais na medida em que somente autoriza o pedido de prorrogação do prazo de preservação por duas vezes e prevê um prazo máximo de quinze dias para a eliminação dos registros. De uma forma geral, esta proposta é a alternativa mais proporcional uma vez que busca compatibilizar a devida persecução criminal com os direitos e princípios constitucionais como presunção de inocência, o direito fundamental à liberdade de comunicação, à privacidade e à proteção de dados pessoais.

Não se ignora o problema real da desinformação e da poluição do ambiente informacional de natureza política no Brasil (o modo como as pessoas se informam sobre os fatos e constituem sua noção de pertencimento a uma comunidade política, cada vez mais mediado por aplicações de Internet). Diante desse cenário, entretanto, apresentamos recomendações de atuação política e jurídica com enfoque no aumento das proteções aos direitos digitais e à proteção de dados pessoais. Em síntese, recomenda-se que:

- O esforço de atuação legislativa deve mirar em como os dados pessoais dos cidadãos potencializam o direcionamento de propagandas políticas e de campanhas de desinformação;

- Há necessidade de políticas de transparência, não só a respeito do financiamento de conteúdos políticos, mas sobre todo o ciclo de tratamento de dados pessoais. A exposição de técnicas de *profiling* e a prestação de contas sobre o uso de dados

**6** Errata: na versão divulgada no dia 19 de outubro desta nota técnica, onde se lia "não prevê a retenção prospectiva de metadados", na verdade se lê "prevê a retenção prospectiva de metadados".

**7** Esta proposta, de relatoria de Laura Schertel Mendes, foi apresentada na Câmara dos Deputados em 09 de setembro de 2020 pela Comissão de Juristas responsável pela elaboração do Anteprojeto de Lei sobre proteção de dados em segurança pública e investigações criminais. Disponível em: <https://www.internetlab.org.br/wp-content/uploads/2020/09/Manifestac%CC%A7a%CC%83o-da-Comissa%CC%83o-de-Juristas-da-Ca%CC%82mara.pdf>. Acesso em: 20 out 2021.

pessoais caracteriza-se como elemento chave desse fenômeno complexo que é a desinformação;

- Para coibir a desinformação, importa que a sociedade e as instituições estejam a par de quem faz parte e qual é a lógica do ecossistema informacional, qual aporte financeiro é desembolsado nos diferentes tipos de mensagem, a partir de qual base de dados estes atores elaboram suas estratégias, quais métodos de perfilização comportamental são utilizados e como estes servem para elaborar e direcionar determinadas mensagens a determinado grupo;
- As investigações de ilícitos devem ter como enfoque o tratamento de dados pessoais em violação à Lei Geral de Proteção de Dados Pessoais, como é o caso do repasse de bancos de dados com informações de milhões de pessoas (e.g. clientes de uma determinada empresa de telecomunicações) para que uma empresa de "estratégia digital" possa fazer o disparo automatizado por meio do dado pessoal do número de telefone;

- O problema de desinformação no Whatsapp pode ser atacado pela investigação de modelos de negócio de "marketing digital" e "estratégia digital", que dependem de dados pessoais obtidos ilegalmente. Incrementar os direitos de proteção de dados pessoais e investigar o modo de operação desses mercados (o modo de funcionamento de serviços de gestão de grupos no WhatsApp) é uma forma mais cautelosa e estratégica de atacar o problema do que adotar soluções normativas com propostas apressadas, que podem violar direitos fundamentais.

As recomendações, ao final, são transformadas em sugestões de texto legislativo, com o objetivo de aprimorar a versão atual do Projeto de Lei 2630/2020.

Espera-se que esta contribuição de natureza pública, endereçada à Câmara dos Deputados e toda a sociedade, possa colaborar para um processo de discussão democrática do texto de lei, que, por se tratar de uma norma relacionada ao uso da Internet no Brasil, precisa se ater aos princípios de abertura, colaboração, exercício da cidadania, proteção dos direitos humanos e fundamentais e governança multiparticipativa.

PARTE I

# Por que o projeto de lei viola direitos fundamentais?

Nesta primeira parte, aponta-se por que o projeto de lei colide com os direitos à privacidade e à proteção de dados pessoais, bem como outros direito fundamentais. A análise é prioritariamente jurídica, centrando-se esforços acerca da (in)constitucionalidade de alguns dos dispositivos do Projeto de Lei 2630/2020 com o objetivo de auxiliar a análise a ser realizada pela Comissão Parlamentar na Câmara dos Deputados.

## 1.1. Alargamento do regime de retenção de metadados I (artigo 10): rastreabilidade e relativização do princípio da presunção de inocência

Um dos mecanismos de prevenção e combate à disseminação de *fake news* proposto pelo Projeto de Lei nº 2630/2020 é o alargamento do regime de retenção de dados por provedores de aplicações[8]. O Projeto determina que sejam retidas informações (quem encaminhou, data e horário do encaminhamento e quantidade de usuários que receberam) de mensagens que, no período de 15 dias, tenham sido encaminhadas para, pelo menos, 5 (cinco) pessoas, a fim de rastrear o caminho percorrido pela mensagem e alcançar a sua origem.

A obrigação de retenção de metadados não é uma discussão recém-adquirida no Brasil. O sistema jurídico brasileiro já possui normas que determinam a obrigação de guarda de dados por provedores de telecomunicações e aplicações, como a Lei das Organizações Criminosas e o Marco Civil da Internet[9]. Ao alargar tal regime de retenção de dados, a proposição legislativa em discussão acaba por colidir com uma das principais garantias constitucionais do estado democrático de direito.

A Constituição Federal estabelece em seu art. 5º, LVII que "ninguém será considerado culpado até trânsito em julgado de sentença penal condenatória", positivando, assim, o princípio da presunção da inocência[10]. O Projeto de Lei, bem como todas as normas que preveem a retenção preventiva indis-

**8** Mais especificamente, o projeto estipula obrigações para serviços de mensageria privada. O projeto define "serviços de mensageria privada" (SMP) como "provedores de aplicação que prestam serviços de mensagens instantâneas por meio de comunicação interpessoal, acessíveis a partir de terminais móveis com alta capacidade de processamento ou de outros equipamentos digitais conectados à rede, destinados, principalmente, à comunicação privada entre seus usuários, inclusive os criptografados, ressalvados os serviços de correio eletrônico". Enquadram-se como SMP aplicações como Whatsapp, Telegram e Signal. Todavia, esse conceito, em si, também pode ser interpretado de forma bem mais abrangente, até mesmo para incluir sistemas de mensageria simples, como os enviados entre estabelecimentos comerciais para falar com seus clientes se valendo de sistemas de *push notification*.

**9** Artigos 13 e 15 da Lei nº 12.965/2014.

**10** ABREU, Jaqueline. Guarda Obrigatória de Registros de Telecomunicações no Brasil: sobre as origens da retenção de dados e as perspectivas para direitos fundamentais, **Nuevos Paradigmas de la Vigilancia?**, Disponível em: <http://lavits.org/wp-content/uploads/2017/08/P5_De_Souza_Abreu.pdf>. Acesso em: 14 de outubro de. 2021.

criminada e generalizante de metadados, flexibilizam tal garantia constitucional. **Isto porque, todos os indivíduos teriam informações sobre suas comunicações monitoradas e armazenadas antes mesmo de serem acusados de algum ilícito que justificasse tal ato.**

O que está em jogo, nesse caso, não é apenas a garantia do sigilo das comunicações, atrelada ao direito à privacidade, mas também o direito fundamental à proteção de dados. Além da Lei Geral de Proteção de Dados já em vigor, recentes julgamentos no Supremo Tribunal Federal endereçam essas violações, desde os casos de bloqueio do Whatsapp, até o caso IBGE mais recente (melhor explorado no item 1.5). Destes episódios obteve-se o reconhecimento de que a proteção de dados pessoais é uma garantia fundamental autônoma e distinta do direito à privacidade, o que conversa com a proposta do PL 2630 para o problema conceitual do público x privado.

A previsão de retenção de metadados adotada pelo Projeto de Lei em questão remonta, de forma hipertrofiada, ao caso emblemático da Diretiva europeia relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrônicas (Diretiva 2006/24/EC). Após forte reação e com inúmeros pedidos de declaração de inconstitucionalidade da Diretiva pela sociedade alemã, o Tribunal Constitucional Alemão[11] estabeleceu algumas mudanças no escopo da lei, sobretudo relacionadas ao tempo de retenção dos metadados, apontando para a potencialidade de se construir perfis complexos de personalidade a partir das informações providas pelos metadados.

Diversos recursos foram interpostos contra a Diretiva em países europeus, e, após a Suprema Corte Irlandesa e a Corte Constitucional Austríaca terem questionado o Tribunal de Justiça da União Europeia acerca da compatibilidade da norma com a Carta Europeia de Direitos Fundamentais, decidiu-se pela anulação-invalidação da Diretiva.

Na decisão[12], o Tribunal afirmou que seria necessária a adoção de um fundamento específico para a retenção geral de dados e apontou para a **impossibilidade de que toda a população fosse considerada como suspeita, sob risco de se ferir o princípio da presunção da inocência dos indivíduos**. Nessa perspectiva, o Tribunal determinou que o ponto de partida da diretiva deveria ter sido a ponderação entre o dever de segurança do Estado e o direito à privacidade dos indivíduos.

A Corte identificou que a ponderação necessária entre o direito fundamental à privacidade e o dever de segurança não foi adequadamente implementada no caso da Diretiva europeia, uma vez que a retenção geral de metadados foi estabelecida com vagueza acerca dos critérios de acesso e conservação dos dados e sem limitar a retenção somente para fins de persecução de crimes graves[13].

**11** Vorratsdatenspeicherung, Urteil des Ersten Senats vom 02. März 2010 (Bundesverfassungsgericht 0203, 2010).

**12** Acórdão Digital Rights Ireland e outros (Processos apensos C-293/12 e C-594/12), Disponível em: <https://curia.europa.eu/juris/document/document.jsf?text=&docid=150642&pageIndex=0&doclang=PT&mode=lst&dir=&occ=first&part=1&cid=17350605>. Acesso em: 14 de outubro de 2021.

**13** SILVEIRA, Alessandra; FREITAS, Pedro Miguel. Implicações da declaração de invalidade da Diretiva 2006/24 na conservação de dados

Adicionalmente, o Tribunal enfatizou que a retenção de metadados pode gerar potenciais riscos para outras liberdades, relacionados à criação de um ambiente de vigilância, colocando em xeque o exercício de direitos fundamentais como o da liberdade de expressão. **É o que se convencionou a chamar de efeito de resfriamento - *chilling effects*[14] - pelo qual as pessoas deixam de livremente se expressar diante do receio das suas opiniões estarem sendo compiladas e, futuramente, voltarem-se contra elas, especialmente em ambientes autoritários**. Algo, aliás, que é contraditório ao objetivo principal da proposta legislativa em questão, que é o propiciar um ambiente saudável para a livre circulação de ideias.

Sobre o assunto, em entrevista realizada pelo InternetLab, o Prof. Hans-Jörg Albrecht, diretor do Max-Planck-Institute, apontou para a ideia de que a guarda massiva de dados seria um "problema jurídico, político e, particularmente, também um problema com relação à organização do Estado e sua relação com os cidadãos"[15]. **Em poucas palavras, a política legislativa em torno de um regime de retenção de dados é, em si, uma interferência sobre uma série de direitos e liberdades fundamentais, devendo ser extensamente justificada e articulada para que não seja desproporcional.**

A esse respeito, é importante relembrar o processo de construção e elaboração do Marco Civil da Internet quanto à guarda de metadados. Os artigos 13 e 15 da Lei foram alvo de intensas discussões, uma vez que estabeleceram o armazenamento prévio de *logs*[16], ou metadados, de conexão e aplicação. Após longo processo de formulação da lei, ficaram definidos critérios como o tempo de armazenamento (um ano) e a manutenção desses dados em ambiente sigiloso e controlado e, especialmente, que não seriam todos os metadados passíveis do dever de guarda. Tal recorte no conjunto de informações que deveriam ser armazenadas não foi por acaso. Pelo contrário, é decorrência, justamente, da percepção de que quanto maior fosse o seu escopo, maior seria a sua falta de aderência ao princípio da presunção de inocência.

