Matéria na versão impressa e digital da Folha de S. Paulo, com a participação do especialista em Direito Digital, Dr. José Milagre, sobre o Registro da Cadeia de Encaminhamentos do WhatsApp, previsto no Projeto de Lei das Fakenews (PL 2630/2020).

Uma das matérias mais profundas sobre este tema, que pode vir a ameaçar toda a construção de direitos e garantias a todos os usuários de Internet do Brasil.

Quer saber mais detalhes, então acesse https://www1.folha.uol.com.br/poder/2020/07/regra-para-armazenar-cadeia-de-mensagens-do-whatsapp-pode-ser-ineficaz-em-projeto-de-fake-news-no-congresso.shtml e fique por dentro!

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

Novo Projeto de Lei das Fake News 3063/2020: 10 pontos que merecem atenção antes de qualquer votação

O que o legislativo brasileiro não pode desconsiderar ao tratar de um PL sobre a possível desinformação na Internet.

Em 02 de junho de 2020 foi apresentado um novo Projeto de Lei que institui a Lei Brasileira de Liberdade, Responsabilidade e Transparência na Internet. A norma projetada destina-se às redes sociais e serviços de "mensageria privada" que ofertam serviços de Internet, com o escopo de desestimular o abuso ou a manipulação destes, dando causa a danos individuais ou coletivos.

Não se aplica ao provedor de aplicação de redes sociais com menos de dois milhões de usuários registrados. Logo, é evidente o foco da Legislação para grandes aplicações como Twitter, Facebook, WhatsApp, Instagram e outros grandes serviços populares no Brasil e mundo, campos de batalha digital em período eleitoral. Sua aplicabilidade também se dá a empresas estrangeiras, desde que haja pelo menos uma integrante do grupo econômico presente no Brasil.

Os objetivos são contemplados no artigo 3 o ., como o fortalecimento do processo democrático com base no combate ao comportamento "inautêntico", distribuição artificial de conteúdo e fomento à diversidade de informações. Em seu artigo 4º, define o que seria uma conta "inautêntica", conta essa,

criada ou usada com o propósito de assumir identidade inventada ou de terceiros para enganar o público, ressalvados o direito à pseudonímia, bem como o explícito ânimo humorístico ou de paródia. Do mesmo modo, descreve o que seriam “contas automatizadas”, como contas geridas por qualquer programa de computador ou tecnologia para simular, substituir ou facilitar atividades humanas na distribuição de conteúdo em aplicações de internet ou aquelas geridas por ação preponderantemente humana e que complementam a atuação automatizada da conta, ainda que esporadicamente.

A legislação projetada preocupa-se com a criação de “redes de distribuição artificial”, caracterizadas como sendo um comportamento coordenado e articulado de contas automatizadas ou por tecnologia não fornecida pelo provedor de aplicação, com o fim de implantar de forma artificial a distribuição de conteúdos.

No artigo 5º, simplesmente informa que os provedores de aplicação de internet deverão adotar medidas para vedar contas inautênticas, contas automatizadas cujo caráter automatizado não foi comunicado aos referidos provedores. Ainda, em seu artigo 6 o , inclui diversas atividades e deveres para as redes sociais, dentre as quais medidas que demandam levantamento de dados
excessivos e desnecessários para o efetivo combate às Fake News. Chega a anotar como obrigatório relatório com o “número total de redes de distribuição artificial” detectadas. Ora, será preciso uma perícia em informática acurada, e ainda assim, receia-se que será temeroso demais às redes sociais terem que rotular um grupo de perfis como uma “rede de distribuição artificial”.

O usuário passa a ter o direito de ser notificado pela própria

rede social, sempre que ocorrer um processo de análise de conteúdos e contas violadoras. Este poderá, nos termos do art. 8º, contestar eventual denúncia de conteúdo irregular. Do mesmo modo, são previstos recursos das decisões, nos termos do art. 9º do Projeto de Lei.

A norma assegura que em caso de conteúdos que tenham sido equivocadamente identificados como irregulares ou violadores dos padrões do provedor de aplicações, caberá ao mesmo reparar o dano, informando o erro de maneira destacada e garantindo a exposição da correção, no mínimo, aos usuários inicialmente alcançados. Caso ocorra a revisão judicial de conteúdo tornado indisponível, assegura em seu art. 11 que a rede social deverá substituir o conteúdo tornado indisponível pela ordem judicial que deu fundamento à correção. Destaca-se que a nova versão do PL veda a indisponibilização de conteúdos com fundamento na própria lei, exceto em casos de decisão judicial.

