NOTA PÚBLICA

do IRIS sobre o Projeto de Lei nº 2.418/2019

iris

INSTITUTO
DE REFERÊNCIA
EM INTERNET
E SOCIEDADE

INSTITUTO
DE REFERÊNCIA
EM INTERNET
E SOCIEDADE

AUTORIA
Ana Bárbara Gomes Pereira
Gustavo Ramos Rodrigues

PROJETO GRÁFICO, CAPA, DIAGRAMAÇÃO E FINALIZAÇÃO
Felipe Duarte

NOTA SOBRE O PROJETO DE LEI Nº 2.418/2019

Ana Bárbara Gomes Pereira[1]
Gustavo Ramos Rodrigues[2]

Belo Horizonte, 29 de agosto de 2022

O Instituto de Referência em Internet e Sociedade (IRIS) é um centro de pesquisa independente e interdisciplinar dedicado a produzir e comunicar conhecimento científico sobre os temas de internet e sociedade, bem como a defender e fomentar políticas públicas que avancem os direitos humanos na área digital. Em conformidade a essa missão institucional e a seu posicionamento prévio sobre o tema[3], o IRIS vem a público manifestar-se acerca do Projeto de Lei nº 2.418/2019, de autoria do deputado José Medeiros (PODE/MT), que "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".

Em tramitação na Câmara dos Deputados, o texto original do PL nº 2.418/2019 adiciona um artigo 21-A à Lei 12.965/2014, o Marco Civil da Internet (MCI). Esse novo artigo compeliria todos os provedores de aplicação que possuam mais de 10.000 (dez mil) assinantes ou usuários (§2º) a "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" (Lei Antiterrorismo) . Tais publicações deverão ser "repassadas às autoridades competentes, na forma do regulamento" (§1º). Se o cumprimento desse dever for justificadamente impossível, os referidos provedores ficam obrigados a "permitir a instalação de softwares ou equipamentos pelas autoridades competentes que permitam o monitoramento para o mesmo fim" (§3º).

A proposta original previa (art. 3º), ainda, "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", mediante comando judicial militar. Em seu parecer na Comissão de Segurança Pública e Combate ao Crime Organizado (CSPCCO) da Câmara dos Deputados, o relator, deputado Delegado Pablo (UNIÃO/AM), propôs a supressão desse artigo, bem como o aumento do número mínimo de usuários ou assinantes da aplicação para 100.000 (cem mil).

O conteúdo do PL nº 2.418/2019 é atécnico e inconstitucional, pois viola os princípios da presunção de inocência, da reserva de jurisdição e da livre iniciativa, bem como os direitos fundamentais à privacidade, à liberdade de expressão e à proteção de dados pessoais. Ademais, infringe o princípio infralegal da inimputabilidade da rede, essencial à governança e ao uso da internet no Brasil, bem como viola o princípio da preservação da funcionalidade, segurança e estabilidade da rede, assegurado expressamente pelo próprio Marco Civil da Internet (art. 3º, V).

1 Coordenadora de Políticas Públicas do Instituto de Referência em Internet e Sociedade

2 Diretor do Instituto de Referência em Internet e Sociedade

3 GOMES, Ana Bárbara. RAMIRO, André. RODRIGUES, Gustavo. et al. **Decálogo de Recomendações sobre Direitos Digitais e Produção de Provas**. Instituto de Referência em Internet e Sociedade (IRIS); Instituto de Pesquisa em Direito e Tecnologia do Recife (IP.rec). 25 de agosto de 2021. Disponível em: https://irisbh.com.br/publicacoes/decalogo-de-recomendacoes-sobre-direitos-digitais-e-producao-de-provas/. Acesso em 29 de agosto de 2022.

Ao compelir provedores de aplicação à identificação dos conteúdos que impliquem atos preparatórios ou ameaças de crimes hediondos ou de terrorismo, o projeto os obriga efetivamente à análise ampla e massiva de todas as publicações de todos usuários. Inexiste mecanismo para determinar de antemão quais conteúdos se encaixam na categoria visada, especialmente considerando a enorme envergadura de seu escopo semântico. Destaca-se que a definição de terrorismo inclui elementos subjetivos de difícil apreciação, como a motivação da conduta.

