O Senhor Ministro **CRISTIANO ZANIN** (Vogal): Trata-se de recurso extraordinário com agravo interposto pelo Ministério Público do Estado do Rio de Janeiro (MPRJ) contra decisão que inadmitiu o recurso extraordinário com fundamento na aplicação da Súmula n. 279 do STF.

No recurso extraordinário, interposto com base no art. 102, III, *a*, da Constituição da República (CR), alega-se que o acórdão do Tribunal de Justiça do Rio de Janeiro (TJRJ), que absolveu o réu por reconhecer a ilicitude da prova obtida mediante acesso não autorizado ao conteúdo do seu celular, teria ofendido o art. 5º, XII e LVI, da CR (doc. 4, p. 80).

Transcrevo a ementa do acórdão impugnado:

> APELAÇÃO CRIMINAL – PENAL E PROCESSUAL PENAL – ROUBO DUPLAMENTE CIRCUNSTANCIADO PELO EMPREGO DE ARMA DE FOGO E PELO CONCURSO DE AGENTES (...) DURANTE A FUGA, O IMPLICADO DEIXOU CAIR UM APARELHO DE TELEFONIA CELULAR, O QUAL FOI ARRECADADO POR POLICIAIS CIVIS, QUE VERIFICARAM A EXISTÊNCIA DE FOTOGRAFIAS DO IMPLICADO NA MEMÓRIA DO APARELHO, O QUE NORTEOU A REALIZAÇÃO DE DILIGÊNCIAS QUE POSSIBILITARAM A IDENTIFICAÇÃO E PRISÃO DO RECORRENTE, NA MANHÃ DO DIA SEGUINTE AOS FATOS – IRRESIGNAÇÃO DEFENSIVA DIANTE DO DESENLACE CONDENATÓRIO, PLEITEANDO A MITIGAÇÃO DA SANÇÃO, A PARTIR DA FIXAÇÃO DA PENA BASE EM SEU PATAMAR MÍNIMO LEGAL, ALÉM DA APLICAÇÃO DA MENOR FRAÇÃO PREVISTA CORRESPONDENTE AO RECONHECIMENTO DA DÚPLICE CIRCUNSTANCIAÇÃO DO ROUBO – PROCEDÊNCIA DO RECURSO DEFENSIVO – **IDENTIFICAÇÃO DO AUTOR QUE SE DEU EXCLUSIVAMENTE A PARTIR DO ILÍCITO E DESAUTORIZADO MANUSEIO PELOS POLICIAIS CIVIS, DO APARELHO DE TELEFONIA CELULAR, SUPOSTAMENTE DE PROPRIEDADE DO IMPLICADO E QUE TERIA CAÍDO AO CHÃO DURANTE A FUGA DESTE,**

VINDO A SER ARRECADADO PELA VÍTIMA E ENTREGUE POR ESTA EM SEDE POLICIAL – DEPOIMENTO PRESTADO PELO POLICIAL CIVIL MAYKE QUE ESCLARECE QUE APÓS O DESAUTORIZADO MANEJO DAQUELE APARELHO E COM OS DADOS NELE COLHIDOS, FOI POSSÍVEL A REALIZAÇÃO DA POSTERIOR INVESTIGAÇÃO PARA SE DETERMINAR A IDENTIDADE DO IMPLICADO, BEM COMO OS ENDEREÇOS DO SEU DOMICÍLIO E DE SUA NAMORADA, PARA QUEM AQUELE TERIA EFETUADO A ÚLTIMA LIGAÇÃO CONSTANTE DA AGENDA DO APARELHO, O QUAL AINDA TEVE VIOLADO O HISTÓRICO DE CHAMADAS E O ARQUIVO DE ARMAZENAMENTO DE FOTOGRAFIAS – **FLAGRANTE E INDISFARÇÁVEL QUEBRA DA PROTEÇÃO CONSTITUCIONAL INCIDENTE SOBRE A INVIOLABILIDADE DO SIGILO DOS DADOS E DAS COMUNICAÇÕES TELEFÔNICAS ALI EXISTENTES, O QUE APENAS PODERIA SE DAR, POR EXCEÇÃO, MEDIANTE EXPRESSA AUTORIZAÇÃO JUDICIAL PARA TANTO**, MAS O QUE FOI IGNORADO E DESRESPEITADO PELOS AGENTES DA LEI, MUITO EMBORA NÃO ENCERRASSE MAIOR DIFICULDADE A OBSERVÂNCIA DA EXIGÊNCIA LEGAL, BASTANDO PARA TANTO QUE O POLICIAL CIVIL QUE RECEBEU O REFERIDO APARELHO TELEFÔNICO, DE IMEDIATO, ENCAMINHASSE ESTE AO DELEGADO DE POLÍCIA INFORMANDO A RELEVÂNCIA DO OBJETO, DE MODO A QUE TAL AUTORIDADE POLICIAL REPRESENTASSE JUNTO AO PLANTÃO JUDICIÁRIO DE MODO A OBTER A AUTORIZAÇÃO PARA O ACESSO E VERIFICAÇÃO DOS DADOS PRETENDIDOS – PANORAMA OBTIDO DE CONFIGURAÇÃO DA ILICITUDE, TANTO ORIGINÁRIA, COMO DERIVADA, QUANTO À PROVA COLHIDA NA DETERMINAÇÃO DE AUTORIA, SEGUNDO OS ESCUSOS MEIOS UTILIZADOS PARA TANTO, DE MOLDE A NULIFICAR TUDO O QUE DAÍ ADVINDO, O QUE, NO CASO EM COMENTO, ALCANÇA A INTEGRALIDADE DO CONTINGENTE PROBATÓRIO –

> MANUTENÇÃO DA CONDENAÇÃO DO RECORRENTE QUE EQUIVALERIA A SE COONESTAR COM A COMPROVADA OCORRÊNCIA DE VIOLAÇÃO A ESPECÍFICA GARANTIA CONSTITUCIONAL, ALÉM DE AGASALHAR COMO VÁLIDA A INFAME "LEI DE GÉRSON", SIMPLESMENTE UMA VERSÃO MAIS ATUALIZADA DE QUE "OS FINS JUSTIFICAM OS MEIOS", MAS O QUE PASSA AO LARGO DE SE COADUNAR COM OS PRINCÍPIOS ATINENTES A UM ESTADO DEMOCRÁTICO DE DIREITO, NÃO PODENDO SER CHANCELADO SOB QUALQUER PRETEXTO – INDIGÊNCIA PROBATÓRIA ASSIM INSTALADA E QUE TRAZ COMO ÚNICA SOLUÇÃO POSSÍVEL A ABSOLVIÇÃO DAQUELE, COM FULCRO NO ART. 386, INC. Nº VII DO C.P.P. – PROVIMENTO DO APELO DEFENSIVO (doc. 4, p. 34-37).

Segundo argumenta o recorrente, "a simples verificação de registros gravados no próprio aparelho não configura prejuízo ao direito de sigilo, eis que não se trata de violabilidade da comunicação telefônica, mas simples acesso a dados contidos em objeto apreendido na cena do crime, cuja apreensão e perícia é obrigatória pela autoridade policial" (doc. 5, p. 12).

