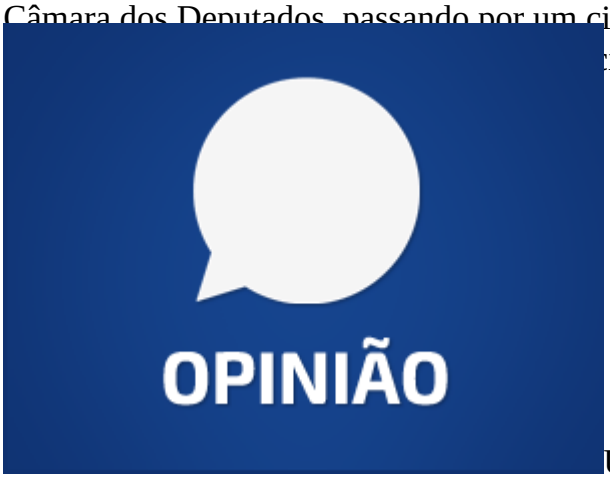
OpiniÃ£o: Novos mitos sobre rastreabilidade contra a desinformaÃ§Ã£o

O Projeto de Lei nº 2630/2020, que visa a instituir a Lei Brasileira de Liberdade, Responsabilidade e Transparência na Internet, vem sendo discutido desde meados de 2020 entre o Congresso Nacional, especialistas e ativistas de direitos digitais. O PL foi aprovado no Senado e agora está em debate na Câmara dos Deputados, passando por um ciclo de audiências públicas temáticas que visam a destrinchar pontos específicos da proposta.



Um destaque questionável está no artigo 10, que estabelece um regime de rastreamento de mensagens em aplicativos de mensageria privada, regime que ficou conhecido no debate público como "rastreabilidade". Pelo mecanismo apresentado no projeto de lei, as plataformas de mensageria privada deverão *"guardar os registros dos envios de mensagens veiculadas em encaminhamentos em massa pelo prazo de três meses"*, considerando-se encaminhamento em massa *"o envio de uma mesma mensagem por mais de cinco usuários, em intervalo de até 15 dias, para grupos de conversas, listas de transmissão ou mecanismos similares"*.

O dispositivo foi pensado a partir dos disparos em massa ocorridos desde as eleições de 2018, para evitar a contaminação do debate público com a disseminação de desinformação em um ambiente em que as informações não podem ser verificadas e que se dispersam muito rapidamente. Não obstante esse seja um problema a ser tratado, haja vista a corrosão social que vem causando, alguns argumentos merecem ser apresentados contra o remédio proposto.

Em que pese os suficientes esclarecimentos da comunidade acadêmica sobre os riscos de segurança relativos à interferência na criptografia e dos grupos ligados à garantia de direitos na rede, o debate está sendo reposto sob "novos" termos: ao invés da rastreabilidade em todas as comunicações de aplicações de mensageria, seria implementada a guarda de registro dos envios apenas de grupos públicos. Tal diferença (entre grupos públicos e privados, ou comunicação pública e íntima) não merece prosperar, nem mesmo o eventual tratamento diferenciado entre elas. Entretanto, ante o desenho do debate nestes termos, assumir-se-á, para fins argumentativos, a dicotomia.

Alega-se que, se, por um lado, as mensagens interpessoais — entre duas pessoas — carregavam maior necessidade de proteção à privacidade, por outro, os grupos públicos seriam "declaradamente" acessíveis, visibilizados e, portanto, não mereceriam o mesmo nível de proteção. Algumas razões deixam evidente que tal assertiva é politicamente contestável e tecnicamente frágil.

A gangorra dos riscos e da ineficácia

Apesar da aparência de maior razoabilidade e proporcionalidade a um mecanismo de monitoramento, alguns pontos frágeis merecem ser desmistificados. O grau de publicidade conferido a um grupo público — no WhatsApp, por exemplo — não extrapola o ato de compartilhamento por um dos integrantes do grupo com legitimidade para fazê-lo. Por mais "popular" que seja um grupo, sua publicização ainda pertence, fundamentalmente, ao círculo de autonomia do usuário em compartilhá-lo — inexistindo qualquer possibilidade, por exemplo, de indexação automática do grupo em ferramentas de busca como o Google.

Em outras palavras: o link de compartilhamento para entrada em grupos de mensageria privada existe por padrão e não fica disponível em mecanismos de busca, exceto quando os próprios usuários do grupo compartilham o mesmo em algum suporte da web. Propostas mais contundentes e profiláticas, como a proibição temporária de compartilhamento e a mudança do link do grupo após determinado período, podem ser mais eficazes quando se visa romper uma cadeia de compartilhamento danosa.

