VOTO - MINISTRO FLÁVIO DINO:

I. CONSIDERAÇÕES INICIAIS

Inicialmente a jurisprudência desta Suprema Corte, com base na distinção doutrinária sustentada por Tercio Sampaio Ferraz Júnior, no sentido da inviolabilidade das comunicações não se estender aos dados registrados, rejeitou a proteção constitucional a dados registrais. Nesse sentido, trago à colação precedente da Segunda Turma:

> "HABEAS CORPUS. NULIDADES: (1) INÉPCIA DA DENÚNCIA; (2) ILICITUDE DA PROVA PRODUZIDA DURANTE O INQUÉRITO POLICIAL; VIOLAÇÃO DE REGISTROS TELEFÔNICOS DO CORRÉU, EXECUTOR DO CRIME, SEM AUTORIZAÇÃO JUDICIAL; (3) ILICITUDE DA PROVA DAS INTERCEPTAÇÕES TELEFÔNICAS DE CONVERSAS DOS ACUSADOS COM ADVOGADOS, PORQUANTO ESSAS GRAVAÇÕES OFENDERIAM O DISPOSTO NO ART. 7º, II, DA LEI 8.906/96, QUE GARANTE O SIGILO DESSAS CONVERSAS. VÍCIOS NÃO CARACTERIZADOS. ORDEM DENEGADA.
>
> 1. Inépcia da denúncia. Improcedência. Preenchimento dos requisitos do art. 41 do CPP. A denúncia narra, de forma pormenorizada, os fatos e as circunstâncias. Pretensas omissões — nomes completos de outras vítimas, relacionadas a fatos que não constituem objeto da imputação — não importam em prejuízo à defesa.
>
> **2. Ilicitude da prova produzida durante o inquérito policial - violação de registros telefônicos de corréu, executor do crime, sem autorização judicial. 2.1 Suposta ilegalidade decorrente do fato de os policiais, após a prisão em flagrante do corréu, terem realizado a análise dos últimos registros telefônicos dos dois aparelhos celulares apreendidos. Não ocorrência. 2.2 Não se confundem comunicação telefônica e registros telefônicos, que recebem, inclusive, proteção jurídica distinta. Não se pode interpretar a cláusula do artigo 5º, XII, da CF, no sentido de proteção aos dados enquanto registro, depósito registral. A proteção constitucional é da comunicação de dados e não dos dados. 2.3 Art. 6º do CPP: dever da autoridade policial de proceder à coleta do material comprobatório da prática da infração penal. Ao proceder à**

pesquisa na agenda eletrônica dos aparelhos devidamente apreendidos, meio material indireto de prova, a autoridade policial, cumprindo o seu mister, buscou, unicamente, colher elementos de informação hábeis a esclarecer a autoria e a materialidade do delito (dessa análise logrou encontrar ligações entre o executor do homicídio e o ora paciente). Verificação que permitiu a orientação inicial da linha investigatória a ser adotada, bem como possibilitou concluir que os aparelhos seriam relevantes para a investigação. 2.4 À guisa de mera argumentação, mesmo que se pudesse reputar a prova produzida como ilícita e as demais, ilícitas por derivação, nos termos da teoria dos frutos da árvore venenosa (fruit of the poisonous tree), é certo que, ainda assim, melhor sorte não assistiria à defesa. É que, na hipótese, não há que se falar em prova ilícita por derivação. Nos termos da teoria da descoberta inevitável, construída pela Suprema Corte norte-americana no caso Nix x Willioms (1984), o curso normal das investigações conduziria a elementos informativos que vinculariam os pacientes ao fato investigado. Bases desse entendimento que parecem ter encontrado guarida no ordenamento jurídico pátrio com o advento da Lei 11.690/2008, que deu nova redação ao art. 157 do CPP, em especial o seu § 2º.