Ao impor tal avaliação, generalizada e permanente, o projeto inverte a presunção de inocência e passa a tratar todos como suspeitos. Ainda, prejudica a privacidade e a liberdade de expressão, ao promover um cenário de vigilância policial exercida por atores privados que prestam serviços online. Nesse ambiente, a capacidade fática de manifestação dos usuários pode ser severamente restringida, pelo chamado efeito amedrontador ou inibitório ("*chilling effect*"), diante da ciência de que todo seu conteúdo está sendo permanentemente monitorado, sobretudo para a identificação de tipos penais definidos de modo tão amplo e impreciso quanto terrorismo.

Ao tornar os provedores de aplicação juízes sobre a existência de elementos suficientes para a caracterização de suspeita de atos preparatórios de quaisquer crimes hediondos ou de terrorismo, afronta-se o princípio da reserva de jurisdição: transferem-se competências exclusivas do juízo penal para o setor privado. Quanto ao princípio da inimputabilidade da rede, verifica-se que este é igualmente lesado pela proposta, pois o combate a ilícitos deixa de atingir somente os responsáveis finais e passa a incidir sobre os meios de acesso e transporte. Assim, localiza-se na vigilância irrestrita imposta pelo projeto a delegação, a intermediários privados de internet, tanto do dever-poder de polícia dos agentes de aplicação da lei e quanto da competência jurisdicional do poder público.

Ainda, as disposições contidas no §3º do novo artigo 21-A proposto para o Marco Civil da Internet representam graves riscos à segurança dos sistemas cibernéticos. A obrigação de monitoramento prévio generalizado é não apenas excessiva e indevida, como tecnicamente inviável pelas razões descritas, sujeitando os provedores a requerimentos para debilitar a segurança de seus sistemas, a fim de facilitar a "instalação de softwares e equipamentos pelas autoridades competentes". Essa obrigação de redução da segurança colocaria em risco a livre iniciativa para implementar e manter soluções técnicas adequadas aos melhores padrões de segurança em seus sistemas. Ademais, contraria o direito fundamental à proteção de dados pessoais, que exige dos agentes de tratamento a adoção de medidas técnicas e organizacionais para evitar incidentes de segurança.

A prática de exploração estatal de vulnerabilidades de segurança cibernética é conhecida como hacking governamental e não encontra previsão legal expressa no ordenamento brasileiro, sendo o recurso a ela contrário à submissão do processo penal à legalidade estrita, que deve regê-lo. Ainda, a legislação processual penal vigente não oferece parâmetros expressos de proporcionalidade, necessidade, supervisão pública ou salvaguardas efetivas quando dessa incursão sobre os direitos de usuários e provedores. Esse dispositivo ocasionaria, portanto, um cenário generalizado de insegurança jurídica para usuários e provedores, mediante uma norma propensa a abusos (com efeitos danosos imediatos) e à contestação judicial (com impactos negativos futuros ao sucesso da própria persecução penal).

Ademais, o texto proposto sugere modificar o Marco Civil da Internet sem que haja amplo debate e engajamento de todos os setores envolvidos. Essa norma representa um exemplo importante de construção multissetorial e democrática para regulação jurídica do ambiente digital no Brasil, mediante um processo extenso, diverso e participativo, envolvendo sociedade civil, comunidade científica e tecnológica, setor privado e poder público. A lei resultante, fundamentada em direitos civis e com abordagem protetiva aos usuários, é referência mundial no contexto de normatização do uso da internet. Seria, portanto, equivocado modificá-la de forma tão substancial sem o devido diálogo com a

comunidade, colocando em risco direitos e liberdades individuais e coletivos tão caros.

Isto posto, recomenda-se **o arquivamento do PL nº 2.418/2019**, considerando os riscos gravíssimos que a proposta carrega para a proteção de direitos num ambiente digital seguro e democrático.

INSTITUTO
DE REFERÊNCIA
EM INTERNET
E SOCIEDADE