Consultor Jurídico
conjur.com.br

DIREITO DIGITAL

Vigilância em massa ou combate à desinformação: o dilema do rastreamento

4 de agosto de 2020, 14h07

Por Juliana Abrusio, Ricardo Campos, Matthias Kettemann e Florian Wittner

A transformação digital criou novos espaços e métodos para a circulação de informações[3] e um deles é sem dúvida o "serviço de mensageria privada" utilizado em larga escala pela população tanto para informação quanto para desinformação. O Projeto de Lei nº 2630/2020, em tramitação na câmara dos deputados, aborda o serviço em duas ocasiões: primeiramente em seu art. 5º inciso IX definindo o que seria "serviço de mensageria privada" e, em seu artigo 10, estabelecendo um dever de guarda de determinados dados. Esse é o ponto mais polêmico e mais criticado do PL em questão. Nota-se, entretanto, uma discrepância no debate público sobre o tema e o que realmente o artigo 10 regula e inova no ordenamento jurídico. Visando trazer mais informações para o debate, faz-se necessário observar a regra concreta do artigo 10, a tradição brasileira da guarda de dados e a prática do direito comparado. Assim, consegue-se separar o que é simples polêmica desinformativa do real potencial lesivo a direitos fundamentais e possível efetividade da regra em questão para o combate à desinformação.

O teor do artigo dispõe que "os serviços de mensageria privada devem guardar os registros dos envios de mensagens veiculadas em encaminhamentos em massa pelo prazo de três meses, resguardada a privacidade do conteúdo das mensagens". Dois pontos importantes a serem notados. Primeiro: o dever de guarda refere-se apenas aos registros eletrônicos de envio (dados de tráfego) e não ao conteúdo das mensagens. Segundo: o dever de guarda fica restrito aos encaminhamentos de massa excluindo da obrigação a comunicação entre indivíduos.

Colocando apenas esses dois pontos iniciais, fica claro o quão deslocado está o debate em torno da rastreabilidade. Guardar dados de envio de contas com comportamento inautêntico violaria a privacidade do individuo? De fato o artigo 10 diz uma coisa e o debate público sobre ele diz outra.

Nesse ponto percebe-se também a marca central que ronda o espírito do PL das *fake news*: o combate a desinformação em escala industrial (e não individual). Duas são as condições específicas para a obrigação de armazenamento: (1) encaminhamento (2) em massa. Assim, estabelece-se uma importante distinção entre a comunicação interpessoal e a comunicação massiva com potencial de manipulação da formação da opinião pública, ou seja, da democracia. O dever de guarda recai sobre casos de *encaminhamento* e não de *envio* diferenciando assim o envio de mensagens individuais de autoria própria do encaminhamento massivo de mensagens não autorais.

Em outras palavras, para fins do artigo 10, as mensagens que são criadas pelo remetente (mensagens autorais) não se submetem à regra do dever de guarda do PL 2630/2020[4]. Ou seja, a privacidade do indivíduo continua inviolável, mesmo quanto aos registros de envio. Já a comunicação sobre-humana em escala industrial passa a deixar rastros legais imposta pela obrigação do artigo para uma posterior responsabilização legal, sem ser censurada previamente.

Mas o que há de novo no dever de guarda de registros de envio imposto pelo art. 10 do PL frente ao atual regime posto pelo Marco Civil da Internet (Lei n 12.965/2014)? O Marco Civil da Internet, em seu artigo 10, dispõe sobre o tema do dever de guarda e disponibilização dos registros de conexão e de acesso a aplicações de internet, incluindo dados pessoais e conteúdo de comunicações, com a ressalva de que a intimidade, a vida privada, a honra e a imagem das partes direta ou indiretamente envolvidas devem ser preservadas. O mesmo artigo em seus parágrafos estabelece um regime diferenciado para o fornecimento de dados armazenados decorrentes da obrigação legal: dados cadastrais que informem qualificação pessoal, filiação e endereço podem ser fornecidos mediante requerimento de autoridade administrativa, desde que detenha competência legal para sua requisição. O restante dos dados exige decisão judicial[5].

Em relação ao tempo de guarda, o Marco Civil da Internet, em seu artigo 15, impõe aos provedores de aplicação o dever de guarda dos registros eletrônicos pelo prazo de seis meses. Portanto, empresas de internet que oferecem aplicações, como o WhatsApp, já são obrigadas a guardar os registros de envio quanto ao nº IP, data, horário dos acessos aos serviços sob sua responsabilidade, porém de forma indistinta, e não condicionadas a determinadas circunstâncias comportamentais de quem utiliza a plataforma. Os registros eletrônicos de aplicações de que trata o Marco Civil levará a identificação do usuário da aplicação, após obtenção de dados complementares junto ao provedor de conexão atrelado a determinado IP (*Internet Protocol*).

Outros estatutos brasileiros também contem essa obrigação de guarda ou retenção de dados, como a Lei de Lavagem de Dinheiro (Lei nº 9.613/1998)[6] e a Lei de Organizações Criminosas (Lei nº 12.850/2013)[7], sendo essa última o dever de guarda pelo prazo de cinco anos às empresas de telefonia.