3. Ilicitude da prova das interceptações telefônicas de conversas dos acusados com advogados, ao argumento de que essas gravações ofenderiam o disposto no art. 7º, II, da Lei n. 8.906/96, que garante o sigilo dessas conversas. 3.1 Nos termos do art. 7º, II, da Lei 8.906/94, o Estatuto da Advocacia garante ao advogado a inviolabilidade de seu escritório ou local de trabalho, bem como de seus instrumentos de trabalho, de sua correspondência escrita, eletrônica, telefônica e telemática, desde que relativas ao exercício da advocacia. 3.2 Na hipótese, o magistrado de primeiro grau, por reputar necessária a realização da prova, determinou, de forma fundamentada, a interceptação telefônica direcionada às pessoas investigadas, não tendo, em momento algum, ordenado a devassa das linhas telefônicas dos advogados dos pacientes. Mitigação que pode, eventualmente, burlar a proteção jurídica. 3.3 Sucede que, no curso da execução da medida, os diálogos travados entre o paciente e o advogado do corréu acabaram, de maneira automática, interceptados, aliás, como qualquer outra conversa direcionada ao ramal do paciente. Inexistência, no caso, de relação jurídica cliente-advogado. 3.4 Não cabe aos policiais

> executores da medida proceder a uma espécie de filtragem das escutas interceptadas. A impossibilidade desse filtro atua, inclusive, como verdadeira garantia ao cidadão, porquanto retira da esfera de arbítrio da polícia escolher o que é ou não conveniente ser interceptado e gravado. Valoração, e eventual exclusão, que cabe ao magistrado a quem a prova é dirigida.
>
> 4. Ordem denegada."
>
> (**HC 91.867/PA**, Rel. Min. Gilmar Mendes, Segunda Turma, j. 24.4.2012, DJe 20.9.2012)

Anoto, contudo, que este precedente é de 2012. De lá pra cá, muita coisa mudou! O desenvolvimento tecnológico se acentuou, as comunicações por meio de mensagens de texto e aplicativos foram facilitadas, o tráfego de dados aumentou e os smartphones se popularizaram.

No século XXI, parte significativa da vida privada da maior parte dos brasileiros descortina-se por meio dos respectivos celulares. Mais do que estações para fazer e receber chamadas, ou meros espelhos negros quando inativos dentro dos bolsos e bolsas, os telefones celulares, uma vez ativados em nossas mãos, convertem-se em janelas luminosas para a nossa intimidade.

Uma estante inteira de álbuns de fotografia da família se comprime em um único aplicativo. A porta giratória da agência bancária cedeu lugar à senha digitada na tela, à impressão digital coletada detrás dela ou ao reconhecimento facial. No mesmo dispositivo, a porta de entrada para mensagens que respondemos e as que ainda nem visualizamos. Os textos lidos e os textos por ler. As conversas que tivemos, os planos futuros e os desejos íntimos compartilhados com amigos, na crença de que ninguém mais está a ouvi-los, lê-los ou vê-los. Os objetos antes guardados nas gavetas dos escritórios e prateleiras das salas de estar - nessa condição protegidos de invasão arbitrária (art. 5º, XI, CF) - hoje converteram-se em impulsos eletromagnéticos que transitam, por cabos ou ondas, entre os circuitos eletrônicos dos celulares e sistemas de armazenamento chamados de "nuvem".

Os aparelhos de telefone móvel guardam muito mais da vida privada e intimidade de seus proprietários do que as portas e paredes,

gavetas e armários do domicílio de cada um deles, cuja inviolabilidade não temos dificuldade alguma em reconhecer.

A hipótese, portanto, a meu juízo, é de verdadeira mutação constitucional. Passo a explicar.

II. DIREITO À INTIMIDADE, À PRIVACIDADE E À VIDA PRIVADA

É certo que a Constituição da República qualifica como invioláveis, na condição de direitos fundamentais da personalidade, a intimidade, a vida privada, a honra e a imagem das pessoas, conferindo-lhes especial proteção, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação (art. 5º, X, CF).

Tal como a liberdade de manifestação do pensamento — e seus desdobramentos como a liberdade de expressão intelectual, artística e científica e a liberdade de imprensa —, o assim chamado direito à privacidade (right to privacy)—e os seus consectários direito à intimidade, à honra e à imagem — também emana do reconhecimento de que a personalidade individual merece ser protegida em todas as suas manifestações.

