

Moura: STF deve reconhecer a importância do domicílio virtual

21/11/2020

No último dia 10, os autores Lenio Luiz Streck e Marcelo Augusto Rodrigues de Lemos publicaram o texto "Os dados do smartphone estão ou não protegidos pela Constituição?" nesta **ConJur** [1].



A análise feita pelos autores tem por base a questão

discutida no ARE 1.042.075, em trâmite no STF, que se resume a saber se "*é necessária autorização judicial para acesso aos dados inseridos em smartphones (contatos, agenda telefônica etc.)? Tais dados estão protegidos pelas garantias constitucionais presentes no art. 5.º, incs. X e XII, da Constituição?*" [2] e traz os votos até então proferidos pelo ministro Toffoli que aduz ser a reserva de jurisdição apenas para a comunicação de dados, e não dos dados em si e do ministro Gilmar, que abriu divergência pela proteção, tendo o ministro Fachin acompanhado a contraposição.

A questão não é de hoje, sendo que há decisão do STJ proferida no ano de 2018 pela proteção constitucional dos dados e da reserva de jurisdição, como se observa no HC 422299/SP, relatado pelo ministro Felix Fischer, cuja ementa traz o seguinte trecho: "*A jurisprudência deste Tribunal Superior firmou-se no sentido de ser ilícita a prova oriunda do acesso aos dados armazenados no aparelho celular, relativos a mensagens de texto, SMS, conversas por meio de aplicativos (WhatsApp), obtidos diretamente pela polícia no momento da prisão em flagrante, sem prévia autorização judicial. III – In casu, os policiais tiveram acesso aos dados do aplicativo WhatsApp contidos no aparelho celular do paciente no momento da prisão em flagrante, sem autorização judicial. Todavia, ainda que a referida prova seja desconsiderada, porquanto nula, subsistem elementos autônomos suficientes para manter a condenação pelo crime de tráfico de drogas*" [3]. O mesmo argumento é repetido em outras decisões mais recentes, inclusive do ano de 2020, como no AgRg no HC 611762/SC e no AgRg no HC 580795/SP.

Portanto, não se trata apenas de uma discussão nova, rasa ou meramente formal, mas há de se discutir o surgimento de um novo bem jurídico a ser protegido pelo Direito, qual seja, o domicílio virtual.

Decisão da Suprema Corte dos EUA (*CARPENTER v. UNITED STATES, CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE SIXTH CIRCUIT*, No. 16-402. *Argued November 29, 2017—Decided June 22, 2018*) equiparou o *smartphone* a uma tornozeleira eletrônica, para decidir que a polícia não poderia ter acesso ou obter dados de localização do celular sem supervisão judicial, ou seja, a invasão do domicílio virtual deve ser justificada e controlada pelo Poder Judiciário, pois se trata de uma invasão gravíssima à privacidade e à intimidade do cidadão [4].

No início deste ano tivemos um caso semelhante, com a criação, pelo governo de São Paulo, do Sistema de Monitoramento Inteligente (Simi) para identificar os locais onde há mais concentração de pessoas por meio do rastreamento e georreferenciamento dos aparelhos celulares dos paulistas, cuja inconstitucionalidade é flagrante na forma e no mérito, sob a batuta de que a pandemia causada pela Covid-19 justificaria tal ato.

A pandemia demonstrou claramente que o poder tende sempre a se expandir, por isso, necessita de controle diuturno e, para tanto, há que se invocar aqui o conceito de domicílio virtual, na esteira do constitucionalismo digital [5], tanto para os casos de acesso a *smartphones* pela polícia no momento da prisão em flagrante, sem autorização judicial, quanto para acesso aos dados de localização para outros objetivos, já que se está diante da "casa eletrônica" do cidadão, cujo conteúdo é inviolável.

Na Carta Magna, um dos bens jurídicos tutelados é a inviolabilidade do domicílio, previsto no artigo 5º, XI, sancionado pelo Direito Penal com o crime de violação de domicílio previsto no artigo 150 do Código Penal.

E qual a relação existente entre a proteção constitucional dos *smartphones* e a violação de domicílio? A resposta é: a necessidade de proteção da inviolabilidade do seu domicílio virtual ou informático, assim como a casa.

Na era da tecnologia, da internet das coisas, bem como do uso diuturno de diversos dispositivos informáticos, os dados que estão inseridos nesses aparelhos são mais íntimos e privados do que a própria casa.

Ora, a privacidade e a intimidade no século XXI estão "guardadas" em computadores pessoais, tablets, *smartwatch*, *smartphones* e outros objetos, que armazenam dados mais privados do que aqueles que estão em sua própria casa, demandando uma ampliação do conceito de casa nos moldes anteriores.

Nesses aparelhos, é possível visualizar dados da sua vida, fotos, preferências, lugares visitados, sítios pesquisados, trabalhos realizados, documentos profissionais, conversas personalíssimas e de trabalho, enfim, toda sua vida privada em seu âmbito, além da vida profissional. Tudo isso está materializado nestes aparelhos, o que atrai o conceito de domicílio virtual ou informático e, por conseguinte, a sua necessária proteção na esteira do bem constitucionalmente tutelado.

Com efeito, o consentimento do ofendido é elemento primordial para se permitir o acesso a esses dados, assim como no crime de violação de domicílio. Tanto é que há semelhança de redação entre o crime de invasão de dispositivo informático, que utiliza a expressão "*sem autorização expressa ou tácita do titular do dispositivo*", e o crime de violação de domicílio, que usa a expressão "*contra a vontade expressa ou tácita de quem de direito*".

