RASTREABILIDADE, METADADOS & DIREITOS FUNDAMENTAIS: NOTA TÉCNICA SOBRE O PROJETO DE LEI 2630/2020

24 de julho de 2020

DataPrivacyBR RESEARCH

RASTREABILIDADE, METADADOS E DIREITOS FUNDAMENTAIS: NOTA TÉCNICA SOBRE O PROJETO DE LEI 2630/2020

24 de julho de 2020

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) por uma perspectiva jurídica, centrada no exame de proporcionalidade da medida para direitos fundamentais, considerando seu objetivo de assegurar a integridade do ambiente informacional, ao mesmo tempo 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 nota técnica defende que:

- A retenção preventiva indiscriminada e generalizante de metadados flexibiliza garantias constitucionais, considerando toda a população como suspeita e, portanto, entra em rota de colisão com o princípio da presunção de inocência dos indivíduos;
- 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, permitindo que técnicas para burlar o sistema sejam utilizadas por grupos já profissionalizados;

- O metadado é uma espécie de envelope do processo comunicacional, de modo que 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 de informações que, quando agregadas e analisadas, podem chegar a até possibilitar o 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;
- Medidas que exigem o monitoramento e armazenamento de dados de mensagens (metadados), mesmo que haja critérios para esse rastreamento, geram mais riscos do que benefícios.

Diante do 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), 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 transparências, 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 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 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;
- As investigações de 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;
- 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.

SUMÁRIO

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 outras liberdades 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.[1] 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 15 dias, tenham sido encaminhadas para, pelo menos, 5 pessoas, a fim de rastrear o caminho percorrido pela mensagem e alcançar a sua origem.

A obrigação de retenção de metadados não é 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[2]. Ao alargar tal regime de retenção de dados, tal proposição legislativa 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[3]. O Projeto de Lei, bem como todas as normas que preveem a retenção preventiva indiscriminada 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**.

A previsão de retenção de metadados adotada pelo Projeto de Lei em questão remonta, de forma hipertrofiada, o 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[4] estabeleceu algumas mudanças no escopo da lei, sobretudo relacionadas ao tempo de retenção dos metadados, apontando para a

---

[1] 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.

[2] Artigos 13 e 15 da Lei nº 12.965/2014.

[3] 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>.

[4] Vorratsdatenspeicherung, Urteil des Ersten Senats vom 02. März 2010 (Bundesverfassungsgericht 0203, 2010).

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 com a Carta Europeia de Direitos Fundamentais, decidiu-se pela anulação-invalidação da Diretiva.

Na decisão[5], 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. [6]

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[7] - 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 autoritário**s. 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-Instituit, apontou para a ideia de que a guarda massiva de dados seria um "problema jurídico, político e, particularmente, também um problema com relação a organização do Estado e sua relação com os cidadãos".[8] **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[9], ou metadados, de conexão e aplicação. Após longo processo de formulação da lei, ficaram definidos critérios como o tempo de

---

5 Acórdão Digital Rights Ireland e outros (Processos apensos C-293/12 e C-594/12), Disponível em: <http://curia.europa.eu/juris/celex.jsf?celex=62012CJ0293&lang1=pt&type=TXT&ancre=>.

6 SILVEIRA, Alessandra; FREITAS, Pedro Miguel. Implicações da declaração de invalidade da Diretiva 2006/24 na conservação de dados ("metadados") nos Estados-Membros da UE: uma leitura jusfundamental. **Journal of Law and Regulation**, v. 3, n. 1, p. 281–302, 2017.

7 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 jul. 2020.

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

9 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."

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, mas, muito 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. Enquanto a proposta aqui discutida amplifica desproporcionalmente o espectro do dever de guarda de dados, permitindo o rastreamento de conversas de todos os indivíduos que estejam envolvidos na cadeia de mensagens.

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 ao longo da (in)evolução do projeto do PL 2630/2020 é o "dilema da porta lógica",[10] embate já conhecido enfrentado pelo judiciário brasileiro. Esse debate é importante pois relaciona-se à natureza dos metadados e as obrigações de retenção e compartilhamento dos mesmos.