Apesar da muita tinta despendida a respeito, o conceito de privacidade permanece, nas palavras de Richard Posner, elusivo (vago, impreciso) e mal definido[1]. No clássico artigo The Right to Privacy, escrito a quatro mãos pelos juízes da Suprema Corte dos Estados Unidos Samuel D. Warren e Louis D. Brandeis, sugere-se a relação de tal estado de coisas com o fato de as mudanças políticas, sociais e econômicas demandarem incessantemente o reconhecimento de novos direitos, impondo, de tempos em tempos, a redefinição da exata natureza e extensão da proteção à privacidade do indivíduo[2].

Em uma abordagem contemporânea e integradora, pode-se dizer que o direito à privacidade visa a proteger a subjetividade emergente, dinâmica, dos esforços de valores comerciais e governamentais para tornar indivíduos e comunidades fixos, transparentes e predizíveis. Ele protege as práticas (...) através das quais a capacidade de

autodeterminação se desenvolve[3].

Assim compreendida a privacidade, a conclusão inarredável é a de que a sua proteção é uma característica estrutural indispensável das sociedades democráticas.

O direito à privacidade tem como objeto, na quase poética expressão de Warren e Brandeis, a privacidade da vida privada. O escopo da proteção são os assuntos pessoais, em relação aos quais, a princípio, não se vislumbra interesse público legítimo na sua revelação, e que o indivíduo prefere manter privados.

III. DIREITO À PROTEÇÃO DE DADOS PESSOAIS E NECESSIDADE DE AUTORIZAÇÃO JUDICIAL PARA ACESSO A TAIS ELEMENTOS

Vale observar, ainda, que os maiores desafios contemporâneos à proteção da privacidade têm a ver com a proliferação de sistemas de vigilância e a emergência das mídias sociais, juntamente com a manipulação de dados pessoais em redes computacionais por inúmeros, e frequentemente desconhecidos, agentes públicos e privados.

Nesse contexto, pertinente, ainda, a contribuição de Alan Westing à doutrina jurídica da privacidade no mundo contemporâneo, ao caracterizar a estrutura desse direito como controle sobre os usos da informação pessoal. Nesse sentido, a privacidade, afirma, é a pretensão de indivíduos, grupos ou instituições de determinarem para si quando, como e em que extensão a informação sobre eles será comunicada a outros (WESTING, Alan. Privacy and Freedom, 1968).

É por essa razão que, na quadra atual, a privacidade não assume meramente a feição individualista, enquanto "direito a ser deixado em paz" na expressão cunhada pelos Justices da Suprema Corte americana, mas também *o direito de manter o controle sobre suas próprias informações e de determinar como a privacidade é alcançada e, em última instância, como o direito de escolher livremente seu modo de vida*. (RODOTÀ, Stefano. In diritto diavere. Roma: Laterza, 2012, p. 321.)

Tal concepção do direito à privacidade está alinhada com o reconhecimento do seu papel social na própria preservação da personalidade e no desenvolvimento da autonomia individual.

A privacidade produz um ambiente seguro para que pensamentos, ideias e opiniões sejam compartilhados em círculos limitados e testados antes de serem publicamente expostos. Permite, dito de outro modo, o espaço de liberdade onde se processa a experimentação necessária ao progresso social.

Com efeito, a facilidade com que a privacidade será protegida ou exposta transforma-se à medida em que evoluem as tecnologias da informação e da comunicação.

Se, de um lado, sucedem-se ou alternam-se tecnologias de comunicação — carta, telégrafo, telefone, telefone móvel, redes sociais, aplicativos de mensagens — de outro, adaptam-se e apuram-se as tecnologias voltadas à vigilância — interceptação, raio-x, acesso furtivo a sistemas, desencriptação etc.

Nessas condições, não podem a hermenêutica constitucional e o desenvolvimento legislativo ficarem alheios a essas mudanças no tempo, tendo em vista a manutenção do equilíbrio entre a proteção da privacidade e os limites da atuação do Estado. É que a Constituição, assim como o estado da técnica, institui um conjunto de restrições à atuação do Estado. Como analisa o professor Lawrence Lessig, em ensaio seminal acerca das implicações do desenvolvimento das tecnologias de comunicação em rede para a interpretação constitucional, é a combinação de constrangimentos tecnológicos e constrangimentos legais que define, em um dado momento, as restrições efetivamente enfrentadas pelo Estado, caso este deseje intervir em determinado aspecto do domínio privado de um cidadão[6].

