V O T O

O Senhor Ministro **Ricardo Lewandowski** (Relator): Bem reexaminados os autos, tenho que a decisão ora atacada não merece reforma ou qualquer correção, pois os seus fundamentos harmonizam-se estritamente com a jurisprudência desta Suprema Corte que orienta a matéria em questão.

Inicialmente, reafirmo que, apesar de o presente *writ* ter sido impetrado em substituição a recurso ordinário, inexiste óbice ao seu conhecimento, na linha do que decidiu o Plenário deste Supremo Tribunal no julgamento do HC 152.752/SP, relator Ministro Edson Fachin. Cito, ainda, o voto por mim proferido no julgamento do HC 164.493/PR, redator para o acórdão o Ministro Gilmar Mendes.

Na sequência, relembro que é desnecessário o revolvimento de matéria fático-probatória na hipótese, pois é incontroverso que o Ministério Público do Estado do Paraná expediu ofícios aos provedores Apple e Google, solicitando a preservação de informações nas contas dos sócios da empresa Infosolo, dentre as quais, "[…] informações cadastrais, histórico de localização e pesquisas, conteúdo de *e-mails* e *iMessages/hangouts*, fotos e nomes de contatos [...]" (documento eletrônico 2). A solicitação prévia encaminhada pelo *Parquet* determinava o congelamento dos dados desde 1º/6/2017, ao passo que o pedido de quebra de sigilo da paciente só foi submetido ao Juízo em 29/11/2019, sendo deferido em 3/12/2019 (documentos eletrônicos 3 e 4).

Por outro lado, a alegação ministerial de que os ofícios não resultaram na resposta da *Apple* e *Google* – sim essa - leva à necessidade de revolvimento fático-probatório, o que não se concebe nesta via estreita. O que se afirma nesta seara diz respeito a um procedimento ofensivo às balizas legais, para além do que é autorizado, por mais tempo do que se determina, de registros de conexão e de acesso a aplicações de internet. Então, o tema aqui versará exclusivamente sobre o que aconteceu **antes** da autorização judicial e fora do rol taxativo de hipóteses legais para a preservação da integralidade do conteúdo telemático da agravada.

Ademais, nem se diga, com a devida vênia, sobre ausência de

prejuízo. Ora, no caso concreto, o prejuízo suportado pela investigada me parece evidente, até porque já foi denunciada e tornando-se ré nos autos de uma ação penal, com todas as consequências sabidamente daí advindas. E assim o foi, ao menos em parte, em razão da ilegal impossibilidade de administrar uma vasta gama de informações íntimas/pessoais, mesmo sem que houvesse qualquer decisão judicial impondo-lhe essa proibição. Sob tal enfoque, afigura-se intuitivo que o congelamento dos dados telemáticos violou, por diversas formas, uma gama de direitos individuais da paciente.

Pois bem. De saída, sublinho que inexiste, nestes autos, **nenhuma discussão a respeito da constitucionalidade** de dispositivos da Lei 12.965/2014 (Marco Civil da Internet), tampouco da validade das inovações normativas trazidas por esse importante marco legal. Bem ao contrário, o presente *writ* discute **exclusivamente** a validade de parte – não da integralidade - da prova colhida no caso concreto, ou seja, apenas se, parcialmente, a prova arrecadada durante essa específica investigação ultrapassou ou não as prerrogativas dadas ao Ministério Público pela lei regente.

Com efeito, antes mesmo do advento da Lei Geral de Proteção de Dados Pessoais (Lei 13.709/2018), a consolidar, de forma ampla e efetiva, a preservação dessas informações de ordem subjetiva, em boa hora, o Marco Civil da Internet (Lei 12.965/2014) trouxe relevantes balizas sobre esse mesmo tema, remetendo às mais diversas problemáticas que o mundo pós-moderno impõe. Exemplo disso é a Emenda Constitucional 115/2022, que incluiu o direito à proteção dos dados pessoais, inclusive nos meios digitais, no art. 5º da Constituição Federal (LXXIX), mostrando que vive-se ainda em um momento embrionário, mas de extrema consideração e preocupação acerca do tema da privacidade no Brasil.

Ainda sobre esse ponto introdutório, ao tratar do direito à privacidade, da guarda e da disponibilização dos registros de conexão e de acesso a aplicações de internet, na forma disposta no art. 10 da Lei 12.965/2014, a doutrina especializada destaca o seguinte:

> "Fica evidente no *caput* do art. 10 da lei 12.965/14 (MCI) de forma clara, a preocupação do legislador com a privacidade. Esta que é um Direito fundamental, além de ser um direito da

personalidade, tem por regra a sua proteção, tanto de dados cadastrais, quanto dados de registro. O que revela a necessidade de que seus tratamentos e eventuais exposições, ocorram única e exclusivamente dentro das balizas e exceções legislativas. Isto posto, a privacidade encontra sua barreira restritiva, frente às requisições judiciais, é o que fica evidenciado nos parágrafos do próprio art. 10:

> '§ 1º O provedor responsável pela guarda somente será obrigado a disponibilizar os registros mencionados no *caput*, de forma autônoma ou associados a dados pessoais ou a outras informações que possam contribuir para a identificação do usuário ou do terminal, mediante ordem judicial, na forma do disposto na Seção IV deste Capítulo, respeitado o disposto no art. 7º .
>
> § 2º O conteúdo das comunicações privadas somente poderá ser disponibilizado mediante ordem judicial, nas hipóteses e na forma que a lei estabelecer, respeitado o disposto nos incisos II e III do art. 7º .
>
> § 3º O disposto no *caput* não impede o acesso aos dados cadastrais que informem qualificação pessoal, filiação e endereço, na forma da lei, pelas autoridades administrativas que detenham competência legal para a sua requisição.
>
> § 4º As medidas e os procedimentos de segurança e de sigilo devem ser informados pelo responsável pela provisão de serviços de forma clara e atender a padrões definidos em regulamento, respeitado seu direito de confidencialidade quanto a segredos empresariais.'