Mas o que são tais registros? As portas lógicas[11] 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.[12] Nos últimos anos, o endereço IP vem passado por um longo processo de transição[13] 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[14] 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 3.4×10^{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,[15] 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

---

[10] 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.

[11] 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.

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

[13] IETF. **Request for comment 2460**. Disponível em: https://tools.ietf.org/html/rfc2460. Acesso em: 17 de julho 2020.

[14] 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.

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

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 direitos fundamentais. As hipóteses de guarda de metadados são taxativas e, por conseguinte, uma opção do legislador.[16]

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.[17] 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[18]. 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.[19]

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",[20] 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**.

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

---

[16] 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.

[17] 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.

[18] 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

[19] REsp 1826221, agravo 2102827-94.2019.8.26.0000, agravo 2240522-27.2018.8.26.0000, processo 1080088-48.2013.8.26.0100.

[20] 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.

determina que serviços como o Whatsapp e o Telegram salvem toda a cadeia de quem encaminhou uma mensagem que tenha viralizado"[21].

Um dos pontos falhos é a ideia de identificar quem é o autor de um "conteúdo ilícito" circulando na plataforma, mesmo ignorando 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*)[22]. 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.

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"[23].

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 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 (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

---

[21] 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

[22] 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”.

[23] 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

mensagem a fazer "uma espécie de carimbo em toda e qualquer mensagem enviada"[24]. 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 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 judicial 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"[25], 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, permitindo que técnicas para burlar o sistema sejam utilizados por grupos já profissionalizados, que operam na “economia política da desinformação”[26].

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. É uma espécie de envelope do processo comunicacional, de modo que metadados 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 de informações que, quando agregadas e analisadas, podem chegar a até possibilitar o perfilhamento comportamental do indivíduo[27].

---

[24] 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

[25] 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

[26] 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 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").

[27] 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 16 jul. 2020.

Assim, metadados enquadram-se, via de regra, na definição de dado pessoal, na medida em que tornam uma pessoa identificada ou identificável[28]. Trata-se, portanto, de uma informação protegida pela legislação e pelo direito fundamental à proteção de dados pessoais[29].[30] Logo, metadados, ao contrário do que percorreu em parte da discussão ao longo da célere tramitação do PL 2630/2020, são tão ou talvez mais críticos que outros tipo 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 sobre a vida de uma pessoa já foram tomadas com base em metadados[31]. Este é o nível de sensibilidade das informações a que o projeto de lei busca expandir o seu dever de guarda.

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.[32] 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.

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

---

[28] A Lei Geral de Proteção de Dados define, em seu art. 5º, I, que "dado pessoal: informação relacionada a pessoa natural identificada ou identificável;".

[29] BRASIL. Supremo Tribunal Federal. Ação Direta de Constitucionalidade nº 6387… Op. cit.

[30] 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".

[31] 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 jul. 2020.

[32] 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 jul. 2020.

No dia 6 e 7 de maio deste ano, 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 pessoas como um direito fundamental autônomo ao da privacidade e ao de sigilo das comunicações.

Com isso, o julgado desmistifica a equivocada percepção de que não havendo a violação do conteúdo da comunicação, não haveria interferência em direito algum[33]. 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 são dados pessoais e, assim, merecer ser tutelados.

Ao avaliar no julgamento a proporcionalidade da Medida Provisória nº 954/2020, o Min. Gilmar Mendes aponta o direito à autodeterminação informativa como uma regra a ser seguida, sendo as interferências, exceções justificadas, o que é um ônus por parte do legislador e, o mais importante, aponta que toda e qualquer proposição legislativa deve-se cercar 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 2630/2020 tendem a ter a sua constitucionalidade desafiada.

[33] ASSOCIAÇÃO DATA PRIVACY BRASIL DE PESQUISA, **Petição de Amicus Curiae ao Supremo Tribunal Federal**, Dara Privacy Brasil Research, disponível em: <https://www.dataprivacybr.org/wp-content/uploads/2020/05/dpbrr_amicuscuria_stf_ibge.pdf>, acesso 17 jul. 2020..

