As nebulosidades e riscos do art. 10 do Projeto de Lei das Fake News

O registro de encaminhamento de mensagens efetivamente contribuirá para o combate a crimes digitais e Fake News?

Aprovado no Senado o Projeto de Lei 2.630/2020, que trata do combate a Fake News, por 44 votos a 32. A matéria, no entanto, causou controvérsia, sobretudo no seu artigo 10, que obriga os aplicativos, como o WhatsApp, a registrarem os encaminhamentos de mensagens realizadas, rastreando o que alguém envia para outrem. Mas será que este artigo é fundamental para o combate a crimes digitais e Fake News?

Muitos mensageiros privados já informam medidas para combate às Fake News em tempos de pandemia. O WhatsApp, por exemplo, anuncia em suas políticas sobre limites de encaminhamentos de conversas: *"Para tornar o WhatsApp ainda mais pessoal, criamos o conceito de mensagens encaminhadas muitas vezes e adicionamos uma etiqueta de setas duplas para indicar que essas mensagens não foram criadas pelo contato que as enviou. Geralmente, as mensagens encaminhadas muitas vezes podem conter informações falsas e não são tão pessoais quanto as mensagens típicas enviadas pelos seus contatos no WhatsApp. Agora, atualizamos o limite de encaminhamento para que essas mensagens só possam ser encaminhadas para uma conversa por vez."*

Informa que as mensagens de WhatsApp já possuem um contador que registra quantas vezes a mensagem é encaminhada, informando ainda que o contador também é protegido pela criptografia ponta a ponta, e somente o aparelho do usuário e destinatário possui. O App alega que "não tem acesso a quantas vezes uma mensagem foi encaminhada". Se esta tese for

verdadeira, o próprio app no aparelho armazena a contagem e diante de número elevado aciona uma função condicional, limitando a possibilidade de encaminhamento.

O artigo 10, no entanto, determina que os serviços de comunicação instantânea devam guardar os chamados "registros de encaminhamento", o que vem sendo considerado uma "tornozeleira digital" pelos provedores de aplicação e um grande retrocesso. Basicamente, os provedores de aplicação deverão registrar metadados, "dados sobre dados", relativos aos envios de mensagens veiculadas em encaminhamentos em massa, custodiando estes registros por três meses. A argumentação aqui é que se possa chegar à averiguação da origem de uma Fake News. Será?

O que se pretende guardar aqui seria, em nossa visão, data, hora, número/terminal ou Ids envolvidos nos envios, fuso horário e quantitativo total dos usuários que receberam a mensagem. Assim, a partir de uma mensagem recebida ou descoberta pela vítima, se poderia, com base na Lei Projetada (Lei Brasileira de Liberdade Responsabilidade e Transparência na Internet) requerer uma ordem judicial para que o mensageiro apresentasse, judicialmente, o registro de todos os encaminhamentos (cadeia de encaminhamentos), desde o primeiro existente no período de guarda, contanto que a mensagem deve se enquadrar nos critérios que obrigam o armazenamento, previstos em lei. Caso negativo, o provedor de aplicações deverá, em tese, justificar em juízo o não fornecimento. Quais critérios são esses?

Não se busca aqui, como visto, o conteúdo das mensagens e a princípio não se identifica os destinatários das mensagens. Faltava, no entanto, definir o que seriam os chamados "encaminhamentos em massa". Na PL, ficou definido como o envio de uma "**mesma mensagem"**, por mais de 5 (cinco) usuários em intervalo de até 15 (quinze) dias, para grupos de conversas, lista de transmissão ou mecanismos similares de agrupamentos de múltiplos signatários, sendo obrigado a guardar apenas as

mensagens que alcançarem 1.000 ou mais usuários. O acesso, só deve se dar por ordem judicial. A questão é, como a suposta vítima vai saber se a "notícia falsa" está inserida no contexto de um encaminhamento em massa? Quais são os critérios para identificá-las? Uma mensagem pode não ter alcançado 1.000 usuários em uma semana, e na outra sim… Assim, na dúvida, resta indisfarçável que se este artigo calhar, muitas supostas vítimas irão pedir tais registros ao Judiciário, mesmo sem saber se trata de encaminhamento em massa, e isso pode gerar um aumento considerável de processos e requerimentos. O Judiciário deverá ser muito criterioso nas análises. As aplicações se recusarão a fornecer dados informando que não há registros para a mensagem, pois não atingiu os critérios legais para armazenamento.