Longe de ter seu significado usurpado, a Constituição escrita no mundo analógico há de ser traduzida para o mundo digital, de modo a preservar, neste, os interesses, os direitos e as liberdades que originalmente preservava. Desse modo, o sentido das palavras da Constituição e o alcance da proteção constitucional são preservados em face da mudança do contexto.

Ainda em 1967, no paradigmático julgamento do caso Katz v. United States[7],a Suprema Corte dos EUA superou a sua jurisprudência anterior para assentar que a escuta e a gravação de comunicações telefônicas equivalem aos procedimentos de busca e apreensão e, como tais, sujeitam-se aos limites traçados pela Quarta Emenda à Constituição daquele país, que essencialmente assegura o direito à inviolabilidade da intimidade, da vida privada e do domicílio contra certas modalidades de ações estatais arbitrárias.

A proteção constitucional contra a invasão estatal arbitrária passou a se estender, na redefinição empreendida pela Corte sob a liderança do Chief Justice Earl Warren, a qualquer expectativa razoável de privacidade. Transcrevo:

> "A atividade do Estado pelo qual foram ouvidas e registradas eletronicamente as palavras do peticionário violou a privacidade na qual ele justificadamente se fiava ao utilizar a cabine telefônica, e constitui, portanto, uma 'busca e apreensão' na acepção da Quarta Emenda. O fato de o dispositivo eletrônico empregado para atingir tal objetivo não ter atravessado a parede da cabine não tem nenhuma relevância constitucional"[8].

A Constituição brasileira, a fim de instrumentalizar tais direitos, prevê, no art. 5°, XII, a inviolabilidade do sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução penal.

O art. 5°, XII, da CF protege, cumpre salientar, a comunicação dos dados, o evento pelo qual dados ou informações são transmitidos ou recebidos do ponto A ao ponto B. Já a proteção do sigilo de dados armazenados tem amparo no art. 5°, X, da CF, como decorrência do direito à privacidade.

Destaco, nesse contexto, que no julgamento da ADI. 6.387/DF, o plenário desta Suprema Corte, a partir da interpretação sistemática da Constituição Federal, notadamente dos arts. 1°, III, 5°, X, XII, LXXII,

compreendeu existir, em nosso ordenamento jurídico, como direito autônomo, a proteção a dados pessoais, inclusive, os armazenados:

> "MEDIDA CAUTELAR EM AÇÃO DIRETA DE INCONSTITUCIONALIDADE. REFERENDO. MEDIDA PROVISÓRIA № 954/2020. EMERGÊNCIA DE SAÚDE PÚBLICA DE IMPORTÂNCIA INTERNACIONAL DECORRENTE DO NOVO CORONAVÍRUS (COVID-19). COMPARTILHAMENTO DE DADOS DOS USUÁRIOS DO SERVIÇO TELEFÔNICO FIXO COMUTADO E DO SERVIÇO MÓVEL PESSOAL, PELAS EMPRESAS PRESTADORAS, COM O INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA.FUMUS BONI JURIS. PERICULUM IN MORA. DEFERIMENTO.
>
> 1. Decorrências dos direitos da personalidade, o respeito à privacidade e à autodeterminação informativa foram positivados, no art. 2º, I e II, da Lei n° 13.709/2018 (Lei Geral de Proteção de Dados Pessoais), como fundamentos específicos da disciplina da proteção de dados pessoais.
>
> 2. Na medida em que relacionados à identificação - efetiva ou potencial - de pessoa natural, o tratamento e a manipulação de dados pessoais hão de observar os limites delineados pelo âmbito de proteção das cláusulas constitucionais assecuratórias da liberdade individual (art. 5º, caput), da privacidade e do livre desenvolvimento da personalidade (art. 5º, X e XII), sob pena de lesão a esses direitos. O compartilhamento, com ente público, de dados pessoais custodiados por concessionária de serviço público há de assegurar mecanismos de proteção e segurança desses dados.
>
> 3. O Regulamento Sanitário Internacional (RSI 2005) adotado no âmbito da Organização Mundial de Saúde exige, quando essencial o tratamento de dados pessoais para a avaliação e o manejo de um risco para a saúde pública, a garantia de que os dados pessoais manipulados sejam "adequados, relevantes e não excessivos em relação a esse propósito" e conservados apenas pelo tempo necessário."
> (artigo 45, § 2º, alíneas "b" e "d").
>
> 4. Consideradas a necessidade, a adequação e a proporcionalidade da medida, não emerge da Medida Provisória n° 954/2020, nos moldes em que editada, interesse público legítimo no compartilhamento dos dados pessoais dos usuários dos serviços de telefonia.

