Panorama sobre o Acesso aos Dados Armazenados em Celular em Situação de Flagrante Delito no Brasil

Overview on Brazil's Access to Data Stored on Cell Phones in a Situation of Flagrant Delicto

AMANDA MATIAS CAVALCANTE DE OLIVEIRA[1]
Universidade Católica de Brasília (UCB).

NÉFI CORDEIRO[2]
Universidade Católica de Brasília (UCB).

RESUMO: O constante desenvolvimento tecnológico dos aparelhos celulares possibilitou a extração de dados que impactam as investigações criminais com relativa facilidade, notadamente nas buscas promovidas pelas autoridades policiais por ocasião de situações de flagrante delito. Partindo da explicação do conceito de dado digital e das distinções dos níveis de tutela dos dados extraíveis dos referidos telefones, o presente trabalho visa traçar um panorama sobre efeitos práticos da distinção entre apreensão e acesso de *smartphones* pelo agente policial em situações de flagrante, impactos nos direitos do suspeito e entendimento jurisprudencial sobre os limites a serem observados em busca da elucidação dos fatos delituosos. Com base nas definições em referências, por meio da revisão da doutrina especializada, dos limites legais impostos pela Constituição Federal, pelo Código de Processo Penal e legislação específica sobre dados digitais, e de precedentes históricos sobre o tema, proferidos tanto pelo Superior Tribunal de Justiça quanto pelo Supremo Tribunal Federal, pretende-se obter um panorama sobre a validade do acesso ao conteúdo armazenado nos aparelhos telefônicos quando houver certeza visual dos crimes, de modo a traçar contornos claros aos agentes policiais das hipóteses e da extensão da visualização do conteúdo dos *smartphones* quando promovidas, sem amparo em decisão judicial prévia, nos casos de prisão em flagrante.

PALAVRAS-CHAVE: Celular; dados; flagrante; apreensão; acesso; garantias.

1 Orcid: https://orcid.org/0000-0001-7142-1767.
2 Orcid: https://orcid.org/0000-0002-1490-3118.

ABSTRACT: The constant technological development of cell phones made it possible to extract data that impact criminal investigations with relative ease, especially in searches carried out by police authorities in cases of flagrante delicto. Departing from the explanation of the concept of digital data and the distinctions in the levels of protection of data extractable from those phones, this paper aims to provide an overview of the practical effects of the distinction between seizure and access of smartphones by police officers in flagrant situations, impacts on suspect's rights and jurisprudential understanding on the limits to be observed in the search for elucidation of the criminal facts. Based on the definitions in references, through the review of specialized doctrine, the legal limits imposed by the Federal Constitution, the Code of Criminal Procedure and specific legislation on digital data, and historical precedents on the subject, issued both by the Superior Court of Justice as for the Federal Supreme Court, it is intended to obtain an overview of the validity of access to content stored on telephone devices in the cases of visual certainty of crimes, in order to draw clear outlines to police officers of the hypotheses and the extent of visualization of the content of the smartphones when promoted, without the support of a previous court decision, in cases of arrest in flagrante delicto.

KEYWORDS: Cell phone; data; flagrant; seizeure; access; guarantees.

INTRODUÇÃO

A versatilidade dos aparelhos de telefonia móvel reconfigurou o estilo de vida da sociedade em uma perspectiva global, reformulando antigos hábitos, criando novas rotinas no âmbito pessoal e profissional e, principalmente, revolucionando a forma de comunicação. Da possibilidade de acesso às notícias, passando por movimentações bancárias e compras a distância, não tardou para que o desenvolvimento tecnológico também fosse adaptado para a prática de toda sorte de delitos.

Diante da popularização dos *smartphones* e ante seu emprego por vezes na execução de delitos cibernéticos, próprios e impróprios, a requisição de acesso aos mencionados dispositivos passou a constituir condição frequente em abordagens policiais: muitas vezes antes mesmo de qualquer indício da prática delitiva.

A apreensão dos aparelhos celulares permite, lícita ou ilicitamente, a possibilidade de acesso investigatório aos contatos, histórico de chamadas, vídeos, fotos, *sites* pesquisados, *e-mails* e mensagens trocadas de forma instantânea por meio de aplicativos, dentre outros tantos elementos úteis à investigação. Surge, então, a necessária discussão dos limites de acesso e de

validade das provas obtidas em dados de celulares: as fronteiras da licitude na apreensão e acesso de celular em atuação policial.

Nessa perspectiva, a compreensão da relevância da prova digital, como representação de um universo de dados nem sempre depreendidos pelos sentidos e somente apreendidos de forma completa por um olhar técnico, permite entender que a possibilidade de acesso ao conteúdo armazenado em um aparelho celular pode representar uma janela para visualizar uma infinidade de elementos: nem sempre úteis à comprovação da hipótese inicial da investigação e, muitas das vezes, exponencialmente invasivos sob a perspectiva do investigado e do seu círculo de convívio.

Repensar a lógica da arrecadação de elementos indiciários de prova sob o viés digital possibilita delimitar o alcance da medida investigativa. Por se tratar de dispositivo informático, que utiliza não apenas as redes tradicionais de telecomunicações, mas, sobremaneira, as redes de internet, tudo o que é acessado no *smartphone* pela autoridade pública, sem autorização judicial, importa em volumoso conjunto de dados.

Dentro do conjunto de informações, a tipologia dos elementos que compõem os dados passíveis de coleta do aparelho celular (base, tráfego e conteúdo), ainda que nem sempre sejam coletados no momento da busca pessoal e da apreensão do dispositivo informático, demonstra a expansão do horizonte de possibilidades de comprovação dos indícios de materialidade e autoria delitiva. Por isso, entender o conceito de dado digital, sua classificação tripartite, a regulamentação no ordenamento jurídico e principalmente o modo como o tema vem sendo abordado pelas Cortes Superiores do país alertam para a necessidade de profunda reflexão sobre o tema no âmbito da academia.

A relevância da pesquisa é demonstrada não apenas pela discussão sobre os elementos que compõem a comunicação, como também para que seja sintetizada a distinção sobre quais garantias constitucionais são aplicadas aos dados armazenados nos *smartphones*. A análise da literatura especializada, ainda escassa, e do repertório de decisões judiciais proferidas pelo Supremo Tribunal Federal e pelo Superior Tribunal de Justiça demonstram que o regramento do acesso às informações disponíveis nos *smartphones* não é claro em asseverar qual é a garantia constitucional a ser acionada nos casos de devassa na situação extrema do flagrante delito ou, ainda, qual meio deve ser empregado para obter seu conteúdo.

Apesar de parecer lógico, a inviolabilidade do sigilo de comunicação telefônica e de dados, prescrita no art. 5º, XII, da Constituição Federal, é limitada ao objeto de sua comunicação e, ainda assim, guarda distinção de tratamento em razão do processo de transmissão ou da finalização do diálogo. E o que se verifica nos precedentes adiante examinados é que a solução encontrada pelos Tribunais Superiores pátrios reside no deslocamento do bem jurídico selecionado para tutela. Agora, a proteção contra a devassa de um aparelho celular não é mais vista em razão do direito à propriedade do bem ou de sua fonte originária de utilização, mas sim pela perspectiva da guarda da privacidade de seu usuário e do consequente respeito à reserva legal.

Com o objetivo de apurar os limites da apuração da verdade no momento das buscas que antecedem à prisão em flagrante, o presente artigo abordará, com apoio na literatura e na jurisprudência dos Tribunais Superiores brasileiros, os limites da atuação do Estado-policial. Por meio da revisão da doutrina especializada sobre o universo da prova digital, a perspectiva constitucional da comunicação travada pelos aparelhos celulares e a ótica do processo penal sobre as diligências cabíveis nas hipóteses de verificação do flagrante descrito, o presente trabalho pretende demonstrar a importância da coleta de dados digitais nos contextos extremos ora apontados.