Adicionalmente, a "rastreabilidade de mensagens apenas para grupos públicos" acarretaria em uma "quebra" da corrente de confiança, conferida pela criptografia, no caso de uma mensagem legítima ser repassada de um grupo privado a um grupo público (não sendo rastreável para, então, ser rastreável). Mais uma vez, um efeito inibitório cercearia a liberdade de expressão do indivíduo que receia ter sua comunicação monitorada. Além disso, até que ponto seria eficaz — sob a ótica da proposta — uma rastreabilidade que encontre limites nos grupos privados? Ela seria facilmente "quebrada" quando a mensagem perseguida atravessasse um grupo privado.

A rastreabilidade também pode ser contornada por outras medidas simples: o fato de copiar a mensagem e colar em outro grupo "zeraria" a cadeia de compartilhamento ou criaria "evento perturbador" do rastreio, trazendo uma insegurança quanto à origem da mensagem. À luz do princípio constitucional da presunção da inocência, eventuais erros poderão colocar no polo passivo de investigações e ações judiciais usuários que nada têm com cadeias de desinformação.

Outro argumento que salta aos olhos na defesa da rastreabilidade é o de que "o usuário teria autonomia para decidir sobre o nível de privacidade" — e de criptografia — sobre suas comunicações. Essa perspectiva ignora as décadas de construção de governança da privacidade exemplificadas no conceito de "privacidade por desenho", mais especificamente na exigência de "privacidade por padrão", cristalizada no artigo 46, §2º, da Lei Geral de Proteção de Dados Pessoais.

A lei faz incidir comando expresso: para suprir uma lacuna informativa orgânica ao usuário que desconhece a lógica técnica e mercadológica das aplicações, além de coibir tratamentos inadequados ou ilícitos, será necessário "nivelar por cima", por padrão, as configurações e a arquitetura dos mecanismos que garantam a segurança e a privacidade do usuário. Uma consequência direta é o recurso de *encriptação por padrão*, tendência das melhores práticas em aplicativos de mensageria no mundo todo. Supor que um usuário poderia optar por um grau de segurança menor em suas comunicações é, no mínimo, simplório e um desserviço aos avanços em regulações de proteção de dados pessoais e sobre segurança do ecossistema de aplicações.

A proposta não considera que a criptografia por padrão é também medida de segurança da informação num contexto crescente de crimes cibernéticos. Faz parte da técnica criptográfica a elevação dos níveis de segurança comunitários, impedindo que agentes maliciosos explorem vulnerabilidades de outras partes do sistema — como senhas fracas, ausência de verificação em duas etapas, entre outros. O tema tem um paralelo, no contexto atual que vivemos, com a noção de proteção comunitária entre vacinas e a derrota de agentes patológicos, como os vírus pandêmicos.

Engana-se quem acredita que o usuário, ao fazer parte de grupo público, abre mão de seus direitos relativos ao uso da plataforma. Não somente agentes maliciosos fazem uso de grupos público: coletivos de assistência social, jurídica e psicológica a minorias e grupos vítimas de violência sistêmica, como LGBTQIA+, de luta por direitos raciais ou pessoas em situação de violência doméstica acessam, com frequência, grupos públicos em seu livre direito à reunião e associação.

Trabalhos de articulação política também fazem amplo uso de grupos interinstitucionais e interpartidários, muitas vezes públicos, para amadurecer entendimentos e construir estratégias de atuação democrática. Rastrear, mandatoriamente, essas comunicações de alta sensibilidade — apesar do interesse público — é fragilizar esses direitos, tão intimamente ligados à confiabilidade conferida às plataformas de mensageria.

Após décadas de debate, está consolidado que a possibilidade de interferir no potencial de criptografia, via intermediário da aplicação, para coibir crimes implica em um risco desproporcional à segurança e aos direitos conexos à criptografia. Enquadrar a rastreabilidade como um "mal necessário" ao combate à desinformação é se alinhar a notórios advogados da vigilância, notadamente marcados pela aversão ao sigilo das comunicações, sob a égide de um suposto interesse coletivo.

O "novo" regime de rastreabilidade proposto segue atacando a privacidade, a liberdade de expressão e os direitos de associação e reunião, além de não ser eficaz em razão das suas próprias fragilidades. O histórico recente do Brasil já conta com suficientes políticas públicas pautadas na negação científica e nas repercussões sociais, políticas e econômicas derivadas de análises que não escutam acadêmicos e a ampla maioria da sociedade civil organizada. Será necessário refletir se a defesa dos mecanismos de rastreabilidade, tal como proposta, não está ampliando essa cultura.