O registro de conexão do qual, portanto, o Marco Civil da Internet impõe o dever de guarda pelas aplicações mantém-se no escopo de metadados específicos que permitiriam identificar um indivíduo para fins de persecução penal. Já a proposta aqui discutida amplifica desproporcionalmente o espectro do dever de guarda de dados, permitindo o rastreamento de todos os indivíduos que estejam envolvidos na cadeia de mensagens.

("metadados") nos Estados-Membros da UE: uma leitura jusfundamental. **Journal of Law and Regulation**, v. 3, n. 1, p. 281–302, 2017.

**14** BÜCHI, Moritz; FOSCH VILLARONGA, Eduard; LUTZ, Christoph; *et al*. **Chilling Effects of Profiling Activities: Mapping the Issues**. Rochester, NY: Social Science Research Network, 2019. Disponível em: <https://papers.ssrn.com/abstract=3379275>. Acesso em: 22 de julho de 2020.

**15** Albrecht, H.-J. (2015). Direito à Privacidade e a Guarda Obrigatória de Dados para Investigações. (F. Brito Cruz, & B. Kira, Entrevistadores) São Paulo: InternetLab.

**16** Brasil. Lei 12.965/2014. Marco Civil da Internet: "registro de conexão: o conjunto de informações referentes à data e hora de início e término de uma conexão à internet, sua duração e o endereço IP utilizado pelo terminal para o envio e recebimento de pacotes de dados;respeitando-se o princípio do uso mínimo de dados e proporcionalidade."

Em conclusão, o PL 2630/2020, ao ampliar o já controverso regime de retenção de metadados no Brasil, desconsidera não só o amplo debate realizado ao longo do processo de elaboração do Marco Civil da Internet, como, também, outras jurisdições que já invalidaram propostas até mesmo menos intrusivas.

### 1.2. Alargamento do regime de retenção de metadados II (artigo 35): portas lógicas

Um outro ponto em que se percebe a (in)evolução do projeto do PL 2630/2020 é o "dilema da porta lógica"[17], embate já conhecido e enfrentado pelo judiciário brasileiro. Esse debate é importante pois relaciona-se à natureza dos metadados e as obrigações de retenção e compartilhamento relativas a eles.

Mas o que são tais registros? As portas lógicas[18] são elementos que indicam uma espécie de "fim de uma linha" de comunicação e também se relacionam com parte fundamental da arquitetura e funcionamento da rede, o protocolo TCP/IP[19]. Nos últimos anos, o endereço IP vem passado por um longo processo de transição[20] de sua versão antiga (IPv4) para sua versão nova (IPv6), uma vez que o crescimento da rede mundial de computadores levou ao esgotamento de números IPv4[21] para identificação de aparelhos que se conectam à internet. Com o novo protocolo, o anterior montante de aproximadamente 4.3 bilhões de endereços passou a $3.4 \times 10^{38}$ endereços, uma quantidade virtualmente inesgotável. A transição, porém, é lenta e requer uma série de adaptações, e as portas lógicas são parte desse processo: através da NAT,[22] pensada para viabilizar o acesso à rede durante a transição, mais de um usuário pode compartilhar o mesmo IP, acrescidos de portas lógicas numeradas ao fim do endereço para identificar e apontar cada dispositivo de forma singular.

Como esses registros não entram na definição legal de registros de conexão e de aplicações do MCI, o debate que surgiu foi se as portas lógicas de origem fazem parte do dever de guarda de metadados no Brasil. O MCI só trata do dever de retenção de metadados específicos, de modo que não há indicativos de que tal obrigatoriedade se estenda aos registros não mencionados pelo texto da lei - ou de que seja plausível fazê-lo. Esse raciocínio leva em consideração o princípio de intervenção mínima em sede de

**17** ANTONIALLI, Dennys; CRUZ, Francisco Brito; FRAGOSO, Nathalie. **O Marco Civil da Internet e o dilema da 'porta lógica'**. Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/o-marco-civil-da-internet-e-o-dilema-da-porta-logica-22082019>. Acesso em: 17 de julho de 2020.

**18** CGI.BR. A Porta Lógica e seus responsáveis. Disponível em: <https://200.160.4.6/videos/ver/viii-forumbr-a-porta-logica-e-seus-responsaveis/>. Acesso em: 17 de julho de 2020.

**19** MEYNELL, Kevin. **Final report on TCP/IP migration in 1983**. Disponível em: <https://www.internetsociety.org/blog/2016/09/final-report-on-tcpip-migration-in-1983/>. Acesso em: 17 de julho de 2020.

**20** IETF. **Request for comment 2460**. Disponível em: <https://tools.ietf.org/html/rfc2460>. Acesso em: 17 de julho de 2020.

**21** LACNIC. Fases de Esgotamento do IPv4. Disponível em: <https://www.lacnic.net/1077/3/lacnic/fases-de-esgotamento-do-ipv4>. Acesso em: 17 de julho de 2020.

**22** DUARTE, Otto. **NAT - Network Address Translation**. Disponível em: <https://www.gta.ufrj.br/grad/01_2/nat/>. Acesso em: 17 de julho de 2020.

direitos fundamentais. As hipóteses de guarda de metadados são taxativas e, por conseguinte, uma opção do legislador[23].

Vale ressaltar que tanto o MCI quanto o seu Decreto Regulamentador (Decreto nº 8.771/2016) receberam, cada qual, mais de 1.5 mil contribuições de diversos setores[24]. O debate sobre portas lógicas também foi especificamente endereçado. Ao final, o Decreto 8.771/2016 não trouxe nenhum outro dever de retenção de dados, limitando-se às hipóteses do Marco Civil da Internet.

Ainda nesse sentido, outro ponto que não pode passar despercebido é o de que o Marco Civil da Internet optou por não abordar tantas outras formas de identificação de usuários. Muitas espécies de dados com potencial de identificação deixaram de fazer parte do dever de guarda dos provedores[25]. A porta lógica é apenas um elemento de um conjunto cuidadosamente não englobado pelo dever de retenção, tendo em vista a difícil equação entre o direito à segurança pública e a tutela de direitos e garantias fundamentais[26].

Por fim, mas não menos importante, deve-se considerar que tal previsão se prende a uma tecnologia específica - portas lógicas - que pode e provavelmente será descontinuada quando for completada a transição do IPV4 para o IPV6. Dessa forma, em termos de técnica legislativa, o artigo 35 do PL 2630/2020 é criticável por não ser "tecnologicamente neutro"[27], na medida em que o comando normativo pode se tornar obsoleto com a emergência de um novo padrão tecnológico.

### 1.3. A falsa solução da rastreabilidade: problemas de efetividade

A proposta em questão justifica o rastreamento das mensagens compartilhadas com mais de cinco usuários para a finalidade de se identificar o usuário que originalmente compartilhou a mensagem. Supondo que fosse tecnicamente e juridicamente possível o rastreamento, **não existe comprovação, estudo, ou caso em nenhuma parte do mundo em que o método se demonstrou eficaz no combate à desinformação.**

**23** RAMOS, Pedro *et. al.* **Armazenamento de portas lógicas à luz do MCI**. Disponível em: <https://baptistaluz.com.br/institucional/a-discussao-sobre-armazenamento-de-portas-logicas-a-luz-do-mci/#_ftnref5>. Acesso em: 17 de julho de 2020

**24** MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA. **Decreto do Marco Civil da Internet recebe mais de 1.500 comentários**. Disponível em: <https://www.justica.gov.br/news/decreto-do-marco-civil-da-internet-recebe-mais-de-1-500-comentarios>. Acesso em: 22 de julho de 2020.

**25** CRUZ, Francisco. **Porta lógica e provedores de aplicação**. Disponível em <http://www.omci.org.br/jurisprudencia/99/porta-logica-e-provedores-de-aplicacao/> Acesso em: 15 de julho de 2020.

**26** Vide os seguintes litígios judiciais: REsp 1826221, agravo 2102827-94.2019.8.26.0000, agravo 2240522-27.2018.8.26.0000, processo 1080088-48.2013.8.26.0100.

**27** O conceito de "*technology-neutral regulation*" tem sido evocado para se discutir o desenho de modelos regulatórios capazes de estimular e acompanhar o desenvolvimento tecnológico, sem engessá-lo nem ser permissivo a riscos. Sobre isso: BAPTISTA, Patrícia; KELLER, Clara. Por que, quando e como regular as novas tecnologias? Os desafios trazidos pelas inovações disruptivas. Revista de Direito Administrativo, n. 273, p. 123-163, set./dez. 2016.

Especialistas consultados no Brasil sobre a efetividade da proposta apontam que ela carece de evidências. Em matéria escrita por Renata Galf para a Folha de São Paulo, esse ponto é examinado em profundidade. Galf destaca que um dos pontos polêmicos do PL 2630/2020 "é o item que determina que serviços como o Whatsapp e o Telegram salvem toda a cadeia de quem encaminhou uma mensagem que tenha viralizado"[28].

Um dos pontos falhos é a ideia de identificar quem é o autor de um "conteúdo ilícito" que circula na plataforma, ignorando o fato de que muitas vezes os conteúdos são compartilhados entre diferentes plataformas (vídeos do Youtube são compartilhados no Whatsapp, do mesmo modo que prints de Twitter são compartilhados no Facebook), por vezes eliminando a possibilidade de identificação precisa de autoria de conteúdo.

Ao criar um sistema rígido ou uma padronização para a rastreabilidade de mensagens, é provável que isso abra a oportunidade de técnicas para "enganar o sistema" (*game the system*). Ao ouvir especialistas, Renata Galf destaca algumas. Seria fácil, por exemplo, automatizar um *script* para que um mesmo texto desinformador fosse editado de inúmeras formas distintas, por meio de pequenas modificações em número de caracteres, uso de vírgulas e pontuação, ou mesmo substituição de palavras sinônimas.

Neste caso, abriria-se uma situação peculiar. Uma empresa de "estratégia digital" especializada em disparos de mensagens por Whatsapp poderia utilizar uma equipe de programadores para desenvolver uma solução deste tipo — algo que pudesse enganar o sistema e evitar a rastreabilidade —, ao passo que todas as pessoas comuns, que repassam mensagens por motivações políticas espontâneas, teriam os dados pessoais coletados. Além desse, outros mecanismos poderiam burlar a cadeia de rastreabilidade proposta, desde a famosa prática de "copiar e colar", passando pela referida programação de *scripts* e chegando no uso de laranjas e telefones e dispositivos no exterior, que acabariam por colocar os criminosos em um "ponto cego" dessa arquitetura.

Não é sem razão que Patrícia Rossini, da Universidade de Liverpool, chamou isso de um "problema de gato e rato". Como reportado pela Folha, "pessoas que de fato estão por trás de grandes esquemas de desinformação poderiam sair impunes, enquanto pessoas manipuladas a passar determinado conteúdo para frente poderiam ser pegas"[29].

A ideia de armazenar data, horário e I.P. pode parecer inofensiva. Porém, não é. No modelo do projeto, as cadeias de encaminhamento de mensagens devem ser armazenadas se, dentro de 15 (quinze) dias, forem encaminhadas para grupos e listas de transmissão, por mais de cinco usuários, atingindo mais de mil usuários. As empresas (como Whatsapp e Telegram) seriam então obrigadas a incluir nos registros

**28** GALF, Renata. **Regra para armazenar cadeia de mensagens do WhatsApp pode ser ineficaz em projeto de fake news no Congresso**, Folha de São Paulo, 17/07/2020. Disponível em: <**https://www1.folha.uol.com.br/poder/2020/07/regra-para-armazenar-cadeia-de-mensagens-do-whatsapp-pode-ser-ineficaz-em-projeto-de-fake-news-no-congresso.shtml**>. Acesso em: 14 de outubro de 2021.

**29** Ibidem;

(i) o usuário que encaminhou, (ii) data e hora de encaminhamento e (iii) quantidade de usuários atingidos.

A Folha de São Paulo faz um exercício bastante ilustrativo. Imagine que a jornalista Larissa envia uma mensagem para três grupos, cada um com 250 membros. Dentro desses grupos, três outros jornalistas (Gabriel, Alessandra e Pedro) encaminham essa mesma mensagem para Grupos de Checadores. No Grupo de Checadores, Miguel e Beatriz analisam a mensagem e retornam para o Grupo de Jornalistas. Neste caso, o Whatsapp teria que salvar por três meses que a mensagem foi enviada pelos usuários Larissa, Gabriel, Alessandra, Pedro, Miguel e Beatriz, com data e hora de cada encaminhamento e número de usuários atingidos.