Para tanto, a primeira seção do artigo será dedicada à compreensão da criação de um marco legal dos dados digitais decorrentes do processo de uso e armazenamento de informações nos aparelhos de telefonia celular, trilhando o histórico do processo, a enunciação do conceito de prova digital, a visão tripartite dos dados nele contidos e os direitos fundamentais relacionados à utilização dos referidos dispositivos.

A segunda seção apresenta o processo de obtenção das provas digitais extraídas de aparelhos celulares no contexto da prisão em flagrante. Nesse ponto, será apresentada uma visão crítica ao processo de abordagem das prisões em flagrante no cenário brasileiro, os limites legais de atuação policial em relação à apreensão e acesso dos dados armazenados nos aparelhos celulares dos suspeitos e um panorama sobre a construção do conceito de prova digital válida a ser obtida no contexto do flagrante.

O tópico final abordará, de forma sucinta, o histórico das principais decisões sobre o tema, o que se entende como passível de acesso sem autorização judicial prévia e os rumos a que se direciona a jurisprudência do Supremo Tribunal Federal na análise de precedente submetido à sistemática

da repercussão geral dos recursos. Ao cabo, pretende-se formular um levantamento sobre os critérios e limites de devassa dos dados armazenados nos *smartphones* pelos agentes policiais, de modo a propiciar a utilização válida e eficiente das informações na investigação e futura instrução processual penal.

1 MARCO LEGAL DA PROVA DIGITAL

1.1 Considerações iniciais sobre o tema

Acompanhado da revolução promovida pela internet e do desenvolvimento do fenômeno da convergência (Barreto, 2020, p. 44), o telefone passou de simples dispositivo de ligações telefônicos entre ausentes para se tornar verdadeiro microcomputador portátil. Nessa transformação, os novos telefones móveis passaram a englobar tanto seu uso original, não mais necessariamente transmitido por redes de telefonia, como também opções de conexão à internet, de acesso a vídeos, fotos, áudios, mapas, dentre outras inúmeras opções constantemente criadas e atualizadas.

Prova disso é o resultado da Pesquisa Nacional por Amostra de Domicílios Contínua, do IBGE – Instituto Brasileiro de Geografia e Estatística (2021, p. 1), que comprovou que, no ano de 2019, o uso do aparelho celular obedecia à seguinte escala de prioridades dentre os entrevistados: 1º) envio e recebimento de mensagens de texto, voz e imagens por aplicativos (95,7%); 2º) conversa por chamada de voz ou vídeo (91,2%); 3º) assistir a vídeos, inclusive de programas, séries e filmes (88,4%); e 4º) envio e recebimento de *e-mails* (61,5%).

A multifuncionalidade do aparelho transformou a vida de todos os seus portadores, que passaram a concentrar, com maior ou menor grau de intensidade, parte considerável de informações pessoais nas memórias dos *smartphones* ou de dispositivos de armazenamento em nuvem instalados no dispositivo e contratados pelo usuário.

Além dos dados nele inseridos, a própria destinação do aparelho, infelizmente, também caminhou para facilitar a execução de toda sorte de delito, aqui englobados aqueles praticados contra a inviolabilidade dos sistemas informáticos (cibercrimes próprios ou puros) e aqueles que podem ser praticados tanto no meio virtual quanto de formas tradicionais (cibercrimes impróprios ou impuros) (Kist, 2019, p. 67-69). Prova disso é a recente publicação da Lei nº 14.155/2021 (Brasil, 2021), que demonstra a preocupação

do legislador ordinário com o agravamento das penas nos casos em que delitos contra o patrimônio ou de fraude forem executados com o auxílio de dispositivos eletrônicos ou informáticos, como os *smartphones* disponíveis no mercado.

O aumento da conectividade dos telefones por meio de serviços de internet disponibilizados por franquias pagas ou por redes sem fio, cada vez mais populares na vida cotidiana, propiciou uma profunda mudança de costumes, a ponto de esses bens se tornarem itens de porte indispensáveis. E, com o aumento da portabilidade, a possibilidade de identificar com maior facilidade os rastros da prática de um crime por meio de um aparelho de fácil manuseio e que contempla tantos dados pessoais tornou o celular um item de extrema valia nas investigações policiais.

Apesar de propiciar o aumento da eficiência dos meios investigatórios, deve haver a preocupação com a criação de limites do acesso estatal à vida privada e à intimidade do titular do aparelho, seja por limites prévios – se possível legais –, seja por controle casuístico da necessidade dessa prova invasiva. Embora portátil e acessível em qualquer revista física, o volume de informações de um celular o diferencia muito de outros objetos de posse pessoal, razão pela qual, na visão de Gloeckner e Eilberg (2019), o acesso ao seu conteúdo demanda não só o recurso à prévia manifestação do Poder Judiciário, e sim à decisão judicial precisa.

Diante da sensibilidade desses dados, o acesso ao aparelho telefônico por terceiro deve ser promovido com cautela tanto da forma de visualização quanto dos limites do que se pode ver e em quais situações. Não pela proteção à propriedade do telefone, mas do que ele contém e até do que representa: a garantia de livre comunicação e de transmissão e guarda de dados, sem interferências de terceiros ou do Estado.

Diante da pluralidade de bens jurídicos a serem tutelados, forçoso reconhecer que a comunicação por meio de telefone, seja ela materializada por voz, imagem ou escrita, possui desníveis no plano constitucional. Numa primeira concepção sobre o tema, o aparelho celular é resguardado pelo sigilo de comunicações telefônica e de dados, aqui compreendida a forma telemática, e passível de quebra por decisão judicial, para fins de prova em investigação criminal ou em instruções penais, na forma da Lei de Interceptações Telefônicas posteriormente editada, por força do prescrito no art. 5º, XII, da Constituição Federal.

Os ditames da Lei nº 9.296/1996, todavia, encontram limite na comunicação em processo de transmissão, que não pode ser captada de outra forma, sob pena de perecimento. E, nesse sentido, importante o registro de que a imposição ao acusado de disponibilização de ligações no modo viva-voz não pode ser confundida com a interceptação autorizada judicialmente. Aliás, esse modo informal de escuta é taxado como ilícito pelo Superior Tribunal de Justiça desde 2017, em prol da proteção contra a autoincriminação, tal como decidido no precedente exarado no Recurso Especial nº 1.630.097/RJ (Brasil, 2017).

Quanto aos demais dados transmitidos ou comunicados pelo aparelho celular, a saída, como proposto por Mendes e Branco (2021), está em repensar o sigilo das comunicações telefônicas como mecanismo a propiciar a liberdade de manifestação do pensamento. Ou, como proposto por Badaró (2010), como "[...] mecanismo de salvaguarda do direito à liberdade de manifestação do pensamento de forma reservada [...]".

E se é possível ponderar que o pensamento externado pelo uso do telefone, na perspectiva do art. 5º, XII, da CF/1988, tutela a comunicação em si, forçoso reconhecer que os demais dados armazenados em aparelhos telefônicos não possuem uma proteção tão clara assim no ordenamento jurídico pátrio. Aliás, em relação às comunicações já finalizadas, armazenadas no aparelho celular e não mais passíveis de interceptação, defendem Antonialli *et al.* (2019) que não há sequer consenso sobre o dispositivo constitucional aplicado, sobre os requisitos de padrão probatório de eventual decisão judicial de quebra de sigilo ou sobre a possibilidade de emprego da busca e apreensão como regime jurídico de obtenção de informações armazenadas nos celulares.

Em razão do eloquente silêncio do legislador constitucional e ordinário, a proteção dos dados disponíveis nos mencionados aparelhos, sejam eles decorrentes de comunicações pretéritas ou de outros elementos relativos ao conteúdo da mensagem, passou a ser amparada pela proteção à privacidade e à intimidade, na forma do art. 5º, X, da Carta Magna, como vem reconhecendo a jurisprudência das Cortes Superiores do País.

E, nesse sentido, defende Costa Júnior (2019, p. 127) que "[...] a cláusula de jurisdição continua necessária diante da inevitável subsunção com o inciso X do mesmo dispositivo [...]". Referida tese é corroborada pela edição do Marco Civil da Internet que, nos termos do art. 7º, III, impôs a exigência de ordem judicial para a quebra de sigilo de comunicações armazenadas,

produzidas ou gravadas em meios eletrônicos intermediados pela internet, forma majoritária de comunicação via *smartphone*.

