

Um celular na cena do crime: o STF e a proteção dos dados estáticos

20/09/2024

Tramita no Supremo Tribunal Federal o ARE-Agravo em Recurso Extraordinário nº 1.042.075/RJ,¹ que debate se o acesso policial aos dados contidos em aparelho celular encontrado na cena do crime estaria ou não gravado pela reserva de jurisdição. O debate foi suspenso em 13 de setembro de 2024, com o pedido de vista do ministro Cristiano Zanin.

Até o momento, votaram os ministros Dias Toffoli, Gilmar Mendes, Edson Fachin e Flávio Dino, todos contrários ao acesso policial aos dados do celular sem decisão judicial prévia. O caso teve repercussão geral reconhecida (Tema 977), o que significa que a decisão servirá de orientação para as instâncias ordinárias em situações semelhantes.

O processo envolve um réu denunciado por roubo no Rio de Janeiro. Na fuga, o sujeito teria deixado cair seu celular na cena do crime, aparelho que foi recolhido pela vítima e entregue à polícia, que acessou, sem autorização judicial, a lista de contatos e o histórico de ligações. Com base nestas informações, a polícia identificou o suspeito, que foi preso e condenado em primeiro grau de jurisdição.



No entanto, em sede de apelação, o TJ-RJ reformou a sentença, absolvendo o réu. O tribunal fluminense entendeu que houve violação da proteção constitucional ao sigilo de dados, uma vez que a polícia não estaria autorizada a acessar as informações gravadas no aparelho celular sem autorização judicial.

O então procurador-geral da República, Augusto Aras, se manifestou no caso, sustentando que a autoridade policial poderia acessar livremente os registros telefônicos, a agenda de contatos e outros dados gravados sem autorização judicial e sem que a medida representasse violação ao sigilo das comunicações, ao direito à intimidade ou à privacidade do indivíduo.

Avanço da tecnologia muda entendimento

Após um voto inicial concordando com a tese da Procuradoria-Geral da República, proferido pelo ministro relator do processo Dias Toffoli, o ministro Gilmar Mendes inaugurou a divergência, ressaltando que o avanço da tecnologia impõe a necessidade de revisão da jurisprudência do STF sobre dados armazenados, propondo a tese:

“O acesso a registro telefônico, agenda de contatos e demais dados contidos em aparelhos celulares apreendidos no local do crime atribuído ao acusado depende de prévia decisão judicial que justifique, com base em elementos concretos, a necessidade e a adequação da medida e delimite a sua abrangência à luz dos direitos fundamentais à intimidade, à privacidade e ao sigilo das comunicações e dados dos indivíduos (CF, artigo 5º, X e XX).”

Em seu voto, Dias Toffoli modificou seu voto inicial aderindo à divergência inaugurada por Gilmar Mendes e concluindo pela inadmissibilidade de se permitir à autoridade policial a devassa do conteúdo de aparelhos celulares apreendidos na cena do crime independentemente de prévia autorização judicial.

Argumentou pela superação da distinção entre proteção conferida a dados em trânsito e não proteção dos dados armazenados, propondo como tese: “O acesso a registro telefônico, agenda de contatos e demais dados contidos em aparelhos celulares apreendidos no local do crime atribuído ao acusado depende de prévia decisão judicial que justifique, com base em elementos concretos, a necessidade e a adequação da medida e delimite sua abrangência à luz dos direitos fundamentais à intimidade, à privacidade, ao sigilo das comunicações e à proteção dos dados pessoais, inclusive nos meios digitais (CF, artigo 5º, incisos X, XII e LXXIX)”.

Por fim, o último voto declarado, do ministro Flávio Dino, ressaltou que, embora o STF tenha inicialmente conferido reserva de jurisdição apenas ao trânsito de dados e não aos dados registrais, estar-se-ia diante de verdadeira “mutação constitucional”, que leva a conclusão diversa, propondo a seguinte tese:

“Visando proteger os direitos fundamentais à privacidade e intimidade, o acesso a qualquer conteúdo de aparelho celular apreendido depende de decisão judicial fundamentada. Contudo, a apreensão do aparelho celular, nos termos do artigo 6º do CPP, ou em flagrante delito, bem como a determinação de preservação dos dados e metadados de suspeitos ou investigados, não está sujeita à reserva de jurisdição.”

Regras e princípios

Embora a Constituição de 1988 tenha, em seu artigo 5º, XII, protegido apenas a comunicação dos dados pessoais, a Emenda Constitucional 115, de 2022, ampliou este leque ao inserir no artigo 5º o inciso LXXIX, que estabelece que “é assegurado, nos termos da lei, o direito à

Spacca



opinião

proteção dos dados pessoais, inclusive nos meios digitais”, de modo que a distinção, para fins de reserva de jurisdição, entre proteção de dados estáticos e dados em trânsito perdeu consistência, como ressaltado pelos Ministros que já declararam seus votos no julgamento do tema.

