SENADO FEDERAL

Gabinete do Senador MECIAS DE JESUS

PROJETO DE LEI DO SENADO Nº 2021

Altera a Lei nº 13.105, de 16 de março de 2015 - Código de Processo Civil, para dispor sobre a aplicação de astreintes.

O CONGRESSO NACIONAL decreta:

Art. 1º. Esta lei altera a Lei nº 13.105, de 16 de março de 2015 - Código de Processo Civil, para dispor sobre a aplicação de astreintes.

Art. 2º. O art. 537 da Lei nº 13.105, de 16 de março de 2015, passa a vigorar acrescido do seguinte § 6º:

"Art. 537. .....

.....

§ 6º. Não se aplica astreintes por descumprimento de decisão judicial de quebra de sigilo de dados, em virtude da impossibilidade técnica, haja vista o emprego de criptografia de ponta a ponta." (NR)

Art. 3º. Esta Lei entra em vigor na data de sua publicação.

JUSTIFICATIVA

O objetivo desse Projeto de lei é pacificar o entendimento que hoje prevalece nos tribunais superiores sobre a aplicação de astreintes por descumprimento de decisão judicial de quebra de sigilo de dados.

As astreintes configuram um mecanismo de execução indireta respaldado no art. 537 do CPC, cuja finalidade é coagir o devedor que deixar de atender a ordem judicial mediante a imposição de multa pecuniária diária pelo descumprimento.

Não obstante a existência das normas legais que lhe dão o devido suporte, o fato é que, na prática, a imposição das astreintes acabou, ao longo do tempo, gerando uma infinidade de situações não previstas em lei, as quais, por sua vez, obrigaram o Judiciário,

em especial, o STJ e o STF, a se posicionarem diante das inúmeras discussões daí decorrentes.

A discussão recente mais notória sobre o tema se deu em maio do presente ano, no âmbito do STF. Trata se de dispositivos da Lei nº 12.965/2014 (Marco Civil da Internet) que têm sido invocados para justificar decisões judiciais determinando a suspensão de serviços que permitem a troca de mensagens entre usuários da Internet. Decisões judiciais dessa natureza, notadamente em relação ao aplicativo WhatsApp, foram impugnadas na Arguição de Descumprimento de Preceito Fundamental 403 (Relator Ministro Edson Fachin) e na ADI 5527 (Relatora Ministra Rosa Weber).

A ministra Rosa Weber e o Ministro Edson Fachin decidiram sobre a possibilidade de aplicação de astreintes a empresa whatsapp, pelo descumprimento de ordem judicial que determinava a quebra de sigilo de dados de usuário.

Na ocasião do julgamento, ambos os eminentes Ministros chegaram à mesma conclusão: **o ordenamento jurídico brasileiro não autoriza, em detrimento da proteção gerada pela criptografia de ponta a ponta, em benefício da liberdade de expressão e do direito à intimidade, sejam os desenvolvedores da tecnologia multados por descumprirem ordem judicial incompatível com encriptação**.

Criptografia de ponta a ponta é a proteção dos dados nas duas extremidades do processo, tanto no polo do remetente quanto no outro polo do destinatário. Nela, há dois tipos de chaves são usados para cada ponta da comunicação, uma chave pública e uma chave privada. As chaves públicas estão disponíveis para as ambas as partes e para qualquer outra pessoa, na verdade, porque todos compartilham suas chaves públicas antes da comunicação. Cada pessoa possui um par de chaves, que são complementares. O conteúdo só poderá ser descriptografado usando essa chave pública junto à chave privada. Essa chave privada é o único elemento que torna impossível para qualquer outro agente descriptografar a mensagem, já que ela não precisa ser compartilhada.

Ao buscar mecanismos de proteção à liberdade de expressão e comunicação privada, por meio da criptografia de ponta a ponta, as empresas estão protegendo direito fundamental, reconhecido expressamente na Constituição Federal.