Nathalia Sautchuck, pesquisadora da Universidade de São Paulo e do Núcleo de Informação e Coordenação do Ponto BR, afirma nesta matéria que este mecanismo obrigaria os serviços de mensagem a fazer "uma espécie de carimbo em toda e qualquer mensagem enviada"[30]. Para se chegar a toda a reconstrução da cadeia e avaliar os critérios do projeto (se atinge mais de 1.000 pessoas e se há cinco pessoas envolvidas nos disparos), seria necessário registrar os números dos destinatários dentro do prazo de 15 (quinze) dias, para posteriormente avaliar se serão destruídos ou não.

É por esta razão que o diretor do InternetLab, Francisco Brito Cruz, afirmou que, em um sistema autoritário, esse modelo permite um "acesso a dados massivos". Investigadores e juízes poderiam obter a rede de encaminhamento de mensagens, em um sistema inédito de vigilantismo.

Em entrevista para Juliana Gragnani, da BBC Brasil, Francisco Brito Cruz destacou que tal modelo jurídico nunca foi testado em nenhuma jurisdição no mundo. Seria uma pseudo-solução "que não resolve nenhum problema"[31], por ignorar a lógica de rede da internet, por ignorar os problemas de compartilhamento entre plataformas que impossibilitam a identificação direta de autoria e por gerar uma espécie de receita para grupos organizados que pretendem burlar o sistema de rastreabilidade.

Por essas razões, a análise custo-benefício se mostra frustrada. As vantagens não são grandes o suficiente, considerando os problemas fundamentais de orientação da medida (a expectativa de identificar a autoria não será possível) e o fato de que a rastreabilidade afetará provavelmente um número grande de jornalistas, ativistas e pessoas comuns, ao mesmo tempo em que permitirá que técnicas para burlar o sistema sejam utilizadas por grupos já profissionalizados, que operam na "economia política da desinformação"[32].

**30** Ibidem.

**31** GRAGNANI, Juliana. **PL das fake news pode acirrar polarização política, diz pesquisador**, BBC News Brasil, 17/07/2020. Disponível em: <https://www.bbc.com/portuguese/brasil-53418555>. Acesso em: 14 de outubro de 2021.

**32** SANTOS, João Vitor. **Economia política da desinformação é a principal ameaça à democracia**. Entrevista especial com Rafael Zanatta, Instituto Humanistas Unisinos, 17/12/2018. Disponível em: <http://www.ihu.unisinos.br/159-noticias/entrevistas/585561-economia-politica-da-desinformacao-e-a-principal-ameaca-a-democracia-entrevista-especial-com-rafael-zanatta>. "Os processos de desinformação precisam ser estudados em sua organização econômica [as empresas que se dedicam a explorar a organização de grupos e a criação de conteúdo] e nessa

## 1.4. A sensibilidade de metadados: questionando a premissa do debate político de que seriam dados que mereceriam um menor tipo de proteção

Conforme explicado anteriormente, metadados constroem o cenário em que a comunicação se deu sem revelar o conteúdo da mensagem. São uma espécie de "envelope" do processo comunicacional e englobam vários tipos de dados (i.e. dados sobre o usuário que realiza a comunicação, localização, tipo de mensagem, a rede utilizada, horário, duração). Por isso, fornecem uma alta quantidade e variedade de informações que, quando agregadas e analisadas, podem chegar ao perfilhamento comportamental do indivíduo[33].

Assim, metadados enquadram-se, via de regra, na definição de dado pessoal, na medida em que tornam uma pessoa identificada ou identificável[34]. Trata-se, portanto, de uma informação protegida pela legislação e pelo direito fundamental à proteção de dados pessoais[35-36]. Logo, metadados, ao contrário do que se sustentou em parte da discussão ao longo da célere tramitação do PL 2630/2020, são tão ou talvez mais críticos que outros tipos de dados pessoais, como o conteúdo em si de mensagens.

Historicamente, metadados são usados para fins de segurança pública e persecução criminal e, com as novas tecnologias, tem-se intensificado o questionamento sobre o uso dessas informações. Um exemplo sintomático foi a declaração do ex-diretor da National Security Agency (NSA), Michael Hayden, sobre o quão potente seria tal tipo de informação para fins de vigilância, a ponto de tornar irrelevante ou, ao menos, mais custosa e ineficiente a análise do conteúdo das comunicações. Até mesmo decisões

infraestrutura de criação de conteúdo, que se vale de uma espécie de "propaganda feedback loop" de baixo custo [a mesma mensagem falsa sendo replicada em canais de YouTube, páginas e contas de Facebook e Instagram". Acesso em: 14 de outubro de 2021.

**33** NI LOIDEAIN, Nora, EU Law and Mass Internet Metadata Surveillance in the Post-Snowden Era, Media and Communications, Special Issue on Surveillance: **Critical Analysis and Current Challenges**, 2015, p. 3. Disponível em: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2613424>. Acesso em: 16 de julho de 2020.

**34** A Lei Geral de Proteção de Dados define, em seu art. 5º, I, dado pessoal enquanto "informação relacionada a pessoa natural identificada ou identificável".

**35** BRASIL. Supremo Tribunal Federal. Ação Direta de Constitucionalidade nº 6387... Op. cit.

**36** O voto do ministro Fachin na ADI 5527/ADPF 403 expõe sete premissas básicas para o debate sobre direitos digitais em sede constitucional no Brasil: "Primeira: o impacto tecnológico das mudanças porque passa a sociedade reclamam um permanente atualizar do alcance dos direitos e garantias fundamentais. Segunda: os direitos que as pessoas têm *offline* devem também devem ser protegidos *online*. Direitos digitais são direitos fundamentais. Terceira: a garantia do direito à privacidade e à liberdade de expressão nas comunicações é condição para o pleno exercício do direito de acesso à internet. Quarta: a privacidade é o direito de manter o controle sobre a sua própria informação e de determinar a maneira de construir sua própria esfera pública. Quinta: A liberdade de expressão tem primazia *prima facie* e constitui condição essencial ao pluralismo de ideias, vetor estruturante do sistema democrático de direito. Sexta: Na internet, a criptografia e o anonimato são especialmente úteis para o desenvolvimento e compartilhamento de opiniões, o que geralmente ocorre por meio de comunicações *online* como o e-mail, mensagens de texto e outras interações. A criptografia, em especial, é um meio de se assegurar a proteção de direitos que, em uma sociedade democrática, são essenciais para a vida pública. Sétima: É contraditório que em nome da segurança pública deixe-se de promover e buscar uma internet mais segura. Uma internet mais segura é direito de todos e dever do Estado. Medidas que, à luz da melhor evidência científica, trazem insegurança aos usuários somente se justificam se houver certeza comparável aos ganhos obtidos em outras áreas"

sobre a vida de uma pessoa já foram tomadas com base em metadados[37]. Este é o nível de sensibilidade das informações a que o projeto de lei busca expandir o seu dever de guarda.

Ademais, metadados detêm um certo tipo de valor agregado para fins de vigilância que decorre de sua alta confiabilidade. Isto porque, na medida em que são dados gerados pelo próprio sistema operacional, não são facilmente alteráveis. Em contrapartida, o conteúdo de comunicações e dados pessoais fornecidos por seu titular podem ser simulados, especialmente quando o alvo da investigação suspeita estar sendo monitorado. Em resumo, trata-se de um tipo de dado pessoal que coloca o seu titular em uma posição de extrema vulnerabilidade.

Ainda sobre a relevância de metadados, retoma-se que, na decisão do Tribunal Constitucional Alemão que invalidou a Diretiva 2006/24/EC, o ponto chave da argumentação era o potencial desses dados para fins de formação de perfil comportamental. Na decisão, atentou-se para a necessidade de observância ao princípio da proporcionalidade em sede de intervenção de direitos fundamentais[38]. Nesse sentido, medidas que exigem o monitoramento e armazenamento de dados de mensagens, mesmo que haja critérios para esse rastreamento, geram mais riscos do que benefícios.

Por outro lado, pela mesma razão de os metadados serem dados muito completos, eles podem servir como um apoio para a persecução penal, desde que haja implementação complementar de salvaguardas para preservação de direitos fundamentais e para evitar a coleta massiva. Isso pois, conforme mencionado, não serão facilmente editados e não carregarão os vieses que os conteúdos das comunicações, por exemplo, podem ter. São completos a ponto de não ser necessário o acesso ao conteúdo e nem a outros dados pessoais, ou até mesmo acesso aos aparelhos em si, permitindo que as investigações não sejam prejudicadas e evitando ações desnecessárias[39].

Disso não decorre, entretanto, a necessidade da retenção prévia e indiscriminada dos dados, até porque uma outra hipótese, como a preservação apenas de metadados selecionados e relacionados a indícios concretos de ilícitos, permite uma "visão mais limpa" sobre o todo. O acúmulo de dados coletados de forma indiscriminada dificulta a análise e impede que sejam observadas as interações que resultam em ilícitos. A tomada seletiva de dados de interação, por outro lado, é mais benéfica à persecução criminal por incluir a cadeia de interação, sem precisar invadir demasiadamente a esfera de outros usuários que

**37** NEWS, A. B. C., **Ex-NSA Chief: "We Kill People Based on Metadata"**, ABC News, disponível em: <**http://abcnews.go.com/blogs/headlines/2014/05/ex-nsa-chief-we-kill-people-based-on-metadata**>. Acesso em: 16 de julho de 2020.

**38** ABREU, Jaqueline, **Uma nova lei de retenção de dados para a Alemanha – dessa vez constitucional?**, InternetLab, disponível em: <**https://www.internetlab.org.br/pt/opiniao/uma-nova-lei-de-retencao-de-dados-para-a-alemanha-dessa-vez-constitucional/**>. Acesso em: 17 de julho de 2020.

**39** Um exemplo de uso de metadados foi a investigação no caso Marielle Franco, em que foi utilizada triangulação de sinal de celular. Ressalta-se que o uso destas informações deve ser feito de forma cautelosa, e preservando os direitos fundamentais, para afastar abusos e desproporcionalidades. Ver: PADRÃO, Márcio. Caso Marielle: como celulares levaram a acusados e por que isso é um avanço. **Tilt**. 13 mar 2019. Disponível em: <**https://www.uol.com.br/tilt/noticias/redacao/2019/03/13/como-os-celulares-ajudaram-a-achar-o-assassino-de-marielle-franco.htm?cmpid=copiaecola**>. Acesso em: 07 de outubro de 2021.

podem não ter nenhum envolvimento com a infração[40].

### 1.5. O que o recente julgamento do STF nos ensina acerca da proposta legislativa em discussão

No dia 6 e 7 de maio de 2020, foi realizado no Supremo Tribunal Federal (STF) o julgamento referente ao compartilhamento de dados de clientes de operadoras de telecomunicações e o IBGE para execução de pesquisas. O julgamento, relatado pela Min. Rosa Weber, é um marco histórico no Brasil por ter reconhecido a existência do direito à proteção de dados pessoais como um direito fundamental autônomo à privacidade e ao sigilo das comunicações.

Dentre vários pontos emblemáticos, o julgado desmistifica a equivocada percepção de que, não havendo a violação do conteúdo da comunicação, não haveria interferência em direito algum[41]. As comunicações estão acompanhadas de diversos outros dados que vão muito além do conteúdo das mensagens, e que possuem caráter pessoal. Os dados, antes considerados secundários, passam a ser um indicador comportamental central. Os metadados, por serem dados pessoais, são igualmente merecedores de tutela, já que "não há mais dados insignificantes".

Ao avaliar no julgamento a proporcionalidade da Medida Provisória nº 954/2020, o Min. Gilmar Mendes apontou o direito à autodeterminação informativa como uma regra a ser seguida, sendo as interferências exceções justificadas por parte do legislador e, o mais importante, defendeu que toda e qualquer proposição legislativa deve cercar-se de todas as medidas de salvaguardas para que não haja uma interferência desproporcional sob tal direito fundamental. Ao se conjugar as considerações tecidas sobre o histórico nacional e estrangeiro em torno de políticas legislativas sobre o dever de guarda de metadados, somado a sua questionável eficiência para fins de combate à desinformação, os artigos 10 e 35 do PL nº 2.630/2020 tendem a ter a sua constitucionalidade desafiada.