Interferindo nos serviços de mensagens privadas, o regulamento ainda tenta limitar o número de encaminhamentos de mensagens a usuários e grupos e o número de membros dos mesmos. Diante do art. 14, o Telegram, por exemplo, encontrará um problema no seu modelo de negócios, permitindo grupos com centenas de usuários. O usuário deverá sempre dar permissão
prévia antes de receber uma mensagem de serviço de comunicação em massa nos mensageiros, o que impõe também medidas técnicas por parte de inúmeros aplicativos.

Proíbe-se, no artigo 15, o uso e a comercialização de ferramentas externas aos provedores de aplicação de mensageria privada, voltadas ao disparo em massa de mensagens. Esta questão pode interferir em inúmeros negócios lícitos hoje existentes, macros, automatizadores, chatbots e outros recursos. Muitas ferramentas não tem como fim “o envio” de

mensagens em massa, mas possuem a função, para usuários cadastrados e sem qualquer finalidade de espalhe de Fake News.

Percebe-se, por parte do legislador, igualmente, uma tentativa de se "descobrir à fórceps" quem começou uma corrente de possível "Fake News" nos serviços de mensageria privada, uma vez que o artigo 17 estabelece que o provedor de aplicação que apresenta funcionalidade e o reencaminhamento similar de conteúdos, deve guardar os registros da cadeia de reencaminhamentos até sua origem, pelo prazo mínimo de 1 (um) ano, resguardada a privacidade do conteúdo das mensagens, podendo esses registros ser solicitados mediante ordem judicial nos termos da Seção IV da Lei 12.965 de 2014. A norma, no entanto, não trata explicitamente da proibição de novos compartilhamentos de conteúdos indevidos, a partir da extração de metadados dos arquivos e seu cheksum, medidas aliás determinadas em alguns casos judiciais no país.

Em relação aos conteúdos impulsionados, os usuários passam a ter direitos, dentre os quais, o de saber quais as fontes de informação e quais os critérios utilizados para a definição de público alvo do conteúdo que teve contato. Basicamente, repisando parte do que já era disposto na Lei 12.965 de 2014, a Lei projetada destina sete artigos para tratar da atuação do Poder Público, que deverá incluir capacitação para o uso consciente da internet e deverá realizar campanhas sobre a importância do combate ao comportamento inautêntico na Internet.

As penalidades para o descumprimento estão previstas no artigo 29 do projeto e não excetuam sanções civis, criminais ou administrativas. As penalidades são advertência, multa e suspensão temporária das atividades. Nesta versão, não existe a penalidade de proibição das atividades.

Caberá, ainda, ao Comitê Gestor da Internet do Brasil, definir um grupo de trabalho multissetorial que deverá estabelecer proposta legislativa que conceitue “conteúdo desinformativo”, bem como apresentar as formas de combate a desinformação a partir de boas práticas internacionais em estudo. Este grupo multissetorial teria 1 (um) ano, a partir da publicação da Lei, para apresentar a proposta.

Passa a ser considerada violação à Lei de Improbidade Administrativa o fornecimento de acesso às contas de redes sociais de órgãos públicos à administradores externos ou que não tenham relação contratual com a administração pública, e também o emprego de recursos públicos para condutas que violem a Lei Brasileira de Liberdade, Responsabilidade e Transparência na
Internet (Art. 11, XI e XII).

Do mesmo modo, a Lei das organizações criminosas (12.850) é alterada para também abranger às organizações formadas para a criação e ou operação de contas inautênticas, contas automatizadas não identificadas e ou redes de distribuição artificial não identificadas por meio do emprego de recursos financeiros e técnicos que praticam ilícitos.

Por fim, a norma exige que as redes sociais e mensageiros nomeiem mandatários judiciais no Brasil, aos quais serão dirigidos os atos processuais decorrentes desta Lei. Feito este resumo dos principais pontos do novo PL, ao qual está se impingindo um ritmo desproporcional à atenção que um projeto desta natureza merece, elencamos 10 (dez) pontos de atenção e consideração, antes de qualquer votação e que demandam esclarecimentos sob pena de consequências gravíssimas:

1) Existe grande risco a aplicativos que não usam contas automatizadas, mas utilizam tecnologias conectadas às redes sociais, uma vez que podem ser consideradas “rede de distribuição artificial”. Como se avaliará a finalidade destes aplicativos? Quem definirá o que realmente é conteúdo artificial? Como as redes farão este papel?