Em sua decisão, a ministra Rosa Weber observou que, como a maior parte dos aplicativos de mensagens utiliza criptografia de ponta a ponta, para que apenas remetente e destinatário tenham acesso ao conteúdo, "**a lei não pode ser interpretada de forma a impor punição pela não disponibilização de mensagens às quais o prestador de serviços não tem acesso.** A criptografia é amplamente utilizada porque torna as comunicações online mais seguras e possibilita, por exemplo, o comércio eletrônico, as

transações bancárias eletrônicas e até mesmo a segurança de grupos de direitos humanos que atuam contra regimes opressivos em todo o mundo".

Para a Ministra, a criptografia é hoje uma ferramenta indispensável à proteção da privacidade e não é possível obrigar as empresas a deixarem de utilizá-la, sob pena de violar os princípios da proteção do sigilo das comunicações e das informações. "Qual seria o sentido de uma Constituição que em 2020 protegesse o sigilo das comunicações telegráficas, mas não o fizesse quanto ao sigilo das comunicações pela internet ou por qualquer outro meio pelo qual as pessoas lancem mão para se comunicar, inclusive de forma instantânea?", questionou.

A ministra afastou qualquer interpretação da lei que permita a punição pela inobservância de ordem judicial que determine a disponibilização de conteúdo de comunicações mediante a fragilização deliberada dos mecanismos de criptografia voltados à proteção da privacidade.

Assim, em ponderação de valores os benefícios advindos da criptografia de ponta a ponta se sobrepõem às eventuais perdas pela impossibilidade de se coletar os dados das conversas dos usuários da tecnologia.

Ainda, que a Lei 12.965/14 permita o acesso a registros de acesso mediante ordem judicial, essa disposição deve ser interpretada a luz da Constituição Federal. Não podemos nos esquecer que o Marco Civil da internet foi desenhado a partir de três fundamentos essenciais os quais norteiam a relação das empresas prestadoras de serviços de internet com os seus clientes. São eles: a neutralidade da rede, a **privacidade do usuário** e a fiscalização.

O intérprete da Lei deve considerar a distinção conceitual entre a quebra de sigilo de dados armazenados e a interceptação do fluxo de comunicações. Lembrando que o art. 5º, X, da CF/88 garante a inviolabilidade da intimidade e da privacidade, inclusive quando os dados informáticos constarem de banco de dados ou de arquivos virtuais mais sensíveis.

Vale ressaltar, que não somente a Google vem contestando com insistência esse tipo de requisição judicial, mas também outras empresas de tecnologia e provedores de serviços na Internet vêm se negando a fornecer os dados que armazenam, ainda que para fins de investigação criminal ou instrução processual. Essa discussão sobre a amplitude e requisitos da ordem judicial para quebra do sigilo telemático também está na pauta de cortes judiciárias em diversos outros países.

O problema central das requisições judiciais de quebra de sigilo de dados de usuário diz respeito ao alcance da medida que considera certas coordenadas geográficas num determinado município em certo lapso de tempo. Isso quer dizer

que todo mundo que estiver se comunicando através de whatsapp numa determinada região, num determinado espaço de tempo terão o sigilo de suas comunicações quebrado.

Conforme alegou a Google em sua defesa, a quebra do sigilo telemático de um conjunto não identificado de pessoas, que sequer ostentam a condição de suspeitos, unidas tão somente pela circunstância de terem transitado num mesmo local, num mesmo período de tempo, não tem previsão constitucional ou base legal.