Por outro lado, não se questiona a correção da regra estabelecida no artigo 6º, inciso III, do CPP, segundo a qual logo que tiver conhecimento da prática do crime, a autoridade policial deverá “colher todas as provas que servirem para o esclarecimento do fato e suas circunstâncias”, de modo que a apreensão dos vestígios deixados na cena do crime não encontra qualquer embaraço desde que atenta à legalidade e aos procedimentos da cadeia de custódia, estabelecida nos artigos 158-A e 158-B, do CPP, com o fim de registrar a correção metodológica e científica da coleta dos vestígios deixados em locais ou vítimas de crimes.

Ora, sistemas jurídicos são sistemas complexos gravados pela sobreposição de comandos aparentemente divergentes ou sobrepostos. Diz-se “aparentemente” porque a ciência do direito conta com todo um arsenal de instrumentais técnicos predispostos a resolver problemas de conflitos normativos, e tanto o direito penal material quanto o direito processual penal conhecem suas próprias regras de resolução de situações divergentes.

Partindo do pressuposto que princípios são mandados de otimização e que regras são comandos de execução do sistema jurídico, o que parece estar em debate no STF é a busca pela otimização do sistema, mantendo a boa estrutura de execução da investigação criminal, sem prejuízo do respeito aos direitos fundamentais. Neste passo, não parece haver contradição a ser sanada, mas apenas mais uma pauta de adequação do CPP ao modelo democrático da Constituição.

Processo penal é garantia na investigação

Como ressaltam Aury Lopes Júnior e Alexandre Morais da Rosa, “ao mesmo tempo em que um culpado não pode deixar de ser responsabilizado, um inocente não pode ser o bode expiatório. Para isso o processo penal é o instrumento de garantia de ambos”[1], de modo que o trabalho da dogmática processual penal e da jurisprudência é exatamente conciliar interesses que somente na aparência são divergentes.

A norma estabelecida no artigo 5º, LXXIX, da Constituição parece representar verdadeiro comando constitucional de execução do sistema, conectado em maior nível de abstração ao mandado de otimização da proteção à privacidade, previsto no artigo 5, X, da Carta, do qual decorre como uma função linear, ou seja, onde a otimização de um pressupõe a otimização do outro como causa e efeito.

Quanto à norma do artigo 6º, inciso III, do CPP, não resta dúvida que represente uma regra de execução do sistema. Comandos de execução não se encontram em função linear com princípios, mas em função escalonada, de modo que a otimização de seus comandos necessita ser obtida “mediante recurso a uma função auxiliar externa” que opere para “estabelecer, dentro dos parâmetros de mínimo e máximo, aquilo que possa servir de critério para o preenchimento da função básica, de modo a otimizar essa função”[2].

Inviolabilidade domiciliar

Isso significa dizer que a otimização da investigação criminal precisa ser valorada a partir de um princípio externo conciliador, o que já foi realizado por exemplo no Tema 280, quando o STF considerou que a entrada em domicílio em situações de flagrante delito de crimes permanentes pode ser adequada com a garantia da inviolabilidade domiciliar no período noturno, se o crime em execução não representar violência ou grave ameaça atual ou iminente à pessoa.

O comando de execução do artigo 6, III, do CPP não importa — nem poderia importar sem tornar o próprio dispositivo incompatível com a ordem jurídica — qualquer obstáculo à otimização da proteção de dados individuais estáticos gravados em aparelhos de telefonia celular encontrados em cenas de crime; por outro lado, a proteção constitucional desses dados não representa atraso considerável a obstaculizar a agilidade das investigações policiais que, com uma simples alteração legislativa, poderia contar com gatilho semelhante ao do §4º, do artigo 13-B, do CPP, em caso de crimes graves.

De modo que o debate presente no tema, embora marcado por preconceitos, e interesses corporativos, parece apontar para solução adequada de compatibilização do sistema: os vestígios encontrados na cena do crime podem e devem ser colhidos pela autoridade policial, segundo o comando de execução do artigo 6, III, do CPP e no caso de aparelho de telefonia celular, após autorização do juiz competente, acessado pela polícia científica para verificação dos dados gravados, respeitados os procedimentos metodológicos adequados e a documentação da cadeia de custódia.

Dados abertos e dados fechados

Uma questão ainda não pautada no debate do tema é a da relevância do bloqueio ou não do aparelho celular por algum mecanismo de segurança inserido por seu usuário. Nenhum dos votos dos ministros que se manifestaram até agora opinou no sentido de que somente o aparelho de telefonia celular bloqueado estaria protegido pela reserva de jurisdição.

Debate similar surgiu há aproximadamente 12 anos no Brasil após a promulgação da Lei 12.737, de 30 de novembro de 2012, alcunhada “Lei Carolina Dieckmann”, que inseriu no Código Penal o crime do artigo 154-A, denominado “invasão de dispositivo informático”. Em sua redação originária, a lei exigia que o meio de execução do crime se operasse “mediante violação indevida de mecanismo de segurança” (senha, reconhecimento facial, leitura de digital ou qualquer outro meio de fechamento dos dados).