Sob o ponto de vista constitucional, pois, há nítida distinção entre as garantias da intimidade e da privacidade (inciso X), quando comparadas ao sigilo de comunicações (inciso X), que demanda tanto a reserva jurisdicional (expressão "salvo, no último caso, por ordem judicial") quanto a legal (nos termos do vernáculo "na forma que a lei estabelecer"). Referida diferença implica a concretização do acesso estatal por indispensável lei prévia, não servindo a tanto a direta autorização constitucional (Souza, 2020, p. 409). A lei prévia sempre seria recomendável, mesmo na proteção da intimidade e privacidade, mas sua exigência constitucional se dá tão somente na proteção ao sigilo das comunicações.

Em consonância com esse entendimento, observa Souza que a obrigação de prévia autorização judicial, fruto da reserva constitucional de jurisdição, é limitada pela Constituição Federal de 1988 apenas à proteção da inviolabilidade do domicílio, do sigilo das comunicações e da vedação das prisões arbitrárias, direitos fundamentais elencados como mais relevantes pelo Poder Constituinte Originário. Dessa forma, em prol da reserva constitucional da jurisdição, compete ao Poder Judiciário dar a primeira e a última palavra sobre eventual relativização dos referidos direitos (Souza, 2020, p. 406-407).

No acesso e proteção aos dados digitais armazenados nos aparelhos celulares, passíveis de busca e apreensão, sem os limites típicos de proteção da interceptação telefônica ou telemática, coube à jurisprudência brasileira a definição dos limites e dos requisitos de admissibilidade, inclusive quanto à reserva de jurisdição. Assim surge o exame do dado digital.

1.2 Definição de prova digital

Alerta Doneda (2019, p. 136) que o dado, ainda que possa ser representado por uma informação, não se confunde com este, pois antecede-a, tratando-se de um conhecimento inventado antes mesmo da própria interpretação.

De igual modo, Hoffmann-Riem observa que, no campo da teoria da informação, os dados, compostos de sinais ou símbolos criados e transportados por meios tecnológicos, não possuem um significado em si. Defende-os, todavia, como juridicamente importantes, a ponto de serem tutelados por

leis de proteção específica porque "[...] o significado é atribuído a eles quando entram em um processo de comunicação de informações por um remetente e geração de informações pelo destinatário, ou seja, tornam-se o objeto da comunicação [...]" (Hoffmann-Riem, 2021, p. 13-14).

Em consonância com o posicionamento do doutrinador alemão, é possível compreender a concepção de dado por meio da reprodução do conteúdo do art. 5º, I, da Lei nº 13.709/2018, popularmente conhecida como LGPD – Lei Geral de Proteção de Dados, que descreve o dado pessoal como "[...] informação relacionada a pessoa natural identificada ou identificável [...]" (Brasil, 2021).

Anote-se ainda que a LGPD distingue o dado pessoal, acima descrito, daqueles pessoais sensíveis e anonimizados, nos termos do art. 5º, II e III, da norma em referência. Os primeiros guardam informações de natureza extremamente íntima e que merecem ser resguardados acima de tudo, versando sobre questões de raça, religião, opinião política, orientação filosófica, religiosa e sexual, informações genéticas, de saúde e biometria. Os demais tratam de elementos informativos pessoais protegidos por regras de anonimato, impossibilitando a identificação do sujeito por métodos razoáveis e disponíveis de filtragem.

Demonstrada a relevância do dado originário para o processo de comunicação e delimitado o objeto das informações que compõem os dados pessoais, nos termos da lei brasileira, o conceito de dado digital passa a ser complementado por uma abordagem técnica, que permite entender a especificidade da comunicação pela via digital.

Conforme classificação tripartite apresentada por Kist (2019, p. 110), os elementos de informação digitais são compostos por dados de base, tráfego ou de conteúdo. O primeiro relaciona-se aos elementos cadastrais fornecidos pelo usuário do serviço de telecomunicação e de informações técnicas que permitam sua conexão à rede, como número de acesso, IP, *login* e senha. Diante de sua instrumentalidade, referidas informações possuem menor grau de proteção, sendo passíveis de obtenção por autoridades administrativas ou por órgãos de persecução penal, independentemente de prévia autorização judicial, na forma do art. 10, § 3º, da Lei nº 12.965/2014 e art. 15 da Lei nº 12.850/2013, respectivamente.

Por sua vez, os dados de tráfego são aqueles produzidos de forma automática pelo sistema em razão do processo de transmissão da comunicação, englobando informações sobre os usuários (nome, número, en-

dereço) e sobre a comunicação promovida (duração, horário, volume de dados produzidos, forma de transmissão da mensagem) e localização dos equipamentos utilizados.

Os dados de localização, verdadeira subespécie dos referidos dados de tráfego, ganham especial relevância no campo das buscas e apreensões de provas digitais porque, de acordo com sua precisão, podem certificar a posição geográfica exata do aparelho celular (latitude, longitude, altitude), o sentido de deslocamento e até mesmo a quais estruturas de telecomunicação está se conectando (Santos, 2004, p. 48), a exemplo das ERBs – Estações Radio Base ou dispositivos de conexão *wi-fi* que encontra pelo caminho.

Traçado o panorama técnico dos dados digitais, de forma assertiva, observa Kist que compõem o objeto da comunicação tanto os componentes anteriores tratados, que desempenham elementos funcionais da mensagem transmitida em si, quanto os dados de conteúdo, que materializam não só o diálogo, como também a própria comunicação (Kist, 2019, p. 111-112).

Na escala de gradação da tipologia apresentada, os últimos merecem maior tutela porque, além de identificar emissores e receptores da comunicação, revelam o real teor dessa interação, seja por meio de elementos textuais, imagens, vídeos ou áudios. Diante de sua natureza reveladora, são protegidos, juntamente com os dados de tráfego, pelas regras de inviolabilidade das comunicações e de sigilos profissionais (Santos, 2004, p. 45).

Feitas essas considerações sobre as informações pessoais e técnicas que compõem o que denominamos de dado digital, é possível enunciar a prova produzida nesse âmbito tecnológico como "[...] qualquer tipo de informação que possa ser extraída de sistemas de computadores ou de outros dispositivos digitais e que possa ser usada para ou refutar uma ofensa ou violação de política [...]" (Maras, 2015, p. 76 – tradução livre).

E, dentro dessa proposta, também deve ser considerada válida a enunciação proposta por Thamay e Tamer (2020, p. 33) de prova digital como "[...] meio de demonstrar a ocorrência de um fato ocorrido em meio digital, ou que tem no meio digital um instrumento de demonstração de determinado fato de seu conteúdo [...]".

Mais do que a formalização de um conceito estanque, a enunciação do que seja uma prova digital é importante para a seara processual penal porque permite ao intérprete compreender a complexidade de informações coletadas de dispositivos tecnológicos como os *smartphones*, vistos não

mais como um telefone, como também como microcomputadores que produzem toda sorte de informações, com maior ou menor grau de intimidade.

Assim, por todo o exposto, não se pode limitar referida concepção de prova digital ao arquivo de foto ou à mensagem postada em um aplicativo de conversas, facilmente depreendidas pela simples visualização. Dessa forma, a compreensão da referida prova deve agregar em seu conceito o local de sua extração, importante referência para aferir o grau de autenticidade, integridade e de respeito à cadeia de custódia, assim como a perspectiva plural do dado a ela relacionada, apta a captar tanto o conteúdo quanto informações técnicas de extrema valia para a instrução probatória.