Aduziu que qualquer medida de quebra de sigilo informacional pressupõe necessariamente a individualização dos alvos da ordem, isto é, a especificação das pessoas suspeitas e que são objeto da investigação, nos termos do que dispõem o art. 2º. da Lei n. 9.296/96, a Resolução CNJ n. 59/2008, o art. 22 do "Marco Civil da Internet do Brasil" (Lei n. 12.965/14) e o art. 11 do Decreto Federal n. 8.771/2016. Afirmou que inexiste autorização legal para a determinação de quebra de sigilo de uma gama de pessoas não individualizadas, a partir do mero fornecimento de coordenadas geográficas referentes ao local de ocorrência de certo crime, pois a ordem jurídica brasileira não prevê, como medida investigativa, a exploração de plataformas de empresas de internet para fornecimento de dossiês de informações de usuários indeterminados, sem a delimitação de salvaguardas para as prerrogativas individuais dos cidadãos.

A ordem constitucional não permite que se afaste a privacidade de um grande número de indivíduos apenas por terem estado em determinado local em dado momento. Nesse aspecto, a medida impugnada constitui uma violação ao princípio da legalidade (art. 5º., II, e 37, *caput*, da CF), pois teria que estar prevista em lei.

Quebras de sigilo são admitidas apenas em face daqueles contra os quais existam indícios de envolvimento em atividade ilícita. Ainda, quando movido pelo interesse de investigar crimes, o Estado não pode atuar fora da legalidade. Se o meio de prova decorrente do uso de novos recursos tecnológicos ainda não possui regramento em lei, a prova recolhida é ilícita.

A mera alegação da finalidade de elucidação de crimes não é suficiente, sendo imprescindível que o magistrado justifique a necessidade da restrição a direitos individuais.

Cumpre salientar, que a solicitação de quebra de sigilo de dados viola o princípio da proporcionalidade, pois não se tem garantia de que as informações requisitadas levem aos autores do delito investigado, em razão da imprecisão dos dados. Diversos fatores como meio de conexão, qualidade do sinal, horário e local de captação, a geografia do lugar, o modelo de dispositivo (aparelho celular) geram aleatoriedade na coleta dos dados de localização e podem tornar a produção dos dados requisitados infrutífera, uma vez que, podem deixar de indicar usuários que

estiveram no local ou mesmo apontar pessoas que não estiveram, com potencial de gerar falsos indícios.

Penso que essas circunstâncias retiram a utilidade da medida e afastam a confiabilidade desse meio de obtenção de prova. Para ser válida, a restrição a um direito fundamental necessita ser capaz de satisfazer o fim a que se destina. É preciso que fique demonstrada a adequação da medida de quebra do sigilo de dados à finalidade pretendida. Nota-se que existem outras medidas alternativas e menos invasivas, capazes de levar à individualização dos suspeitos. Por exemplo, o art. 2º. da Lei n. 9.296/96 exige, para a quebra de sigilo telefônico e de dados telemáticos, não somente a demonstração de indícios de autoria ou participação da pessoa investigada, mas também de que a prova seja necessária, não havendo outros meios menos invasivos.

A Resolução n. 59/2008 do CNJ, que disciplina a interceptação telefônica e telemática, reforça a necessidade na ordem judicial de quebra de sigilo da indicação de indícios razoáveis de autoria ou participação dos alvos na infração criminal investigada. O Decreto Federal n. 8.771/16 também veda "pedidos genéricos ou inespecíficos" de dados cadastrais, determinando que "devem especificar os indivíduos cujos dados estão sendo requeridos e as informações desejadas" (art. 11, § 3º.).

Por fim, a quebra de sigilo de dados não atende o requisito da proporcionalidade em sentido estrito, pois provoca dano colateral exagerado consistente na quebra do sigilo de inocentes.

A amplitude e a extensão da medida, que afeta uma área muito grande e exige a entrega de uma massa enorme de informações, revelando o seu potencial invasivo, sem garantias de assegurar a eficiência da investigação criminal, gera mais prejuízos do que benefícios sociais, o que por si só denota a desproporcionalidade da ordem judicial.

Diante do exposto, peço o apoio dos nobres pares para a aprovação deste projeto de lei.

Sala das sessões, 26 de outubro de 2021.

Senador MECIAS DE JESUS

(REPUBLICANOS/RR)