A repercussão geral da matéria foi reconhecida em 23/11/2017, em acórdão assim ementado:

> CONSTITUCIONAL. PROCESSUAL PENAL. PERÍCIA REALIZADA PELA AUTORIDADE POLICIAL EM APARELHO CELULAR ENCONTRADO FORTUITAMENTE NO LOCAL DO CRIME. ACESSO À AGENDA TELEFÔNICA E AO REGISTRO DE CHAMADAS SEM AUTORIZAÇÃO JUDICIAL. ACÓRDÃO RECORRIDO EM QUE SE RECONHECEU A ILICITUDE DA PROVA (CF, ART. 5º, INCISO LVII) POR VIOLAÇÃO DO SIGILO DAS COMUNICAÇÕES (CF, ART. 5º, INCISOS XII). QUESTÃO

> EMINENTEMENTE CONSTITUCIONAL. MATÉRIA PASSÍVEL DE REPETIÇÃO EM INÚMEROS PROCESSOS, A REPERCUTIR NA ESFERA DO INTERESSE PÚBLICO. TEMA COM REPERCUSSÃO GERAL (doc. 10).

A então Procuradora-Geral da República manifestou-se no seguinte sentido:

> AGRAVO EM RECURSO EXTRAORDINÁRIO. PROCESSUAL PENAL. OFENSA AOS ARTS. 5º-XII E LVI DA CONSTITUIÇÃO. INQUÉRITO POLICIAL. PROVA OBTIDA POR MEIO DE ACESSO A REGISTROS E INFORMAÇÕES EM APARELHO CELULAR, SEM AUTORIZAÇÃO JUDICIAL. LICITUDE.
>
> I - Recurso Extraordinário leading case do Tema 977 da sistemática da repercussão geral: licitude da prova produzida durante o inquérito policial relativa ao acesso, sem autorização judicial, a registros e informações contidos em aparelho de telefone celular, relacionados à conduta delitiva e hábeis a identificar o agente do crime.
>
> II -A Constituição assegura, no art. 5º-XII, a proteção das comunicações telefônicas, cujo sigilo só pode ser quebrado, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal – tema regulado pela Lei 9.296/96.
>
> III - O objeto da Lei 9.296/96 não abrange a quebra do sigilo de dados telefônicos. Não se tratando de captação de comunicações telefônicas em andamento – em relação as quais o art. 5º- XII da Carta Magna exige prévia autorização judicial –, mas sim da obtenção de registros de ligações pretéritas, mensagens, acesso a fotos, mensagens e dados que possam ser armazenados no aparelho, é indiscutível a possibilidade que tem a autoridade policial, uma vez de posse do objeto, de investigar seu conteúdo.
>
> IV - O art. 6º do Código de Processo Penal dispõe que a

> autoridade policial tem o dever de proceder à coleta do material comprobatório da prática da infração penal, colhendo todas as provas que servirem para o esclarecimento do fato e suas circunstâncias. Desde que haja justa causa para a quebra do sigilo de dados telefônicos, não se considera violada a intimidade do acusado, porque, neste caso, o interesse público deve prevalecer sobre o direito fundamental de proteção à intimidade. Afinal, o sigilo de dados não tem natureza absoluta e as liberdades públicas não podem funcionar como mecanismo de salvaguarda de práticas ilícitas.
>
> V - Proposta de tese de repercussão geral: É lícita a prova produzida durante o inquérito policial relativa ao acesso, sem autorização judicial, a registros, fotos, vídeos e demais informações contidos em aparelho de telefone celular, relacionados à conduta delitiva.
>
> – Parecer pelo conhecimento do agravo e provimento do recurso extraordinário, para fixação da tese sugerida (doc. 54).

O Instituto Brasileiro de Ciências Criminais e o Ministério Público do Estado de Santa Catarina foram admitidos como *amici curiae* (doc. 140).

Inicialmente, o eminente Relator, Ministro Dias Toffoli, havia votado no sentido de dar provimento ao agravo e ao recurso extraordinário, para cassar o acórdão recorrido e determinar o prosseguimento do julgamento da apelação. Ademais, propôs a fixação da seguinte tese de repercussão geral:

> É lícita a prova obtida pela autoridade policial, sem autorização judicial, mediante acesso a registro telefônico ou agenda de contatos de celular apreendido ato contínuo no local do crime atribuído ao acusado, não configurando esse acesso ofensa ao sigilo das comunicações, à intimidade ou à privacidade do indivíduo (CF, art. 5º, incisos X e XII).

O eminente Ministro Gilmar Mendes, por sua vez, divergiu do Ministro Relator e votou no sentido de negar provimento ao recurso, propondo a seguinte 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, art. 5º, X).

Na sequência, o eminente Ministro Edson Fachin acompanhou a divergência.

Após, o eminente Relator, Ministro Dias Toffoli, reajustou o seu voto para também acompanhar o posicionamento inaugurado pelo Ministro Gilmar Mendes, em voto assim ementado:

> EMENTA Recurso extraordinário com agravo. Julgamento sob a égide da sistemática da repercussão geral (arts. 1.035 e 1.036 do CPC). Constitucional. Processual penal. Aparelho celular encontrado fortuitamente no local do crime pela vítima. Entrega do aparelho aos agentes policiais. Apreensão do aparelho pela autoridade policial. Dever de coleta de provas (CPP, art. 6º). Flagrante impróprio. Acesso à agenda telefônica, aos registros de chamadas e às fotografias arquivadas no aparelho sem prévia autorização judicial. Condenação em primeira instância. Acórdão recorrido. Reconhecimento de ilicitude da prova (CF, art. 5º, inciso LVII) por violação do sigilo das comunicações (CF, art. 5º, incisos XII). Necessidade de autorização judicial prévia. Multifuncionalidades dos aparelhos celulares. Proteção jurídica conferida pelas legislações mais

recentes aos dados relativos a conversas armazenadas e aos dados pessoais. Superveniência do MCI, da LGPD e da EC nº 115, de 2022. Direito à proteção dos dados pessoais nos meios digitais. Superação do entendimento firmado no HC nº 91.867/PA, Rel. Min. Gilmar Mendes. Ofensa à intimidade, à privacidade e ao direito à proteção dos dados pessoais, inclusive nos meios digitais. Prova ilícita. Exigência de celeridade de atuação dos órgãos de persecução penal. Prioridade de tramitação do pedido da autoridade de persecução penal no Poder Judiciário. Prioridade de apreciação de pedido pelo Poder Judiciário. Recurso não provido. 1. No caso dos autos, o aparelho celular foi encontrado fortuitamente pela vítima no local dos fatos, o qual foi entregue aos agentes policiais e, na sequência, apreendido pela autoridade policial (CPP, art. 6º, inciso II). A identificação do autor do delito decorreu do exame da agenda telefônica, dos registros de chamadas e de fotografias constantes do aparelho celular pelos agentes policiais sem autorização judicial prévia, permitindo a coleta de evidências que nortearam a realização de diligências que culminaram na prisão em flagrante (flagrante impróprio) e na posterior condenação do recorrido, em primeira instância, pelo crime de roubo. 2. O Tribunal de Justiça do Estado do Rio de Janeiro, reconhecendo a ilicitude da prova colhida determinante para a identificação da autoria delitiva e, por derivação, da integralidade do aparato probatório constante dos autos, deu provimento ao recurso defensivo para determinar a absolvição do réu com base no art. 386, inciso VII, do Código de Processo Penal. No recurso extraordinário, alega-se que não houve ofensa à inviolabilidade do sigilo de dados e das comunicações (CF/88, art. 5º, incisos X e XII), invocando-se precedentes da Suprema Corte que encamparam a tese de que a inviolabilidade do sigilo das comunicações se refere à comunicação de dados, isto é, aos dados em trânsito, e não aos dados estáticos ou armazenados em equipamentos eletrônicos. 3. No contexto atual, franquear o acesso ao aparelho celular de alguém implica, na prática, liberar, autorizar, conceder ou, ao

