COMISSÃO DE SEGURANÇA PÚBLICA E COMBATE AO CRIME ORGANIZADO

PROJETO DE LEI Nº 2418, DE 2019

Altera a Lei nº 12.965/2014, para criar obrigação de monitoramento de atividades terroristas e crimes hediondos a provedores de aplicações de Internet e dá outras providências.

Autor: Deputado JOSÉ MEDEIROS
Relator: Deputado DELEGADO PABLO

VOTO EM SEPARADO

(Do Sr. Capitão Alberto Neto)

I - RELATÓRIO

A proposição em tela tem por objetivo principal alterar a Lei nº 12.965/2014 (Marco Civil da Internet - MCI), para que provedores de aplicação monitorem ativamente publicações que impliquem em atos preparatórios ou ameaças de crimes hediondos e ataques terroristas, determinando a notificação compulsória da autoridade competente assim que identificada a ameaça.

A proposta foi distribuída às Comissões de Segurança Pública e Combate ao Crime Organizado; Ciência e Tecnologia, Comunicação e Informática e Constituição e Justiça e de Cidadania (Mérito e Art. 54, RICD), sendo este, o primeiro colegiado a analisá-la. Está sujeita à apreciação conclusiva pelas comissões, em regime de tramitação ordinário.

Encerrado o prazo regimental, não foram apresentadas emendas.

É o relatório.

II - VOTO EM SEPARADO

Não obstante a boa intenção do excelentíssimo autor do projeto, o PL esbarra em vedações constitucionais e legais, pois implica o monitoramento prévio generalizado da internet e dos usuários, contrariando o direito fundamental à privacidade, a proibição de censura prévia e mesmo os princípios da presunção de inocência e da livre iniciativa.

Embora a intenção seja monitorar "apenas" determinadas práticas, essa separação não é possível de se fazer na prática. Ou se monitora amplamente a internet, violando a privacidade dos usuários, ou não se monitora; não é possível criar uma espécie de lente mágica que olhe apenas para situações específicas. Ainda mais em se tratando de "atos terroristas" e "crimes hediondos", conceitos legais que somente em cada caso concreto podem se verificar, não a priori. E se verificar a partir da atuação dos agentes de aplicação da lei, não por empresas privadas.

É obrigação, portanto, inviável e indesejada, podendo acarretar censura.

Dentre as atribuições dos provedores de conexão e de aplicação de Internet não cabem, nem poderiam caber, funções de monitoramento ou bloqueio de conteúdos (art. 9, §3º, do Marco Civil). Essa vedação ao monitoramento prévio reside não apenas na necessidade de se preservar a neutralidade de rede e a saúde de toda a infraestrutura que serve de base para a provisão do acesso à internet, mas para preservar os direitos e garantias fundamentais. Nessa linha, o Marco Civil prevê mecanismos tecnicamente seguros e juridicamente adequados para indisponibilização de conteúdos considerados infringentes e provimento de dados de identificação do usuário (arts. 19 e 21).

Uma obrigação de monitoramento como a proposta, além de ensejar censura prévia, representaria indevida intervenção estatal no domínio privado. Essa questão é objeto da Declaração Conjunta sobre a Liberdade de Expressão e Internet

(ONU, OEA, OSCE, e CADHP), segundo a qual, “não se deveria exigir dos intermediários que controlem conteúdo gerado por usuários”.

Os tribunais brasileiros, principalmente o Superior Tribunal de Justiça, vêm reforçando esse princípio do não monitoramento da internet, pois isso significaria impor censura prévia, equiparando-se "à quebra do sigilo da correspondência e das comunicações", e traria "enorme retrocesso ao mundo virtual, a ponto de inviabilizar serviços que hoje estão amplamente difundidos no cotidiano de milhares de pessoas." (REsp 1342640[1]).

O dever de monitoramento prévio também fere o princípio da reserva de jurisdição, ao transformar provedores ao mesmo tempo em juízes e delatores das atividades realizadas por seus usuários, atribuindo a entes privados funções investigativas que são tipicamente públicas.

