Nota técnica da Electronic Frontier Foundation sobre o PL 2630/2020

No presente documento, a Electronic Frontier Foundation (EFF), vem apresentar suas principais preocupações em relação ao PL 2630/2020 conforme texto aprovado no Senado Federal. A EFF é uma organização de atuação internacional, sem fins lucrativos, apoiada por mais de 30.000 membros ao redor do mundo e que há 30 anos trabalha na defesa da liberdade de expressão, privacidade, segurança e inovação no contexto digital.

Essa nota se concentra nas disposições acerca de *identificação de usuários* (art. 5º, I art. 7º, art. 15, II e art. 17), *acesso remoto aos bancos de dados* (art. 32) e *rastreabilidade* (art. 10 e art. 11). O foco adotado não significa que outras disposições do projeto de lei, como o art. 12, §6º, não levantem preocupações relevantes. Contudo, abordamos aqui os temas que vimos tratando com mais profundidade no acompanhamento deste projeto de lei.

(1) Identificação massiva de usuários

Se comparada a versões anteriores do projeto de lei, a redação atual do **artigo 7º** reduz as hipóteses em que poderia ser obrigatória, a critério dos provedores de aplicação, a identificação dos usuários dessas plataformas, "inclusive por meio da apresentação de documento de identidade válido." No entanto, as hipóteses remanescentes são amplas e, em conjunto com o parágrafo único deste artigo, podem levar a uma obrigação geral de monitoramento dos usuários pelos provedores de aplicação, criando oportunidades consideráveis para abusos. Primeiro, simples denúncias de violação da lei como hipótese suficiente para requerer a identificação abre a porta para denúncias abusivas ou alegações imprecisas. Por exemplo, uma pessoa mal-intencionada poderia apresentar denúncia falsa como maneira de identificar uma conta específica com o objetivo de assediar o usuário. O abuso de mecanismos de denúncia em redes sociais não é novidade, tampouco excepcional, e tende a atingir desproporcionalmente grupos vulneráveis.

Segundo, o **parágrafo único do art. 7º** determina que as redes sociais e os aplicativos de mensagens privadas devem desenvolver medidas técnicas para detectar fraude no cadastro e uso de contas em desacordo com a legislação. A redação do parágrafo único é ampla, ou mesmo ambígua, ao parecer se referir a um monitoramento de "uso de contas em desacordo com a legislação." Pode ser interpretado e implementado de forma a caracterizar uma obrigação geral de monitoramento do comportamento dos usuários na plataforma, o que viola parâmetros de necessidade e proporcionalidade associados a garantias de liberdade de expressão e privacidade. Somando-se as disposições do art. 7º à definição de "conta identificada" que permanece no **art.**

5º, I, os provedores tenderão a exigir a identificação de maneira excessiva comprometendo a privacidade dos usuários em geral.

O Ministério Público Federal já manifestou no ciclo de debates promovido pela Câmara dos Deputados que os dados disponíveis por força do Marco Civil da Internet – Lei 12.965/2014 – são suficientes para a identificação de usuários específicos no âmbito de investigações (são esses dados: registros de acesso a aplicações, registros de conexão e os dados cadastrais fornecidos à plataforma). Ainda de acordo com o representante do MPF, a exigência de documentos de identidade traz, inclusive, possibilidades de falsificação e desafios quanto à autenticidade dos documentos apresentados. Terceiro, tais previsões adicionais de identificação são desnecessárias, desproporcionais e contrariam princípios de proteção de dados pessoais, presentes na Lei Geral de Proteção de Dados e protegidos pela Constituição Federal, que afirmam a minimização no tratamento de dados, cuja coleta deve ser limitada ao que é necessário a uma determinada finalidade. **Por essas razões, os dispositivos citados deveriam ser suprimidos**.

Vemos com preocupação também o **art. 15, II e art. 17** do projeto de lei. O último exige a confirmação da identidade real do usuário para o impulsionamento de qualquer conteúdo em qualquer valor, o que muitas vezes pode envolver temas associados a questões sensíveis como orientação sexual. Ainda que o acesso à identificação só se dê com ordem judicial, novamente se questiona a necessidade de exigir identificação adicional de qualquer impulsionamento, em qualquer valor, considerando os dados de usuários já disponíveis para as plataformas. A exigência implica, ainda, uma camada adicional de complexidade para a publicação de qualquer conteúdo patrocinado.