menos, desobstruir o acesso a um espectro enorme de dados pessoais (e não pessoais), o que torna possível uma investigação completa e, diga-se de passagem, muito eficiente acerca de suas preferências, de suas relações familiares e interpessoais, de seus afetos, de seus hábitos de vida, trabalho e consumo e, em última análise, de sua forma de pensar, agir e decidir. Isso sem falar, obviamente, das facilidades que o acesso proporciona para a intrusão indevida e para o futuro, a partir da instalação de softwares espiões. 4. Considerando a referida nova realidade, resultante da acelerada transformação digital das últimas duas décadas, e a maior percepção sobre os riscos sistêmicos e ocultos que as tecnologias atuais e suas potencialidades acarretam aos direitos fundamentais, após revisitar o entendimento formado a partir da análise do RE nº 418.416/SC, Rel. Min. Sepúlveda Pertence, julgado pelo Plenário em 2006, e, sobretudo, do HC nº 91.867/PA, Rel. Min. Gilmar Mendes, julgado pela Segunda Turma em 2012, verifica-se que a jurisprudência do Supremo Tribunal Federal acabou encampando, ao menos em parte, o texto seminal do Professor Tércio Sampaio Ferraz Júnior, para quem, o sigilo, no inciso XII do art. 5º, está referido à comunicação, no interesse da defesa da privacidade. À luz do citado texto, contudo, os dados estáticos, ou armazenados, também são passíveis de proteção jurídica e, embora não se revistam sempre e incondicionalmente de caráter sigiloso, podem alcançar tal qualidade em diferentes níveis, a depender das circunstâncias, quando, por exemplo, digam respeito à intimidade, à vida privada, à honra, encontrando guarida, portanto, no disposto no art. 5º, inciso X, do texto constitucional. 5. Ademais, a Emenda Constitucional nº 115, de 2022, ao introduzir no art. 5º da Constituição o inciso LXXIX, segundo o qual é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais, e as Leis nº 12.695/14 e nº 13.709/18, que instituíram no ordenamento jurídico brasileiro, respectivamente, o Marco Civil da Internet e a Lei Geral de Proteção de Dados, passaram a conferir proteção jurídica reforçada aos dados pessoais. Assim,

enquanto o primeiro diploma legal elevou a direito dos usuários de internet a inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial e o não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei (art. 7º, incisos III e VII), a segunda lei citada alçou os dados pessoais a uma categoria dotada de autonomia com relação aos direitos à privacidade e à intimidade, previstos no art. 5º, inciso X, da Constituição Federal, mas igualmente merecedora de proteção jurídica. Afinal, protegendo-se os dados, protege-se a informação neles contida, assegurando-se a privacidade e/ou a intimidade. 6. A factibilidade de se acessar, por meio de aparelhos celulares, bem mais que metadados relativos à comunicação telefônica havida a partir de terminal específico introduz na discussão travada nos autos, inevitavelmente, a questão da inviolabilidade da intimidade, da vida privada, da honra e da imagem (CF/88, art. 5º, inciso X), agora reforçada pelo direito à proteção dos dados pessoais, inclusive nos meios digitais (CF/88, art. 5º, inciso LXXIX), introduzido pela Emenda Constitucional nº 115, de 2022. São eles fatos empíricos e normativos, supervenientes ao julgamento do HC nº 91.867, que justificam e conferem proteção jurídica especial aos dados armazenados, o que enseja a superação do precedente e a construção de uma solução distinta, mais condizente com a nova realidade, qual seja, a conclusão pela inadmissibilidade de se permitir à autoridade policial a devassa do conteúdo de aparelhos celulares apreendidos, independentemente de prévia autorização judicial. 7. Nas hipóteses como a dos autos, de apreensão de aparelhos celulares com fundamento no art. 6º do CPP, a autoridade policial deverá requerer ao juízo competente, justificadamente, autorização para acessar os dados ali contidos. O requerimento formal possibilitará ao juízo competente sopesar, diante das peculiaridades e circunstâncias do caso concreto, a adequação, a necessidade e a

> proporcionalidade em sentido estrito da medida, estabelecendo a abrangência da extração e da análise dos dados coletados e, especialmente, assegurará a lisura da cadeia de custódia das provas porventura obtidas a partir daí, como determinam o art. 158-A e seguintes do CPP, inseridos pela Lei nº 13.964, de 2019. 8. Recurso extraordinário com agravo ao qual se nega provimento, fixando-se a seguinte tese de repercussão geral: **1. 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 e ao sigilo das comunicações e à proteção dos dados pessoais, inclusive nos meios digitais (CF, art. 5º, incisos X, XII e LXXIX). 2. Em tais hipóteses, a celeridade se impõe, devendo a autoridade policial atuar com a maior rapidez e eficiência possível e o Poder Judiciário conferir tramitação e apreciação prioritárias aos pedidos dessa natureza, inclusive em regime de plantão** (grifei).

Ato contínuo, o eminente Ministro Flávio Dino acompanhou, com ressalvas, o voto reajustado do Ministro Relator, elaborando nova proposta de 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.

Na sequência, pedi vista dos autos para melhor analisar o caso e a

questão jurídica sob exame.

É o relatório. Passo ao voto.

I. Os direitos fundamentais à proteção de dados, à autodeterminação informacional e à garantia da confiabilidade e da integridade dos sistemas informáticos

A questão aqui colocada é **se a prova obtida mediante acesso não consentido e sem autorização judicial ao conteúdo dos dados coletados de aparelho celular, apreendido no local dos fatos, poderia ou não ser considerada lícita,** tendo em vista se tratar de uma **intervenção no direito fundamental à privacidade (art. 5º, XII, CR),** além de afetar outros direitos fundamentais dele derivados, como os **direitos à proteção de dados e à autodeterminação informacional (art. 5º, LXXIX, CR).**

A discussão acerca dos fundamentos e limites para o acesso a dados obtidos por meio de aparelho celular na persecução penal é relevante e atual. A temática está na ordem do dia no debate internacional e foi abordada recentemente em importantes precedentes do Tribunal de Justiça da União Europeia (processo C-548/2021, j. 20.4.2023), da Corte Constitucional da Áustria (G 352/2021-46, j. 14.12.2023) e da Corte Europeia de Direitos Humanos (Case Nezirić v. Bosnia and Herzegovina, Application n. 4088/21, j. 5.11.2024).