2 A OBTENÇÃO DA PROVA DIGITAL ORIUNDA DE TELEFONE CELULAR NO CONTEXTO DA PRISÃO EM FLAGRANTE

A prisão em flagrante, descrita nos arts. 301 e seguintes do Código de Processo Penal, constitui medida de natureza pré-cautelar, por meio da qual o particular pode e o agente estatal deve, diante da certeza visual da prática de um delito, restringir a liberdade do autor do fato mediante voz de prisão, colocando-o à disposição do Poder Judiciário para posterior análise criteriosa do preenchimento dos requisitos do *periculum libertatis* e do *fumus comissi delicti* (Lopes Júnior, 2021, p. 260).

Essa possibilidade de comprovação direta pelo sentido da visão delimita o conceito de flagrante delito que, nos termos do art. 302 do CPP, depende da certeza visual do crime (Brasil, 1941). E, para instrumentalizar a comprovação dessa fundada suspeita de que um crime foi praticado, faz-se necessária a coleta pela autoridade policial de evidências, independentemente de autorização judicial – com claro intento probatório (reunir elementos) e de segurança na prisão.

Como alerta Lopes Júnior (2021, p. 230), essa concepção abstrata do que seja fundada suspeita, resquício do autoritarismo da época da publicação do Código, acaba por permitir que a autoridade policial aborde e reviste indivíduos sem critérios claros, o que pode permitir direcionamento para alvos específicos, com potencial discriminatório ou de perseguição pessoalizada. Ressalta o autor, inclusive, que referidos abusos, ainda que passíveis de responsabilização na forma da Lei nº 13.869/2019, incredulamente são frequentemente referendados pelo Poder Judiciário.

Sobre a dificuldade de conceituação da fundada razão que autoriza a busca e a apreensão, o Supremo Tribunal Federal já havia debatido a possibilidade de dar-se contorno à atuação policial em casos de flagrante delito por ocasião do julgamento do Recurso Extraordinário nº 603.616/RO (Brasil, 2015). Muito embora o tema tenha sido abordado no contexto de ingresso em domicílio sem autorização judicial em hipóteses de flagrante por crime permanente, no caso submetido à técnica da repercussão geral, a Corte Suprema já havia observado que a atuação do agente estatal movido pelas fundadas razões deve estar adstrita à exigência de justificação da atuação da polícia por meio de controle a ser exercido *a posteriori* pelo Poder Judiciário, sob pena de nulidade da prova e de responsabilidade disciplinar, civil e penal.

Com a popularização da tecnologia, as afrontas verificadas no cotidiano brasileiro ganharam um novo capítulo na discussão da prevalência da eficiência probatória estatal em desfavor do respeito aos direitos fundamentais. Considerando o conhecimento público de que o aparelho de telefonia móvel hoje é carregado por boa parte da população e que seu uso é cada vez mais intenso, não tardou para que o acesso ao seu conteúdo fosse promovido de forma rotineira como pontapé de toda sorte de investigações.

Assim, além da prática da revista nas vestes e nos automóveis dos suspeitos, referendadas pelo Código de Processo Penal, as fundadas suspeitas passaram a ser fundamento para ação do Estado-policial de realizar a devassa de aparelhos telefônicos, analisados no local do possível flagrante sem qualquer critério, direcionando a autoridade policial para uma atuação exitosa apenas após o conhecimento de algum dado digital revelador.

Tal como defendido por Rosa e Oliveira (2020), o elevado grau de possibilidades de levantamento de indícios propiciados pela evolução dos meios tecnológicos, por mais que aproxime a vigilância estatal de provas da verdade real dos fatos no processo penal, acaba por instrumentalizar a ação penal com elementos que seduzem o senso comum pelo conteúdo. Assim, a preocupação com a legalidade da forma de sua obtenção e, consequentemente, dos direitos violados em razão de sua obtenção em situações extremas, inverte a ordem lógica da análise da prova, de modo que a avaliação do conteúdo da prova é promovida sem grandes questionamentos sobre a validade de sua obtenção.

Além do acesso ilícito à privacidade, permite essa busca exploratória o conhecimento de dados de toda espécie, até mesmo de extremada intimida-

de, seja por fotografias e vídeos, seja pelas ligações registradas, seja mesmo por dados outros contidos no aparelho celular. Por isso, diante da sensibilidade das informações tanto do titular do aparelho quanto dos terceiros de seu convívio, tal como leciona Mendes (2019), é mister a adoção de limites claros ao que denomina de buscas subjetivas em dispositivos informáticos: sobretudo para o uso dos referidos elementos e do conhecimento de informações que não guardam relação com o objeto da fundada suspeição policial.

2.1 Da absoluta distinção entre apreensão e acesso aos dados do aparelho celular apreendido em flagrante

Depreende-se da leitura do disposto nos arts. 240 e 244 do Código de Processo Penal que a única forma de comunicação expressamente disciplinada pelo instituto da busca pessoal é a epistolar, passível de arrecadação pela autoridade policial, "[...] abertas ou não, destinadas ao acusado ou em seu poder, quando haja suspeita de que o conhecimento do seu conteúdo possa ser útil à elucidação do fato [...]" (Brasil, 1941), tal como prescreve a alínea *f* do art. 240, § 1º, da mencionada norma.

Muito embora inexista regramento específico na lei processual penal sobre a apreensão de telefones móveis, notadamente daqueles dotados de microcomputadores como os *smartphones* atualmente disponíveis no mercado, não se pode esquecer que o CPP é datado da década de 1940, quando referido serviço de telecomunicação sequer existia. E isso, por si só, demonstra o descaso do legislador com meio probatório tão complexo, relegando para a apreciação do Poder Judiciário a difícil tarefa de lidar com a casuística.

Em consonância com a crítica à deficiência de tratamento da prova digital na legislação processual penal, Gloeckner e Eilberg (2020) ressalvam que a confusão remete à própria inserção do instituto da busca e apreensão no Título VII do Código de Processo Penal, dedicado às provas. A ausência de parâmetros claros sobre os limites de prova e regime jurídico de obtenção de provas digitais, na visão dos autores, "[...] contribui enormemente para a manutenção de desalinhos e desacordos constitucionais e convencionais [...]" (Gloeckner; Eilberg, 2020), notadamente porque o instituto da busca e apreensão, a despeito de estar atrelado ao devido processo legal e ao preenchimento de auto circunstanciado detalhado, hoje se mostra ineficiente para a tutela de todos os direitos fundamentais envolvidos nessa operação.

E isso é facilmente perceptível pelo tratamento do tema na esfera do Poder Judiciário brasileiro, que precisou dirimir conflitos desde os anos 2000 sobre a compatibilidade legal do acesso ao conteúdo armazenado nos aparelhos celulares nas hipóteses de prisão em flagrante com base em interpretações extensivas e analógicas.

A título exemplificativo, a despeito da antiguidade dos dados coletados, relevante pesquisa divulgada no ano de 2019, promovida com base na amostra inicial de 183 decisões proferidas em sede revisional por 10 distintos Tribunais de Justiça do País entre 12.05.2016 e 14.09.2017, concluiu que há um tratamento díspar na jurisprudência sobre as provas extraídas de aparelhos celulares em situações de flagrante. Dentre os 37 julgados em que o acesso ocorreu após a configuração do flagrante, 73% das provas foram consideradas lícitas, 13,5% ilícitas e outras 13,5% não foram analisadas. Já nos casos em que o policial acessou os dados em operação, sem a verificação do estado de flagrância, a jurisprudência restou dividida no percentual de 50% dos 12 casos analisados (Antonialli *et al.*, 2019).

Sobre o tema, não mais se discute que a visualização de informações pessoais, sensíveis ou não, pelo indevido acesso ao conteúdo do aparelho telefônico móvel acarrete danos às garantias da intimidade e da privacidade, dos sigilos de comunicações e de dados e, até numa visão minoritária, ao domicílio digital (Dezem, 2020; Souza, 2020), tal como assegurado no art. 5º, X, XI e XII, da Carta Magna de 1988. Todavia, o ponto principal das nulidades das provas digitais oriundas desse contexto aparenta ser algo que antecede a análise de seu conteúdo: a abordagem fora das hipóteses legais ou, quando amparadas por força da reserva jurisdicional, em limites que a extrapolem.