2) As medidas para a vedação de contas “automatizadas” previstas no artigo 5º da legislação são genéricas, não definidas, onerosas e podem implicar na exclusão de conteúdos e perfis legais, isto porque um perfil real ou serviço poderá automatizar alguma tarefa em redes sociais e sem finalidade de praticar desinformação, o que poderá gerar um falso positivo nos registros da rede social.

3) As medidas para a verificação de contas inautênticas já existem hoje em grande parte das redes sociais, porém, não existe o monitoramento prévio, o que é salutar, e somente quando provocado judicialmente os provedores agem em respeito às disposições do Marco Civil da Internet. O Twitter, por exemplo, faz um questionário prévio antes liberar acesso à sua API. Medidas automatizadas poderão implicar em remoções de perfis legítimos, para pesquisas ou autorizados pelas pessoas reais e na limitação de direitos.

4) O relatório de dados que os provedores de aplicação deverão produzir a cada três meses possuem dados excessivos e desnecessários. Como as redes sociais poderão identificar “redes de distribuição artificial”? Qual critério? Qual metodologia e parâmetros para estas conclusões? Como aplicar na prática esta disposição legislativa?

5) Como uma rede social irá lidar com contestações e recursos

de pessoas envolvidas em processos de notificação irregular? A rede social passará a julgar conteúdos? Quais as responsabilidades de um julgamento que exclua liberdade de expressão ou opinião? Não se está criando redes policialescas?

6) Como ficará a responsabilidade das redes sociais, a partir da inserção do art. 13 da Lei da Responsabilidade na Internet, quando algoritmos automaticamente reduzirem alcance de conteúdos ou removerem os mesmos? O artigo estabelece que é vedada a indisponibilização de conteúdo com fundamento nesta Lei, exceto por decisão judicial específica e fundamentada.

7) Ao proibir sistemas não oferecidos pelos mensageiros e que permitem o disparo de mensagens em massa, como lidar com serviços legais oferecidos por chatbots por exemplo, onde é possível enviar "broadcasts" aos usuários que optaram por receber os
referidos conteúdos? É possível considerar todos os serviços de disparo em massa como ilegais? E se o usuário concordou com o recebimento?

8) Como estender o conceito de "registros de acesso à aplicação" definidos no Marco Civil da Internet, para englobar também os tais "registros de cadeia de reencaminhamento" previstos na legislação projetada? O que seria este registro? Quais campos o compõe? Estaríamos tratando de data, hora, ip, número telefônico e fuso horário em ordem crescente dos encaminhamentos, desde a primeira publicação no serviço ou mensageiro? Quais os riscos à privacidade dos usuários?

9) Como interpretar um conteúdo desinformativo, se o grupo multissetorial que irá definir seu conceito, terá um ano, após a edição da norma, para defini-lo? Como se produzirá a prova

de improbidade administrativa para identificar que agentes públicos cederam a administração de redes sociais a terceiros sem contratos com a administração pública?

10) Como definir “desinformação” de forma clara e justa? Como não tratar usuários de internet como potenciais infratores?

Não há dúvidas que a estas primeiras questões, muitas outras são acrescentadas por associações, entidades de Direito Digital, peritos em informática, cientistas da informação, provedores de aplicações, pesquisadores e sociedade em geral.

Como se verifica, o Projeto de Lei retirado de pauta (2630/2020) trazia uma série de questões polêmicas e exigência de dados excessivos, como documentos de identidade para criação de perfis, além de enaltecer a responsabilização das plataformas, o que confrontava o Marco Civil da Internet e poderia estimular as redes a controlarem conteúdos das redes sociais e ampliar a censura.

Não obstante, a nova proposta, mais amena, também apresenta riscos e pontos que dependem de esclarecimentos e maior tempo de análise, e como concebida, ao obrigar as redes a classificarem e detectarem quem é bot e quem não é, pode gerar um ambiente perigoso e ainda mais nocivo a direitos e garantias fundamentais. Um projeto, com tantos pontos a serem esclarecidos, como o presente, não pode, de forma alguma, tramitar à toque de caixa. Um amplo debate, que enfrente os quesitos aqui levantados, com dilatada participação da sociedade civil, é fundamental. Trata-se, aqui, de um tema sensível a todos, como impactos diretos em direitos e garantias fundamentais. A pressa é inimiga, e poderá culminar em graves consequências à inovação, liberdade de expressão e

informação e a outros direitos.

