

Ibccrim questiona quebra de sigilo telemático coletiva

No ordenamento jurídico atual, não há permissão para que as agências de segurança tenham acesso a dados pessoais de um sem-número de indivíduos. Esse tipo de prática viola o direito fundamental à proteção de dados e representa grave risco de instauração de um cenário de vigilância permanente.

SCO/STF



Relatora da matéria é a presidente do Supremo, ministra Rosa Weber
SCO/STF

Essa é uma das conclusões de parecer do Instituto Brasileiro de Ciências Criminais (Ibccrim), que atua como *amicus curiae* no Recurso Extraordinário 1.301.250. No caso, o Supremo Tribunal Federal discute a viabilidade de quebra de sigilo de históricos de pesquisa na internet de um número não determinado de pessoas em investigações policiais.

A relatora da matéria é a ministra Rosa Weber. O STF reconheceu a repercussão geral do caso (Tema 1.148) em 2021. Ainda não foi definida data para o julgamento, que irá acontecer no Plenário físico da Corte.

No parecer, o Ibccrim sustenta que, além de não existir previsão legal para esse tipo de quebra de sigilo de um grupo indeterminado de pessoas, a medida representa um risco altíssimo a direitos coletivos difusos, como o livre desenvolvimento da personalidade e a liberdade de expressão.

“O cenário é agravado pela ausência de previsão legal para tanto, sendo possibilitado apenas por uma leitura analógica do Marco Civil da Internet, cujos limites teriam de ser definidos por decisão judicial”, diz a entidade.

O instituto também alega que não é possível a aplicação análoga de outras legislações no caso, não apenas por ferir princípios de Direito Penal, mas também porque se trata de situação nova, oriunda de novas tecnologias de alcance jamais imaginado por qualquer outra técnica de investigação.

Caso concreto

O recurso foi interposto pelo Google contra decisão do Superior Tribunal de Justiça que restabeleceu sentença que determinou a quebra de sigilo de um grupo de pessoas que fizeram pesquisas relacionadas



à vereadora Marielle Franco, nos quatro dias anteriores ao atentado que provocou a sua morte e a do motorista Anderson Gomes em 14 de março de 2018, no Rio de Janeiro.

A decisão questionada ordenou que a empresa identifique os IPs e aparelhos que tenham acessado o Google e pesquisado os seguintes termos: "Marielle Franco"; "vereadora Marielle"; "agenda vereadora Marielle"; "Casa das Pretas"; "Rua dos Inválidos, 122" ou "Rua dos Inválidos".

O STJ considerou que a decisão estava devidamente fundamentada e tem como objetivo permitir que os agentes de segurança obtenham dados de aparelhos utilizados por pessoas que tenham alguma relação com o crime.

O Google, por sua vez, sustenta que uma quebra de sigilo em espectro amplo é inconstitucional por violar o direito à privacidade de pessoas que não têm relação com o crime investigado. A empresa argumenta que esses indivíduos estão resguardados tanto pela cláusula geral de proteção da intimidade (artigo 5º, inciso X da Constituição Federal) quanto pela norma específica de sigilo de dados (artigo 5º, XII).

Ao se manifestar pelo reconhecimento da repercussão, Rosa Weber afirmou que é preciso compatibilizar as quebras de sigilo de dados com requisitos constitucionais mínimos.

Clique [aqui](#) para ler o parecer do Ibccrim

RE 1.301.250

Date Created

22/05/2023