2.2 Do panorama jurisprudencial sobre o tema

A dificuldade de balizar os limites de obtenção de provas digitais pelo agente policial no momento da apuração do flagrante pode ser visualizada na prática cotidiana e também na própria evolução jurisprudencial acerca do tema. Sem que se pretenda esgotar o histórico das decisões judiciais proferidas pelos Tribunais Superiores pátrios, com apoio nos principais precedentes ecoados pela doutrina especializada e reverberados pelas decisões judiciais do Superior Tribunal de Justiça e do Supremo Tribunal Federal, o presente tópico promoverá uma breve síntese dos caminhos trilhados pela

jurisprudência sobre as provas digitais arrecadadas de aparelhos celulares até a presente data.

Data de 2006 um dos registros mais antigos sobre a dificuldade de distinção entre apreensão e acesso ao conteúdo do aparelho celular. À época, quando a função principal do dispositivo era a comunicação telefônica, ao julgar o *Habeas Corpus* nº 66.368/PA, considerou o Superior Tribunal de Justiça como válido o acesso aos registros das últimas chamadas pela autoridade policial (Brasil, 2006).

A controvérsia sobre o reconhecimento de quebra de sigilo das comunicações telefônicas foi afastada pelo ministro relator, de forma sucinta, sob o argumento de que o conhecimento dos registros telefônicos não se confunde com o do conteúdo das conversas efetuadas pelo aparelho. Pelo contrário, a checagem da lista de chamadas efetuadas e recebidas no aparelho do suspeito derivaria do dever de cautela geral de arrecadação de elementos informativos na forma prescrita no art. 6º, II e III, do Código de Processo Penal (Brasil, 2006). Pelo que se concluiu da análise do referido julgado, a preocupação da Corte restou limitada à definição do que seria um registro telefônico e de seu impacto em eventual reconhecimento da quebra de sigilo telefônico pelo acesso do agente policial às informações sem prévio amparo judicial.

Em contexto fático semelhante, o Supremo Tribunal Federal também concluiu, no ano de 2012, que o acesso aos registros das últimas chamadas de telefones não configuraria quebra de sigilo telefônico, oportunidade na qual a Corte distinguiu a diferença de tutela entre comunicação telefônica e de registros telefônicos. Na ocasião, a Suprema Corte, nos autos do *Habeas Corpus* nº 91.867/PA, observou que o art. 5º, XII, da Constituição Federal visa proteger a comunicação de dados, e não os dados *per si*, sob pena de inviabilidade de qualquer espécie de investigação criminal.

Em seu voto, o Ministro Gilmar Mendes, relator do *writ*, traçou importantes considerações sobre a distinção entre a apreensão do aparelho celular pela autoridade policial, nos termos do art. 6º do CPP, identificado como meio material indireto da prova, e o efetivo acesso às informações contidas no telefone (registros telefônicos) ou àquelas cadastradas na respectiva empresa de telefonia. E simplifica a distinção ao assentar que "[...] o dado, como no caso, mera combinação numérica, *de per si* nada significa, apenas um número de telefone [...]" (Brasil, 2012), razão pela qual não ha-

veria nenhuma violação à intimidade ou à privacidade do agente criminoso que teve o celular vasculhado pela autoridade policial.

Depreende-se da análise dos dois precedentes acima citados, intensamente debatidos pela doutrina especializada, que a construção do emprego da prova digital extraída dos aparelhos celulares era atrelada ao conhecimento pela autoridade pública de registros telefônicos. Isso porque a proteção auferida pela inviolabilidade do sigilo de comunicações, prescrita no art. 5º, XII, da Constituição Federal, era compreendida como forma de tutelar o ato de se comunicar, e não os dados isoladamente considerados. Assim, acessar, buscar e apreender o telefone celular nas hipóteses de prisão em flagrante era visto pela jurisprudência tanto do Superior Tribunal de Justiça como do Supremo Tribunal Federal como providência legitimada pela previsão do art. 6º do CPP.

Com a evolução dos referidos dispositivos, o conhecimento dos números registrados no histórico de chamadas ou na agenda dos celulares, equiparados ao conhecimento de um papel com anotações encontrado nas vestes do suspeito, perdeu espaço para a nova realidade dos aparelhos de telefonia móvel. Aquele celular, antes limitado ao recebimento e efetivação de ligações telefônicas, transformou-se em verdadeiro computador portátil, migrando sua função originária pela popularização do uso de aplicativos de troca de conversas textuais instantâneas, dentre outras funcionalidades hábeis a facilitar a vida cotidiana.

Data de 2016 importante julgado proferido pela Corte Superior de Justiça, que constitui um marco no tratamento do tema da obtenção de provas por meio do acesso ao conteúdo armazenado nos *smartphones*. Conforme consignado pelo relator do Recurso Ordinário em *Habeas Corpus* nº 51.531/RO, a despeito da possibilidade de acesso, os dados contidos no celular dependem necessariamente de prévia autorização judicial motivada, sob pena de violação ao sigilo telefônico e de dados prescritos no art. 5º, X e XII, da Constituição Federal, dos arts. 1º e 5º da Lei de Interceptações Telefônicas, do art. 3º, V, da Lei de Organização dos Serviços de Telecomunicações (Lei nº 9.472/1997) e art. 7º, I, II e III, do Marco Civil da Internet (Brasil, 2016).

Ainda que se trate de decisão datada pelo ininterrupto avanço da tecnologia, considerando especialmente que o uso de mensageiros instantâneos hoje engloba ligações telefônicas via VoIp e também de chamada de vídeo, o paradigma possui extrema relevância por colocar em destaque a

necessidade de proteção dos dados contidos no aparelho celular em contexto semelhante ao atual, sobremaneira por abranger a questão da proteção dos dados como comunicação complexa, que engloba múltiplas funções de uso.

Digno de nota que referido precedente trouxe a lume tormentosa conclusão, anteriormente afastada nos paradigmas já apreciados: a visualização do conteúdo disposto no *smartphone* pela autoridade policial, diante de sua sensibilidade, afronta a garantia constitucional da privacidade e da intimidade e deve ser precedida de autorização judicial para ser considerada válida (art. 5º, X, da CF/1988 e art. 7º do Marco Civil da Internet). Superada, portanto, a limitação da análise do acesso ao aparelho celular àquilo que era registro ou comunicação propriamente dita, com a consequente demarcação da garantia à privacidade como pedra angular da proteção das comunicações e informações armazenadas nos *smartphones*.

Importante registrar que a ordem identificada no referido acórdão era a tentativa de desatrelar o caso concreto à análise promovida pelo Supremo Tribunal Federal nos autos do *Habeas Corpus* nº 91.867/PA (Brasil, 2012) diante da revolução tecnológica que propiciou que o aparelho celular dispusesse de muito mais elementos do que os telefones existentes no ano de 2012. Com o objetivo de situá-lo historicamente, o Ministro Rogério Schietti Cruz ponderou que o elevado repositórios desses aparelhos permitiria a importação da doutrina americana do direito probatório de terceira geração, que trata do regramento de provas tecnológicas altamente invasivas, dependentes de autorização judicial prévia para sua obtenção (Brasil, 2016, p. 16).

Outro ponto de destaque, levantado pela Ministra Maria Thereza de Assis Moura (Brasil, 2016, p. 27), foi a consignação do argumento de que o acesso *incontinenti* ao conteúdo do telefone móvel também visa atender outro parâmetro constitucional: o direito à segurança pública, prescrito no art. 144 da CF/1988. Dessa forma, tal como defendido pela Magistrada, é importante relembrar que a proteção individual do direito à privacidade do suspeito, como todo direito fundamental, não goza de tutela absoluta. Assim, diante do conflito de interesses entre os órgãos de persecução penal e o titular do aparelho, deve ser posto em prática o juízo de ponderação de interesses, ressalvadas situações excepcionais que autorizariam o imediato acesso ao conteúdo do aparelho, tal como ressalvado pela ministra:

> [...] Não descarto, de forma absoluta, que, a depender do caso concreto, caso a demora na obtenção de um mandado judicial pudesse trazer prejuízos concretos à investigação ou especialmente à vítima do delito, mostre-se possível admitir a validade da prova colhida através do acesso imediato aos dados do aparelho celular. Imagine-se, por exemplo, um caso de extorsão mediante sequestro, em que a polícia encontre aparelhos celulares em um cativeiro recém-abandonado: o acesso incontinenti aos dados ali mantidos pode ser decisivo para a libertação do sequestrado. [...] (Brasil, 2016, p. 27)

Ao cabo, a Corte Superior de Justiça concluiu pela ilicitude da prova decorrente da apreensão de aparelho celular pela autoridade policial, promovida por ocasião da prisão em flagrante, sem autorização judicial, por meio da qual diversos dados pessoais foram devassados pelo agente estatal após o acesso do conteúdo do celular e, especialmente, das mensagens travadas por meio do aplicativo WhatsApp.