Já o **artigo 15** trata do impulsionamento de propaganda eleitoral ou de conteúdos que mencionem candidato, coligação ou partido. Neste caso, a identificação real do anunciante, por meio do seu CPF ou CNPJ, deverão ser disponibilizadas ao público de antemão e sem qualquer crivo judicial. Tal obrigação é desproporcional e expõe o número de documento de identidade de qualquer pessoa que patrocine publicação mencionando os termos citados. Não é difícil prever como isso pode resultar em autocensura, perseguição ou mesmo servir à ação criminosa que se vale da facilidade de acesso a dados pessoais, como fraude.

(2) Acesso remoto a bancos de dados localizados em outros países

O **art. 32** obriga grandes provedores de redes sociais e aplicações de mensagens privadas a terem sede no país. Também obriga essas empresas a fornecer acesso remoto a seus bancos de dados para que seus funcionários no Brasil sejam impelidos a entregá-los diretamente. Esse tipo de solução apresenta problemas por desprezar mecanismos e instâncias adequados de cooperação jurídica internacional, bem como por implicar riscos à segurança e à privacidade dos usuários.

A natureza global da Internet desafia autoridades ao redor do mundo quando os dados estão armazenados em outros países, já que, por padrão, os países só podem aplicar suas leis em seu próprio território. Iniciativas como a proposta no art. 32 negam o princípio da territorialidade e as salvaguardas de privacidade que o acompanham. As diferenças entre marcos legais em cada país incluem quais tipos de condutas são ou poderiam ser um crime, o que as autoridades policiais precisam provar antes de ter acesso a dados pessoais e se os diferentes tipos de dados pessoais são legalmente protegidos. Há casos, ainda, em que a lei de um país estrangeiro não está em conformidade com padrões internacionais de direitos humanos. Tratados e acordos de cooperação jurídica internacional partem do reconhecimento e respeito à soberania dos diferentes Estados e se destinam a estabelecer as regras e mecanismos adequados para que essas questões sejam ponderadas e pedidos de autoridades de um país possam ser satisfeitos no território (e na jurisdição) de outro.

O que faz o art. 32 é desconsiderar completamente esses mecanismos e os fundamentos jurídicos que os justificam para criar um "canal direto" entre as autoridades brasileiras e os bancos de dados armazenados em outros países. Contudo, o estabelecimento dessa obrigação em uma lei brasileira não resolverá as limitações legais que as empresas enfrentam para a entrega de dados conforme as normas às quais estão sujeitas e devem cumprir nos Estados Unidos. O princípio da territorialidade seguirá se colocando como um obstáculo concreto ao efetivo cumprimento dessa regra, se aprovada. Por outro lado, está pendente de julgamento no Supremo Tribunal Federal a ação declaratória de constitucionalidade dos Acordos de Cooperação Jurídica Mútua (ADC 51). A proposta de art. 32 poderá ser considerada inconstitucional por tentar contornar a aplicação desses acordos a depender do julgamento do STF. Em paralelo, o Brasil está em processo de adesão à Convenção sobre Crimes Cibernéticos (Convenção de Budapeste). Essa convenção estabelece parâmetros para a cooperação jurídica internacional no acesso a evidências eletrônicas entre os Estados Parte, entre eles, os Estados Unidos.

Se é relevante que as autoridades brasileiras possam conduzir suas investigações de forma eficiente, não é isso que o art. 32 realmente oferece ao pretender contornar princípios do direito internacional, assim como debates e processos relevantes atualmente em curso.

Além disso, propostas como as do art. 32 apresentam implicações práticas extremamente prejudiciais à privacidade e à segurança dos usuários. Colocá-la em prática significa aumentar o número de funcionários (e dispositivos) que podem acessar dados confidenciais e reduz a capacidade da empresa de controlar vulnerabilidades e acessos não autorizados. Cada nova pessoa e cada novo dispositivo adicionam um novo risco de segurança; em escala global e exigida por diferentes países, os riscos se multiplicam. Mecanismos de cooperação jurídica internacional existem para buscar assegurar que as leis, e os direitos, sejam adequadamente respeitados. Soluções que contornam esses mecanismos terminam por comprometer também direitos humanos e fundamentais.