A tecnologia vem avançando a passos cada vez mais largos. Atualmente, os *smartphones* armazenam não apenas informações de comunicação, mas um extenso conjunto de dados pessoais, que incluem históricos de navegação, localização, hábitos de consumo, registros financeiros e até mesmo os aspectos mais íntimos da vida privada.

Os *smartphones* têm funcionado quase que como uma extensão dos corpos de seus usuários, acompanhando-os em praticamente todos os momentos da vida. Isso não apenas para realizar telefonemas — o que, com os serviços de mensageria, caiu até em desuso —, mas para desempenhar tantas outras funções antes desenvolvidas por diferentes ferramentas, servindo como computador, calculadora, agenda, câmera fotográfica, GPS, carteira, plataforma de entretenimento e meio de acesso a redes sociais, a serviços bancários e até a documentos oficiais.

A esse respeito, escreveu Luís Greco, em estudo recente:

> Mais do que quase qualquer outro objeto, o *smartphone* é um símbolo e, acima de tudo, a personificação da digitalização da vida que ocorreu nos últimos anos. Não há necessidade de entrar em detalhes sobre a enorme função que esse pequeno dispositivo desempenha. Ele permite a comunicação constante por meio de conversas, mensagens (de texto, voz e vídeo) ou e-mails; a participação em redes sociais, a navegação na Internet e a realização de pedidos online; o acesso a *streaming* de músicas, vídeos ou podcasts; a coordenação de compromissos, a reserva de uma mesa em um restaurante, o recrutamento de pessoas para todos os fins imagináveis (sim, especialmente para esses); funciona como bilhete de viagem e de voo, como cartão de entrada e bancário, se não como carteira de identidade, pelo menos como carteira de vacinação; combina e substitui em grande parte o relógio e o calendário, a revista e o livro, o mapa e o álbum de fotos, o rádio e a televisão, o computador e o console, até mesmo a família e os amigos (sim, especialmente esses também) - e, até certo ponto, nossa memória, possivelmente nossa inteligência (GRECO, Luís. Ermittlungsziel: Smartphone. *Strafverteidiger*, 2024, p. 276 — tradução livre do gabinete).

Essa evolução tecnológica e, em especial, a concentração de informações em um único dispositivo intensificam o potencial de violação de direitos fundamentais no caso de acessos não autorizados por autoridades policiais. O acesso a um *smartphone* permite não apenas o exame de informações diretamente relacionadas ao objeto de investigações, mas uma verdadeira incursão em camadas profundas da privacidade do titular, expondo uma grande quantidade de dados alheios aos fatos investigados e permitindo a formação de perfis de personalidade.

Conforme ressaltou Luís Greco, o "*smartphone* fornece uma imagem da pessoa, na medida em que isso sequer possa ser retratado. O acesso ao *smartphone* é aquilo que chega mais próximo de um **acesso à alma humana**" (GRECO, Luís. Ermittlungsziel: Smartphone, p. 279 — tradução livre do gabinete). Alguns dizem até que o *smartphone* seria um "segundo cérebro" (a respeito, cf. EL-GHAZI, Mohamad. Beschlagnahme und Auswertung von Handys, Laptops & Co. *Neue Juristische Wochenschrift - Beilage*. 2024, p. 46).

Essa problemática é agravada pela possibilidade de analisar os dados extraídos com o uso de ferramentas avançadas de inteligência artificial, como destacado no voto do eminente Relator, Ministro Dias Toffoli, as quais permitem o cruzamento e a interpretação de informações de modo abrangente e automatizado.

O caráter indispensável desses aparelhos para a vida contemporânea reforça a relevância do debate ora travado. Possuir um *smartphone* não é mais uma mera faculdade, mas uma necessidade imposta pela sociedade moderna. Diversos serviços — até mesmo públicos — exigem o uso de aplicativos específicos para atendimento.

Para uma análise adequada da questão aqui debatida, é imprescindível compreendê-la a partir não apenas dos impactos da

tecnologia na proteção do direito à privacidade, mas sobretudo da evolução do direito de proteção de dados ocorrida nos últimos anos.

O caso ora julgado ocorreu em 2013, antes do reconhecimento expresso pelo STF do direito à autodeterminação informacional (ADIs 6.387, 6.388, 6.389, 6.393, 6.390, da relatoria da eminente Ministra Rosa Weber, julgadas em 2020), assim como da promulgação do Marco Civil da Internet (Lei n. 12.965/2014), da Lei Geral de Proteção de Dados (Lei n. 13.709/2018) e da Emenda Constitucional n. 115/2022, que consagrou expressamente como direito fundamental o direito à proteção de dados pessoais (Art. 5º, "LXXIX - é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais.").

Como se nota, a jurisprudência e a legislação da última década reformularam a forma como enxergamos os direitos fundamentais à privacidade (art. 5º, X, CR) e à proteção de dados (art. 5º, LXXIX, CR) — e esse novo olhar sobre a disciplina afeta a análise e a fundamentação da decisão a ser tomada no presente caso. É possível até mesmo falar, conforme ressaltaram os eminentes Ministros Gilmar Mendes e Flávio Dino, em uma mutação constitucional, a qual tem o seu auge com a promulgação da Emenda Constitucional n. 115/2022.

Com efeito, não estamos tratando aqui a respeito da inviolabilidade do sigilo sobre as comunicações de dados, consagrada no art. 5º, XII, CR, porquanto essa proteção específica conferida pela Constituição da República abrange, de fato, apenas as comunicações em fluxo e não os dados armazenados.

Isso não significa, contudo, que a Constituição não proteja a privacidade e a autodeterminação informacional do indivíduo em relação a dados de sua titularidade armazenados em sistemas digitais.

Até porque se, antes, o fluxo das comunicações merecia uma

proteção especial, em um cenário em que o armazenamento e a manipulação de informações eram escassos e tinham alcance limitado, hoje, no contexto de uma sociedade da informação em que a quantidade de dados acessíveis e as tecnologias para seu processamento tomaram uma dimensão antes inimaginável, **os dados armazenados revelam muito mais sobre o indivíduo do que as comunicações em fluxo**, contendo informações das quais talvez nem mesmo o próprio titular se recorde.

O direito à privacidade garante aos indivíduos um espaço para o livre desenvolvimento da personalidade, no qual eles possam expressar convicções, "sentimentos, reflexões, visões de mundo e experiências pessoais sem medo de estar sendo observados por órgãos estatais" (GRECO, Luís; GLEIZER, Orlandino. A infiltração online no processo penal – Notícia sobre a experiência alemã. *Revista Brasileira de Direito Processual Penal*, Porto Alegre, vol. 5, n. 3, set./dez. 2019, p. 1495).

Isso abrange não apenas as telecomunicações, mas também a autonomia individual sobre os próprios dados pessoais que, sobretudo se analisados em conjunto, expressam a individualidade do sujeito.