Por fim, vale mencionar as ameaças democráticas. A proposta que visa montar uma base de dados tende a não atingir os profissionais e os maiores *stakeholders* que comandam as cadeias de disseminação de fake news, porque estes irão e já estão sofisticando seus métodos. Quem estará catalogado e fichado são grupos de minorias, muitas vezes ativistas e jornalistas que ainda não contam com apoio e cuidados mínimos de segurança da informação. É ingênuo pensar que essa grande base de dados seria somente usada para fins legítimos e não seria abusada.

**40** DONEDA, Danilo. Um novo caminho para investigações em aplicativos de mensagens. **Jota**. 05 out. 2021. Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/um-novo-caminho-para-investigacoes-em-aplicativos-de-mensagens-05102021>. Acesso em: 07 de outubro de 2021.

**41** ASSOCIAÇÃO DATA PRIVACY BRASIL DE PESQUISA, Petição de Amicus Curiae ao Supremo Tribunal Federal, Data Privacy Brasil Research, disponível em: <https://www.dataprivacybr.org/wp-content/uploads/2020/05/dpbrr_amicuscuria_stf_ibge.pdf>. Acesso em: 17 de julho de 2020.

Dos episódios terrificantes da Segunda Guerra Mundial, passando pelo período ditatorial no Brasil e mais recentemente em casos, ainda a serem analisados pelo STF, há enormes riscos e, por conseguinte, de uma catástrofe que essas bases de dados sejam utilizadas para fins autoritários e de perseguição. A democracia depende da privacidade e liberdade dos usuários desses serviços de comunicação, hoje uma ferramenta indispensável para a vida em sociedade. Desse modo, ao descumprir com princípios de proporcionalidade e necessidade, a proposta acaba por criar mais riscos à democracia do que soluções.

PARTE 2

# Quais as alternativas regulatórias viáveis para combater a desinformação e a desproteção dos dados pessoais?

Nesta segunda parte, apontam-se alternativas regulatórias viáveis, focadas no aprimoramento das capacidades de repressão ao fenômeno da desinformação por meio do modo como os dados pessoais são utilizados de forma ilegal ou abusiva. Não obstante as particularidades do cenário brasileiro, entendemos que as melhores estratégias regulatórias são as que encontram alguma ressonância na comunidade internacional e que não apresentam graves riscos aos direitos fundamentais.

## 2.1. O reforço necessário de medidas de transparência sobre perfilização *(profiling)*

A transparência como resposta vai ao encontro das medidas que têm sido adotadas e discutidas no cenário global, que, atualmente, também se preocupa com a ameaça democrática da desinformação. Países como EUA, Canadá e membros da União Europeia têm implementado políticas que reforçam a prestação de contas sobre o direcionamento de anúncios e o uso de dados para tanto. **O enfoque principal é o da necessidade de medidas de *accountability* sobre as atividades de direcionamento de conteúdo, que devem ser mais transparentes não só no que diz respeito ao seu financiamento, mas, também, ao seu próprio funcionamento interno**. Isto é, como os dados pessoais dos cidadãos potencializam o direcionamento de propagandas políticas. O modo como as informações pessoais dos indivíduos são coletadas e processadas para esse tipo de uso precisa ser evidenciado. No cenário global, essa já é entendida como a chave do problema da desinformação[42].

Em 2018, o Information Commissioner's Office (ICO) do Reino Unido, produziu um relatório[43] acerca do uso de informações pessoais para influência política, "*Democracy disrupted? Personal Information and political influence*". Neste, o órgão já apontava a falta de transparência acerca do uso de dados pessoais da população como um problema central da manipulação política. Para o ICO, os partidos deveriam prestar contas a respeito de como obtém e como utilizam as informações pessoais por eles detidas, de modo a sujeitá-los ao escrutínio público. Essa é a mesma abordagem dos que sugerem[44] a criação de um repositório que espelhe o quanto os partidos políticos gastam em direcionamento de conteúdos e quais as mensagens e promessas estão sendo distribuídas para cada segmento populacional.

**42** Panoptykon Foundation, ePaństwo Foundation and SmartNet Research & Solutions. Who (really) targets you? Facebook in Polish election campaigns. Disponível em: <https://panoptykon.org/political-ads-report>. Acesso em: 14 de outubro de 2021.

**43** Information Commissioner's Office. *Democracy disrupted? Personal information and political influence*. UK. 2018. Disponível em: <https://ico.org.uk/media/2259369/democracy-disrupted-110718.pdf>. Acesso em: 14 de outubro de 2021.

**44** BORGESIUS, F.J.Z.; MÖLLER, J. KRUIKERMEIER, S.; FATHAIGH, R.; IRION, K; DOBBER, T. BODO, B.; VREESE, C. Online Political MIcrotargeting: Promises and Threats For Democracy. Utrech Law review. v14, 2018. p. 94.

Alguns países, como o Canadá e membros da União Europeia, já experienciaram o funcionamento de repositórios[45] que se propunham a clarificar o *microtargeting* político em aplicações. A experiência destes apenas reafirma a importância de uma regulamentação que objetive uma maior transparência de agentes que promovem conteúdos. Tais repositórios, também chamados de *"Ad Library"*, são ações de conformidade às legislações que passaram e exigir o registro e transparência dos anúncios promovidos por partidos políticos. O que pesquisadores constataram foi que, apesar de uma melhora do cenário de transparência, ainda há um déficit muito grande, principalmente do que diz respeito ao modo como os dados pessoais são tratados para a formulação de perfis comportamentais, perfis estes que são o norte do direcionamento de conteúdos.

## 2.2. Reforço da estrutura de regulação em proteção de dados pessoais

Esse cenário justifica a afirmação de Colin Bennett[46], no sentido de que uma melhora da transparência das propagandas políticas deverá ser acompanhada do aprimoramento da proteção de dados. Investigando o tema, a Panoptykon Foundation realizou pesquisa[47] sobre a forma de operação da plataforma *"Ad Library"* na Polônia, concluindo existirem falhas graves da ferramenta em de fato informar os titulares a respeito de como seus dados estavam sendo processados e como informações pessoais diversas eram inferidas para caracterizar seu perfil comportamental. O estudo aponta que, se por um lado, o repositório indicava que o direcionamento de conteúdos era embasado por categorias gerais como idade, sexo e geolocalização, por outro, tais categorias não explicavam completamente por que determinados conteúdos alcançavam determinados indivíduos. Os pesquisadores descobriram que as categorias de perfis então disponibilizadas eram incompletas e, ao observarem as *tags* disponíveis para anunciantes, perceberam a existência de uma classificação de indivíduos muito maior e mais detalhada. Para além disso, notaram a existência de categorias de interesse que facilmente poderiam ser associadas a informações sensíveis. O órgão indicou a existência de tags de interesse como *"LGBT"*, *"Sustainability"*, *"Gender"* e *"Climate"*, as quais são costumeiramente associadas à agenda política da esquerda. A constatação é preocupante, pois expõem a falta de consciência que a população tem a respeito de como seus dados pessoais são tratados e utilizados, ao ponto de informações sensíveis servirem a agentes políticos e do mercado a fim de influenciar comportamentos de forma abusiva e pouco transparente.

No âmbito brasileiro, a Coding Rights elaborou relatório[48] a respeito da indústria do marketing

**45** CPDP 2020: Political micro-targeting under investigation: Lessons from 2019 campaigns. Jan. 2020. Disponível em: <https://www.youtube.com/watch?v=c_5baNxKj3I>. Acesso em: 14 de outubro de 2021.

**46** Ibidem. BENNETT, Colin. *"The increased Transparency of inline political advertising must be matched by enhanced data protection for our political parties."* Disponível em: <https://www.youtube.com/watch?v=c_5baNxKj3I>. Acesso em: 14 de outubro de 2021.

**47** Panoptykon Foundation, ePaństwo Foundation and SmartNet Research & Solutions. *Who (really) targets you? Facebook in Polish election campaigns*. Disponível em: <https://panoptykon.org/political-ads-report>. Acesso em: 14 de outubro de 2021.

**48** CODING RIGHTS e TACTICAL TECHNOLOGY COLLECTIVE. *Data and elections in Brazil 2018*. Relatório. Outubro 2018. p.49. Disponível em: <https://www.codingrights.org/wp-content/uploads/2018/11/Report_DataElections_PT_EN.pdf>. Acesso em: 14 de outubro de 2021.

político digital, explorando como agências de publicidade, plataformas de mídia social e *data brokers* tornaram-se agentes centrais na definição de campanhas eleitorais e, indiretamente, para o fenômeno da desinformação. A pesquisa levanta a complexidade e obscuridade do modo de operação desses agentes, são inúmeras camadas de diversas empresas que fornecem, vendem, combinam e analisam dados pessoais para classificar e perfilar indivíduos, a fim de criar estratégias de influência sobre seu comportamento. Nesse processo, nenhuma das fases do fluxo informacional é clara. A coleta, o armazenamento, as técnicas de perfilização utilizadas e as razões de determinadas mensagens serem direcionadas a determinados grupos não são práticas esclarecidas por controladores ou operadores, o que é um problema imediatamente relacionado à ausência de uma cultura robusta de proteção de dados.

**Portanto, o quadro retorna para a necessidade de políticas de transparência, não só a respeito do financiamento de conteúdos políticos, mas sobre todo o ciclo de tratamento de dados pessoais. A exposição de técnicas de *profiling* e a prestação de contas sobre o uso de dados pessoais caracteriza-se como elemento chave.**

A desinformação está atrelada ao cenário de extrema falta de transparência, o que envolve todo o sistema de uso de dados para segmentação de perfis e promoção de conteúdos. Ainda, como levantado nas discussões globais acerca do tema, a clareza do tratamento de dados tem que ser generalizada sobre todo tipo de promoção de conteúdo, não se restringindo àqueles qualificados como propaganda política. A pesquisa da Panoptykon levanta, a título exemplificativo, o financiamento russo de conteúdos polarizantes durante as eleições presidenciais de 2016 dos EUA[49]. Estes anúncios e publicações não faziam alusão direta a determinado partido ou candidato, mas se engajavam em debates acesos e que serviam como *proxies* políticos. Em tal contexto, é essencial que seja evidente ao usuário quem se esconde por detrás da informação por ele consumida e as razões pelas quais lhe foram direcionadas determinadas mensagens.

Uma abordagem focada na transparência dos agentes e não na exposição dos indivíduos a riscos de violação à intimidade é parte importante do instrumental adequado para enfrentar o problema, além de ser mais aderente às discussões e experiências internacionais. Para coibir a desinformação, importa que a sociedade e as instituições estejam a par de quem faz parte e qual é a lógica do ecossistema informacional, qual o aporte financeiro é desembolsado nos diferentes tipos de mensagem, a partir de qual base de dados estes atores elaboraram suas estratégias, quais métodos de perfilização comportamental são utilizados e como estes serviram para elaborar e direcionar determinada mensagem a determinado grupo. É esse tipo de clareza que permite à generalidade da população, que é a vítima e não agente da desinformação, conduzir um juízo de valor próprio sobre as informações que lhe são dirigidas.

**49** Panoptykon Foundation, ePaństwo Foundation and SmartNet Research & Solutions. *Who (really) targets you? Facebook in Polish election campaigns*. Available at: <https://panoptykon.org/political-ads-report>. Acesso em: 14 de outubro de 2021.

## 2.3. **Investigações criminais sobre uso ilegal de dados e o mercado de *data brokers* em desinformação**

Em matéria jornalística, produzida em outubro de 2018, Patrícia Campos Mello, da Folha de São Paulo, denunciou um esquema onde empresas bancavam disparos de mensagens nas redes (Folha de São Paulo, ano 98, n. 32.705). A matéria de Patrícia destacou como empresas de marketing digital fariam o "disparo em massa" usando "base de usuários do próprio candidato ou bases vendidas por agências de estratégia digital".