Fomos citados em 3 (três) oportunidades na Manifestação da PROCURADORIA GERAL DA REPÚBLICA 154141/2020, em trâmite no Supremo Tribunal Federal – STF

Muito feliz, fomos citados em 3 (três) oportunidades na Manifestação da PROCURADORIA GERAL DA REPÚBLICA 154141/2020, assinada pelo Procurador AUGUSTO ARAS, na ARGUIÇAÕ DE DESCUMPRIMENTO DE PRECEITO FUNDAMENTAL 403/SE, em trâmite no Supremo Tribunal Federal – STF e da relatoria do Ministro Edson Fachin.

O parecer do PROCURADOR-GERAL DA REPÚBLICA, manifesta-se pela procedência do pedido, para obstar o bloqueio nacional do WHATSAPP como meio coercitivo para cumprimento de decisões judiciais, sem prejuízo de outras providências para cumprimento das ordens judiciais.Feliz em colaborar com o entendimento da corte MÁXIMA sobre o tema!

MINISTÉRIO PÚBLICO FEDERAL
PROCURADORIA-GERAL DA REPÚBLICA

ARGUIÇÃO DE DESCUMPRIMENTO DE PRECEITO FUNDAMENTAL 403/SE

RELATOR: MINISTRO EDSON FACHIN

REQUERENTE: PARTIDO POPULAR SOCIALISTA (PPS)

INTERESSADO: JUIZ DE DIREITO DA VARA CRIMINAL DA COMARCA DE LAGARTO/SE

MANIFESTAÇÃO ASSEP/PGR Nº 154141/2020

ARGUIÇÃO DE DESCUMPRIMENTO DE PRECEITO FUNDAMENTAL. BLOQUEIO JUDICIAL DO APLICATIVO *WHATSAPP*. IMPOSSIBILIDADE. DESPROPORCIONALIDADE DA MEDIDA. VIOLAÇÃO ÀS LIBERDADES COMUNICATIVAS.

1. A prática generalizada de crimes cibernéticos é coibida pela legislação brasileira, que prevê a interceptação do fluxo das comunicações em sistemas de informática e telemática (Lei 9.296/96).

2. A utilização de aplicativos de conversação por integrantes de organizações criminosas tem originado decisões judiciais de quebra do sigilo das comunicações, cuja possibilidade é prevista na Lei do Marco Civil da Internet (Lei 12.965/14).

3. Embora sediada no exterior, a *WhatsApp Inc.* há de observar a legislação brasileira e as ordens emanadas do Poder Judiciário (art. 11, Lei 12.965/14), inclusive no que concerne a fornecer o conteúdo de comunicações privadas (art. 7º, II e III e art. 10, § 2º, Lei 12.965/14).

4. O bloqueio nacional dos serviços e atividades da *WhatsApp Inc.* como meio de induzir o cumprimento das decisões judiciais é desproporcional e viola as liberdades comunicativas (art. 5º, IV e IX, CF) e, portanto, implica lesão a preceito fundamental, podendo o magistrado valer-se de aplicação de astreintes e cominação de sanções.

A conjugação dos dispositivos mencionados permite a interpretação pela qual, embora não haja mandamento explícito de guarda dos registros de comunicação que o usuário realiza em uma aplicação, a custódia desses dados pode ser determinada por ordem judicial. Nesse sentido, parte da doutrina estabelece[5]:

> *O Marco Civil silencia, no entanto, se os Provedores de aplicações teriam o dever de coletar e armazenar as comunicações que ocorrem em seus serviços, referindo-se apenas aos 'registros de acesso e aplicações'. Por outro lado, os incisos II e III do art. 7º do Marco Civil estabelecem que o sigilo das comunicações pode ser quebrado por ordem judicial. Logo, estaria implícita a obrigação de guarda dos registros de comunicação que o usuário realiza em uma aplicação? Em verdade, não.* ***O entendimento coerente é que ordem judicial pode determinar a guarda de registros de comunicação, que deverá ocorrer a partir da ordem****, não legitimando o art. 7º, inc. II e III, do Marco Civil, qualquer postura de provedores de aplicação no sentido do dever de guardarem todas as comunicações de seus usuários, sempre, ou antes mesmo de ordem judicial assim obrigando, em caso específico.* - Grifo nosso.