Portanto, o dever de guarda não é novo no ordenamento jurídico brasileiro. O Projeto de Lei nº 2630, por sua vez, inova ao impor o dever de guarda especificamente dos metadados (não de conteúdo) relacionados ao registro de envio de reencaminhamentos em massa, sendo que tais dados somente podem ser revelados por ordem judicial[8]. Parece uma medida proporcional frente ao objetivo da lei em combater a escala industrial de produção de desinformação preservando o âmbito da privacidade do individuo.

Ou seja, se for para usar o termo rastreabilidade (que em nenhum momento aparece no texto), o PL nº 2630 não inova ao trazer rastreabilidade de *dados* mas sim ao impor rastreabilidade de *comportamento* às plataformas de serviços de mensageria privada. Com isso, o legislador coloca as empresas digitais como protagonistas no combate às *fake news*, e mira o controle por via comportamental e não pelo conteúdo propriamente dito de forma proporcional e sem violar a privacidade dos indivíduos.

No Direito Comparado há também a figura da obrigação de guarda de dados em diversos estatutos com diversas finalidades. Importante notar, entretanto, que a Europa afastou-se do chamado *Vorratsdatenspeicherung* ou *Data Retention* com a anulação da Diretiva de Retenção de Dados (2006/24/CE) pelo Tribunal de Justiça Europeu em 2014. O Tribunal Constitucional Alemão também já havia julgado inconstitucional a implementação da mesma Diretiva na Alemanha, no ano de 2010[9]. A tendencia europeia tem sido afastar-se da obrigação de guarda indiscriminada para a guarda seletiva e clara em seus objetivos. Isso ocorre por exemplo na recente reforma da lei de regulação de redes alemã (Netz-DG) aprovada pelo parlamento alemão[10], que entrará em vigor nas próximas semanas. No seu §3a percebe-se um correlato do art. 10 brasileiro com algumas diferenças[11].

Enquanto o artigo 10 do PL brasileiro obriga a guarda de registros de envio de encaminhamento de mensagens em massa diferenciando-o da comunicação individual, o §3a da lei alemã limita-se aos dados que já foram apagados ou bloqueados e que dão origem à suspeita de um dos crime especificados na lista do estatuto. O §3a da lei alemã obriga, por exemplo, a transmissão dos dados diretamente ao órgão público, enquanto o artigo 10 do PL brasileiro faz distinção entre armazenamento e recuperação pelas autoridades e coloca a recuperação sob condições próprias. A regra alemã também é mais vasta que a brasileira, na medida em que inclui na obrigação não somente os dados de tráfego, mas também o conteúdo das mensagens. Nesse ponto, a regra brasileira é mais protetora da privacidade.

Em conclusão, com uma leitura bastante atenta do artigo 10 do PL nº 2630/2020 fica claro que existe um enorme equívoco por parte dos críticos que afirmam que esse dispositivo trará uma condição de vigilância em massa aos cidadãos. Vigilância, quando interligado com a proteção de dados, sempre denota a possibilidade de formação de perfis individuais pelo Estado. O PL trata do dever de guarda dos registros de envio de encaminhamento de mensagens massivas, o que em nenhuma hipótese abre caminho para a formação de perfis individuais. O PL, ademais, impõe o dever de guarda a uma parcela de dados muito menor das obrigações já existentes no ordenamento jurídico vigente. Também o argumento largamente ventilado de que a obrigação imposta pelo art. 10 do PL atingiria o modelo de negócio da criptografia ponta-a-ponta é infundado, na medida em que a criptografia protege o conteúdo e a obrigação do artigo 10 nao versa sobre conteúdo mas dados de tráfego, os quais as empresas já guardam como fim legítimo da atividade. O artigo do PL visa, assim, a identificar o comportamento artificial, em escala industrial diferenciando-o da comunicação no plano individual, intersubjetivo e privado. Condenável sim, legitimamente justificado pelo interesse público e proporcional em seus fins em tornar responsável juridicamente aqueles que usam a rede privada de serviços de mensageria instantanea, como o *WhatsApp*[12] e outras que venham a surgir para fins de manipulação do mercado de ideias e informações que sustenta qualquer Estado democrático de direito.

[3] V. HOFFMANN-RIEM, Wolfgang. Big Data. Desafíos también para el Derecho. Tradução de Eduardo Knor Argote. Navarra: Civitas, 2018, p. 122.

[4] Segundo o artigo 10 e seus parágrafos do Projeto de Lei nº 2630, o envio de mensagens em massa estará caracterizada quando presentes, cumulativamente, quatro circunstâncias, são elas: 1) envio de mensagem veiculadas em *encaminhamento* a grupos (e não a singulares); 2) a mensagem encaminhada precisa ter sido enviada por mais de cinco usuários; 3) a mensagem encaminhada atinja um total de pelo menos mil usuários; 4) as três primeiras circunstâncias precisam ocorrer dentro do intervalo de quinze dias.