Conforme ressalta José Afonso da Silva, a privacidade abrange o conjunto de informações a respeito do indivíduo, de modo que apenas ele poderá decidir se deseja mantê-las "sob seu exclusivo controle" ou se prefere comunicá-las, "decidindo a quem, quando, onde e em que condições" quer fazê-lo (SILVA, José Afonso da. *Curso de direito constitucional positiv*o. Rio de Janeiro: Malheiros, 2002. p. 205).

Como frisou o Tribunal Federal Constitucional alemão por ocasião da emblemática decisão do censo (BVerfGE 65, 1), a qual consagrou de forma pioneira o direito à autodeterminação informacional, "o livre desenvolvimento da personalidade sob as condições modernas do processamento de dados, pressupõe a proteção do indivíduo contra

irrestritas faculdades de obtenção, armazenamento, utilização e transferência de seus dados pessoais" (GRECO, Luís. Considerações introdutórias sobre o processo penal alemão. *In*: WOLTER, Jürgen. *O inviolável e o intocável no direito processual penal*. São Paulo: Marcial Pons, 2018, p. 43).

Assim, com a consagração do direito amplo à proteção de dados pessoais, deve-se assegurar, ao lado do sigilo das telecomunicações, outros âmbitos de proteção, como o direito à autodeterminação informacional (a respeito, cf. GLEIZER, Orlandino; MONTENEGRO, Lucas; VIANA, Eduardo. *O direito de proteção de dados no processo penal e na segurança pública*. São Paulo: Marcial Pons, 2021. p. 37), como já reconheceu o Supremo Tribunal Federal no julgamento da ADI 6.387. Esses direitos, analisados em conjunto, permitem que o indivíduo aja com espontaneidade no seu âmbito privado, tendo a liberdade de ser quem ele é, sabendo que, em circunstâncias normais, não será vigiado pelo Estado.

Com efeito, o **direito à autodeterminação informacional atribui ao titular dos dados a liberdade de (auto)determinar e, portanto, de controlar se e dentro de quais limites essas informações que revelam fatos de sua vida pessoal poderão ser objeto de intervenção**. Como demonstrado, ele é um direito autônomo, que tem relação direta com o direito à privacidade (inciso X do art. 5º da CR) e está expressamente protegido pelo novo inciso LXXIX do art. 5º da Constituição, vinculando-se, em última instância, ao direito geral ao livre desenvolvimento da personalidade, inerente à dignidade humana.

Há que se superar, portanto, a considerável diferenciação antes defendida entre a proteção constitucional atribuída a dados em fluxo e a dados armazenados, derivada da clássica distinção sustentada por Tércio Sampaio Ferraz Júnior (Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado. *Revista da Faculdade de Direito da Universidade de São Paulo*, v. 88, 1993, p. 439-59) e incorporada em

importantes precedentes desta Suprema Corte, como no RE 418.416, da relatoria do eminente Ministro Sepúlveda Pertence (Tribunal Pleno, DJ 19/12/2006), e no HC 91.867, da relatoria do eminente Ministro Gilmar Mendes (Segunda Turma, DJe 20/9/2012).

Isso, inclusive, já vem sendo reconhecido pelo Supremo Tribunal Federal:

> 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 168.052, Rel. Min. Gilmar Mendes, Segunda Turma, DJe 2/12/2020).

Não há dúvida de que os chamados "dados estáticos" são também objeto de proteção pela Constituição da República de 1988.

Para além disso, ao analisar a controvérsia inerente ao presente caso, entendo que também é relevante invocar aqui o **direito à garantia da integridade e da confiabilidade dos sistemas informáticos**, reconhecido em um importante precedente pelo Tribunal Federal Constitucional alemão como manifestação do direito à proteção da personalidade (nesse sentido, cf. SAAD, Marta; ROSSI, Helena Costa; PARTATA, Pedro Henrique. A obtenção das provas digitais no processo penal demanda

uma disciplina jurídica própria? Uma análise do conceito, das características e das peculiaridades das provas digitais. *Revista Brasileira de Direito Processual Penal*, v. 10, n. 3, 2024, p. 15).

Sob a perspectiva da Constituição da República de 1988, o direito fundamental à garantia da integridade e da confiabilidade dos sistemas informáticos, vinculado ao livre desenvolvimento da personalidade, encontra guarida na própria dignidade da pessoa humana (art. 1º, III, CR). A respeito desse direito, esclareceu o Tribunal Federal Constitucional alemão:

> O direito fundamental à garantia da integridade e da confiabilidade dos sistemas informáticos é aplicável se a autorização de intervenção abranger sistemas que, isoladamente ou nas suas conexões técnicas, possam **conter dados pessoais do titular dos dados em tal extensão e variedade que o acesso ao sistema permite obter uma visão sobre partes essenciais da vida de uma pessoa ou mesmo obter uma imagem significativa da sua personalidade** (BVerfGE 120, 274, p. 314 — tradução livre do gabinete).

Ao comentar essa decisão, explicam Luís Greco e Jürgen Wolter:

> [...] o tribunal considerou decisivo um novo direito fundamental à integridade e confiabilidade dos sistemas de tecnologia da informação, também derivado do direito geral de personalidade (Art. 2, par. 1, GG). Atualmente, o indivíduo depende do uso de tais sistemas para o desenvolvimento de sua personalidade e, portanto, está exposto a uma variedade de novos perigos; em especial, ele deve poder confiar que não apenas o conteúdo armazenado em seu sistema de tecnologia da informação, mas também a integridade do próprio sistema

> está protegida contra acesso externo (GRECO; WOLTER. § 100b StPO – Online-Durchsuchung. *Systematischer Kommentar zur Strafprozessordnung*: SK-StPO, Band II: §§ 94-136a StPO. Carl Haymmanns, 2016, nm. 8 — tradução livre do gabinete).

A despeito de essa decisão se referir ao debate sobre o acesso oculto a sistemas informáticos por meio de infiltração *online*, o acesso aberto ao conteúdo de um *smartphone* também caracteriza uma intervenção no direito à garantia da integridade e da confiabilidade dos sistemas de tecnologia da informação, tendo em vista que permite igualmente o acesso não consentido à ampla gama de informações ali contida. Nesse sentido, o fato de que o acesso em si é oculto em relação ao seu titular afetaria apenas a intensidade da intervenção nesse direito (GRECO, Ermittlungsziel: Smartphone, p. 279).

O acesso irrestrito a um *smartphone* permite a coleta de dados em larga escala e, com isso, não apenas a formação de perfis de personalidade, de comunicação e de movimentação do usuário por meio do processamento de algumas informações, mas a construção de uma imagem muito concreta daquele indivíduo por meio do tratamento de uma enorme quantidade de dados de significativa profundidade e amplitude. Em termos de quantidade e concentração de informações, talvez sequer seja possível equiparar o acesso ao conteúdo de um *smartphone* ao de um computador, *pen-drive* ou qualquer outro dispositivo informático.