5. Ao não definir apropriadamente como e para que serão utilizados os dados coletados, a MP n° 954/2020 desatende a garantia do devido processo legal (art. 5º, LIV, da CF), na dimensão substantiva, por não oferecer condições de avaliação quanto à sua adequação e necessidade, assim entendidas como a compatibilidade do tratamento com as finalidades informadas e sua limitação ao mínimo necessário para alcançar suas finalidades.

6. Ao não apresentar mecanismo técnico ou administrativo apto a proteger, de acessos não autorizados, vazamentos acidentais ou utilização indevida, seja na transmissão, seja no tratamento, o sigilo, a higidez e, quando o caso, o anonimato dos dados pessoais compartilhados, a MP n° 954/2020 descumpre as exigências que exsurgem do texto constitucional no tocante à efetiva proteção dos direitos fundamentais dos brasileiros.

7. Mostra-se excessiva a conservação de dados pessoais coletados, pelo ente público, por trinta dias após a decretação do fim da situação de emergência de saúde pública, tempo manifestamente excedente ao estritamente necessário para o atendimento da sua finalidade declarada.

8. Agrava a ausência de garantias de tratamento adequado e seguro dos dados compartilhados a circunstância de que, embora aprovada, ainda não vigora a Lei Geral de Proteção de Dados Pessoais (Lei n° 13.709/2018), definidora dos critérios para a responsabilização dos agentes por eventuais danos ocorridos em virtude do tratamento de dados pessoais. O fragilizado ambiente protetivo impõe cuidadoso escrutínio sobre medidas como a implementada na MP n° 954/2020.

9. O cenário de urgência decorrente da crise sanitária deflagrada pela pandemia global da COVID-19 e a necessidade de formulação de políticas públicas que demandam dados específicos para o desenho dos diversos quadros de enfrentamento não podem ser invocadas como pretextos para justificar investidas visando ao enfraquecimento de direitos e atropelo de garantias fundamentais consagradas na Constituição.

10. Fumus boni juris e periculum in mora demonstrados. Deferimento da medida cautelar para suspender a eficácia da Medida Provisória n° 954/2020, a fim de prevenir danos irreparáveis à intimidade e ao sigilo da vida privada de mais

de uma centena de milhão de usuários dos serviços de telefonia fixa e móvel.

11. Medida cautelar referendada".

(**ADI 6387-MC-Ref/DF,** Ministra Rosa Weber, Tribunal Pleno, j. 07.5.2020, DJe 12.11.2020)

Em âmbito infraconstitucional, para que dúvidas não pairassem quanto ao alcance das garantias constitucionais, no que se refere ao ambiente digital, o art. 3º, II, da Lei 12.965/2014, reafirmou a proteção da privacidade como princípio norteador da disciplina do uso da internet no Brasil. Os seus arts. 7º e 8º consagram o papel essencial do acesso à internet para o pleno exercício da cidadania, assegurando, entre outros direitos, a inviolabilidade e o sigilo do fluxo de comunicações do usuário, salvo por ordem judicial, na forma da lei (art. 7°, II), bem como a inviolabilidade e o sigilo das suas comunicações privadas armazenadas, salvo por ordem judicial (art. 7º, III).

O art. 5º, XII, da CF, a seu turno, não dá margem a exegese outra que não a de que a lei somente pode autorizar a suspensão do sigilo de comunicações privadas para fins de investigação criminal ou instrução processual penal. Trata-se de limite ao alcance da atividade legislativa, adstrita que está aos contornos traçados na Lei Maior. Ainda que a legislação não estampe no próprio texto a limitação do seu alcance, é dever do intérprete atentar para a regência constitucional ao aplicar a lei no caso concreto.