As investigações de Campos Mello revelaram que funcionários de empresas de "estratégia digital" utilizavam ilegalmente bases de dados fornecidas por empresas de cobranças ou por funcionários de empresas de telecomunicações. Em posse dos números, funcionários de empresas faziam o tratamento de dados pessoais, administrando grupos de Whatsapp, convidando para que pessoas pudessem ingressar em grupos.

Posteriormente, pesquisadores descobriram um pujante mercado de "gestão de grupos de Whatsapp", com diferentes técnicas de análise do comportamento das pessoas em grupos, catalogando os mais influentes e os mais engajados em disparos de mensagens produzidas de forma distorcida. Evidente, portanto, que a infraestrutura desse modelo de negócios — oferecido para lideranças políticas que querem constituir uma base de disseminadores *online* — ampara-se em práticas abusivas e ilegais de tratamento de dados pessoais.

Pelo que se sabe, até hoje não foi apurada a origem dos dados pessoais utilizados por essas empresas de marketing digital e de estratégia digital, apesar de ter existido pedidos de entidades civis pela instauração de inquérito no Ministério Público do Distrito Federal e Territórios, que possui uma unidade especializada em proteção de dados pessoais[50]. E aí reside um dos problemas fundamentais, considerando a existência de agências especializadas em disparos de mensagens e gestão de grupos, com bases de dados de origem duvidosa da perspectiva legal[51].

**50** Na época, o pedido foi formulado pelo Instituto Brasileiro de Defesa do Consumidor. O inquérito não foi instaurado pois alegou-se que a investigação já estava ocorrendo pela Polícia Federal.

**51** No novo livro, *A Máquina do Ódio*, publicado em julho de 2020 pela jornalista Patrícia Campos Mello pela Companhia das Letras, ela escreve: "Outra maneira de criar a impressão de que "todo mundo está falando sobre determinado assunto" e, assim, ofuscar outros temas é contratar agências que fazem disparos em massa no WhatsApp. Dessa forma é possível enviar para milhares de pessoas em milhares de grupos de WhatsApp memes, textos, áudios ou vídeos que disseminam um ponto de vista. Uma vez 'impulsionada', a narrativa é então propagada naturalmente pelas redes orgânicas, que são as pessoas de carne e osso que acreditam naquilo que está sendo veiculado. Os americanos chamam isso de *firehosing*, derivado de *fire hose*, mangueira de incêndio - trata-se da disseminação de uma informação, que pode ser mentirosa, em um fluxo constante, repetitivo, rápido e em larga escala. As pessoas são bombardeadas de todos os lados por uma notícia - sites de notícias, grupos de WhatsApp, Facebook, Instagram — e essa repetição lhes confere a sensação de familiaridade com determinada mensagem". CAMPOS MELLO, Patrícia. A Máquina do Ódio: notas de uma repórter sobre fake news e violência digital. São Paulo: Companhia das Letras, 2020.

A gestão "profissionalizada" desses grupos, por pessoas naturais ou pessoas jurídicas, depende do tratamento abusivo de dados pessoais, o que viola a integridade do nosso sistema informacional e distorce nosso ambiente democrático.

As investigações desses ilícitos precisam ter como enfoque o tratamento de dados pessoais em violação à Lei Geral de Proteção de Dados Pessoais, como é o caso do repasse de bancos de dados com informações de milhões de pessoas (e.g. clientes de uma determinada empresa de telecomunicações) para que uma empresa de "estratégia digital" possa fazer o disparo automatizado por meio do dado pessoal do número de telefone. Uma das estratégias para se desmantelar esquemas profissionalizados de disparo de mensagens e desinformação, tal como descrito por Patrícia Campos Mello, é atacar o "insumo" dessa atividade econômica (a venda desse tipo de serviço para grupos políticos). Sem bases de dados obtidas ilegalmente, os mecanismos de gestão de grupos e disparos automáticos de mensagens não podem operar. Nesse sentido, a Lei Geral de Proteção de Dados Pessoais prevê mecanismos como o "bloqueio dos dados pessoais a que se refere a infração até a sua regularização", ou a "eliminação dos dados pessoais a que se refere a infração", além da multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício (art. 52, LGPD). Esses mecanismos sancionatórios não excluem a aplicação de sanções penais definidas no Código de Defesa do Consumidor e em legislação específica, conforme assegurado no § 2º do art. 52.

Como sugerido pelo governo dos Estados Unidos da América em 2014, há uma importante cadeia econômica a ser investigada: a dos *data brokers*, que podem operar tanto em um ambiente legal, como no caso de empresas que agregam informações públicas, originadas por conta própria ou obtidas legalmente com consentimento, quanto ilegal, como é no caso de empresas especializadas em negociar dados obtidos ilegalmente[52].

Como observado pela AccessNow no relatório "*Your Data Used Against You*"[53] de 2018, o problema de desinformação no Whatsapp pode ser atacado pela investigação de modelos de negócio de "marketing digital" e "estratégia digital" que dependem de dados pessoais obtidos ilegalmente. Incrementar os direitos de proteção de dados pessoais e investigar o modo de operação desses mercados (o modo de funcionamento de serviços de gestão de grupos no WhatsApp) é uma forma mais cautelosa e estratégica de atacar o problema do que adotar soluções normativas com propostas apressadas que podem violar direitos fundamentais.

**52** O documento foi assinado pelos comissários da Federal Trade Commission Edith Ramirez, Julie Brill, Maureen K. Ohlhausen, Joshua D. Wright e Terrell McSweeny. FTC, Data Brokers: A Call for Transparency and Accountability, May, 2014. Disponível em: Disponível em: <https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission--may-2014/140527databrokerreport.pdf>. Acesso em: 14 de outubro de 2021.

**53** PALLERO, Javier; ARROYO, Verónica. *Your data used against you: reports of manipulation on WhatsApp ahead of Brazil's election*, AccessNow, 26/10/2018. Disponível em: <https://www.accessnow.org/your-data-used-against-you-reports-of-manipulation-on-whatsapp-ahead-of-brazils-election/>. Acesso em: 14 de outubro de 2021.

## 2.4. Avaliação de propostas alternativas

Trazemos, em anexo, um comparativo do texto atual do PL 2630 com outras propostas trazidas a público recentemente, e que variam em grau de interferência nos direitos à privacidade e proteção de dados pessoais. Pelos itens já descritos e os argumentos acima, identifica-se o PL 2630 como um nível altíssimo de interferência, ao violar o princípio constitucional da presunção de inocência e demais direitos, tais como o direito à proteção de dados pessoais e à privacidade.

Conforme demonstrado anteriormente, a proposta A[54] prevê a retenção preventiva dos registros de interação de todos os usuários de uma cadeia de mensagens que atinja um determinado número de pessoas, de modo a criar um verdadeiro mecanismo de rastreamento. Nesse sentido, o Projeto representa a proposta mais agressiva em termos de rastreabilidade.

A proposta de B[55], por sua vez, vai de encontro aos princípios de privacidade e proteção de dados pessoais, uma vez que exige que os serviços de mensageria privada guardem pelo prazo de três meses os registros do envio de mensagens, sendo possível vincular o conteúdo das mensagens aos usuários. No tocante à rastreabilidade, esta proposta se assemelha ao PL em discussão, na medida em que pressupõe a guarda da cadeia de mensagens, possibilitando a vinculação do remetente da mensagem ao conteúdo e, em última instância, legitima práticas de vigilantismo estatal.

De acordo com a proposta B, os registros irão conter uma quantidade de metadados considerável e até mesmo desnecessária, afrontando o princípio da minimização dos dados. Nos termos do dispositivo proposto, os registros devem conter, por exemplo, o identificador da conta ou número de telefone vinculado ao usuário remetente da primeira mensagem. Através do cruzamento dos metadados dos registros, é possível realizar inferências (inclusive, sobre dados sensíveis) e chegar à identidade do usuário.

Vale destacar que a viralização de conteúdos no espaço público *online* não diz respeito somente à funcionalidade do encaminhamento, de maneira que rastrear a cadeia não é uma medida eficaz de combate à desinformação. Existem muitas trocas de conteúdo entre diferentes plataformas, e mecanismos que escapam à mencionada cadeia de rastreabilidade, como copiar e colar uma mensagem ou até mesmo uma captura de tela. Além disso, o texto introduz o conceito de "mensagens passíveis de encaminhamento, por solução técnica", porém não esclarece como isso ocorrerá, apenas afirma que as mensagens passíveis de encaminhamento serão assim definidas pelo próprio usuário remetente. De um modo geral, o texto trazido pela proposta B e o próprio texto da proposta A desconsideram a complexidade do funcionamento das comunicações em rede, uma vez que partem da premissa que a comunicação na internet se dá numa cadeia linear. Na realidade, a cadeia de mensagens apresenta  frágil valor probatório para a definição de

**54** Proposta do art.10 do PL 2630/2020.

**55** A proposta foi apresentada por João Brant. Ver: Aperfeiçoamento de legislação brasileira - Internet. Audiência Pública Extraordinária (Virtual) de 24/08/2021. Câmara dos Deputados. Disponível em: <https://www.camara.leg.br/evento-legislativo/62790> Acesso em: 07 out 2021.

autoria frente ao complexo fluxo informacional no ambiente digital. Em resumo, o chamado "encaminhamento em massa" pode se valer de outras ferramentas não rastreáveis.

Por sua vez, a proposta C[56] traz a importante distinção conceitual entre retenção e preservação, sendo mais alinhada ao princípio da presunção de inocência. Em sua proposta, descarta-se a retenção, considerando-se a preservação como preferível a alternativas não testadas quanto à sua eficácia e comprovadamente deletérias em relação aos seus riscos inerentes.

Enquanto a retenção pressupõe o armazenamento preventivo, massivo e indiscriminado de dados em um sistema para que, posteriormente, sejam identifIcados e utilizados, na preservação ocorre a ponderação de quais dados devem guardados, realizando-se uma espécie de "pesca sustentável"[57]. Nessa hipótese, somente os registros de interações dos usuários contra os quais haja indícios de autoria ou participação em infração penal seriam armazenados. Com isso, a proteção dos usuários seria contemplada, ao mesmo tempo que possibilitaria o monitoramento futuro e a identificação do padrão das interações de suspeitos formalmente investigados em aplicativos de mensageria.

Nesta proposta, porém, a possibilidade do requerimento cautelar pela autoridade policial ou Ministério Público enseja uma interferência considerável nos direitos e garantias fundamentais do usuário, na medida em que basta um mero pedido administrativo para haver a preservação dos dados, deixando a autorização judicial em segundo plano.

Comparativamente à proposta C, o texto sugerido pela proposta D[58] apresenta um menor grau de interferência na esfera de direitos do titular, sendo, portanto, a alternativa mais proporcional.

Esta proposta igualmente recorre à preservação, porém reforça a camada de proteção do usuário ao prever o dever de eliminação dos registros pelo provedor após findo o prazo ou denegado o pedido de prorrogação da preservação. Ou seja, aqui o Poder Judiciário atua no primeiro plano de salvaguardas, impedindo que haja o alargamento da retenção massiva de metadados mediante mero pedido administrativo.

Quanto ao prazo de prorrogação do pedido de preservação, a proposta D é ainda mais restritiva. A proposta C prevê a possibilidade de se renovar o prazo de 15 dias por igual período, até o máximo de

**56** Esta proposta foi elaborada por Flávia Lefèvre e Diego Canabarro, endossada pelo Professor Danilo Doneda. Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/um-novo-caminho-para-investigacoes-em-aplicativos-de-mensagens-05102021>. Acesso em: 20 out 2021.

**57** Ibid.

**58** Esta proposta, de relatoria de Laura Schertel Mendes, foi apresentada na Câmara dos Deputados em 09 de setembro de 2020 pela Comissão de Juristas responsável pela elaboração do Anteprojeto de Lei sobre proteção de dados em segurança pública e investigações criminais. Disponível em: <https://www.internetlab.org.br/wp-content/uploads/2020/09/Manifestac%CC%A7a%CC%83o-da-Comissa%CC%83o-de-Juristas-da-Ca%CC%82mara.pdf>. Acesso em: 20 out 2021.