O STF decidiu pela indelegabilidade do Poder de Polícia para entidades privadas exercerem atividade fiscalizatória. A obrigação imposta também viola o artigo 144 da Constituição Federal, que atribui ao Estado o dever de garantir a segurança pública, não sendo possível exigir de entidades privadas que exerçam a fiscalização de potenciais condutas criminosas de usuários. O PL acaba por privilegiar determinados agentes privados em relação a outros, atribuindo um poder de polícia maquiado de cooperação, ensejando as mais diversas espécies de abusos por parte de grupos com maior poder econômico, que passariam a ser obrigados a monitorar em tempo integral todas manifestações de todos os usuários de seus serviços.

Além disso, a obrigação esbarra também em dificuldades práticas fundamentais, chegando à impossibilidade técnica. Inexistem parâmetros para que o provedor de aplicação identifique publicações que correspondam a atos preparatórios ou ameaças de crimes hediondos ou de terrorismo.

1 https://ww2.stj.jus.br/websecstj/cgi/revista/REJ.cgi/ITA?seq=1568602&tipo=0&nreg=201201860420&SeqCgrmaSessao=&CodOrgaoJgdr=&dt=20170214&formato=PDF&salvar=false

Seria preciso monitorar toda a lista prevista na Lei de Crimes Hediondos[2], que não apenas muda, como contém crimes que sequer poderiam ser "monitorados". Cita-se como exemplo os crimes hediondos de comércio ilegal de armas de fogo e de adulteração de produto medicinal (arts. 1, IX, III e VII-B, da Lei 8.072/90). Nesses delitos, não há como o provedor inferir, apenas com base na postagem, se houve ato preparatório de crime, já que a empresa não detém o conhecimento sobre a existência (ou não) de autorização legal do ofertante para comercializar ou adulterar o produto. Na mesma linha, como diferenciar, por exemplo, o "monitoramento" de lesão corporal culposa da lesão corporal dolosa de natureza gravíssima (esta, sim, considerada crime hediondo)? Ou, ainda, como distinguir o monitoramento de extorsão da extorsão qualificada pela morte?

O mesmo vale para a tentativa de monitoramento de "atividades terroristas", considerando a amplitude do conceito empregado pela Lei Antiterrorismo[3], preenchido apenas na prática, pelos agentes de aplicação da lei brasileira. O critério subjetivo de caracterização do terrorismo cria uma camada adicional de complexidade, já que caberia ao provedor de aplicação julgar se a ação alvo de escrutínio foi praticada por razões de xenofobia, discriminação ou preconceito de raça, cor, etnia e religião.

Vale lembrar que o ordenamento brasileiro já contempla diversos mecanismos para o combate a práticas criminosas, especialmente aquelas envolvendo pedofilia na internet. Não só o Marco Civil já prevê sanções para as infrações às normas de proteção aos registros, dados e comunicações (art. 12), como o ordenamento, de modo geral, já confere ao juiz poderes para fazer garantir o cumprimento de ordem judicial. O Código Penal já tipifica expressamente o crime de desobediência (art. 330), que pode inclusive ser processado sob o rito sumaríssimo (art. 61 da Lei 9.099/1995).

2 http://www.planalto.gov.br/ccivil_03/Leis/L8072.htm
3 http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2016/Lei/L13260.htm

O texto também traz a grave possibilidade de instalação de softwares ou equipamentos pelas autoridades competentes. Ao acertadamente recomendar a supressão do art. 3º (infiltração de agentes), o relator poderia, pelas mesmas razões, suprimir o §3º, do art. 2º. Nota-se que não estão descritos os parâmetros ou o órgão responsável por avaliar a "impossibilidade eventual e justificada de cumprimento do disposto no caput", o que pode gerar interpretações subjetivas e inconsistentes. Assim, qualquer justificativa de provedores de aplicação para não cumprimento do disposto no caput seria respondida com ordem de "instalação de softwares ou equipamentos pelas autoridades competentes que permitam o monitoramento para o mesmo fim". Isso representaria impacto severo e inaceitável nas operações das empresas, em flagrante inconstitucionalidade, por desrespeito à livre iniciativa, fundamento da República Federativa do Brasil (art. 1º, CF) e princípio norteador da atividade econômica (art. 170 CF) e em contrariedade ao MCI, especialmente com relação ao estabelecido nos artigos 2º e 3º, incisos II a VI.