(3) Rastreabilidade de mensagens em aplicativos de mensageria privada

O **artigo 10** obriga provedores de redes sociais e de mensagens privadas a reter a cadeia de todas as comunicações que foram "encaminhadas em massa. O PL 2630/2020 exige três meses de armazenamento de dados de toda a cadeia de comunicação para essas mensagens, incluindo data e hora do encaminhamento, e o número total de usuários que recebem a mensagem. Essas obrigações estão condicionadas a limites de viralidade e se aplicam quando uma mensagem foi encaminhada a grupos ou listas por mais de 5 usuários em 15 dias, em que o conteúdo de uma mensagem tenha atingido 1.000 ou mais usuários. Na prática, pelo menos qualquer mensagem enviada a um grupo ou lista dispararia a obrigação de rastreabilidade, já que não se sabe, de antemão, se sua trajetória atingirá ou não o parâmetro de viralidade estabelecido.

Este dispositivo viola o devido processo legal, obrigando os provedores a rastrear a comunicação de todos antes que qualquer um tenha cometido qualquer ofensa definida legalmente para que as informações possam ser usadas, eventualmente e no futuro, no contexto de uma investigação. Muitas das implementações mais óbvias deste artigo obrigariam as empresas a manter quantidades maciças de dados associados às comunicações (metadados) de todos os usuários ou a quebrar a criptografia para ter acesso ao conteúdo de uma mensagem criptografada.

Mesmo que outras implementações sejam possíveis, não sabemos exatamente como este ou aquele provedor decidirá cumprir a obrigação e a que custo para a segurança, a privacidade e os direitos humanos. Em última análise, todas essas implementações se afastam da engenharia focada na privacidade e na minimização de dados que deve caracterizar aplicativos seguros de mensageria privada. O Brasil não deveria impor restrições ao uso pela sociedade de comunicações privadas e seguras, enfraquecendo, por padrão, suas proteções.

Por esse motivo, defendemos a supressão do art. 10 e desenvolvemos abaixo as principais razões para tanto. A proposta de guardar apenas prospectivamente as interações de um usuário específico, a partir de ordem judicial, em que estas interações sejam os dados de envio e recebimento de mensagens e chamadas, e a data e hora – desvinculados de cada mensagem em si e respeitados os requisitos do art. 2o da Lei 9.296/1996 – apresenta-se como mais proporcional em relação à atual redação do art. 10. Contudo, é fundamental que tal obrigação não implique uma exigência de reengenharia das plataformas para debilitar proteções incutidas na forma como foram desenhadas e implementadas. Estímulos para a implementação de mudanças como essa da maneira mais simples e menos custosa podem levar a vulnerabilidades ou a soluções que acessem mais do que o necessário.

Apresentamos a seguir nossas considerações mais detalhadas quanto à rastreabilidade a partir da redação aprovada pelo Senado.

Como a rastreabilidade frustra a expectativa dos usuários dos serviços seguros de mensageria privada?

Em implementações comuns desses serviços, inclusive do WhatsApp, a criptografia probabilística "ponta a ponta" garante que um adversário não possa nem confirmar nem desmentir suposições sobre o conteúdo da mensagem, inclusive a confirmação da suposição específica de que a mensagem não tratava de determinado tema. Nesses cenários, a rastreabilidade permite que alguém com acesso aos metadados de uma "cadeia de encaminhamento" confirme que um usuário realmente enviou uma mensagem idêntica a outra mensagem (mesmo que o seu conteúdo seja desconhecido). Isso desmente a suposição de que o usuário estava de fato falando sobre algo totalmente diferente, desmente a suposição de que o usuário estava escrevendo algo original e desmente muitas outras suposições possíveis sobre o conteúdo. De forma geral, "encaminhar" *vs*"escrever algo novo" é um tipo de atividade que está fundamentalmente relacionado a saber algo sobre o conteúdo.

Em alguns casos, o fato de uma pessoa ter encaminhado algo pode ser extremamente delicado mesmo que o item encaminhado não seja necessariamente ilegal, por exemplo, quando se deseja punir alguém que tenha vazado algo ou feito uma denúncia. Por essa razão, protocolos usados para a comunicação segura, como o adotado pelo WhatsApp, implementam uma proteção à privacidade desde a concepção que impede que a ponta do servidor da empresa distinga o encaminhamento de outros tipos de mensagem.