PARTE II - 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[34].

Em 2018, o Information Commissioner's Office do Reino Unido, produziu um relatório[35] 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[36] 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.

Alguns países, como o Canadá e membros da União Europeia, já experienciaram o funcionamento de repositórios[37] que se propunham a clarificar o microtargeting político em aplicações. A experiência destes apenas reafirma a importância de uma regulamentação que objetive

---

[34] 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.

[35] 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

[36] 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.

[37] CPDP 2020: Political micro-targeting under investigation: Lessons from 2019 campaigns. Jan. 2020. Available at: https://www.youtube.com/watch?v=c_5baNxKj3I

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[38], 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[39] 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 à agentes políticos e do mercado a fim de influenciar comportamentos de forma abusiva e pouco transparente.

No âmbito brasileiro, a Coding Rights elaborou relatório[40] a respeito da indústria do marketing 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.

---

[38] Ibidem. BENNETT, Colin. "*The increased Transparency of inline political advertising must be matched by enhanced data protection for our political parties*." Available at: https://www.youtube.com/watch?v=c_5baNxKj3I

[39] 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.

[40] 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

Portanto, o quadro retorna para a necessidade de políticas de transparências, 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[41]. 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 à 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.

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,

[41] Panoptykon Foundation, ePaństwo Foundation and SmartNet Research & Solutions. *Who (really) targets you? Facebook in Polish election campaigns*. P. 52. Available at: https://panoptykon.org/political-ads-report.

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.[42] 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.[43]

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

---

[42] 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.

[43] 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.

obtidas legalmente com consentimento, quanto ilegal, como é no caso de empresas especializadas em negociar dados obtidos ilegalmente.[44]

Como observado pela AccessNow no relatório "Your Data Used Against You"[45] 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.

[44] 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

[45] 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/

SOBRE O DATA PRIVACY BRASIL

A Associação Data Privacy Brasil de Pesquisa ("Data Privacy Brasil") 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 R. Bioni e Rafael A. F. Zanatta

Líder de projetos
Mariana Rielli

Pesquisadoras
Gabriela Vergili, Iasmine Favaro, Jacqueline Pigatto, Marina Kitayama & Thaís Aguiar

Contatos da Associação Data Privacy Brasil de Pesquisa
contato@dataprivacybr.org
imprensa@dataprivacybr.org

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. §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. §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. §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). §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)	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 interferências desproporcional ao direito fundamental à 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: "Art.5º …	Supressão	O art. 35 deve ser suprimido porque a ampliação do dever de guarda dos logs para incluir também as portas lógicas do

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; IX - nateamento de IP: o compartilhamento de IP para mais de uma conexão ou usuário único, individualizadas através de diferentes portas lógicas; e 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) "Art. 15. O provedor de aplicações de internet constituído na forma de pessoa jurídica e que exerça essa atividade 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)		IP desarmoniza com as diretrizes principiológicas e direitos e garantias do Marco Civil da Internet e de seu Decreto Regulamentador. 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.
sem correspondente direto (inclusão no artigo 5o referente à definições)	Art. 4º Para os efeitos desta Lei, considera-se: (...) 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 (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:	As técnicas de perfilhamento têm sido utilizadas de modo pouco transparente, criando uma assimetria informacional demasiada das aplicações e anunciantes em relação aos usuários. Assim, é importante que,

	(...) VI – as técnicas e as categorias de perfilhamento VII - cópia eletrônica das mensagens e o nome do responsável pela autorização de seu envio. VIII- os links para o registro se os anúncios eleitorais forem exibidos	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 equivalência de conhecimento sobre o tratamento de suas informações em relação aos agentes que fazem uso de seus dados. 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 (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: I - Se foi aplicado algum tipo de técnica de perfilhamento; II - as categorias de perfilhamento nos quais o usuário foi incluído; III - informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para perfilhamento, nos termos do artigo 20§ 1º, da LGPD	
sem correspondente direto (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: Art. 26 (...) 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.

		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 (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: Art. 26 (...) § 4º (...) 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. 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.