Entendo, nessa linha de raciocínio, que a adequada exegese dos arts. 7º, II e III, e 10, § 2", do Marco Civil da Internet, à luz do art. 5º, XII, da Constituição da República, conduz à conclusão inequívoca de que, à maneira das comunicações telefônicas, a inviolabilidade do sigilo das comunicações realizadas, seja o seu fluxo sejam as armazenadas, pela internet somente pode ser excepcionada, por ordem judicial, no âmbito da persecução penal. Na expressa dicção da Constituição, para fins de investigação criminal ou instrução processual penal.

Consabido que a função de defesa dos direitos fundamentais constrange o Estado a não intervir, salvo situações excepcionais, especialmente quando exista a suspeita da prática de ilícitos. A intervenção estatal deve ser episódica e fundamentada, a possibilitar o

devido controle pelas instâncias competentes. Não assento – e nem poderia – a inviolabilidade absoluta dos dados pessoais, pelo contrário. Reconheço, contudo, **a necessidade de prévia decisão judicial** para acessar os elementos informacionais relativos a comunicações realizadas via internet, seja o seu fluxo, sejam as armazenadas.

O que estou a afirmar, portanto, é que o acesso a tais dados pessoais pelo aparato estatal investigador depende da avaliação prévia do Poder Judiciário, de modo a aferir, à luz do princípio da proporcionalidade, a presença de todos os requisitos previstos na legislação processual penal, tal como a existência de justa causa, a necessidade da medida, a pertinência do acesso, tudo a diminuir os impactos atinentes à restrição do direito fundamental em questão.

Nesse sentido, ressalto que a Segunda Turma desta Suprema Corte, ao julgamento do HC 168.052/SP, em anunciada revisitação de jurisprudência, entendeu imprescindível a necessidade de autorização judicial para acesso a conversas via Whatsapp:

> "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/SP,Rel. Min. Gilmar Mendes, Segunda Turma,j. 20.10.2020,DJe 02.12.2020)

Apesar de não ter sido unânime a decisão — os Ministros Gilmar Mendes, Ricardo Lewandowski e Celso de Mello votaram pela concessão da ordem e os Ministros Edson Fachin e Cármen Lúcia[9] votaram pela denegação da ordem — sequer houve divergência explícita quanto à necessidade de autorização judicial para referido acesso.

Entendo que não podemos nos afastar da realidade fática. É pouco crível que a autoridade policial, sem autorização judicial, acessará um determinado aparelho celular e se limitará a verificar a agenda de contatos e os registros telefônicos nele constantes. Possibilitar o acesso a tais dados levaria a enormes problemas práticos, com a necessidade de solução casuística e, em consequência, com pouca segurança jurídica.

O processo penal precisa equilibrar os direitos fundamentais do investigado com os direitos das vítimas e as expectativas da sociedade na correta aplicação do Direito.

Não há dúvidas de que o acesso ao celular de qualquer investigado ou suspeito atinge diretamente o seu direito fundamental à intimidade e privacidade.

Procurar criar distinções sobre o que atinge ou não a privacidade (como por exemplo agenda telefônica) além de criar uma complexidade fática desnecessária (como garantir quais partes do celular que foram efetivamente achadas?), viola o núcleo essencial do direito de privacidade (não há dúvidas que, atualmente, para uma parcela significativa da população, existem no aparelho celular mais informações sensíveis e íntimas do que na residência).

O tema está sujeito à reserva de jurisdição. Para o acesso ao conteúdo do celular é indispensável a prolação de uma decisão judicial fundamentada.

Contudo, realço que, normalmente, os aparelhos celulares são apreendidos no início da investigação, razão pela qual seria bastante complexo exigir que o juiz delimitasse, nesse primeiro momento, a abrangência do acesso por parte da autoridade policial.

Não se trata de naturalizar uma fishing expedition, mas apenas do fato de que a limitação inicial da investigação tem efeitos deletérios na busca de elementos informativos. Por exemplo, em uma investigação de uma organização criminosa essa limitação prévia impede a descoberta de outros coautores ou partícipes, bem como o esclarecimento da forma de atuação da organização.

Não se olvide que essa exigência de que a decisão judicial delimite **previamente** a abrangência de acesso dos dados inviabiliza, ainda, o encontro fortuito de provas, **no entanto a jurisprudência da Corte é no sentido da validade da serendipidade.**

No caso de inquéritos relativos a crimes multitudinários, por exemplo, a exigência de que o julgador, ao deferir o acesso ao celular, delimite sua abrangência, na prática, tem um potencial muito grande de inviabilizar o sucesso da investigação.