60 dias, permitindo que se faça o pedido por quatro vezes. Já o texto sugerido pela proposta D somente autoriza a renovação por até duas vezes, mediante nova ordem judicial específica. Em síntese, a proposta D representa um caminho viável que compatibiliza a devida persecução criminal com os direitos e princípios constitucionais, tais como presunção de inocência, o direito fundamental à liberdade de comunicação, bem como o direito à privacidade e à proteção de dados pessoais.

ANEXO I

## SUGESTÕES DE REDAÇÃO AO PL 2630/2020

| PL 2630/2020 | Sugestão de Redação | Fundamentação resumida |
|---|---|---|
| Art. 10. Os serviços de mensageria privada devem guardar os registros dos envios de mensagens veiculadas em encaminhamentos em massa, pelo prazo de 3 (três) meses, resguardada a privacidade do conteúdo das mensagens.<br><br>§1º Considera-se encaminhamento em massa o envio de uma mesma mensagem por mais de 5 (cinco) usuários, em intervalo de até 15 (quinze) dias, para grupos de conversa, listas de transmissão ou mecanismos similares de agrupamento de múltiplos destinatários.<br><br>§2º Os registros de que trata o caput devem conter a indicação dos usuários que realizaram o encaminhamento em massa da mensagem, com data e horário do encaminhamento e o quantitativo total de usuários que receberam a mensagem.<br><br>§3º O acesso aos registros somente poderá ocorrer com o objetivo de responsabilização pelo encaminhamento em massa de conteúdo ilícito, para constituição de prova em investigação criminal e em instrução processual penal, mediante ordem judicial, nos termos da Seção IV do Capítulo III da Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). | Supressão | O art. 10 deve ser suprimido pois, ao alargar o regime de retenção de metadados, relativiza o princípio da presunção da inocência e representa uma interferência desproporcional ao direito fundamental à proteção de dados pessoais. |

| | | |
|---|---|---|
| §4º A obrigatoriedade de guarda prevista neste artigo não se aplica às mensagens que alcançarem quantitativo total inferior a 1.000 (mil) usuários, devendo seus registros ser destruídos nos termos da Lei 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais) | | |
| Art. 35 - A Lei nº 12.695, de 23 de abril de 2014 (Marco Civil da Internet), passa a vigorar com as seguintes alterações:<br><br>"Art.5º ...<br>VIII - registros de acesso a aplicações de internet: o conjunto de informações referentes à data e à hora de uso de uma determinada aplicação de internet a partir de um determinado endereço IP e a porta lógica, quando o IP for nateado;<br><br>IX - nateamento de IP: o compartilhamento de IP para mais de uma conexão ou usuário único, individualizadas através de diferentes portas lógicas; e<br><br>X - portas lógicas: os dispositivos que operam e trabalham com um ou mais sinais lógicos de entrada para produzir uma e somente uma saída." (NR)<br><br>"Art. 15. O provedor de aplicações de internet constituído na forma de pessoa jurídica e que exerça essa atividade | Supressão. | O art. 35 deve ser suprimido porque a ampliação do dever de guarda dos logs para incluir também as portas lógicas do IP desarmoniza com as diretrizes principiológicas e direitos e garantias do Marco Civil da Internet e de seu Decreto Regulamentador[59]. Além disso, a inclusão de portas lógicas no dever de guarda ignora o amplo debate multissetorial que optou pela redação anterior, menos abrangente. Por fim, e não menos importante, o art. 35 deve ser suprimido não é tecnologicamente neutro e pode se tornar obsoleto com a emergência de novos padrões tecnológicos. |

**59** BRASIL. Decreto nº 8.771/2016. Regulamenta a Lei nº 12.965, de 23 de abril de 2014, para tratar das hipóteses admitidas de discriminação de pacotes de dados na internet e de degradação de tráfego, indicar procedimentos para guarda e proteção de dados por provedores de conexão e de aplicações, apontar medidas de transparência na requisição de dados cadastrais pela administração pública e estabelecer parâmetros para fiscalização e apuração de infrações. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/d8771.htm>. Acesso em: 08 de outubro de 2021.

| | | |
|---|---|---|
| de forma organizada, profissionalmente e com fins econômicos deverá manter os respectivos registros de acesso a aplicações de internet, inclusive os registros que individualizem o usuário de um IP de uma maneira inequívoca, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 06 (seis) meses, nos termos do regulamento. ..." (NR) | | |
| Sem correspondente direto<br>(inclusão no artigo 5º referente à definições) | Art. 4º Para os efeitos desta Lei, considera-se:<br>(...)<br><br>X – Perfilhamento: qualquer forma de tratamento parcial ou automatizado de dados para avaliar certos aspectos pessoais de uma pessoa natural, especialmente com o relação ao seu desempenho profissional, a sua situação econômica, saúde, preferências pessoais, interesses, localização; | As atividades de perfilhamento são parcela importante do fenômeno da desinformação. Desse modo, conceitualizar o termo é importante para a regulamentação de qualquer prática de direcionamento de conteúdos e mensagens. |
| Sem correspondente direto<br>(inclusão no artigo 15 referente à definições) | Art. 15. Os provedores de redes sociais que fornecerem impulsionamento de propaganda eleitoral ou de conteúdos que mencionem candidato, coligação ou partido devem disponibilizar ao público todo o conjunto de anúncios para efeito de checagem pela Justiça Eleitoral e outros fins, incluindo:<br><br>(...)<br>VI – as técnicas e as categorias de perfilhamento<br>VII - cópia eletrônica das mensagens e o nome do responsável pela autorização de seu envio.<br>VIII- os links para o registro se os anúncios eleitorais forem exibidos | As técnicas de perfilhamento têm sido utilizadas de modo pouco transparente, criando uma assimetria informacional demasiada das aplicações e anunciantes em relação aos usuários.<br><br>Assim, é importante que, sempre que houver a prática de perfilhamento, o usuário possa: (i) saber que conteúdos lhe foram direcionados a partir do uso de tais técnicas; (ii) acessar as categorias utilizadas pela aplicação e selecionadas pelo anunciante para realização do direcionamento de conteúdos; (iii) acessar informações claras a respeito de como lhe foram aplicadas as determinadas categorias. O objetivo é garantir que o titular dos dados possua |

| | | |
|---|---|---|
| Sem correspondente direto<br>(inclusão no artigo 16 referente à definições) | Art. 16. Os provedores de redes sociais devem disponibilizar mecanismos para fornecer aos usuários as informações do histórico dos conteúdos impulsionados e publicitários com os quais a conta teve contato nos últimos 6 (seis) meses, especialmente:<br><br>I - Se foi aplicado algum tipo de técnica de perfilhamento;<br><br>II - as categorias de perfilhamento nos quais o usuário foi incluído;<br><br>III - informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para perfilhamento, nos termos do artigo 20§ 1º, da LGPD | equivalência de conhecimento sobre o tratamento de suas informações em relação aos agentes que fazem uso de seus dados.<br><br>A transparência é um dos princípios da Lei Geral de Proteção de Dados e, nesse caso, assume importância ao permitir que o usuário faça análise crítica a respeito do tratamento de seus dados pessoais e exerça seu controle informacional. |
| Sem correspondente direto<br>(inclusão de novo artigo nas Disposições Finais ) | Art. 35-A. A Lei nº 9.504, de 30 de setembro de 1997 (Lei das Eleições), passa a vigorar com as seguintes alterações:<br><br>Art. 26 (...)<br><br>XVI - despesas relacionadas à contratação de serviço de tratamento de dados; | Importa saber, para fins de uma devida prestação de contas, quais as despesas relativas à contratação de serviços de tratamento de dados. A falta de distinção a respeito das despesas das campanhas com marketing torna difícil saber não só quanto foi gasto, mas onde foi gasto o financiamento. Isso gera um grave problema em relação a falta de transparência sobre a alocação de recursos partidários, assim como facilita o mau uso dos dados pessoais da população.<br><br>Conforme apontado por diversas pesquisas, o tratamento de dados pessoais para fins de elaboração das estratégias de campanha eleitoral é cada vez mais comum e envolve uma série de atores. Assim, importa saber quem são os atores financiados e se o tratamento por eles realizado se dá em conformidade à Lei e aos princípios da proteção de dados. |

| | | |
|---|---|---|
| Sem correspondente direto<br>(inclusão de novo artigo nas Disposições Finais ) | Art. 35-B. A Lei nº 9.504, de 30 de setembro de 1997 (Lei das Eleições), passa a vigorar com as seguintes alterações:<br><br>Art. 26 (...)<br>§ 4o (...)<br><br>III - o registro das suas atividades de tratamento de dados, nos termos do artigo 37 da Lei 13.709, de 14 de agosto de 2018 | Da mesma forma, quando o partido fizer uso de uma base de dados própria, é essencial que se mantenha um nível de transparência sobre as atividades de tratamento desenvolvidas.<br><br>A prestação de contas deve se dar não apenas sob uma camada financeira, mas também informacional,de modo que seja possível avaliar se a coleta, processamento e uso dos dados pelos partidos, candidatos e coligações ocorreu em conformidade à Lei e aos princípios da proteção de dados pessoais. |

## ANÁLISE COMPARATIVA DAS PROPOSTAS SOBRE RASTREABILIDADE – Proposta A

| Dispositivo | Prós | Contras |
|---|---|---|
| Art. 10. Os serviços de mensageria privada devem guardar os registros dos envios de mensagens veiculadas em encaminhamentos em massa, pelo prazo de 3 (três) meses, resguardada a privacidade do conteúdo das mensagens. | O caput do dispositivo indica como se dará o dever de retenção, precisando em que momento se inicia o dever de retenção de dados por parte das provedores de serviços. Isto é, aponta que a guarda irá ocorrer quando houver encaminhamentos em massa e que o armazenamento dos dados descritos posteriormente, para fins desta lei, deverá durar 3 (três) meses. | Ao alargar o regime de retenção de dados, o PL flexibiliza o art. 5º, XVI e LVII, CF, colidindo com uma de garantias constitucionais inerentes ao estado democrático de direito: mais especificamente, o princípio da presunção da inocência e o direito de reunião. Isso se dá porque a guarda da cadeia de rastreabilidade coloca sob vigilância não somente quem distribui falsas informações, mas também aqueles que fazem uso legítimo das plataformas.<br><br>Por outro lado, pode-se falar, ainda, em um efeito inibitório para a liberdade de expressão. Explica-se: o art. 10 promove o rastreamento massivo porque, na prática, não há como antever as mensagens que preencherão as condições do comando normativo, de modo que torna-se necessário o rastreamento *a priori* de todas as mensagens, uma condição não explicitada no texto. O efeito inibitório que resulta de tal medida é ainda mais agravante quando consideradas as revelações que podem advir dos metadados, como a cadeia de comunicação dos usuários. Além de constituir divergência com normas de proteção de dados, o ponto abre margem para perseguição política e exposição de grupos, bem como termina por ameaçar a liberdade de reunião.<br><br>Além disso, também são alarmantes os riscos que o art. 10 |

traz ao princípio da presunção da inocência. Em primeiro lugar, o rastreamento massivo atinge também a parcela populacional fora do escopo de suspeição. Muitos dos conteúdos compartilhados em serviços de mensageria são encaminhados por uma série de razões, nem sempre coniventes com as do autor da mensagem. É o caso de denúncias: com a medida de rastreabilidade, inocentes que realizam encaminhamentos de mensagem para fim de denúncia podem ser considerados partícipes.