Assim, mais do que proteger os dados ali armazenados, trata-se também de garantir a confiança de que os sistemas informáticos, que acumulam tantas informações, não serão acessados sem o consentimento do seu titular, isto é, uma "proteção contra o acesso ao próprio sistema informático que é utilizado para o desenvolvimento comunicativo" (HOFFMANN-RIEM, Wolfgang. A proteção de direitos fundamentais da confidencialidade e da integridade de sistemas próprios de tecnologia da

informação. Trad. Pedro Henrique Ribeiro. *Revista de Direito Civil Contemporâneo*, v. 23, 2020, p. 348).

Considerando que o acesso não autorizado a dados armazenados em um aparelho celular constitui uma intervenção nos referidos direitos fundamentais, a qual é *prima facie* ilícita, caracterizando, inclusive, o delito previsto no art. 154-A do Código Penal (invasão de dispositivo informático), deve-se determinar o fundamento que permite a justificação dessa intervenção para definir o âmbito de legitimidade da medida investigativa estatal.

II. Fundamentos de justificação da intervenção nos direitos fundamentais

O reconhecimento de direitos fundamentais impõe ao Estado um dever geral de abstenção. Se o indivíduo tem o direito de autodeterminar o que é feito com os seus dados pessoais, a regra é que essas informações poderão ser tratadas apenas mediante o consentimento do seu titular (art. 7º, I, Lei Geral de Proteção de Dados [LGPD], Lei n. 13.709/18).

Considerando, contudo, que na persecução penal esses dados hão de ser tratados mesmo sem o consentimento do titular, o dever de abstenção poderá ser afastado por meio de uma justificação especial de intervenção.

Quanto a esse aspecto, apesar de o escopo da LGPD não abranger a persecução penal (art. 4º, III e § 1º, da Lei n. 13.709/18) e de o projeto de uma Lei Geral de Proteção de Dados para a Segurança Pública e a Persecução Penal ainda não ter sido aprovado, não há dúvidas de que a LGPD pode servir como parâmetro interpretativo do direito geral de proteção de dados recém incorporado pela Constituição e, com isso, dos diferentes dispositivos presentes em nossa legislação que autorizam intervenções no direito à autodeterminação informacional no contexto do processo penal, como o aqui debatido.

Portanto, a intervenção no direito fundamental à autodeterminação informacional para fins de persecução penal é possível, mas depende da observância de determinados **limites**. O parâmetro de legitimação dessas intervenções vincula-se sobretudo a dois princípios da dogmática constitucional: o princípio da reserva de lei e o princípio da proibição de excesso, que exige a proporcionalidade da medida interventiva (A respeito, cf. GLEIZER; MONTENEGRO; VIANA. *O direito de proteção de dados no processo penal e na segurança pública*. p. 40).

A exigência de autorização legal deriva não apenas do art. 5º, II, da CR ("II - ninguém será obrigado a fazer ou deixar de fazer alguma coisa senão em virtude de lei"), como também do art. 11, 2, primeira parte, da Convenção Americana sobre Direitos Humanos (Pacto de São José da Costa Rica), da qual o Brasil é signatário (Decreto 678/1992), que estabelece que "[ninguém] pode ser objeto de ingerências arbitrárias ou abusivas em sua vida privada".

Com efeito, o aparelho celular pode ser considerado um "objeto", isto é, uma coisa corpórea e tangível, no sentido do art. 6º, II (apreensão de objetos relacionados com o fato), e do art. 240, § 1º e § 2º, do CPP (busca de objetos necessários à prova da infração):

> Art. 6º Logo que tiver conhecimento da prática da infração penal, a autoridade policial deverá:
>
> II - apreender os objetos que tiverem relação com o fato, após liberados pelos peritos criminais;
>
> [...]
>
> Art. 240. A busca será domiciliar ou pessoal.
>
> § 1º Proceder-se-á à busca domiciliar, quando fundadas razões a autorizarem, para:
>
> e) descobrir objetos necessários à prova de infração ou à defesa do réu;
>
> § 2º Proceder-se-á à busca pessoal quando houver

> fundada suspeita de que alguém oculte consigo arma proibida ou objetos mencionados nas letras b a f e letra h do parágrafo anterior.
>
> Art. 244. A busca pessoal independerá de mandado, no caso de prisão ou quando houver fundada suspeita de que a pessoa esteja na posse de arma proibida ou de objetos ou papéis que constituam corpo de delito, ou quando a medida for determinada no curso de busca domiciliar.

Assim, existe autorização legal para a apreensão do aparelho celular, sem decisão judicial, contanto que preenchidos os pressupostos legais.

A apreensão do aparelho celular há de ser, também, proporcional. Ela somente poderá ocorrer, conforme ressaltou o eminente Ministro Gilmar Mendes em seu voto, quando houver fundadas suspeitas de que o conteúdo do celular pode auxiliar as investigações. Nesse sentido, Luís Greco esclarece que a princípio não seria possível, por exemplo, apreender o celular do suspeito quando for preso em flagrante por dirigir embriagado (GRECO, Luís. Ermittlungsziel: Smartphone, p. 280).

O que esses dispositivos autorizam, contudo, é apenas a apreensão do aparelho e o seu exame físico, por exemplo, no caso de o aparelho encontrado na cena do crime conter manchas de sangue.

Não obstante, a autorização para apreensão do aparelho celular enquanto objeto é insuficiente para permitir que a autoridade policial acesse o conteúdo dos dados imateriais nele contidos ou cujo acesso é possibilitado por meio dele, que é o que verdadeiramente importa para fins probatórios. De fato, "no *smartphone*, o corporal é incidental; importantes são as informações a que ele permite acesso, que cada vez mais sequer são nele armazenadas, mas na chamada nuvem" (GRECO, Luís. Ermittlungsziel: Smartphone, p. 280 — tradução livre do gabinete).

Assim, entendo que esses dispositivos do CPP autorizam que o celular seja apreendido pelos policiais, mas não que o conteúdo dos dados seja acessado sem autorização judicial. Nesse sentido, argumentam o Ministro João Otávio de Noronha e Simone Fernandes:

> Em busca pessoal inserida no contexto de uma prisão em flagrante, o aparelho celular enquadra-se na definição de objeto que pode ter relação com o delito praticado, com potencial aptidão para servir ao esclarecimento do fato e suas circunstâncias, motivo pelo qual pode ser regularmente apreendido pela autoridade policial, nos termos dos arts. 6º, II, e 244 do Código de Processo Penal. Deve-se exigir, sempre, que haja essa correlação, essa aptidão para esclarecimento do fato ilícito praticado ou delineamento de algum dos elementos do tipo, já que não se pode tolerar apreensões imotivadas ou automáticas, sem nenhum liame com o delito investigado.
>
> Nessa linha de raciocínio, não se legitima a apreensão de telefone celular de envolvido, exemplificativamente, em briga de rua entre estranhos, já que o objeto não se prestará a nenhum esclarecimento acerca da lesão corporal praticada. Nossa ordem jurídica não abre espaço para *phishing* investigatório.
>
> Havendo o necessário liame entre o que se pretende provar e o que potencialmente se encontra armazenado no *smartphone*, sua apreensão é providência salutar, mas essa possibilidade não legitima uma devassa em seu conteúdo sem prévia autorização judicial ou consentimento do proprietário. (NORONHA, João Otávio; FERNANDES, Simone dos Santos Lemos. Limites constitucionais ao acesso de smartphones apreendidos em prisões em flagrante. *In*: ESPIÑEIRA, Bruno; COLAVOLPE, Luís Eduardo; MATTOS FILHO, Maurício. *A prova e o processo penal constitucionalizado*: estudos em homenagem ao Ministro Sebastião Reis Júnior. Belo Horizonte: D'Plácido, 2022. p. 297-298).