A rastreabilidade em casos civis e penais cria sérias preocupações sobre a privacidade e a liberdade de expressão. Revelar a cadeia completa de comunicação de uma mensagem encaminhada em massa pode ser invasivo não apenas por revelar relacionamentos individuais: a história completa de certas mensagens pode revelar a estrutura e os membros de uma comunidade inteira. Por exemplo, de pessoas que compartilham determinada crença ou interesse, ou pertençam a algum grupo minoritário, mesmo que nenhuma delas esteja realmente envolvida em atividades ilegais.

O que poderia dar errado em se cumprir com a obrigação de rastreabilidade?

Em primeiro lugar, encaminhar uma mensagem popular não significa que você deva automaticamente ficar sob suspeita. Na verdade, a viralidade da mensagem não altera os direitos do remetente original à privacidade, ao devido processo legal e à presunção de inocência, requisito fundamental da legislação internacional de direitos humanos.

Em segundo lugar, a primeira pessoa a introduzir certo conteúdo em determinado sistema de mensagens privadas pode ser erroneamente vista ou considerada como o autor que encaminhou maciçamente uma suposta mensagem ilegal.

Em terceiro lugar, a pessoa que encaminhe conteúdo por qualquer meio que não a interface de encaminhamento de um aplicativo pode ser incorretamente vista ou considerada como o autor. As pessoas podem ser incriminadas como autores de conteúdo de cuja criação não tenham de fato participado. Pode haver maior temor de compartilhar informações se as pessoas acharem que há mais chances de serem punidas por terem participado de sua disseminação (o que seria outra medida desproporcional para a grande maioria dos usuários inocentes de sistemas de mensageria).

A rastreabilidade não ajudará a identificar com precisão quem deu origem ao conteúdo. Os usuários de aplicativos de mensageria privada os utilizam rotineiramente para compartilhar mídia (imagens, vídeos) obtida em outro lugar, de outro aplicativo ou de algum site. O usuário será simplesmente identificado como a primeira pessoa a introduzir determinado conteúdo em dada cadeia de encaminhamento, o que é obviamente diferente de ele mesmo ser o autor desse conteúdo. Em se tratando de mensagens de texto, qualquer pessoa que redigite a mensagem ou que a copie e cole (talvez de outro aplicativo ou mídia) será similarmente identificada como seu autor original por ter sido a primeira a introduzi-la no aplicativo específico.

Encaminhar algo de outra forma, sem utilizar o recurso de encaminhamento de um aplicativo com rastreabilidade, provavelmente interromperá e reiniciará a sequência. Por exemplo, ao receber mensagens de texto, os usuários do WhatsApp podem copiar e colar seu conteúdo em vez de usar o botão “encaminhar” dentro do WhatsApp. O software não teria como identificar isso corretamente como um tipo de encaminhamento. Da mesma forma, se o número de telefone utilizado for estrangeiro, ele não estará coberto por essa lei e o software não conseguirá rastrear o originador estrangeiro.

Similarmente, a identidade do originador não é autenticada no WhatsApp de modo tecnicamente forte e confiável, sendo apenas mantida como um campo de metadados na mensagem criptografada de encaminhamento, que pode ser visto pela ponta do aplicativo do cliente, mas não pela ponta do servidor da empresa. Por exemplo, o cabeçalho de uma mensagem criptografada poderia dizer que ela foi originada por usuário com determinado número de telefone. Um software-cliente oficial que atenda à obrigação de rastreabilidade poderia copiar esse cabeçalho, sem alterações, ao encaminhar a mensagem a novos destinatários. Isso permitiria a pessoas que utilizem um software-cliente não oficial remover esse cabeçalho, ocultá-lo ou até mesmo incriminar outra pessoa como sendo a responsável pela mensagem. Não haveria forma tecnicamente factível de confirmar se o remetente informado teve ou não real participação na origem da mensagem. (Outras propostas podem conseguir solucionar esses problemas, mas com

significativa perda de privacidade, porque o servidor necessitará de acesso muito mais amplo para confirmar ele mesmo exatamente o que os seus usuários estão fazendo antes que o ato malicioso ocorra.)

Como a proposta de rastreabilidade interage, ou conflita, com garantias de proteção de dados?

