Monitor do Debate Político no Meio Digital
Grupo de Políticas Públicas para o Acesso à Informação
Escola de Artes Ciências e Humanidades - USP

Nota Técnica 11

Perguntas e respostas sobre a rastreabilidade de mensagens virais na mensageria privada

Pablo Ortellado

25 de Agosto de 2020

O que diz o artigo 10 do projeto de lei 2630/ 2020?

O artigo estabelece que mensagens reencaminhadas para múltiplos destinatários que viralizem passem a ter metadados registrados para que se possa determinar a origem e medir o seu alcance.

Porque é necessário um artigo assim?

O WhatsApp é o principal meio por onde se difundem campanhas de desinformação no Brasil. Atores maliciosos se aproveitam do sigilo do aplicativo para difundir mensagens virais que chegam a milhões de pessoas. Para impedir que essas campanhas de massa subterrâneas, secretas e maliciosas sigam operando em sigilo, é necessário introduzir a rastreabilidade das mensagens virais, preservando com rigor e cuidado a privacidade das conversas interpessoais e a criptografia.

O artigo 10 acaba com a privacidade das conversas interpessoais? Vai afetar a privacidade de conversas entre jornalistas e fontes, entre advogados e clientes?

Não, porque se aplica apenas a encaminhamentos com múltiplos destinatários (em grupos ou listas de transmissão) que atingirem grande número de usuários. Nenhuma conversa pessoa a pessoa é afetada pela medida. A medida também não afeta mensagens autorais em grupos.

O artigo 10 acaba com a criptografia do WhatsApp?

Não. Todas as conversas no WhatsApp seguem protegidas por criptografia ponta a ponta e são invioláveis.

Mas como vão ser registrados os encaminhamentos em grupo sem quebrar a criptografia e a privacidade das conversas?

Conteúdos encaminhados hoje já são armazenados nos servidores do WhatsApp para reduzir o tráfego na rede. Quando alguém reencaminha uma mensagem, na verdade manda um apontador para baixar o conteúdo deste servidor e uma chave para descriptografar e verificar a autenticidade. O que o artigo propõe, então, é que se guardem metadados deste conteúdo que permitam a identificação posterior dos primeiros disseminadores, caso o conteúdo seja considerado ilícito por um juiz.

O artigo 10 é coleta de dados em massa, é vigilantismo?

Não. O artigo segue rigorosamente o preceito da Lei Geral de Proteção de Dados de requerer a menor quantidade de dados, apenas o necessário para atingir sua finalidade. São guardados apenas metadados (informações que toda mensagem carrega, sem revelar o seu conteúdo) e apenas i) quando a mensagem for para múltiplos destinatários; ii) quando tiver 5 encaminhamentos ou mais; iii) quando atingir mil pessoas ou mais. Os metadados são também guardados apenas por 3 meses e só podem ser acessados por ordem judicial e com finalidades bem determinadas. Depois todos os dados são destruídos. Para fins de comparação, hoje são guardados registros de acesso a aplicações de internet por 6 meses e registros de ligação telefônica por 5 anos!

E se eu encaminhar um conteúdo para denunciá-lo, vou ser responsabilizado por ele?

Não. O artigo não cria responsabilidade por se encaminhar conteúdos. Ele apenas fornece informações para que uma investigação possa identificar a origem da disseminação de conteúdos virais que deveriam estar na esfera pública, como acontece no Twitter e no Facebook e que no WhatsApp foram escondidos e enterrados.

O artigo inverte a presunção de inocência, tornando todo mundo potencialmente culpado?

Não. Criar registro para controle e investigação posterior, em caso de ilícito, não é inversão da presunção de inocência. A legislação exige que se registrem as placas de todos os automóveis e a numeração de todas as armas de fogo. Na internet, exige que se guardem todos os registros de conexão e todos os registros de acesso a aplicações. Na telefonia, que se guardem todos os registros de ligações.

O governo pode usar desses dados para monitorar as pessoas?

Não. Esses metadados dos reencaminhamentos em massa são guardados pela empresa por um curto período de tempo e só podem ser acessados para finalidades específicas e apenas com autorização judicial.

87% dos brasileiros não são contra a rastreabilidade dos conteúdos virais?

De jeito nenhum. O Facebook, empresa proprietária do WhatsApp, que não quer ser regulada, encomendou uma pesquisa maliciosa na qual perguntou se "as pessoas têm o direito de ter uma conversa privada no WhatsApp sem que suas mensagens sejam rastreadas". Só que não é isso o que diz o artigo 10. O artigo 10 não se aplica a conversas privadas, apenas a encaminhamentos para múltiplos destinatários. O artigo 10 também não quebra a criptografia e não dá acesso aos conteúdos das conversas interpessoais.

Não seria melhor, no lugar do atual artigo 10, um artigo que autorize acesso às interações dos usuários, com ordem judicial?

O Facebook, empresa proprietária do WhatsApp, tem defendido uma substituição inócua para o artigo 10, para dar a aparência de que deu uma solução legislativa para o grave problema da desinformação no WhatsApp. Essa saída é uma espécie de "grampo de metadados"com ordem judicial que permitiria ver os dados de envio e recebimento de mensagens e chamadas de áudio. Só que esse mecanismo já existe e já é rotineiramente solicitado pelo MPF com base no Marco Civil da Internet. Como já existe, colocá-lo na lei é autorizar algo que já se faz, apenas para dizer que algo foi feito. Além do mais, esse mecanismo não permite identificar a origem dos encaminhamentos em massa, que é o verdadeiro problema no WhatsApp.

Meus encaminhamentos de memes vão ser monitorados?

Não! O sigilo da comunicação é inteiramente resguardado. O conteúdo de uma mensagem só é revelado quando um destinatário que teve acesso a ele faz uma queixa. Os registros de encaminhamentos só são acessíveis no contexto de um inquérito sigiloso, com autorização judicial. A medida vai apenas jogar luz sobre aquilo que nas plataformas de mídia social já é público e visível e que no WhatsApp está oculto e enterrado, permitindo a ação de grupos maliciosos. Apenas com um clique qualquer um pode ver todo mundo que retuitou ou compartilhou um determinado post viral no Twitter ou no Facebook e ninguém se sente monitorado por isso. O artigo 10 separa conceitualmente esse tipo de comunicação viral, de massa, que deveria estar na esfera pública, da comunicação interpessoal que deve estar fortemente protegida pela privacidade e pela criptografia ponta a ponta.