Esse meio de execução, como elementar do tipo objetivo, foi abolido com a promulgação da Lei 14.155, de 27 de maio de 2021, que conferiu nova redação ao artigo 154-A, do Código Penal. A partir de então, o crime passou a ser tipificado pela conduta de “invadir dispositivo informático de uso alheio, conectado ou não à rede de computadores, com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do usuário do dispositivo ou de instalar vulnerabilidades para obter vantagem ilícita”, independentemente do fechamento dos dados por senha ou bloqueio similar.

Seja pela modificação inserida pela Lei 14.155/2021 no Código Penal; seja pela inexistência constitucional de qualquer exigência de que o proprietário dos dados bloqueie explicitamente seus dispositivos informáticos; seja pelo silêncio dos ministros do STF que se manifestaram no tema até o momento, a solução que está sendo construída parece seguir no sentido de se exigir a reserva de jurisdição para acesso aos dados registrais contidos no aparelho de telefonia celular apreendido em cenas de crime mesmo quando os respectivos aparelhos não estejam protegidos por qualquer sistema de bloqueio.

Analogia da caderneta

Se a solução se dirigir nesse sentido, poderá ser criticada pela analogia da caderneta. Imagine uma caderneta ou agenda encontrada perdida ou descartada na cena do crime e que contenha dados de contabilidade, contatos telefônicos, anotações de gastos e recebimentos e outras informações que constituam escrituras capazes de demonstrar, ainda que parcialmente ou circunstancialmente crimes em investigação.

A crítica naturalmente se orientaria pela observação de que nesta situação analógica não se faz qualquer exigência de autorização judicial para acesso aos dados ali escriturados. Sequer estariam amparados os dados pelo princípio de que o acusado não é obrigado a produzir ou colaborar com a produção de prova contra si mesmo, já que em se tratando de vestígio descartado ou perdido, a prova não poderia ser caracterizada como invasiva de sua privacidade.

Ocorre que a comparação mencionada é apenas aparentemente analógica, possuindo distinções consideráveis: tanto no caso da caderneta, quanto de outros vestígios encontrados na cena do crime (como materiais orgânicos ou biológicos) que podem ser livremente acessados — mediante coleta e perícia — com o fim de rastrear dados pessoais sensíveis — como é o caso do próprio DNA do agente —, sem necessidade de autorização judicial, no caso do celular apreendido nos parece que se trataria de prova invasiva.

Isso porque o aparelho celular é uma prótese corporal com a finalidade de concentrar e potencializar capacidades humanas (como a audição, a visão, a memória, a comunicação, etc.), que não se destacam funcionalmente dos seus proprietários. Enquanto até materiais orgânicos podem ser livremente descartados, porque fora do corpo perdem suas funções, o aparelho celular não perde essas funções quando separado do corpo humano, continuando atuante no campo virtual ou digital.

Direito fundamental à privacidade

Ainda mais importante que isso: o comando constitucional do artigo 5º, LXXIX, da Constituição (direito fundamental à proteção dos dados pessoais) é norma específica e de função linear em relação ao mandado de otimização presente no artigo 5º, X, da Constituição (direito fundamental à privacidade) e também em relação ao artigo 1º, III, da Constituição (direito fundamental à dignidade).

Ora, sabemos que o critério da especialidade tem por finalidade garantir a otimização da incidência da regra mais ajustada ao fato, o que significa dizer que “a aplicação do critério da especialidade é uma consequência da legalidade estrita, que tem por objetivo limitar a

incidência de normas generalizadoras; quanto mais particularizada é a descrição dos elementos do que se quer disciplinar, maior será a observância de sua legalidade”[3].

Desse modo, o comando constitucional de execução do sistema estabelecido no artigo 5º, LXXIX, da Constituição (direito fundamental à proteção dos dados pessoais), que se coloca numa relação de especialidade frente ao direito fundamental da dignidade da pessoa humana, de modo que já não estamos obrando no campo do mandado de otimização, mas de uma regra específica e de hierarquia constitucional que impõe uma resposta que poderá não ser a desejada pelos órgãos de persecução criminal, mas que parece ser a mais adequada para conciliar a investigação com a proteção da dignidade, erigida a zênite do sistema de garantias da Constituição.

[1] LOPES JR, Aury; ROSA, Alexandre Morais da. Depoimento especial é antiético e pode levar a erros judiciais. 23/01/2015. Disponível em: <https://www.conjur.com.br/2015-jan-23/limite-penal-depoimento-especial-antietico-levar-erros-judiciais/>

[2] TAVARES, Juarez. Crime: crença e realidade. 2. ed. Rio de Janeiro: Da Vinci: 2023, p. 144.

[3] TAVARES, Juarez. Op. cit., p. 148.

Fonte: <https://conjur.jumps.com.br/2024-set-20/um-celular-na-cena-do-crime-o-stf-e-a-protecao-dos-dados-estaticos/>