[5] O Decreto regulamentador do Marco Civil, Decreto nº 8771/2016, impõe, adicionalmente, que tais autoridades administrativas devem indicar o fundamento legal de competência expressa para o acesso e motivação ao pedido de acesso aos dados cadastros. E ainda, por dever de transparência, a autoridade máxima de cada órgão da administração pública federal tem a obrigação de publicar, anualmente, em seu *site* da internet, relatórios estatísticos contendo, quanto aos dados cadastrais, o número de pedidos realizados, a lista de provedores de internet aos quais os dados foram requeridos, o número de pedidos deferidos e indeferidos pelos provedores de conexão e de acesso a aplicações, e o número de usuários afetados por tais solicitações.

[6] Lei nº 9.613/1998, art. 17-B. A autoridade policial e o Ministério Público terão acesso, exclusivamente, aos dados cadastrais do investigado que informam qualificação pessoal, filiação e endereço, independentemente de autorização judicial, mantidos pela Justiça Eleitoral, pelas empresas telefônicas, pelas instituições financeiras, pelos provedores de internet e pelas administradoras de cartão de crédito. Art. 17-C. Os encaminhamentos das instituições financeiras e tributárias em resposta às ordens judiciais de quebra ou transferência de sigilo deverão ser, sempre que determinado, em meio informático, e apresentados em arquivos que possibilitem a migração de informações para os autos do processo sem redigitação.

[7] Lei nº 12.850/2013, art. 15. O delegado de polícia e o Ministério Público terão acesso, independentemente de autorização judicial, apenas aos dados cadastrais do investigado que informem exclusivamente a qualificação pessoal, a filiação e o endereço mantidos pela Justiça Eleitoral, empresas telefônicas, instituições financeiras, provedores de internet e administradoras de cartão de crédito. Art. 16. As empresas de transporte possibilitarão, pelo prazo de 5 (cinco) anos, acesso direto e permanente do juiz, do Ministério Público ou do delegado de polícia aos bancos de dados de reservas e registro de viagens. Art. 17. As concessionárias de telefonia fixa ou móvel manterão, pelo prazo de 5 (cinco) anos, à disposição das autoridades mencionadas no art. 15, registros de identificação dos números dos terminais de origem e de destino das ligações telefônicas internacionais, interurbanas e locais.

[8] Vale lembrar que as regras sobre a guarda e fornecimento quanto aos dados cadastrais, conteúdo de mensagens e aos registros eletrônicos de provedores de aplicação de internet, *não são* objeto do Projeto de Lei de fake news, e continuam a seguir os ditames do Marco Civil da Internet e de outras legislações específicas, conforme visto antes.

[9] Sentença de 2 de março de 2010 1 BvR 256/08.

[10] Sobre o tema da lei alemã ver Ricardo Campos, Georges Abboud, Nelson Nery Jr. (Orgs.) Fake News e Regulação, 2 edição, RT Sao Paulo.

[11] O Art. 10 move-se na direção da retenção (limitada) de dados como no §113b da lei alemã de telecomunicações (TKG), uma vez que os dados podem ser armazenados como uma soma total e depois recuperados pelas autoridades em casos individuais. A rigor, há aqui duas intervenções: uma pela obrigação de armazenar dados, e outra pelo pedido das autoridades para recuperar os dados. Tais obrigações também não são incomuns na Alemanha (ver também §§133a e b TKG). A reserva de jurisdição prevista no parágrafo 3 também seria um requisito obrigatório na Alemanha.

[12] A empresa *WhatsApp,* aliás, por meio de relatório publicado no ano passado confirmou que já realiza controle de comportamento, para fins de evitar a propagação de *fake News*. Cf. Stopping Abuse: How WhatsApp Fights Bulk Messaging and Automated Behavior, p. 7 publicado em 06 Fev.2019. Disponível em <https://scontent.whatsapp.net/v/t61.22868-34/69510151_652112781951150_6923638360331596993_n.pdf/artigo-t%C3%A9cnico-Bloqueio-de-uso-n%C3%A3o-autorizado.pdf?_nc_sid=2fbf2a&_nc_ohc=QrSD7fjLiVEAX_1y30s&_nc_ht=scontent.whatsapp.net&oh=8cdb0aefe2fe0edbdbcd4242a362d0b1&oe=5F2

Juliana Abrusio é diretora do instituto LGPD, doutora em Direito e professora da Universidade Presbiteriana Mackenzie. Sócia da Opice Blum, Bruno, Abrusio e Vainzof Advogados Associados.

Ricardo Campos é diretor do instituto LGPD (Legal Grounds for Privacy Design) e docente assistente na Goethe Universität Frankfurt am Main (ALE).

Matthias Kettemann é consultor do parlamento alemã sobre regulação de redes, doutor e livre-docente pela Goethe Universität Frankfurt am Main.

Florian Wittner é doutorando no Hans-Bredow-Institut für Medienforschung em Hamburgo (ALE).

Revista **Consultor Jurídico**, 4 de agosto de 2020, 14h07