Por todo o exposto, a partir da publicação do referido precedente do Superior Tribunal de Justiça, verifica-se que a longa jornada da evolução jurisprudencial brasileira caminha para a flexibilização de toda a informação armazenada nos *smartphones*, desde que preenchidos os requisitos de mandado de busca e apreensão ou de autorização de acesso durante a prisão em flagrante pelo usuário. Fora dessas situações, admite-se ainda o acesso imediato quando registrado elemento de urgência, tal como a hipótese de extorsão mediante sequestro em que é preciso localizar, com urgência, a vítima e seu cativeiro, como destacado, *obter dictum*, no julgamento do Recurso Ordinário em *Habeas Corpus* nº 51.531/RO (Brasil, 2016, p. 26).

Digno de nota que o precedente acima apontado permanece atual e passou a direcionar a atuação do Poder Judiciário de todo o País na análise das provas extraídas de dados armazenados em telefones celulares pelas autoridades policiais. Em consonância com esse entendimento, deve ser registrado que, no ano de 2020, a 2ª Turma do Supremo Tribunal Federal proferiu decisão semelhante à acima debatida, concluindo também pela impossibilidade de visualização de conversas armazenadas no aplicativo de mensagens instantâneas WhatsApp que levaram à busca domiciliar e à consequente condenação do paciente nos autos do *Habeas Corpus* nº 168.052/SP (Brasil, 2020).

Tal como promovido pela Corte Superior de Justiça, a necessidade de autorização judicial foi o argumento principal para consignar que o acesso aos dados armazenados no aparelho celular, em específico mensagens

particulares trocadas via mensageiro instantâneo, deve respeitar a garantia fundamental à privacidade e à intimidade. Ressaltou o Ministro Gilmar Mendes à época que, diferentemente do sustentado no precedente de 2012 (*Habeas Corpus* nº 91.867/PA), a publicação do Marco Civil da Internet e as alterações substanciais do contexto fático, sobremaneira a nova visão do telefone como microcomputador portátil, justificam a mutação constitucional na interpretação dos direitos fundamentais prescritos no art. 5º, X e XII, da CF/1988 (Brasil, 2020, p. 12).

Dessa forma, concluiu a 2ª Turma do Supremo Tribunal Federal, com apoio no voto do Ministro Gilmar Mendes, que, a despeito da possibilidade de acesso ao referido conteúdo de forma emergencial pela autoridade policial, em prol da garantia à privacidade e com base no princípio da proporcionalidade, naquele caso concreto, o acesso ao referido material inserido no *smartphone* dependeria de prévia autorização judicial (Brasil, 2020, p. 12).

A despeito da relevante decisão da 2ª Turma do Supremo Tribunal Federal, que expressamente referencia no acórdão a publicação do Marco Civil da Internet como aprimoramento das normas que tutelam dados armazenados nos aparelhos telefones móveis, o advento de normas de tutela de dados digitais nesse período (*v.g.*, Marco Civil da Internet e Lei Geral de Proteção de Dados, em 2014 e 2018, respectivamente) pouco possibilitou avanços no regramento de acesso do conteúdo nas hipóteses excepcionais do flagrante delito.

Aliás, resolvida a questão da observância da reserva jurisdicional, observam Silva e Moura (2020, p. 420) que "[...] não se sedimentou ainda se, na hipótese de necessidade de mandado judicial, seria preciso um de interceptação telefônica ou de busca e apreensão. Este parece mais coerente, ante a capacidade do aparelho celular de apresentar inúmeras funções [...]".

Casuísticas à parte, o desenvolvimento da obrigatoriedade de decisão judicial motivada ou de autorização, nas hipóteses de flagrante, para apreensão e posterior acesso aos dados inseridos nos *smartphones*, evoluiu para a delimitação de quais dados digitais seriam passíveis de serem considerados como provas válidas para a persecução penal. Nesse sentido, de forma ilustrativa, resume a jurisprudência do Superior Tribunal de Justiça (HC 542.293/SP, 2019) que:

> [...] Os dados armazenados nos aparelhos celulares – envio e recebimento de mensagens via SMS, programas ou aplicativos de troca de mensagens,

> fotografias etc. –, por dizerem respeito à intimidade e à vida privada do indivíduo, são invioláveis, nos termos em que previsto no inciso X do art. 5º da Constituição Federal, só podendo, portanto, ser acessados e utilizados mediante prévia autorização judicial, com base em decisão devidamente motivada que evidencie a imprescindibilidade da medida, capaz de justificar a mitigação do direito à intimidade e à privacidade do agente. [...]

O precedente acima destacado, reproduzido de forma explícita em outros tantos julgados da referida Corte Superior de Justiça, descreve, com precisão, o elenco dos dados armazenados no celular mais comumente arrecadados pelo agente policial: troca de mensagens textuais e fotografias. Tal como exposto no item 2.2 do presente trabalho, contudo, um mínimo de conhecimento técnico pela referida autoridade possibilitaria o acesso a muitos outros dados relevantes, como os dados de localização.

A amplitude dos casos concretos permanece, de forma geral, adstrita às informações passíveis de visualização de forma mais rotineira, até pela limitação pertinente ao local e às condições da abordagem policial, que não podem ser tão extensas, inclusive por segurança do próprio agente. Assim, a criação de um precedente objetivo sobre o tema parece se dirigir à elucidação da distinção de efeitos jurídicos de apreensão e do acesso aos dados digitais, balizada pela obrigatoriedade ou dispensa da reserva jurisdicional.

A pacificação do tema ainda pende de resolução, vez que o Agravo em Recurso Extraordinário nº 1.042.075/RJ (Brasil, 2020), submetido à apreciação do Supremo Tribunal Federal pelo rito da repercussão geral, encontra-se suspenso desde 04.11.2020 por força de voto-vista do Ministro Alexandre de Moraes.

O caso que motivou o julgamento versa sobre o acesso ao conteúdo de aparelho celular abandonado no local do delito que possibilitou a identificação e prisão do suspeito após devassa de dados de índole privada, como fotos, agenda de contatos e lista de chamadas efetuadas.

Até o presente momento, duas teses diversas foram fixadas pelo Ministro Relator Dias Toffoli (Tema 977 da Repercussão Geral) e pelo voto-divergente do Ministro Gilmar Mendes, este último acompanhado pelo voto do Ministro Edson Fachin, nos seguintes termos, respectivamente (Brasil, 2020):

> Tema 977: É lícita a prova obtida pela autoridade policial, sem autorização judicial, mediante acesso a registro telefônico ou agenda de contatos de ce-

lular 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).

Tese divergente: 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 e XX).

Pelo cenário acima exposto, a tese inicial é de licitude do acesso ao que foi validamente apreendido, no limite de registros (e não comunicações) ou dados de maior privacidade. Seria no máximo aferível como condição o exame casuístico de proporcionalidade, com a aferição da necessidade e adequação da medida, sempre respeitados dados mais invasivos da intimidade e privacidade.