Por outro lado, deve-se fazer uma análise relativa à apreensão do celular e preservação dos dados.

A apreensão do celular e de qualquer elemento informativo que possa ajudar a esclarecer o fato tem previsão legal no art. 6º do CPP.

A Constituição expressamente exige a reserva de jurisdição para a entrada em domicílio, prisão (salvo flagrante) e interceptação das comunicações telefônicas.

Não há previsão de reserva de jurisdição para a apreensão de aparelhos celulares que estejam na cena de um crime ou com pessoa presa em flagrante. Seria inviabilizar o trabalho da polícia exigir tal medida, frustrando um direito fundamental, qual seja o relativo à segurança pública.

Igualmente a necessidade de ordem judicial para o "congelamento" de dados não encontra previsão expressa na Constituição. A Emenda 115 ao incluir o inciso LXXXIX no art. 5º da CF, delegou ao legislador ordinário o tratamento do tema.

Não temos, ainda, uma LGPD penal, mas é fundamental destacar que não existe equivalência entre preservar e acessar dados.

O "congelamento" ou preservação apenas impede que o titular dos dados elimine aquela prova. Não existe, nesse momento, conhecimento do conteúdo das informações preservadas.

Não há direito fundamental de destruir provas. No que se refere aos dados, a regra é sua livre disposição, todavia no curso de uma investigação criminal, tal conduta é contrária ao Direito, ao ponto de a legislação autorizar inclusive a prisão preventiva.

Há o respeito do direito fundamental de autodeterminação informacional na medida em que não há acesso, sem ordem judicial, ao conteúdo dos dados preservados.

Ademais, como Bruno Calabrich destacou, em sua tese de doutorado, a simples preservação de dados não afeta o direito fundamental dos titulares dos dados:

> "Não há que se confundir a preservação dos dados de conteúdo com a impossibilidade absoluta de disposição do titular sobre esses dados. O titular dos dados poderá copiar, divulgar publicamente, enviar para terceiros e até apagar, se quiser, o conteúdo armazenado. Entretanto, o provedor tem a obrigação de preservar o registro daqueles dados, tal qual uma fotografia tirada no momento em que emitida a ordem de conservação (daí ser impertinente qualquer comparação com o congelamento de ativos de uma pessoa investigada". (CALABRICH, Bruno. Tratamento de dados pessoais e persecução penal: A construção de limites para a eficiente tutela de direitos fundamentais, Universidade de Brasília, 2024, p 212)

O reconhecimento da importância, imprescindibilidade e urgência da preservação de dados na investigação criminal foi positivado com a internalização da Convenção de Budapeste (Decreto nº 11491, de 12 abril de 2023) que prevê expressamente:

> Título 2 - Preservação expedita de dados armazenados em computador
>
> Artigo 16 - Preservação expedita de dados de computador
>
> 1. Cada Parte adotará medidas legislativas e outras providências necessárias para permitir que a autoridade competente ordene ou obtenha a expedita preservação de dados de computador especificados, incluindo dados de tráfego, que tenham sido armazenados por meio de um sistema de computador, especialmente quando haja razões para admitir

que os dados de computador estão particularmente sujeitos a perda ou modificação.

2. Se a Parte der efeito ao parágrafo 1 acima por meio de uma ordem a uma pessoa para preservar dados de computador determinados que estejam sob sua posse, detenção ou controle, o Estado adotará medidas legislativas e outras providências necessárias para obrigar essa pessoa a preservar e manter a integridade desses dados de computador pelo período de tempo necessário, até o máximo de 90 (noventa) dias, a fim de permitir à autoridade competente buscar sua revelação. Qualquer Parte pode estipular que tal ordem possa ser renovada subsequentemente.

3. Cada Parte adotará medidas legislativas e outras providências necessárias para obrigar o detentor dos dados ou terceiro encarregado da sua preservação, a manter em sigilo o início do procedimento investigativo por um período estabelecido na sua legislação interna.

4. Os poderes e procedimentos referidos neste Artigo estão sujeitos aos Artigos 14 e 15.

Importante destacar que a urgência é para a preservação, pois o acesso necessariamente dependerá de ordem judicial.