Além disso, o §3º mira e põe em cheque a criptografia de ponta-a-ponta, almejando obrigar os provedores de aplicação a alterar os seus serviços para criar o "backdoor de Estado". Como se sabe, dito assunto encontra-se pendente de análise pelo Supremo Tribunal Federal (ADI 5.527 e ADPF 403), embora vigore o entendimento de que o Estado não pode obrigar que uma empresa enfraqueça a criptografia para facilitar a atividade persecutória.

Como ressaltado anteriormente, tal qual se encontra, o PL é eivado de inconstitucionalidades insanáveis, como desrespeito às garantias fundamentais e interferências injustificáveis na livre iniciativa. Por isso, propomos redação alternativa para sanar esses vícios e poder levar em frente proposta similar à pretendida inicialmente pelo autor, ao substituir a obrigação de monitoramento pela possibilidade de comunicação, pelo provedor de aplicação, de razoável suspeita de risco de prática ou tentativa de terrorismo, atividade criminosa em larga escala e ato criminoso violento com várias vítimas a autoridade com competência legal para receber tais infromações.

A sugestão retira o dever de monitoramento ativo e de fornecimento de conteúdo e possibilita que o provedor de aplicação comunique a suspeita identificada durante a moderação de conteúdo reativa.

A inclusão de expressão “elementos que levem a crer, razoavelmente” possibilita salvaguardas para que não haja comunicação excessiva e sem um mínimo de razoabilidade. “Comunicar a razoável suspeita” busca evitar eventual discussão sobre a obrigação prévia de fornecer qualquer dado. A expressão “autoridade dotada de competência legal” visa assegurar a competência para recebimento de informações, evitando-se eventuais abusos e assegurando a proteção de dados pessoais.

Diante do exposto, votamos pela aprovação do Projeto de Lei nº 2.418, de 2019, na forma do substitutivo apresentado.

Sala da Comissão, em 1 de agosto de 2022

Deputado Capitão Alberto Neto

SUBSTITUTIVO AO PROJETO DE LEI Nº 2418, DE 2019

Altera a Lei nº 12.965/2014, para criar a possibilidade de o provedor de aplicação comunicar razoável suspeita de risco de prática ou tentativa de terrorismo, atividade criminosa em larga escala e ato criminoso violento com várias vítimas a autoridade com competência legal para receber tais informações.

O Congresso Nacional decreta:

Art. 1º. Esta Lei altera a Lei nº 12.965/2014, que estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil, para criar a possibilidade de o provedor de aplicação comunicar razoável suspeita de risco de prática ou tentativa de terrorismo, atividade criminosa em larga escala e ato criminoso violento com várias vítimas a autoridade com competência legal para receber tais informações.

Art. 2º A Lei nº 12.965/2014, que estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil, passa a vigorar acrescida do artigo 21-A, com a seguinte redação:

"Art. 21-A. Os provedores de aplicação que, no curso regular dos serviços e na medida de sua capacidade técnica, identificarem elementos que levam a crer, razoavelmente, no risco de prática ou tentativa de terrorismo, atividade criminosa em larga escala e ato criminoso violento com várias vítimas, deverão comunicar a razoável suspeita à autoridade dotada de competência legal para receber a informação.

§ 1º Para fins do disposto no caput, designa-se a Divisão de Repressão a Crimes Cibernéticos da Polícia Federal como o ponto de contato do Estado Brasileiro.

§ 2º As obrigações estabelecidas nesse artigo somente se aplicam a provedores de aplicações que possuam mais de 100.000 (cem mil) assinantes ou usuários."

Art. 3º Esta lei entra em vigor seis meses após a data da sua publicação.

Sala da Comissão, em 1 de agosto de 2022.

Deputado Capitão Alberto Neto