A Corte Europeia de Justiça já decidiu no sentido de considerar  desproporcional a retenção preventiva de dados, ainda que apenas metadados, considerando o grau de lesividade destas informações.

| | | |
|---|---|---|
| § 1º Considera-se encaminhamento em massa o envio de uma mesma mensagem por mais de 5 (cinco) usuários, em intervalo de até 15 (quinze) dias, para grupos de conversas, listas de transmissão ou mecanismos similares de agrupamento de múltiplos destinatários. | O parágrafo busca estabelecer critérios mínimos para diferenciar mensagens que atrairiam a medida da rastreabilidade. Ao contemplar apenas mecanismos que agregam múltiplos destinatários, como listas de transmissão e grupos de conversas, são excluídas da norma as conversas privadas, trazendo um mínimo de preservação. | Em primeiro lugar, a distinção que se buscou fazer entre comunicações privadas e aquelas que atingem um número maior de usuários não pode ser considerada factível. Como já explicado na análise do caput, o rastreamento de mensagens termina por ocorrer de forma prévia e generalizada para que seja capaz de mapear as mensagens que preencham as condições do art. 10. Portanto, cai por terra qualquer finalidade de definir o que seria o encaminhamento em massa: por razões técnicas e práticas, todo e qualquer encaminhamento de mensagens, em grupos ou conversas privadas, seria atingido pelo rastreamento.<br><br>Ainda mais importante, o comando é inócuo, pois existem diversas formas de burlar o encaminhamento das mensagens à disposição de agentes que tenham a intenção de |

| | | |
|---|---|---|
| | | disseminar conteúdo. Por meio do uso de técnicas bem simples, tais como copiar e colar o teor da mensagem, captura de tela e troca de caracteres, é possível quebrar a cadeia de rastreabilidade. Portanto, o chamado "encaminhamento em massa" pode se valer de outras ferramentas não rastreáveis. Na medida em que o dispositivo não considera outras técnicas de encaminhamento massivo, a proposta sugere um mecanismo de combate à desinformação de baixa eficácia prática. |
| § 2º Os registros de que trata o caput devem conter a indicação dos usuários que realizaram encaminhamentos em massa da mensagem, com data e horário do encaminhamento e o quantitativo total de usuários que receberam a mensagem. | | O cruzamento dos dados mencionados (os metadados) pode levar à identificação do usuário. Os metadados permitem construir um cenário para a comunicação, possibilitando inúmeras inferências, inclusive a dados sensíveis. Ou seja, é possível identificar quem fala o quê e até seu padrão de comportamento, consistindo em vigilância massiva. |
| § 3º O acesso aos registros somente poderá ocorrer com o objetivo de responsabilização pelo encaminhamento em massa de conteúdo ilícito, para constituição de prova em investigação criminal e em instrução processual penal, mediante ordem judicial, nos termos da Seção IV do Capítulo III da Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). | A medida estabelece um rigor mínimo para acesso aos registros. A figura do Poder Judiciário aparece como um ator equidistante para balancear os interesses legítimos da persecução penal e direitos fundamentais dos sujeitos investigados. | Em primeiro lugar, a rastreabilidade não segue o princípio de minimização dos dados, posto tanto pelo Marco Civil da Internet quanto pela Lei Geral de Proteção de Dados Pessoais.<br><br>Além disso, o dispositivo viola frontalmente os princípios da reserva legal e da proporcionalidade em sentido estrito, uma vez se vale do conceito de "conteúdo ilítico" para responsabilizar o usuário, possibilitando que crimes de menor potencial lesivo pudessem ser alvo de medidas extremamente invasivas.<br><br>A proposta se revela ainda ineficaz: ainda que fosse possível identificar a primeira pessoa a compartilhar |

| | | |
|---|---|---|
| | | determinado conteúdo em um aplicativo, não há como garantir que ela é a autora, pois o conteúdo pode ter sido produzido em outros meios ou redes sociais. Seria possível ainda que o usuário interrompesse o registro, iniciando uma nova cadeia de mensagens, o que novamente levaria ao problema de identificação sobre autoria.<br><br>Por fim, considerando que desinformação sequer é definida no PL, nem é tipificada como crime, condutas relacionadas à disseminação de desinformação não se enquadrariam na hipótese delineada no dispositivo. |
| § 4º A obrigatoriedade de guarda prevista neste artigo não se aplica às mensagens que alcançarem quantitativo total inferior a 1.000 (mil) usuários, devendo seus registros ser destruídos nos termos da Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais). | O dispositivo busca excluir da incidência da norma um grupo significativo de mensagens. Além disso, traz menção à Seção IV da LGPD, sobre o término do tratamento de dados pessoais. | A principal questão quanto ao dispositivo é que o alcance das mensagens pode ser burlado, como já mencionado, por outras ferramentas como captura de tela e copiar e colar, o que torna irrelevante o número de 1.000 usuários. A proposta desconsidera o funcionamento de rede da Internet (não é uma cadeia linear).<br><br>Além disso, o parágrafo também é questionável em termos de técnica legislativa. Note-se que o caput do art. 10 é claro ao indicar que apenas mensagens veiculadas em encaminhamentos em massa devem ter seus registros guardados. O §4º, por sua vez, afirma que a guarda de mensagens que atinjam menos de 1.000 usuários não é obrigatória; entretanto, indica que os registros de tais mensagens "devem ser destruídos". Ora, se não há guarda, não há o que ser destruído: aqui, percebe-se uma margem de ambiguidade nas entrelinhas ou, ainda mais grave, a sugestão de que tal registro seria cabível em algum momento, mesmo sem qualquer finalidade aplicável, em desconformidade com a LGPD e garantias processuais penais. |

## AVALIAÇÃO

Grau de interferência na esfera de direitos e garantias fundamentais: **ALTÍSSIMO**

É questionável a eficácia da proposta em vista da série de métodos possíveis que burlariam (gamificariam) a rastreabilidade da cadeia de desinformação. Além disso, o dever de retenção de dados preventivo vai de encontro a uma série de direitos e liberdades fundamentais como da presunção de inocência, liberdade de expressão e direito de reunião de todos os usuários dos serviços de mensageria atingidos pelo dispositivo. Em suma, a análise custo-benefício se mostra frustrada.

## Proposta B

| Dispositivo | Prós | Contras |
|---|---|---|
| Art. XX - Os serviços de mensageria privada devem guardar pelo prazo de três meses os registros do envio de mensagens passíveis de encaminhamento e o quantitativo de usuários alcançados, resguardado o sigilo do conteúdo das mensagens[60]. | O caput do dispositivo indica como se dará o dever de retenção, precisando em que momento se inicia o dever de retenção de dados por parte das provedores de serviços. Isto é, aponta que a guarda irá ocorrer quando houver encaminhamentos em massa e que o armazenamento dos dados descritos posteriormente, para fins desta lei, deverá durar 3 (três) meses. | O fato de mensagens serem encaminhadas em massa não retira desses dados as proteções que lhes são aplicáveis. Em outras palavras, o artigo comete uma confusão conceitual sobre privacidade e proteção de dados, ao sugerir que a publicidade afastaria a proteção.<br><br>Assim como o PL, esta proposta autoriza a guarda da cadeia de rastreabilidade, legitimando um estado de constante vigilância massiva, notadamente infringindo direitos fundamentais.<br>Neste sentido, viola o art. 5º, XVI e LVII, CF, colidindo com o princípio constitucional da presunção de inocência e o direito de reunião. Isso se dá porque a guarda da cadeia de rastreabilidade, coloca sob vigilância não somente quem distribui falsas informações, como quem faz uso legítimo das plataformas.<br><br>Adicionalmente, pode-se falar, ainda, em um efeito inibitório para a liberdade de expressão. Explica-se: o art. 10 promove o rastreamento massivo porque, na prática, não há como antever as mensagens que preencherão as condições do comando normativo, de modo que torna-se necessário o rastreamento a priori de todas as mensagens, uma condição não explicitada no texto. O efeito inibitório que resulta de tal medida é ainda mais agravante quando |

**60** Errata: A Associação Data Privacy Brasil de Pesquisa identificou a existência de um equívoco na transcrição do *caput* do artigo apresentado na Proposta B analisada em nossa nota técnica. A transcrição já foi corrigida neste documento e não alterou nossa análise, fundamentação e conclusão quanto à proposta.

| | | |
|---|---|---|
| | | consideradas as revelações que podem advir dos metadados, como a cadeia de comunicação dos usuários. Além de constituir divergência com normas de proteção de dados, o ponto abre margem para perseguição política e exposição de grupos, bem como termina por ameaçar a liberdade de reunião.<br><br>Inclusive, a Corte Europeia de Justiça já decidiu no sentido de considerar desproporcional a retenção preventiva de dados, ainda que apenas metadados, considerando o grau de lesividade destas informações. |
| §1º São consideradas mensagens passíveis de encaminhamento aquelas que tenham sido definidas assim pelo usuário remetente, por meio de solução técnica oferecida pelos serviços de mensageria privada. | Não foram identificados | Não esclarece como seriam definidas "mensagens passíveis de encaminhamento, por solução técnica". Essa autorização que tornaria a mensagem não só passível de encaminhamento, mas que permitiria a sua retenção, de ser feita por meio de consentimento informado, livre, inequívoco e expresso, vinculado a uma finalidade determinada. De modo a estar alinhado com as previsões do Marco Civil da Internet (art. 7º, IX, e 16) e da Lei Geral de Proteção de Dados (art. 5º, XII), o que não ocorre no texto desta proposta. |
| §2º Os registros de que trata o caput devem conter:<br>I - o registro de acesso à aplicação do usuário que fez o primeiro envio da mensagem<br><br>II - o identificador da conta ou número de telefone vinculado ao usuário remetente da primeira mensagem, quando cabível | Não foram identificados | O cruzamento dos dados mencionados (os metadados) pode levar à identificação do usuário. Os metadados permitem construir um cenário para a comunicação, possibilitando inúmeras inferências, inclusive a dados sensíveis. Ou seja, é possível identificar quem fala o quê e até seu padrão de comportamento, consistindo em vigilância massiva.<br><br>O alcance das mensagens pode ser burlado, como |

| | | |
|---|---|---|
| III - o quantitativo total de usuários alcançados por tal conteúdo em todos os encaminhamentos sucessivos, sem indicação individual destes usuários. | | já mencionado, por outras ferramentas facilmente utilizáveis - como captura de tela e copiar e colar- , o que torna inviável descobrir o quantitativo total de usuários alcançados. A proposta desconsidera o complexo funcionamento de rede da Internet (não opera em uma cadeia linear). |
| §3º O acesso aos registros somente poderá ocorrer com o objetivo de responsabilização pelo encaminhamento de conteúdo mediante ordem judicial, nos termos da Seção IV do Capítulo III da Lei nº 12.965, de 23 de abril de 2014. | A medida estabelece um rigor mínimo para acesso aos registros. A figura do Poder Judiciário aparece como um ator equidistante para balancear os interesses legítimos da persecução penal e direitos fundamentais dos sujeitos investigados. O dispositivo menciona o Marco Civil da Internet, condicionando o acesso aos registros à finalidade de responsabilização. | Embora mencione o Marco Civil da Internet, o dispositivo se revela contraditório uma vez que rastreabilidade não segue o princípio de minimização dos dados, posto tanto pelo Marco Civil da Internet quanto pela Lei Geral de Proteção de Dados Pessoais.<br><br>A proposta também deixa muito amplo o objeto da responsabilização, uma vez que não há nenhuma descrição que precise o tipo de conteúdo que estará sujeito a rastreamento.<br><br>Além disso, proposta se revela ainda ineficaz: ainda que fosse possível identificar a primeira pessoa a compartilhar determinado conteúdo em um aplicativo, não há como garantir que ela é a autora, pois o conteúdo pode ter sido produzido em outros meios ou redes sociais. Seria possível ainda que o usuário interrompesse o registro, iniciando uma nova cadeia de mensagens, o que novamente levaria ao problema de identificação sobre autoria.<br><br>Por fim, considerando que desinformação sequer é definida no PL, nem é tipificada como crime, condutas relacionadas à disseminação de desinformação não se enquadrariam na hipótese delineada no dispositivo. |

## AVALIAÇÃO

Grau de interferência na esfera de direitos e garantias fundamentais: **ALTÍSSIMO**

Esta proposta não traz muitos avanços em termos da proteção dos direitos fundamentais e, em especial, à proteção de dados pessoais, em relação à proposta original. É também questionável a eficácia da proposta em vista da série de métodos possíveis que burlariam (gamificariam) a rastreabilidade da cadeia de desinformação. Além disso, o dever de retenção de dados preventivo vai de encontro a uma série de direitos e liberdades fundamentais como da presunção de inocência, liberdade de expressão e direito de reunião de todos os usuários dos serviços de mensageria atingidos pelo dispositivo. No mais, a proposta falha ao não se basear nos preceitos do Marco Civil da Internet e da Lei Geral de Proteção de Dados Pessoais como a exigência de consentimento informado, livre, inequívoco e expresso, e princípios da proteção de dados como a minimização.