A tese divergente não distingue a espécie de informações registradas no aparelho celular, todas elas passíveis da proteção de dados e intimidade, a dependerem, assim, da prévia autorização judicial para o acesso. Aqui a tendência seria compreender que, nos casos de prisão em flagrante, a licitude das provas digitais extraídas de aparelhos celulares dependeria do cumprimento de um requisito importante: o acesso ao conteúdo do dispositivo dependerá de prévia ordem judicial fundamentada e específica, proferida com amparo nos elementos do princípio da proporcionalidade (necessidade e adequação da medida), nos direitos fundamentais à intimidade, à privacidade e ao sigilo das comunicações e dados dos indivíduos.

Por fim, tal como alertado por Kist (2019, p. 404-406), a abordagem policial, seja fruto de busca e apreensão ou de busca pessoal decorrente do flagrante, deverá ser formalizada pelo agente público de forma oficial e extensa. Referida condição de validade do ato permitirá tanto o controle da atuação do Estado-investigador quanto da validade da cadeia de custódia e da legalidade do dado digital apreendido pelo Poder Judiciário, seja na fase inquisitorial, no recebimento da denúncia ou queixa ou, por fim, por ocasião da sentença resolutiva da ação penal.

CONSIDERAÇÕES FINAIS

De todo o exposto no presente trabalho, é possível aferir que a preocupação com os limites e as possibilidades legais de acesso ao aparelho ce-

lular, tanto do suspeito em situação de flagrante delito quanto daquele que teve o celular recolhido por força de decisão judicial, carece de contornos mais claros.

Isso porque o telefone móvel, dada a convergência de informações, passou a abarcar dados digitais de distintas espécies, ora submetidos à cláusula constitucional da reserva jurisdicional, ora à reserva legal derivada das normas infraconstitucionais. E, dentro desse contorno, a distinção do nível de tutela dos dados extraíveis do aparelho celular, sejam eles técnicos como os de base ou de tráfego, em fluxo de transmissão ou relativos às comunicações já finalizadas, acaba por criar distorções em situações limites de apuração da responsabilidade penal.

Prova disso é a irrefutável conclusão de que o que se avançou até agora deve ser creditado mais ao esforço interpretativo do Poder Judiciário, sobretudo das Cortes Superiores brasileiras, que buscaram contornar a discussão sobre a limitação da tutela do art. 5º, XII, da CF/1988, sobretudo pela impossibilidade de aplicação da Lei de Interceptações Telefônicas às comunicações finalizadas e armazenadas nos aparelhos celulares.

A solução proposta pelo Superior Tribunal de Justiça no ano de 2016, por ocasião do julgamento do Recurso Ordinário em *Habeas Corpus* nº 51.531/RO, mostrou que os dados digitais padeciam de proteção constitucional para serem efetivamente tutelados pelo Estado brasileiro. Assim, o entendimento de respeito à privacidade como limite à devassa dos dados digitais disponíveis nos referidos dispositivos mostrou-se importante instrumento de defesa dos titulares de telefonia móvel, especialmente pela conclusão de que os dados disponíveis nos telefones celulares não poderiam ser taxados como de livre acesso às autoridades da persecução penal, sem critérios de admissibilidade ou proporcionalidade.

Referida escolha de fundamentação, por sua vez, acompanhou o próprio processo de desenvolvimento tecnológico, abandonando a discussão do condicionamento da validade da prova digital à mera distinção entre registros telefônicos e comunicação e guarda de dados, como consagrado no paradigma do Supremo Tribunal Federal datado de 2012 (*Habeas Corpus* nº 91.867/PA). A própria evolução dos aparelhos tecnológicos e o desuso das ligações telefônicas tradicionais pela sociedade, tal como constatado pela pesquisa do Instituto Brasileiro de Geografia e Estatística (Brasil, 2021, p. 1), encaminharam a discussão para outros patamares constitucionais que,

por óbvio, não podem mais estar adstritos apenas à inviolabilidade do sigilo de comunicação telefônica ou telemática.

Noutro viés, a despeito da publicação de diplomas normativos importantes para a temática da prova digital, como o Marco Civil da Internet (Lei nº 12.965/2014) e a Lei Geral de Proteção de Dados (Lei nº 13.709/2018), a ausência de regramento na legislação processual penal das providências a serem adotadas pelo agente estatal cria um cenário nebuloso para o acesso ao celular durante a medida pré-cautelar da prisão em flagrante.

A possibilidade de apreensão de aparelhos telefônicos móveis e a possibilidade de acesso a seus dados deve ser objeto de diretrizes claras, preferencialmente legais e prévias, sempre seguidas de regramentos administrativos detalhados para conhecimento, treinamento e adequação da ação investigatória nas ações policiais.

O mero risco de dano irreparável à intimidade e privacidade, do usuário do aparelho e de terceiros, bem ressalta a imprescindível cautela na proteção máxima possível, como garantia fundamental absoluta. Perigosa é a pretensão de superação da obrigatoriedade da reserva legal de jurisdição, de modo a permitir a devassa do conteúdo físico do celular no momento do flagrante, mesmo em situações excepcionais e com proporcionalidade – o debate na Suprema Corte será marco definidor do tema.

Ainda que busque atender o direito difuso à segurança pública prescrito no art. 144 da CF/1988, a devassa ilícita e desarrazoada do aparelho celular configura abuso estatal, justificador de responsabilização civil, penal e administrativa. E, pelo conceito de proporcionalidade, inadmissível será, de todo modo, a devassa que esgote todo o histórico particular, sem limite temporal, das comunicações travadas pelo usuário do aparelho.

Assim, como forma de superar o entendimento de hierarquia de comunicações em transmissão ou armazenadas no aparelho, ou mesmo de que a tutela da privacidade e da intimidade, derivadas da reserva legal, sejam inferiores às protegidas pela Lei de Interceptações Telefônicas, vê-se, com bons olhos, a definição ao menos de *standards* probatórios jurisprudenciais que enunciem mais claramente a tutela dos dados armazenados nos *smartphones*.

Conclui-se, portanto, que o universo das provas digitais oriundas de aparelhos celulares ainda possui novos horizontes a serem descobertos, notadamente porque a tipologia dos dados digitais e a própria tecnologia

passam a permitir possibilidade da descoberta de variadas informações de grande valia à eficiência da persecução. É um caminhar de validade probatória do novo, que precisará ser eficiente, mas que não poderá conviver com o desprezo às garantias do íntimo, do privado, do que é dado digital, com proporcionalidade e controle jurisdicional.

REFERÊNCIAS

ANTONIALLI, Dennys; ABREU, Jacqueline; MASSARO, Heloisa; LUCIANO, Maria. Acesso de autoridades policiais a celulares em abordagens: retrato e análise da jurisprudência de tribunais estaduais. *Revista Brasileira de Ciências Criminais*, Brasília, n. 154, p. 177-214, abr. 2019.

BADARÓ, Guilherme. *Interceptação de comunicações telefônicas e telemáticas*: limites ante o avanço da tecnologia. Ano 2010. Disponível em: http://www.badaroadvogados.com.br/gustavo-badaro-interceptacao-de-comunicacoes-telefonicas-e-telematicas-limites-ante-o-avanco-da-tecnologia-ano-2010.html. Acesso em: 21 mar. 2020.

BARRETO, Alessandro Gonçalves. *Cibercrimes e seus reflexos no Direito brasileiro*. Salvador: JusPodivm, 2020.

BRASIL. Constituição da República Federativa do Brasil de 1988. Brasília: Presidência da República, [1988]. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acesso em: 15 set. 2021.

_____. Decreto-Lei nº 3.689, de 3 de outubro de 1941. Código de Processo Penal. Brasília: Presidência da República, [1941]. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del3689compilado.htm. Acesso em: 18 set. 2021.

_____. Lei nº 9.296, de 24 de julho de 1996. Lei de Interceptações Telefônicas. Brasília: Presidência da República, [1996]. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9296.htm. Acesso em: 16 set. 2021.

_____. Lei nº 12.965, de 23 de abril de 2014. Marco Civil da Internet. Brasília: Presidência da República, [2014]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 14 set. 2021.

_____. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados. Brasília: Presidência da República, [2018]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 16 set. 2021.