O artigo 10 foi aprovado no Senado, mesmo com destaque em sentido contrário, rejeitado, onde alguns Senadores entenderam que o "registro de encaminhamento" é essencial (pedra de toque) para apuração das Fake News, o que não é uma verdade técnica. O Marco Civil já prevê a guarda dos registros de acesso à aplicação (data, hora, ip e fuso horário) e que já são suficientes para a apuração da autoria de Fake News nos comunicadores instantâneos, ainda que em uma sequência de investigações mais demorada. Deste modo, não se trata de mais textos legislativos, mas de efetiva cooperação das aplicações no cumprimento da legislação já existente.

De outra ordem, existem vários meios técnicos para "burlar" o "registro de encaminhamento" tal como vem sendo arquitetado. E se uma pessoa não "encaminha" a mensagem, mas a partir do conteúdo armazenado em seu dispositivo a reposta? Este registro seria considerado, tendo em vista que a ação foi outra? E se ao invés de encaminhar uma mensagem ou conteúdo visual, alguém printa a tela e reenvia, ou mesmo envia uma "foto da foto", ou ainda, envia o conteúdo não como imagem ou texto, mas como documento. São meios simples de burlar as "etiquetas", quer via metadado, quer via *hashing* que possam

ser aplicadas em um sistema de rastreamento de encaminhamentos.

Como se vê, a exigência do artigo 10 parte de uma premissa equivocada, é pouco eficaz contra as FaKe News e técnicas de subversão possíveis e vai gerar alta onerosidade técnica para os serviços de aplicativos de mensagens, que serão obrigados a ter uma estrutura para gerar e armazenar inúmeros registros de encaminhamentos, *taggeando* mensagens desde o surgimento dela (inserindo uma codificação para que, eventualmente, diante de uma ordem judicial, seja identificada a "mesma mensagem" compartilhada por mais de 5 usuários), mesmo "sem conhecerem o conteúdo" encaminhado, em um "rastreamento preventivo" perigoso. Aliás, se assim não for, outra questão perturbadora é: Como os provedores de aplicação e mensageria privada vão tecnicamente identificar "uma mesma mensagem", enviada em massa, se eles não inspecionam o conteúdo das mensagens, por respeito à privacidade e proteção de dados? Farão por *hash* dos conteúdos (campos)? Desenvolverão uma técnica? Um risco imenso à privacidade se mentaliza.

Do mesmo modo, a argumentação de que são "apenas" registros metadados e não de conteúdos, e que a criptografia ponta-a-ponta do WhatsApp já preserva a privacidade, também não resiste à análise técnica. A privacidade estará ameaçada mesmo que o mensageiro adote a criptografia das conversas, pois com os metadados gerados por usuários e armazenados pelos mensageiros (incluindo números telefônicos) em mãos erradas ou vazados, pode-se ter um dossiê completo sobre as atividades de encaminhamentos, além de outras correlações, com efeito, existem implicações e conflitos nítidos também com o disposto na Lei Geral de Proteção de Dados (13.709/2018).

Como visto, estes são apenas alguns de muitos pontos nebulosos na disposição o artigo 10 da PL 2.630/2020, como por exemplo, como avaliar a intenção do agente que encaminha uma mensagem considerada Fake? Estaria agindo com dolo ou é mais uma vítima que acreditou e repassou? São pontos como estes que demanda

mais debates aprofundados no Senado, que diversamente, não estendeu a discussão para ouvir os especialistas e, rejeitando o destaque de modificação do artigo 10, aprovou o Projeto de Lei. Queremos crer, na Câmara dos Deputados, que o deslinde não seja o mesmo e que a discussão ocorra, no escopo de se corrigir inúmeras falhas deste projeto desproporcional e equilibrá-lo para não afrontar direitos e garantias fundamentais e Leis já estabelecidas, como o Marco Civil da Internet, sobretudo, para que não permaneça com o status de um dos mais restritivos do mundo.

José Antonio Milagre é perito digital, especialista em Crimes Cibernéticos, Advogado, Mestre e Doutorando pela UNESP, Presidente da Comissão de Direito Digital da Regional Vila Prudente da OAB/SP e Diretor do Instituto de Defesa do Cidadão na Internet (IDCI). e-mail: consultor@josemilagre.com.br