A legislação brasileira de proteção de dados classifica como dados pessoais os metadados que se refiram a uma pessoa física identificada ou identificável. Isso significa que as empresas devem coletar, armazenar e utilizar dados pessoais somente para fins legítimos, específicos e explícitos, devendo esse processamento ser pertinente, proporcional e não excessivo relativamente aos seus fins. Em decisão recente e histórica, o Supremo Tribunal Federal enfatizou os fundamentos constitucionais da proteção de dados pessoais como um direito fundamental em paralelo ao direito à privacidade. Ele confere proteção a quaisquer dados atribuídos a pessoas e que podem impactar suas vidas individual e coletivamente, independentemente de tais dados serem mantidos em sigilo ou não. Os legisladores devem considerar o impacto sobre o direito de proteção de dados ao pretender criar uma obrigação de rastreabilidade à luz dessas novidades.

As empresas devem limitar a retenção de dados pessoais ao razoavelmente necessário, proporcional a determinados fins comerciais legítimos. A minimização de dados é um elemento fundamental na caixa de ferramentas de proteção de dados e essencial em todos os sistemas de privacidade desde a concepção. Alguns sistemas foram desenvolvidos para reter menos dados, não rastreando as informações pertinentes, e não necessariamente dispõem de uma forma sensata de começar a rastreá-los, o que pode levar a mudanças tecnológicas que debilitem as proteções à privacidade e à segurança dos usuários.

Por que as novas tecnologias ou sistemas de mensageria terão dificuldades em cumprir as obrigações propostas?

A implementação da rastreabilidade de usuários que "encaminhem" uma mensagem pode depender do controle, hoje inexistente, sobre os aplicativos-cliente. É implausível imaginar que todos os aplicativos-cliente aceitarão, ou mesmo poderão, cooperar da mesma maneira para implementar restrições e limitações.

Alguns sistemas são muito descentralizados (não existe um operador central que possa ficar responsável pelo cumprimento da obrigação). A obrigação presume que os provedores de aplicativos serão sempre capazes de identificar e distinguir o conteúdo encaminhado do não encaminhado e também de identificar a origem de uma mensagem encaminhada. Na prática, isso depende da arquitetura do serviço e da relação entre o aplicativo e o serviço. Se os dois forem independentes, como frequentemente é o caso do e-mail, por exemplo, o serviço não consegue

diferenciar o conteúdo encaminhado do não encaminhado e o aplicativo não armazena o histórico de encaminhamento fora do dispositivo do usuário.

Essa separação de arquitetura é muito utilizada em serviços de Internet e, apesar de hoje ser menos comum nos aplicativos de mensageria privada mais utilizados, a obrigação limitaria o uso de XMPP ou de soluções semelhantes, que também pode impactar negativamente os aplicativos de mensageria de código aberto.

Há alguma conexão entre a rastreabilidade e a inovação, de acordo com os artigos 10 e 11 da do projeto aprovada pelo Senado?

O artigo 10 obriga os aplicativos de mensagens privadas a guardar a cadeia das comunicações que tenham sido "encaminhadas em massa" com base em um parâmetro de "viralidade". O **artigo 11** diz que o uso e o comércio de ferramentas externas pelos provedores de serviços de mensagens privadas, para o encaminhamento em massa de mensagens são proibidas, exceto no caso de protocolos padrão tecnológicos sobre a interação de aplicativos na internet. O projeto requer que o provedor de serviços de mensagens privadas adote políticas dentro dos limites técnicos do seu serviço, para lidar com o uso dessas ferramentas.

Não sabemos como um provedor vai cumprir com os artigos 10 e 11, mas, supõe-se que necessitará de desenvolvedores para tentar bloquear e reprimir, de forma ativa, o uso de software de terceiros que interagem com suas plataformas, controlando estritamente os aplicativos clientes (para garantir que cooperem com o rastreamento do histórico do encaminhamento, registrando se encaminharam ou não encaminharam uma mensagem, e atualizando os registros do histórico).

Muitas propostas de rastreabilidade forçam o desenvolvedor de um sistema de comunicações a impedir outras pessoas de desenvolverem ou usarem software de terceiros que interajam com aquele sistema. Assim, espera-se ou exige-se do desenvolvedor que monopolize a habilidade de fazer ferramentas de aplicativos clientes e, de forma similar, seja o único agente permitido a mudar ou melhorar essas ferramentas. Isso limita a interoperabilidade de uma maneira que tende a ser prejudicial à concorrência e à inovação.

Parte dessa nota reproduz publicação no site da EFF, que apresenta ainda outros argumentos: FAQ: Por que o Projeto de Lei Brasileiro de Tornar Obrigatória a Rastreabilidade em Aplicativos de Mensageria Privada Frustrará a Expectativa de Privacidade e Segurança dos Usuários