O consentimento do ofendido é elemento normativo do tipo, ou seja, se presente no caso concreto, exclui a tipicidade do fato. Todavia, há que se ter cuidado dobrado em casos de prisão em flagrante, uma vez que o acusado sob custódia da autoridade policial pode ser coagido a prestar tal consentimento, para que acessem seus dados inseridos no aparelho móvel, o que o torna inválido, por óbvio.

Outra questão importante é a falha de redação do artigo 154-A do Código Penal que, ao não prever a modalidade "permanecer", deixa lacuna legislativa quando há consentimento anterior para o acesso aos dados do dispositivo informático, porém, sendo ele cessado em momento posterior. Como exemplo de tais condutas cite-se os casos de consentimento parcial pelo acusado para acesso a apenas determinados dados do seu aparelho, ou na ocasião em que, após orientação do seu advogado, revoga o consentimento antes que tenha seu aparelho totalmente vasculhado.

Em ambos os casos, o crime inexistente, todavia, não se retira a possibilidade de discussão da ilicitude da prova por outros argumentos, como a violação da cadeia de custódia, a qual é de suma importância nos crimes informáticos ou nas perícias feitas em aparelhos eletrônicos, em virtude da volatilidade das informações neles armazenadas e da preservação da sua integralidade.

Vale ressaltar que o policial que invade dispositivo informático do acusado sem autorização judicial só comete o crime do artigo 154-A do CP se presentes todos os elementos do tipo, com destaque para o denominado dolo específico para a doutrina tradicional ("*Com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita*"), ressaltando, uma vez mais, que o consentimento do investigado para permitir o acesso deve ser válido, ou seja, ele deve estar em plena capacidade de consentir, o ato consentido deve ser igual ao ato praticado (sem excessos) e o bem jurídico ser disponível, sob pena de nulidade da prova obtida.

Como se não bastasse, o controle judicial da prova é fundamental, já que diante das diversas informações contidas nos telefones móveis, as quais inclusive podem afetar a terceiros alheios ao fato, o Poder Judiciário deve fazer uso apenas daquelas provas diretamente relacionadas ao ilícito penal praticado.

Logo, se a autoridade policial reconhecer o *smartphone* como um elemento potencial para a produção da prova pericial, deve ser responsável por sua preservação, ou seja, deve ser feita a apreensão dentro dos limites legais, solicitando autorização judicial para acesso aos dados, devendo ser circunstanciados, em caso de deferimento da devassa.

Do contrário, a prova é ilícita e contamina todo o devido processo legal, configurando violação ao artigo 5º, X, XI, XII, da Constituição Federal, com destaque para o inciso XII, que garante a

inviolabilidade dos dados.

Todavia, toda regra tem exceções e não há direito absoluto, o que não é diferente com o domicílio virtual ou eletrônico. Mais uma vez, é paradigmático o caso *Carpenter v. United States* supracitado, pois traz exceções à regra ao aduzir "*que os órgãos de segurança não precisam obter um mandado judicial em casos de urgência ou de emergência. Exemplos disso são casos de sequestro de criança, tiroteios, ameaças de bombas, perseguição de um suspeito de crime em fuga, proteção de uma pessoa sob ameaça iminente de sofrer danos ou de impedir a destruição iminente de provas*" [6].

Conclui-se que o domicílio virtual ou eletrônico é um novo bem jurídico decorrente do constitucionalismo digital e, assim como a casa, é inviolável, em virtude da proteção da intimidade, da privacidade e da inviolabilidade dos dados, o que atrai a necessidade de autorização judicial para acesso, sob pena de nulidade da prova obtida por meio do acesso desautorizado, exceto em casos de necessária autotutela devidamente justificados.

Desta feita, espera-se que o Supremo Tribunal Federal reconheça a importância de proteção deste bem jurídico no julgamento do ARE 1.042.075, protegendo os dados dos cidadãos brasileiros, na esteira dos dispositivos constitucionais já apontados, além do respeito ao devido processo legal e outras legislações complementares como o Marco Civil da Internet e a LGPD.

Como diria Friedrich Nietzsche: "*Em homens duros a intimidade é questão de pudor — e algo de precioso*".

[1] Disponível em <https://www.conjur.com.br/2020-nov-10/streck-lemos-dados-smartphone-protegidos-constituicao>. Acesso em 17/11/2020.

[2] Disponível em <https://www.conjur.com.br/2020-nov-10/streck-lemos-dados-smartphone-protegidos-constituicao>. Acesso em 17/11/2020.

[3] Disponível em WWW.stj.jus.br. Acesso em 17/11/2020.

[4] Ver https://cdn-conjur.s3.amazonaws.com/uploads/2020/11/16-402_h315.pdf. Acesso em 17/11/2020.

[5] "(..) o Constitucionalismo Digital evoluiu de uma mera corrente aglutinadora de experiências políticas e passou a compor verdadeiras prescrições normativas para a proteção de garantias individuais no ciberespaço. Estudos como os de Eduardo Celeste⁸, Claudia Padovani e Mauro Santaniello⁹ e Meryem Marzouki¹⁰ atribuíram ao Constitucionalismo Digital a marca de uma verdadeira "ideologia constitucional", a qual se estrutura em um quadro normativo de proteção dos direitos fundamentais e de reequilíbrio de poderes na governança da internet". Disponível em <https://www.conjur.com.br/2020-mai-09/observatorio-constitucional-direitos-fundamentais-servem-leis-gerais->



internet#:~:text=Constitucionalismo%20digital%20e%20direitos%3A%20para,as%20leis%20gerais%
. Acesso em 17/11/2020.

[6] Ver <https://www.conjur.com.br/2018-jun-25/suprema-corte-eua-compara-smartphone-tornozeleira-eletronica>. Acesso em 18/11/2020.

Fonte: <https://conjur.jumps.com.br/2020-nov-21/moura-stf-reconhecer-importancia-domicilio-virtual/>