A meu ver, o efetivo acesso aos dados de conteúdo obtidos por meio

de um aparelho celular apreendido pela autoridade policial é autorizado pelos arts. 7º, III, e 10, § 2º, do Marco Civil da Internet (Lei n. 12.965/2014):

> Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:
>
> III - **inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial**;
>
> [...]
>
> Art. 10. A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet de que trata esta Lei, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas.
>
> § 2º **O conteúdo das comunicações privadas somente poderá ser disponibilizado mediante ordem judicial**, nas hipóteses e na forma que a lei estabelecer, respeitado o disposto nos incisos II e III do art. 7º .

Como se nota, tais dispositivos exigem expressamente a autorização judicial para permitir o acesso ao conteúdo das comunicações privadas armazenadas.

A despeito de nem todos os dados contidos em um aparelho celular serem, estritamente, "comunicados", não é possível dissociar, em um dispositivo, aqueles dados que são ou não objeto de uma comunicação. A depender de como se concebe a comunicação, as fotos, por exemplo, somente caracterizariam "comunicação privada armazenada" se tivessem sido recebidas ou enviadas a uma outra pessoa.

Entendo, portanto, que a expressão "comunicações privadas armazenadas" há de ser compreendida em sentido amplo, abrangendo todos os dados acedidos por meio do dispositivo – isto é, tanto as fotos e

dados de geolocalização quanto as conversas travadas pelo *whatsapp* ou pelo e-mail.

Por se tratar de uma **ingerência consideravelmente grave em direitos fundamentais**, considerando o potencial de invasão da privacidade proporcionado pelo acesso a dados de telefones celulares, fonte de uma ampla gama de dados de significativa profundidade e amplitude, **só é possível proteger esses direitos de forma proporcional por meio da reserva de jurisdição, isto é, pela exigência de fiscalização prévia realizada por um juiz**.

Isso se aplica a todos os aparelhos telefônicos, estejam ou não protegidos por mecanismos de segurança, como senhas. Assim como o fato de a porta estar aberta ou destrancada não descaracteriza uma invasão de domicílio, a inexistência de mecanismos de segurança para acessar o dispositivo não afasta o direito à privacidade do seu titular.

Ao juiz caberá realizar a análise da proporcionalidade da medida no caso concreto, com o objetivo de promover o equilíbrio entre a proteção de direitos fundamentais e os interesses legítimos vinculados à persecução penal e investigação de crimes (cf., no mesmo sentido, a decisão do Tribunal de Justiça da União Europeia, processo C-548/2021, j. 20.4.2023, nm. 103). À luz da proteção constitucional conferida à privacidade, seja a dados em fluxo ou armazenados, nem mesmo o legislador poderia dispensar a ordem judicial nesse caso.

A análise da proporcionalidade da medida — isto é, da necessidade, da adequação e da proporcionalidade em sentido estrito — deverá ser realizada e devidamente justificada (fundamentada) pelo juiz que determinar o acesso ao conteúdo do aparelho celular. Conquanto ainda não haja uma lei que discipline mais concretamente os pressupostos de legitimidade da medida, há parâmetros mínimos de proporcionalidade que devem ser observados pelo juiz no caso concreto.

O acesso deve ser realmente necessário, de modo que os dados somente podem ser tratados se a finalidade do tratamento não puder ser obtida por outros meios igualmente eficazes e menos atentatórios aos direitos fundamentais do afetado. Na análise da proporcionalidade, devem ser ponderados todos os elementos relevantes do caso concreto, inclusive a gravidade do delito e o grau de suspeita que recai sobre o titular dos dados. A esse respeito, esclareceu o Tribunal de Justiça da União Europeia:

> Inserem-se, nomeadamente, nesses elementos, a gravidade dessa restrição introduzida ao exercício dos direitos fundamentais em causa, que depende da natureza e da sensibilidade dos dados a que as autoridades policiais competentes podem ter acesso, a importância do objetivo de interesse geral prosseguido por essa restrição, a relação existente entre o dono do telemóvel e a infração penal em causa ou ainda a relevância dos dados em causa para o apuramento dos factos (processo C-548/2021, j. 20.4.2023, nm. 90).

Para preservar o núcleo essencial do direito fundamental, idealmente o acesso ao conteúdo dos dados deve ser parcial e restrito, limitado aos critérios de busca vinculados ao objeto da investigação, ou seja, os dados a serem acessados devem ser delimitados, na medida do possível, na decisão judicial. Apenas excepcionalmente deve-se admitir autorizações mais genéricas, a exemplo das situações mencionadas pelo Ministro Flávio Dino, tais como investigações em estágio inicial, crimes praticados por organizações criminosas, crimes multitudinários, entre outros.

Entendo que somente em casos de **extrema urgência** seria possível renunciar à exigência de ordem judicial com fundamento no estado de necessidade (art. 24, CP). Isso seria possível, citando os exemplos trazidos

pelo eminente Ministro Gilmar Mendes, nas situações em que o acesso imediato ao conteúdo do telefone for comprovadamente imprescindível para "localizar uma pessoa sequestrada ou evitar um ataque terrorista". Ou seja, a possibilidade de recorrer ao estado de necessidade se vincularia, especificamente, à proteção de bens jurídicos de alto valor, como a vida e a liberdade de locomoção, e preenchendo os demais pressupostos de justificação.

Ainda quanto à exigência de decisão judicial, o eminente Ministro Flávio Dino fez uma importante ressalva a respeito da **possibilidade de preservação dos dados**, sem autorização judicial, para evitar que o titular do dispositivo elimine a prova.

De fato, é possível que o titular do aparelho celular apreendido elimine a prova mesmo após a apreensão — por exemplo, por meio de aplicativo de apagamento remoto do conteúdo do dispositivo ou até mesmo por exclusão dos dados armazenados em nuvem, cujo acesso é possibilitado por meio do acesso físico ao dispositivo. Tal proceder representa um risco aos interesses legítimos da persecução penal de acessar esses dados para fins probatórios.

Contudo, apesar de ainda não implicar uma "violação do sigilo", nos termos empregados pelo Marco Civil da Internet (art. 7º, III), não se pode desconsiderar que até mesmo a coleta dos dados, ainda que sem consultá-los, coloca em perigo os direitos fundamentais aqui debatidos, pois nada impede, hipoteticamente, que a autoridade policial os consulte imediatamente.