_____. Lei nº 14.155, de 27 de maio de 2021. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para tornar mais graves os crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela internet; e o Decreto-Lei nº 3.689, de 3 de outubro de 1941 (Código de Processo Penal), para definir a competência em modalidades de

estelionato. Brasília: Presidência da República, [2021]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/L14155.htm. Acesso em: 17 nov. 2021.

_____. Superior Tribunal de Justiça (5ª Turma). *Habeas Corpus* nº 66.368/PA. Código de Processo Penal. Denúncia formulada com base no acesso ao registro de chamadas do telefone sem autorização judicial. Pacientes: Davi Resende Soares e Lindomar Resende Soares. Impetrado: Câmaras Criminais Reunidas do Tribunal de Justiça do Estado do Pará. Relator: Min. Gilson Dipp, 5 de junho de 2007. Disponível em: https://scon.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=200602016074&dt_publicacao=29/06/2007. Acesso em: 26 set. 2021.

_____. Superior Tribunal de Justiça (6ª Turma). Recurso Ordinário em *Habeas Corpus* nº 51.531/RO. Código de Processo Penal. Lei nº 12.965/2014. Lei nº 9.472/1997. Lei nº 9.296/1996. Acesso ao registro de conversas de WhatsApp pela polícia em telefone sem autorização judicial. Recorrente: Leri Souza e Silva. Recorrido: Ministério Público do Estado de Rondônia. Relator: Min. Nefi Cordeiro, 19 de abril de 2016. Disponível em: https://scon.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=201402323677&dt_publicacao=09/05/2016. Acesso em: 26 set. 2021.

_____. Superior Tribunal de Justiça (6ª Turma). *Habeas Corpus* nº 542.293/SP. Constituição Federal de 1988. Lei nº 12.965/2014. Lei nº 9.472/1997. Prisão em flagrante. Acesso ao conteúdo de mensagens em telefone sem autorização judicial. Paciente: Jhones de Fátima Oliveira Alves. Impetrado: Ministério Público do Estado de São Paulo. Relator: Min. Rogerio Schietti Cruz, 17 de dezembro de 2019. Disponível em: https://scon.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=201903222817&dt_publicacao=19/12/2019. Acesso em: 26 set. 2021.

_____. Superior Tribunal de Justiça (6ª Turma). Recurso Especial nº 1.630.097/RJ. Constituição Federal de 1988. Lei nº 10.792/2003. Código de Processo Penal. Convenção Americana sobre Direitos Humanos. Prova. Conversa travada por função viva-voz do celular. Dúvidas quanto ao consentimento. Autoincriminação. Descoberta inevitável. Recorrente: Ministério Público do Estado do Rio de Janeiro. Recorrido: Marcelo de Azevedo de Freitas. Relator: Min. Joel Ilan Paciornik, 18 de abril de 2017. Disponível em: https://scon.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=201602602406&dt_publicacao=28/04/2017. Acesso em: 26 set. 2021.

_____. Supremo Tribunal Federal (Tribunal Pleno Virtual). Agravo em Recurso Extraordinário nº 1.042.075/RJ. Licitude de provas decorrentes do acesso por autoridade policial de aparelho celular em situação de flagrante independentemente de prévia autorização judicial. Agravante: Ministério Público do Estado do Rio de Janeiro. Recorrido: Guilherme Carvalho Farias. Relator: Min. Dias Toffoli, 11 de novembro de 2020. Disponível em: http://portal.stf.jus.br/processos/detalhe.asp?incidente=5173898. Acesso em: 26 set. 2021.

_____. Supremo Tribunal Federal (2ª Turma). *Habeas Corpus* nº 168.052/SP. Licitude de provas decorrentes do acesso por autoridade policial de aparelho celular em situação de flagrante independentemente de prévia autorização judicial. Violação de domicílio. Nulidade de provas. Paciente: Rodrigo Ricardo Laurindo. Impetrado: Tribunal de Justiça do Estado de São Paulo. Relator: Min. Gilmar Mendes, 20 de outubro de 2020. Disponível em: https://jurisprudencia.stf.jus.br/pages/search/sjur437471/false. Acesso em: 21 nov. 2021.

DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*: fundamentos da Lei Geral de Proteção de Dados. 2. ed. rev. e atual. São Paulo: Thomson Reuters Revista dos Tribunais, 2019.

GLOECKNER, Ricardo Jacobsen; EILBERG, Daniela Dora. Busca e apreensão de dados em telefones celulares: novos desafios diante dos avanços tecnológicos. *Revista Brasileira de Ciências Criminais*, v. 156, p. 353-393, jun. 2019.

HOFFMANN-RIEM, Wolfgang. *Teoria geral do direito digital*: transformação digital: desafios para o direito. Rio de Janeiro: Forense, 2021.

KIST, Dario José. *Prova digital no processo penal*. Leme: JH Mizuno, 2019.

LOPES JÚNIOR, Aury Celso Lima. *Direito processual penal*. 18. ed. São Paulo: Saraiva Educação, 2021. *E-book*.

MARAS, Marie-Hellen. *Computer forensics*: cybercriminals, laws and evidence. 2. ed. Burlington: Jones & Bartlett Learning, 2015.

MENDES, Carlos Hélder C. Furtado. Dado informático como fonte de prova penal confiável (?): apontamentos procedimentais sobre a cadeia de custódia digital. *Revista Brasileira de Ciências Criminais*, v. 161, p. 131-161, nov. 2019.

MENDES, Gilmar Ferreira; BRANCO, Paulo Gustavo Gonet. *Curso de direito constitucional*. 16. ed. São Paulo: Saraiva Educação, 2021. *E-book*.

ROSA, Alexandre Morais da; OLIVEIRA, Daniel Kessler. Novas tecnologias probatórias e o papel do julgador no processo penal. *Revista Brasileira de Ciências Criminais*, v. 167, p. 239-261, maio 2020.

SANTOS, Cristina Máximo dos. As novas tecnologias da informação e o sigilo das telecomunicações. *Revista do Ministério Público*, Lisboa: Sindicato dos Magistrados do Ministério Público, n. 25, p. 44-53, jul./set. 2004.

SILVA, Gabriela Buarque Pereira; MOURA, Tâmara. Prisão em flagrante e o acesso aos dados do celular: desafios entre a privacidade e a investigação criminal. In: ARAS, Vladimir Barros *et al.* (Org.). Associação Nacional dos Procuradores da República (Brasil). *Proteção de dados pessoais e investigação criminal*. Brasília: ANPR, p. 399-430.

SOUZA, Rodrigo Telles de. A exigência de autorização judicial para acesso ao conteúdo de telefone móvel apreendido: uma ampliação da garantia à inviolabilidade domiciliar incompatível com o sistema jurídico brasileiro.

In: SALGADO, Daniel Resende; KIRCHER, Luís Felipe Schneider; QUEIROZ, Ronaldo Pinheiro de (Coord.). *Altos estudos sobre a prova no processo penal*. Salvador: JusPodivm, p. 405-429, 2020.

THAMAY, Rennan; TAMER, Mauricio. *Provas no direito digital*: conceito da prova digital, procedimentos e provas digitais em espécie. São Paulo: Thomson Reuters Brasil, 2020.

Sobre a autora e o autor:

Amanda Matias Cavalcante de Oliveira | *E-mail:* amandamatias.jus@gmail.com

Mestre em Direito pela Universidade Católica de Brasília. Especialista em Direito Constitucional pelo Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa. Bacharel em Ciências Jurídicas pelo Centro Universitário de Brasília. Servidora do Ministério Público Federal.

Néfi Cordeiro | *E-mail:* nefi.cordeiro@msn.com

Doutor e Mestre em Direito pela UFPR, com concentração na área criminal. Professor Universitário – Gradução e Pós-Gradução, *Lato* e *Stricto Sensu*. Graduado em Engenharia Civil (PUCPR). Ex-integrante do Ministério Público e Magistratura estadual no Paraná. Juiz e Desembargador

Data de submissão: 30 de setembro de 2021.
Data de aceite: 2 de dezembro de 2021.