## Proposta C

| Dispositivo | Prós | Contras |
|---|---|---|
| Art. XX. Para fins de constituição de prova em investigação criminal e em instrução processual penal, a autoridade judicial pode determinar aos provedores de serviço de mensageria privada a preservação e disponibilização dos registros de interações de usuários determinados por um prazo de até 15 (quinze) dias, considerados os requisitos estabelecidos no artigo 2º da Lei 9.296/1996, vedados os pedidos genéricos ou fora do âmbito e dos limites técnicos do seu serviço. | O dispositivo fala em "preservação" na qual ocorre ponderação ao se selecionar apenas uma parcela dos dados de interação para serem armazenados, eliminando os riscos que existiriam com sua coleta massiva e integral. A escolha pela preservação dos registros já demonstra uma maior preocupação com os direitos e garantias fundamentais. Ao contrário da retenção, a preservação minimiza os riscos de uma retenção preventiva indiscriminada e generalizante de metadados.<br><br>A menção aos requisitos do art. 2º da Lei 9.296/1996 como condicionantes para o registro de interações adiciona mais uma camada de proteção condizente com as normas de processo penal. | O dispositivo permite monitorar indivíduos sem indícios de autoria ou materialidade, abrindo brecha para que os usuários sejam rastreados mesmo sem serem os efetivos autores da infração.<br>Além disso, a preservação dos registros é disparada mediante mero pedido administrativo e não por uma ordem judicial e, consequentemente, o ato autorizativo do Poder Judiciário se encontra num segundo plano de camadas de salvaguardas. |
| § 1º Os registros de que trata o caput correspondem aos dados de envio e recebimento de mensagens e chamadas de áudio por sua conta e devem incluir data e hora de sua ocorrência, sendo vedada a associação desses registros ao conteúdo das comunicações. | Vedação expressa à associação dos registros de dados de envio e recebimento de mensagens e chamadas de áudio, incluindo data e hora de sua ocorrência com o conteúdo das comunicações. Essa vedação está alinhada com a perspectiva de minimização (princípio da necessidade e adequação). | Ainda há coleta de metadados, que por poderem permitir inferência importantes sobre o titular dos dados, deve ser tratada com cautela. |
| § 2º O prazo de que trata o caput poderá ser renovado por igual período até o máximo de 60 (sessenta) dias, desde que comprovada a indispensabilidade do meio de prova. | A condição para extensão de prazo garante que apenas serão mantidos registros de indivíduos que já estão sendo processados, sendo a renovação decidida por juiz de direito, da mesma forma como ocorre com as interceptações telefônicas. | O texto possibilita que a extensão do prazo chegue ao dobro (60 dias) do máximo previsto na Lei nº 9.296/1996 (15 dias renováveis por igual período).<br><br>Em comparação ao Marco Civil da Internet, o prazo da |

| | | |
|---|---|---|
| | | proposta é inferior uma vez que a legislação estabelece que o provedor de aplicações de internet deverá manter os respectivos registros de acesso a aplicações de internet pelo prazo de 6 (seis) meses (art. 15). |
| § 3º A autoridade policial ou o Ministério Público poderão requerer cautelarmente aos provedores de serviço de mensageria privada a preservação dos dados de que trata o caput, devendo ingressar com o pedido de autorização judicial de acesso aos respectivos registros em prazo não superior a 30 (trinta) dias, contado da requisição de preservação de registros. | O prazo de 15 dias somente pode ser renovado por no máximo 60 dias, mediante o critério de comprovação de indispensabilidade da prova. Além disso, condiciona a continuidade da preservação dos dados ao escrutínio do Poder Judiciário. | A possibilidade do requerimento cautelar pela autoridade policial ou Ministério Público enseja uma interferência considerável nos direitos e garantias fundamentais do usuário na medida em que basta um mero pedido administrativo para haver a preservação dos dados.<br><br>De acordo com o dispositivo, o requerimento cautelar passará pelo crivo do Poder Judiciário posteriormente em até 30 dias. Isto é, a análise da validade do requerimento será feita pelo juiz em caráter *ex post*, deslocando a autorização judicial para um segundo plano da camada de salvaguardas.<br><br>Além disso, a proposta não explicita sob quais critérios ou circunstâncias a autoridade policial ou o MInistério Público podem solicitar a preservação dos registros de forma cautelar. |
| § 4º Diante de decisão judicial que indefira o pedido de disponibilização dos dados objeto de requisição de preservação ou caso não seja apresentado pedido de autorização judicial de acesso aos registros dentro do prazo fixado no § 3º, o provedor de serviço de mensageria privada deverá proceder sua eliminação em até 10 (dez) dias, respectivamente, da referida decisão ou do decurso de prazo. | A requisição de informações adicionais deve vir da autoridade judicial e ocorre somente em relação à indivíduo específico. Além disso, requisição de informações adicionais não implica em demanda por dados além dos já preservados, e não significa uma obrigação a mais para os provedores de serviços, em termos de manutenção de preservação de dados. | A proporcionalidade da interferência em direitos fundamentais está associada à reserva de jurisdição (ou seja, emissão de ordem ou autorização judicial) e especialmente ao princípio da legalidade.<br><br>Nesse sentido, a lei precisa delimitar quais devem ser os tipos de informações adicionais a serem disponibilizadas pelo provedor de serviços, não devendo ficar à cargo da |

| | | |
|---|---|---|
| | | autoridade judicial, numa análise posterior, determinar quais dados seriam. |
| § 5º A autoridade judicial também poderá requisitar a disponibilização de informações adicionais relacionadas ao usuário determinado, na medida de sua disponibilidade para o provedor de serviços nos últimos 60 dias e dentro do escopo e limite de seus serviços, como denúncias de outros usuários do serviço, suspensão ou banimento de conta. | A requisição de informações adicionais deve vir da autoridade judicial e ocorre somente em relação à indivíduo específico. Além disso, requisição de informações adicionais não implica em demanda por dados além dos já preservados, e não significa uma obrigação a mais para os provedores de serviços, em termos de manutenção de preservação de dados. | A proporcionalidade da interferência em direitos fundamentais está associada à reserva de jurisdição (ou seja, emissão de ordem ou autorização judicial) e especialmente ao princípio da legalidade.<br><br>Nesse sentido, a lei precisa delimitar quais devem ser os tipos de informações adicionais a serem disponibilizadas pelo provedor de serviços, não devendo ficar à cargo da autoridade judicial, numa análise posterior, determinar quais dados seriam. |

**AVALIAÇÃO**

Grau de interferência na esfera de direitos e garantias fundamentais: **MÉDIO**

Frente às duas propostas anteriores, esta está mais alinhada ao princípio da presunção de inocência uma vez que não prevê a retenção prospectiva de metadados de alvos específicos e não preventiva da população de forma ampla e geral. No entanto, é problemática por permitir que a preservação dos registros das interações ocorra mediante simples pedido administrativo sem ordem judicial. Além disso, a proposta peca ao não precisar quais seriam os metadados passíveis de serem disponibilizados de acordo com requisição de autoridade judicial, o que fere o princípio (da reserva) da legalidade haja vista que qualquer limitação a direito fundamental deve ser estabelecida por lei e não ser objeto de delegação ao judiciário.

## Proposta D

| Dispositivo | Prós | Contras |
|---|---|---|
| Art. 10. A preservação e o acesso aos registros de interação de usuários nos serviços de mensageria privada somente será admitida mediante autorização judicial específica, circunscrita a usuários determinados sobre os quais recaia fundada suspeita de autoria de infração penal, e para fins de constituição de prova em investigação criminal ou instrução processual penal. | Ao contrário de haver uma retenção preventiva massiva, o dispositivo propõe uma preservação prospectiva e pontual. Assim, a retenção e o acesso aos registros das interações de usuários (registros de envio e recebimento de mensagens de uma conta, data e hora) somente devem ser admitidos em relação a indivíduos determinados e sobre os quais recaia fundada suspeita de cometimento de crimes e após autorização judicial.<br><br>Ao contrário da proposta C, o texto sugerido pela proposta D somente autoriza a preservação mediante ordem judicial de modo e, portanto, a atuação do Poder Judiciário está no primeiro plano das camadas de salvaguardas. | O dispositivo, embora tenha optado pela preservação em detrimento da retenção, ainda assim amplia o quadro já existente de armazenamento de metadados. |
| § 1º A decisão deverá ser fundamentada, evidenciando a necessidade da preservação dos registros para apuração de infração penal, sendo vedados pedidos genéricos. | Reforça a necessidade de fundamentação da decisão que autorizará a preservação e acesso a registros de interação dos usuários de serviços de mensageria. | Não foram identificados |
| § 2º Os registros de que trata o caput correspondem aos dados de envio e recebimento de mensagens de uma determinada conta, incluindo data e hora do envio, sendo vedada a associação desses registros ao conteúdo das comunicações. | Vedação expressa à associação dos registros de dados de envio e recebimento de mensagens (incluindo data e hora) com o conteúdo das comunicações. Assim como a proposta C, essa vedação confere ao titular de dados mais proteção. Em contrapartida ao texto proposto na proposta C, a proposta da Comissão não abre a possibilidade para que o Poder Judiciário amplie ainda mais quais metadados devem ser fornecidos, estando de acordo com o princípio da legalidade. | Não foram identificados |

| | | |
|---|---|---|
| § 3º O fato investigado deve constituir infração penal punida com pena de reclusão; | A proposta busca definir por qual conduta o usuário poderá ser investigado, delimitando escopo do pedido de preservação e acesso aos registros.<br>Isto é, de acordo com a proposta, não se pode solicitar a preservação e acesso aos metadados caso não se trate de uma infração penal punida com pena de reclusão (privativa de liberdade). Dito de outra forma, o texto sugerido traz mais um critério de acesso aos registros na medida que circunscreve o fato investigado àqueles previstos pelo ordenamento jurídico brasileiros como condutas mais gravosas e portanto, sujeitas à pena privativa de liberdade. Nesse sentido, todo ato que não é punido com pena de reclusão está fora do escopo deste dispositivo. | Com essa delimitação, a proposta exclui os demais tipos penais cuja pena não seja reclusão. Desse modo, a aplicação do dispositivo acaba sendo limitada, o que, em certa medida, pode prejudicar a persecução penal já que o pedido de acesso aos registros só poderá ocorrer quando a infração for punida com pena de reclusão. Nos demais casos, esse recurso não poderia ser utilizado, optando-se por meios menos invasivos. |
| § 4º O prazo de preservação não poderá ultrapassar 15 (quinze) dias, podendo ser renovado por até duas vezes mediante nova ordem judicial específica. | Nesse aspecto, o dispositivo é ainda mais restritivo que a proposta C que prevê a possibilidade de se renovar o prazo de 15 dias por igual período em até 60 dias, permitindo que se faça o pedido por quatro vezes.<br><br>A proposta da Comissão somente autoriza a renovação por até duas vezes mediante nova ordem judicial específica, restringindo o acesso aos registros pela autoridade policial e Ministério Público. | Não foram identificados |
| § 5º Denegada a prorrogação da preservação e disponibilização dos dados ou exaurido o prazo de que trata o inciso III, deverá o provedor eliminar os referidos registros no prazo de 15 (quinze) dias. | Nesse ponto, a proposta demonstra uma maior preocupação com os direitos e garantias fundamentais. Consoante com a Lei nº 9.296/96, o dispositivo propõe a fixação de um prazo de modo que após findo esse prazo ou denegada a prorrogação da preservação, os dados devem ser necessariamente eliminados pelos provedores de aplicação em até 15 (quinze) dias. | Não foram identificados |

**AVALIAÇÃO**

Grau de interferência na esfera de direitos e garantias fundamentais: **BAIXO**

Na proposta D, o Poder Judiciário atua no primeiro plano de salvaguardas, impedindo que haja o alargamento da retenção massiva de metadados mediante mero pedido administrativo. Comparativamente à proposta C, o texto sugerido pela Comissão é mais cuidadoso e preocupado com o ciclo de vida dos dados pessoais na medida em que somente autoriza o pedido de prorrogação do prazo de preservação por duas vezes e prevê um prazo máximo de quinze dias para a eliminação dos registros. De uma forma geral, esta proposta é a alternativa mais proporcional uma vez que busca compatibilizar a devida persecução criminal com os direitos e princípios constitucionais como presunção de inocência, o direito fundamental à liberdade de comunicação, à privacidade e à proteção de dados pessoais.