Além disso, não há dúvidas de que a "mera" extração dos dados do dispositivo constitui um tratamento de dados pessoais, conforme conceituação da própria LGPD (Lei n. 13.709/2018):

> Art. 5º Para os fins desta Lei, considera-se:

> [...]
> X - tratamento: toda operação realizada com dados pessoais, como as que se referem a **coleta**, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;

Diante disso, a possibilidade de preservação dos dados, a meu ver, depende da criação de mecanismos técnicos destinados a garantir que os dados não serão acessados enquanto não houver decisão judicial.

Assim, seria em tese possível admitir o espelhamento sigiloso dos dados, contanto que a autoridade policial consiga demonstrar tecnicamente que não foi realizado nenhum outro tratamento desses dados, especialmente que não houve acesso efetivo ao seu conteúdo antes da autorização judicial. Com isso, garante-se não apenas a confiabilidade e autenticidade dos dados, mas sobretudo o direito à privacidade do titular dos dados, isto é, a garantia que as informações ali contidas não serão efetivamente acessadas antes de se obter a ordem judicial.

Entendo, outrossim, que a questão aqui debatida não pode ser diretamente comparada à possibilidade de solicitação, pela autoridade policial ou pelo Ministério Público, de guarda de registros de conexão por provedores de aplicação por prazo superior ao previsto no Marco Civil da internet (art. 13 da Lei n. 12.965/2014).

Isso porque essa possibilidade, na minha compreensão, tem a ver com a mera solicitação de aumento do prazo, para além daquele previsto em lei, para a guarda de metadados (registros de conexão) pelos provedores de aplicação, e não para a preservação de dados de conteúdo, em relação aos quais não há deveres de guarda previstos no Marco Civil da Internet.

A meu ver, a preservação dos dados deve ter caráter excepcional e pode ocorrer apenas quando houver fundado receio de que os dados serão eliminados pelo seu titular ou por terceiros. Deve-se dar prioridade, contudo, à obtenção célere e eficiente de autorização judicial para acessar o conteúdo dos dados, devendo o Poder Judiciário, conforme ressaltado pelo eminente Relator, Ministro Dias Toffoli, "conferir tramitação e apreciação prioritárias aos pedidos dessa natureza, inclusive em regime de plantão".

III. O caso concreto

No caso paradigma, o suspeito do crime havia deixado cair, durante a fuga, o seu aparelho de telefonia celular, o qual foi acessado, sem autorização judicial, pelos policiais civis, que, a partir dos dados ali contidos, como histórico de chamadas e fotografias, identificaram o autor do delito.

É imperativo reconhecer a ilicitude e consequente inadmissibilidade dessa prova, tendo em vista a intervenção não justificada no direito fundamental à privacidade do suspeito (art. 5º, X e LVI, CR), assim como todas as provas dela derivadas, tendo em vista que a identificação do suspeito somente foi possível em razão do acesso aos dados do dispositivo.

IV. Sobre a tese de repercussão geral

Em seu voto reajustado, o eminente Ministro Relator, Dias Toffoli, propôs a seguinte tese de repercussão geral:

> 1. 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 e ao sigilo das comunicações e à proteção dos dados pessoais, inclusive nos meios digitais (CF, art. 5º, incisos X, XII e LXXIX). 2. Em tais hipóteses, a celeridade se impõe, devendo a autoridade policial atuar com a maior rapidez e eficiência possível e o Poder Judiciário conferir tramitação e apreciação prioritárias aos pedidos dessa natureza, inclusive em regime de plantão.

O eminente Ministro Flávio Dino, por sua vez, propôs uma tese alternativa:

> 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.

A partir das teses elaboradas pelo eminente Relator, Ministro Dias Toffoli, e pelo eminente Ministro Flávio Dino, proponho alguns ajustes com o objetivo de esclarecer que os dados a serem acessados podem estar tanto armazenados no próprio dispositivo quanto em nuvem; que pode se tratar de aparelhos apreendidos não apenas no local do crime e não necessariamente de titularidade do suspeito; e que a exigência de decisão judicial não se aplica aos casos em que o titular dos dados consente validamente no acesso.

Sugiro também a menção à proporcionalidade, em termos gerais, que abrange a necessidade, a adequação e a proporcionalidade em

sentido estrito. Além disso, elaboro uma proposta intermediária quanto à possibilidade de preservação dos dados.

Eis os termos da tese sugerida:

> 1. O acesso a dados obtidos a partir de aparelhos celulares depende do consentimento do titular dos dados ou de prévia decisão judicial (arts. 7º, III, e 10, § 2º, da Lei n. 12.965/2014) que justifique, com base em elementos concretos, a proporcionalidade da medida e delimite sua abrangência à luz dos direitos fundamentais à intimidade, à privacidade, à proteção dos dados pessoais e à autodeterminação informacional, inclusive nos meios digitais (art. 5º, X e LXXIX, CR).
>
> 2. A apreensão do aparelho celular, nos termos do art. 6º do CPP, ou em flagrante delito, não está sujeita à reserva de jurisdição.
>
> 3. Nas hipóteses de acesso não consentido a dados de telefone celular, a celeridade se impõe, devendo a autoridade policial atuar com a maior rapidez e eficiência possível e o Poder Judiciário conferir tramitação e apreciação prioritárias aos pedidos dessa natureza, inclusive em regime de plantão. Apenas excepcionalmente será possível a preservação dos dados e metadados do titular do dispositivo, antes da autorização judicial, caso em que a autoridade policial deve (i) justificar o fundado receio de que os dados sejam eliminados pelo seu titular ou por terceiros e (ii) demonstrar, por meios técnicos, que não foi realizado nenhum outro tratamento desses dados.

V. Dispositivo

Posto isso, acompanho com ressalvas o voto do eminente Ministro

Relator, Dias Toffoli, para negar provimento ao agravo em recurso extraordinário e propor a seguinte tese de repercussão geral para o Tema 977:

1. O acesso a dados obtidos a partir de aparelhos celulares depende do consentimento do titular dos dados ou de prévia decisão judicial (arts. 7º, III, e 10, § 2º, da Lei n. 12.965/2014) que justifique, com base em elementos concretos, a proporcionalidade da medida e delimite sua abrangência à luz dos direitos fundamentais à intimidade, à privacidade, à proteção dos dados pessoais e à autodeterminação informacional, inclusive nos meios digitais (art. 5º, X e LXXIX, CR).

2. A apreensão do aparelho celular, nos termos do art. 6º do CPP, ou em flagrante delito, não está sujeita à reserva de jurisdição.

3. Nas hipóteses de acesso não consentido a dados de telefone celular, a celeridade se impõe, devendo a autoridade policial atuar com a maior rapidez e eficiência possível e o Poder Judiciário conferir tramitação e apreciação prioritárias aos pedidos dessa natureza, inclusive em regime de plantão. Apenas excepcionalmente será possível a preservação dos dados e metadados do titular do dispositivo, antes da autorização judicial, caso em que a autoridade policial deve (i) justificar o fundado receio de que os dados sejam eliminados pelo seu titular ou por terceiros e (ii) demonstrar, por meios técnicos, que não foi realizado nenhum outro tratamento desses dados.

É como voto.