A Lei 12965/14 prevê expressamente a possibilidade de a autoridade policial ou o Ministério Público requerer, sem a intervenção do Judiciário, o "congelamento' dos dados.

Art. 13. Na provisão de conexão à internet, cabe ao administrador de sistema autônomo respectivo o dever de manter os registros de conexão, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 1 (um) ano, nos termos do regulamento.

§ 1º A responsabilidade pela manutenção dos registros de conexão não poderá ser transferida a terceiros.

§ 2º A autoridade policial ou administrativa ou o Ministério Público poderá requerer cautelarmente que os registros de conexão sejam guardados por prazo superior ao previsto no caput.

§ 3º Na hipótese do § 2º, a autoridade requerente terá o prazo de 60 (sessenta) dias, contados a partir do requerimento, para ingressar com o pedido de autorização judicial de acesso aos registros previstos no caput.

> § 4º O provedor responsável pela guarda dos registros deverá manter sigilo em relação ao requerimento previsto no § 2º, que perderá sua eficácia caso o pedido de autorização judicial seja indeferido ou não tenha sido protocolado no prazo previsto no § 3º.
>
> § 5º Em qualquer hipótese, a disponibilização ao requerente dos registros de que trata este artigo deverá ser precedida de autorização judicial, conforme disposto na Seção IV deste Capítulo.
>
> § 6º Na aplicação de sanções pelo descumprimento ao disposto neste artigo, serão considerados a natureza e a gravidade da infração, os danos dela resultantes, eventual vantagem auferida pelo infrator, as circunstâncias agravantes, os antecedentes do infrator e a reincidência.

O termo "cautelarmente' inserto no §2º do art.13 está em seu sentido comum, não no sentido técnico de uma decisão ou processo cautelar, mas de um requerimento urgente.

O desenho legal garante a última palavra ao Judiciário sobre o acerto da decisão do "congelamento" e a exigência de decisão judicial para o acesso (§5º do art. 13 da lei 12965/14).

Ferrajoli, no livro Direito e Razão (3.ed. RT, 2002, pág. 38), destaca que "*se uma justiça penal integralmente com verdade constitui uma utopia, uma justiça penal completamente sem verdade equivale a um sistema de arbitrariedade*". É indispensável, então, encontrar um equilíbrio entre os extremos. A melhor forma de compatibilização dos diversos interesses legítimos no tema é exigir reserva jurisdicional para acesso ao aparelho celular apreendido e, para preservar a verdade possível, não exigir decisão judicial para a apreensão, nos termos do art.6º do CPP, ou a preservação dos dados.

No caso concreto, a Polícia acessou o celular do investigado sem ordem judicial, razão pela qual se justifica a manutenção da decisão recorrida que considerou a prova obtida como ilícita.

IV CONCLUSÃO

Diante do exposto, nego provimento ao agravo em recurso

extraordinário e faço a seguinte proposta de Tese de repercussão geral para o Tema nº 977:

> "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".

É como voto.

[1] POSNER, Richard A. The Right to Privacy. Georgia Law Review. Vol. 12. N. 3, 1978.

[2] WARREN, Samuel D.; BRANDEIS, Louis D. The Right to Privacy. Harvard Law Review, Vol. IV, December 15, 1890.

[3] COHEN, Julie. What Privacy is For. Havard Law Review. Maio, 2013, tradução livre.

[4] WESTING, Alan. Privacy and Freedom, 1968.

[5]RODOTÀ, Stefano. In diritto diavere. Roma: Laterza, 2012, p. 321.

[6] LESSIG, Lawrence. Reading the Constitution in Cyberspace. 45 emory L.J. N. 3 (1996).

[7] Katz v. United States, 389 U.S. 347, 88 S. Ct. 507, 19 L. Ed. 2d 576 (1967).

[8] Katz v. United States, 389 U.S. 347, 88 S. Ct. 507, 19 L. Ed. 2d 576 (1967).

[9]Os Ministros Edson Fachin e Cármen Lúcia votaram pela denegação da ordem ao fundamento da imprescindibilidade de análise fático-probatória, o que seria inviável em sede de *habeas corpus*, tendo em vista que as instâncias ordinárias haviam assentado a existência de provas autônomas não decorrentes do acesso ao celular.