PROJETO DE LEI Nº , 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.

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 obrigação de monitoramento de atividades terroristas e crimes hediondos a provedores de aplicações de Internet e dá outras providências.

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 aplicações deverão monitorar ativamente publicações de seus usuários que impliquem atos preparatórios ou ameaças de crimes hediondos ou de terrorismo, nos termos da Lei nº 13.260/2016.
> § 1º As publicações mencionadas no *caput* deverão ser repassadas às autoridades competentes, na forma do regulamento.
> § 2º As obrigações estabelecidas nesse artigo somente se aplicam a provedores de aplicações que possuam mais de 10.000 (dez mil) assinantes ou usuários.
> § 3º Na impossibilidade eventual e justificada de cumprimento do disposto no *caput*, os provedores de aplicações deverão permitir a instalação de softwares ou equipamentos pelas autoridades competentes que permitam o monitoramento para o mesmo fim."

Art. 3º A infiltração de agentes dos órgãos de inteligência e dos órgãos de segurança pública nas redes de comunicações telefônicas ou

telemáticas para o levantamento, processamento e análise de informações acerca de ataques terroristas e homicidas e outros delitos será precedida de autorização judicial devidamente circunstanciada e fundamentada.

Parágrafo único. A autorização para os órgãos de inteligência será emitida por autoridade judiciária militar.

Art. 4º Esta lei entra em vigor seis meses após a data da sua publicação.

JUSTIFICAÇÃO

Atentados terroristas publicizados na Internet, em fóruns online e em redes sociais estão se tornando cada vez mais comuns. Após ataques terroristas como os da Catedral de Campinas, que deixou 5 mortos, o da escola municipal do Realengo, no Rio de Janeiro, com 12 mortos, e, mais recentemente, o da escola de Suzano, que tirou a vida de 8 pessoas inocentes, não é mais possível ficarmos inertes. Isso sem falar no ataque terrorista na cidade de Christchurch, na Nova Zelândia, que deixou 50 mortos e foi transmitido em tempo real por meio de uma rede social.

As redes sociais e buscadores são muitas vezes utilizados como plataformas para se planejar os ataques, criar incentivos, reunir pessoas extremistas com a mesma visão de mundo, adquirir as ferramentas do crime, trocar ideias sobre a melhor forma de proceder e, mesmo, anunciar em alto e bom som a intenção criminosa.

No último episódio, os terroristas de Suzano frequentaram fóruns extremistas na Internet, tornaram públicas várias de suas intenções em páginas de redes sociais. Apesar de muitas mensagens terem sido trocadas na chamada *deep web*, ou Internet escondida, outras foram publicizadas em perfis dos autores em redes sociais e, certamente, foram realizadas buscas de

conteúdo e realizadas compras em outros sites e aplicações de acesso público na de Internet[1].

A regulação sobre a *deep web*, no entanto, seria mais problemática e complexa, devendo, portanto, ser objeto de uma legislação específica. Não é o caso dos provedores de aplicações que operam na Internet aberta e sobre os quais já recaem obrigações constante da Lei do Marco Civil da Internet, aprovado pela lei nº 12.965/2014.

Os próprios sites de redes sociais e buscadores, provedores de aplicações, reconhecem essa cota de responsabilidade. A criação do Fórum Global de Combate ao Terrorismo (*Global Internet Forum to Counter Terrorism)*, formado por Microsoft, Facebook, Youtube e Twitter, as redes sociais e empresas de tecnologia tem procurado cooperar mundialmente na identificação e prevenção de atividades terroristas.

O que pretendemos com o presente projeto é clamar para que os provedores de conteúdo na Internet passem a assumir uma parcela da responsabilidade em monitorar atividades suspeitas e potencialmente criminosas, especificamente aquelas mais gravosas, que envolvem crimes hediondos e atos de terrorismo, nos termos da Lei nº 13.260/2016.

Nesse sentido, propusemos que os provedores de aplicações realizem monitoramento ativo de publicações de seus usuários que impliquem atos preparatórios ou ameaças de realização de crimes hediondos ou de terrorismo, nos termos da Lei nº 13.260/2016. As informações obtidas deverão ser repassadas às autoridades competentes, na forma da regulamentação.

As obrigações de monitoramento recairiam, portanto, sobre os atos preparatórios e sobre as ameaças que tenham como objetivo o cometimento de crimes hediondos ou de terrorismo.

Atos preparatórios são aqueles que, embora como regra não puníveis, são imprescindíveis e visam facilitar a realização do crime, como adquirir as armas, ainda que legais, planejar o local e a hora do crime, entre outras ações semelhantes. A ameaça, embora configure crime por si só, será

---

[11] Vide em: https://oglobo.globo.com/brasil/frequentadores-de-foruns-extremistas-na-internet-comemoram-ataque-em-suzano-23522564 . Acesso em 18/03/2019.

objeto da obrigação de monitoramento apenas quando a ameaça seja referente a crime hediondo ou crime de terrorismo, este último nos termos da Lei n.º 13.260/2016.

Há repetidos casos em que ameaças e atos preparatórios de terrorismo anunciados e alardeados nas redes sociais são sucedidos por atentados reais. Não é mais possível que fiquemos passivos diante de dessa afronta anunciada à vida e aos direitos fundamentais.

Há, porém, provedores que, pelo reduzido número de usuários ou em razão do baixo orçamento, ou por não fazerem exploração econômica do serviço, não teriam condições técnico-financeiras de cumprir o disposto na presente proposta. Em razão disso, determinamos que as obrigações estabelecidas nesse artigo somente incidam sobre provedores de aplicações que possuam mais de 10.000 (dez mil) assinantes ou usuários.

Caso exsurja eventual e justificada impossibilidade no cumprimento das obrigações de monitoramento, os provedores de aplicações deverão permitir a instalação de softwares ou equipamentos pelas autoridades competentes que permitam o monitoramento para a mesma finalidade.

Entendemos que as redes sociais, os buscadores e outros provedores de aplicações de Internet devem exercer sua parcela de responsabilidade sobre discursos e atitudes incompatíveis com a lei e, no caso, específico, que tenham potencial de resultar em ataques terroristas, como os que vimos no Brasil nos últimos anos.

Por outro lado, a instrumentalização jurídica dos órgãos de inteligência e dos órgãos de segurança pública para que possam efetuar o monitoramento dessas potenciais ameaças se dará mediante autorização judicial. Todavia, no caso de as ameaças dizerem respeito à segurança do Estado, indo, portanto, além da competência dos órgãos de segurança pública e passando à esfera dos órgãos de inteligência, essa autorização caberá à autoridade judiciária militar.

Estando certos da relevância do presente projeto de lei, e convictos de sua conveniência e oportunidade, conclamamos o apoio dos nobres Pares para a sua aprovação.

Sala das Sessões, em de de 2019.

Deputado JOSÉ MEDEIROS