

Opinião: Imprestabilidade da Lei 9.296/96 para quebra de dados

16/11/2021

O artigo 4º, inciso III, e parágrafo 1º da Lei Geral de Proteção de Dados define que o tratamento de dados em investigações policiais será definido por lei específica, que até a presente data ainda não foi criada. Ocorre que juízos criminais já se deparam com buscas e apreensões de celulares e computadores com grande quantidade de dados e de tipos variados, e a quebra do sigilo se faz necessária para apuração de fatos supostamente criminosos. Assim, com essa justificativa, vem se adotando a Lei 9.296/96 para basear decisões de quebra de sigilo de dados das pessoas envolvidas no inquérito, nesses bens de comunicação apreendidos.



Não é preciso grande esforço para perceber que as comunicações

(telefônicas e telemáticas) e a ciência de dados são duas coisas diferentes, e que a inteligência da Lei 9.296/96 se presta pouco, ou nada, ao tratamento de dados pessoais, pelo fato de também não ser contemporânea à atual cultura de proteção de dados, que se impõe no Brasil e no mundo, com o avanço constante e uso diário de internet e redes sociais.

Portanto, a Lei 9.296/96 é incompatível com a matéria de ciência de dados e não tem a menor função com tratamento de dados pessoais. Nesse sentido, o Superior Tribunal de Justiça já decidiu em caso isolado da seguinte maneira:

"Ademais, cumpre ressaltar ainda que à quebra de sigilo de dados telefônicos não se aplica a Lei 9.296/96, que regulamenta o procedimento de interceptação telefônica, sendo institutos distintos e, portanto, sendo lhes conferido tratamento diferenciado, razão pela qual não se exige que a autoridade demonstre a impossibilidade de obtenção da prova por outros meios, mas apenas que a decisão seja devidamente motivada, o que se verificou, in casu." [HC 690369, Ministro OLINDO MENEZES (DESEMBARGADOR CONVOCADO DO TRF 1ª REGIÃO) Decisão 06/10/2021]

Porém, a realidade de decisões de quebra de dados estarem fundamentadas nessa lei é uma evolução que surgiu com a necessidade de autorização judicial para análise de dados de telefones apreendidos em inquérito, pois não é novidade que autoridades policiais faziam, ou fazem, buscas em aparelhos eletrônicos sem nenhuma permissão judicial, atingindo a garantia de privacidade no sigilo de informações pessoais, consagrado no artigo 5º, inciso XII, da Constituição Federal, que acarretava, e acarreta, na anulação das provas colhidas e produzidas.

Conforme o julgado:

"Habeas corpus. 2. Acesso a aparelho celular por policiais sem autorização judicial. Verificação de conversas em aplicativo WhatsApp. Sigilo das comunicações e da proteção de dados. Direito fundamental à intimidade e à vida privada. Superação da jurisprudência firmada no HC 91.867/PA. Relevante modificação das circunstâncias fáticas e jurídicas. Mutação constitucional. Necessidade de autorização judicial. 3. Violação ao domicílio do réu após apreensão ilegal do celular. 4. Alegação de fornecimento voluntário do acesso ao aparelho telefônico. 5. Necessidade de se estabelecer garantias para a efetivação do direito à não autoincriminação. 6. Ordem concedida para declarar a ilicitude das provas ilícitas e de todas dela derivadas." (HC 168052. STF. Segunda Turma Relator(a): Min. GILMAR MENDES Julgamento: 20/10/2020 Publicação: 02/12/2020)



Nesse mesmo sentido, o Superior Tribunal de Justiça, em:

"São nulas as provas obtidas por meio da extração de dados e de conversas privadas registradas em correio eletrônico e redes sociais (v.g. Whatsapp e Facebook) sem a prévia autorização judicial." (Tese 19 da edição nº 69: Nulidades do Processo, STJ)

E também:

"é ilícita a prova colhida mediante acesso aos dados armazenados no aparelho celular, relativos e mensagens de texto, SMS, conversas por meio de aplicativos (Whatsapp), e obtida diretamente pela polícia, sem prévia autorização judicial." (Tese 7 da edição nº 111: Provas no Processo Penal 2)

Ocorre que é insuficiente a fundamentação de uma decisão com base em uma lei que não disciplina o caso concreto, restando não fundamentada a decisão, contrariando o artigo 93, inciso IX da Constituição Federal, e caindo na regência do artigo 564, inciso V, do Código de Processo Penal.

Ao se exigir autorização judicial, os tribunais asseveram a necessidade de se ponderar os princípios de sigilo de dados e interesse público de segurança. São nesses objetivos constitucionais que devem ser observados de forma concreta ao caso, quando decidir sobre a quebra de dados pessoais, e talvez, avaliando-se for caso de analogia, possa se usar a norma da Lei nº 9296/96.

Se difere as situações de quebra e tratamento de dados. Na quebra, quando há a autorização judicial, existe o paradigma de ponderação de princípios e o possível uso de analogia, e no tratamento, tem-se que cuidar das informações extraídas, para que não haja contaminação das provas, à luz do que se concebe na disciplina da Cadeia de Custódia da Prova.

Quanto ao tratamento reside a maior das incertezas, pois não há parâmetro legal que oriente o manejo desses dados pela polícia, levando em consideração a ciência e engenharia de dados. A decisão que autorizar a quebra de dados tem que, além de trazer o paradigma de ponderação dos princípios, tem que determinar os critérios e métodos para o tratamento dos dados, e diante de dúvidas ou falta de conhecimento, pode intimar a defesa e abrir vista ao Ministério Público para que indiquem os critérios e métodos para perícia, com base no artigo 155 do Código de Processo Penal.

A sistemática é complexa, mas é o que se apresenta enquanto não a lei que regule algo cotidiano e de mudança constante, resultando em maiores probabilidades de contaminação, sem a garantia de um rito legal. Ressaltando que estamos em uma cultura de proteção de dados, a partir do Marco Civil da Internet e da Lei Geral de Proteção de Dados.

Fonte: <https://conjur.jumps.com.br/2021-nov-16/opiniao-impresabilidade-lei-929696-quebra-tratamento-dados/>