5 JESUS, Damásio de. MILAGRE, José Antônio. **Marco Civil da Internet.** Comentários à Lei n. 12.965/14. São Paulo: Saraiva, 2014. pp. 33-34.

Conforme esse entendimento, pelo menos a partir da decisão judicial, subsiste o dever de armazenar os registros de comunicação. Isso se confirma da leitura de outros dispositivos legais, a exemplo do artigo 10, § 2º, pelo qual *"O conteúdo das comunicações privadas somente poderá ser disponibilizado mediante ordem judicial"*.

Em comentário ao artigo 10, § 2º, a doutrina esclarece[6]:

> *Embora não preveja se os provedores devam guardar e por quanto tempo o conteúdo das comunicações, fato é que, do disposto neste parágrafo (e também dos incs. II e III do art. 7º do Marco Civil), é possível concluir que, embora não deva guardar o conteúdo das comunicações de seus usuários,* ***ordem judicial poderá obrigar os provedores a assim fazerem,em relação a um usuário específico, guarda esta que será, sempre, a partir de uma ordem judicial.***
> *[...]*
> *Se o Marco Civil não prevê o dever de coletar e armazenar as comunicações, os provedores não são obrigados a tal nem a fornecer o que não possuem ou não custodiam. Como dito,* ***ordem judicial poderá determinar a guarda, sem que o provedor possa ser responsabilizado, no entanto, porque não guardou tais registros no passado, mas somente se descumprir a obrigação a partir da intimação ou ciência de ordem judicial específica***. - Grifo nosso.

6 JESUS, Damásio de. MILAGRE, José Antônio. **Marco Civil da Internet.** Comentários à Lei n. 12.965/14. São Paulo: Saraiva, 2014. p. 47.

A legislação brasileira tem incidência quando provedores estrangeiros prestam serviço neste país, bastando que qualquer fase do tratamento de dados ocorra em território nacional. O artigo 11 aplica-se, por exemplo, às redes sociais e comunicadores populares no Brasil[7].

IV. Das alegadas dificuldades técnicas de implementação das decisões judiciais

O problema nasce da dificuldade prática apresentada pela *WhatsApp Inc.* em dar cumprimento às decisões do Poder Judiciário Brasileiro. Quando juízes determinam o fornecimento das comunicações entre usuários, no bojo de processos ou procedimentos criminais, alega-se que a tecnologia da *"criptografia de ponta a ponta"* seria obstáculo pretensamente intransponível.

Argumenta-se que, uma vez criptografados, somente os interlocutores podem ter acesso ao conteúdo remetido. Supostamente, nem mesmo a *WhatsApp Inc.* conseguiria acessar o teor das comunicações, porque as chaves especiais que decodificam os dados permaneceriam com remetente e destinatário.

---

7 JESUS, Damásio de. MILAGRE, José Antônio. **Marco Civil da Internet.** Comentários à Lei n. 12.965/14. São Paulo: Saraiva, 2014. p. 51.

MINISTÉRIO PÚBLICO FEDERAL
PROCURADORIA-GERAL DA REPÚBLICA

Sabe-se que, atualmente, crimes cibernéticos são cometidos por aplicativos de conversação. Muitos delitos são ordenados do interior das unidades prisionais, inclusive, execuções e atentados.

Entretanto, a autoridade das ordens judiciais de interceptação telemática pode ser assegurada por outros meios que impliquem um sacrifício menor aos direitos fundamentais da sociedade, a exemplo da imposição de astreintes ou a cominação de sanções.

Em face do exposto, o PROCURADOR-GERAL DA REPÚBLICA manifesta-se pela procedência do pedido formulado na arguição de descumprimento de preceito fundamental, para obstar o bloqueio nacional dos serviços do *Whatsapp* como meio coercitivo para cumprimento de decisões judiciais, sem prejuízo da adoção de outras providências para cumprimento das ordens judiciais.

Brasília, data da assinatura digital.

Augusto Aras
Procurador-Geral da República
Assinado digitalmente

Para ter acesso ao inteiro teor, acesse: http://portal.stf.jus.br/processos/detalhe.asp?incidente=4975500