Pelos parágrafos 1º e 2º, que tratam tanto dos registros, como do próprio conteúdo das comunicações, temos de forma expressa, que a restrição legislativa imposta à privacidade, **se dá por meio de ordem judicial, e apenas desta forma, o sigilo pode ser quebrado e as informações expostas, sob pena de ser considerada uma prova ilícita, caso tenham acesso sem a referida ordem**.

[...]

Encontramos maior problemática, quando adentramos à inteligência do parágrafo 3º do referido artigo, pois este, traz uma exceção expressa as demais normas postas nos parágrafos anteriores, assim como ao *caput*.

O MCI excepcionou a regra da necessidade de ordem judicial, permitindo que as autoridades administrativas,

> obtenham acesso aos dados cadastrais, que informem qualificação pessoal, filiação (a fim de evitar homônimos) e endereço, mediante requisição direta, desta forma, importante se faz a necessidade de delimitar os limites desta exceção. **Fica evidente pelo texto legal, que a exceção apenas se aplica aos dados cadastrais de qualificação pessoal, filiação e endereço, qualquer pedido que extrapole os limites expressamente impostos pela letra da lei, se caracterizariam como um abuso de poder**". (Laura Porto, Disponível em: https: / /www. migalhas. com. Br/depeso/380308/reflexoes – sobre-o-art-10-do-marco- civil-da-internet-lei-12-965-14. Acesso em 27/3/2023, grifei)

Volvendo os olhos para o caso sob exame, rememoro, mais uma vez, que o debate recai sobre o ato do Ministério Público do Estado do Paraná em expedir ofícios a provedores de internet, sem autorização judicial, determinando a preservação dos dados e *IMEI*s, informações cadastrais, histórico de localização e pesquisas, conteúdo de *e-mails* e *iMessages*/*hangouts*, fotos e nomes de contatos de pessoas investigadas.

E para que não haja espaço para nenhuma dúvida sobre o que se discute no caso concreto, a lei é didática e traz todos os conceitos necessários para o deslinde da controvérsia.

Segundo o art. 13, § 2º, da Lei 12.965/2014, "a autoridade policial ou administrativa ou o Ministério Público poderá requerer cautelarmente que os **registros de conexão** sejam guardados", por prazo superior a 1 ano, cabendo à autoridade requerer a devida autorização judicial para acesso a eles no prazo de até 60 dias. O diploma é autoexplicativo, pois, permite o congelamento prévio, pelo *Parquet*, sem autorização judicial, apenas dos chamados "**registros de conexão**".

Para que fique claro, a própria lei regente dá o conceito de"**registros de conexão**". Ele está no seu art. 5º, VI, estabelecendo que eles consistem no "conjunto de informações referentes à **data e hora** de **início** e **término** de uma conexão à internet, sua **duração** e o **endereço IP** utilizado pelo terminal para o **envio e recebimento** de pacotes de dados" (grifei).

Sobre o tema, extraem-se, ainda, informações do sítio oficial da Casa Civil acerca do sentido do termo "registros de conexão":

> "Registros de conexão - IP atribuído ao computador, hora e data de início e término de sua conexão à Internet: Cada vez que um computador é conectado à Internet, ele é identificado por um número de endereço IP, que identifica aquela conexão (em alguns casos, uma mesma conexão pode ser partilhada por mais de um terminal, sendo que todos eles serão identificados na Internet pelo mesmo número IP (este é o caso dos roteadores *wifi* domésticos, por exemplo). São as empresas que prestam o serviço de conexão que atribuem aos seus usuários os endereços IP. Essas empresas, como qualquer prestadora de serviço, mantêm cadastros de seus usuários. Logo, um provedor de conexão já é capaz, hoje, de identificar seus usuários a partir do endereço IP. (CASA CIVIL. Perguntas e respostas sobre Marco Civil da Internet. Disponível em: https:// casa- civil. jusbrasil.com.br/ noticias /2816963/ perguntas-e-respostas-sobre-marco-civil-da-internet >. Acesso em 22/11/2022).

Ora, a lei autoriza ao Ministério Público o requerimento de preservação de registros de conexão - repita-se -, em conceitos legais, relativos a: (i) data e hora de início e término da conexão; (ii) a sua duração; e (iii) endereços IP utilizados pelos terminais para o envio e recebimento de pacotes de dados. Isso é tudo. Entretanto, no caso sob exame, **a acusação pleiteou muito mais aos provedores**, buscando a preservação dos "dados e *IMEI*'s coletados nas contas vinculadas aos investigados, informações cadastrais, histórico de localização e pesquisas, conteúdo de *e-mails* e *iMessages/hangouts*, fotos e nomes de contatos".

A distância entre aquilo que se pode fazer e aquilo que se fez é axiomática.

O direito de qualquer cidadão de administrar e dispor do conteúdo pessoal de *e-mails*, mensagens, contatos e históricos de localização é uma garantia individual enrijecida pelo direito à preservação da intimidade, da vida privada, da honra e da imagem das pessoas (art. 5º, X, da Constituição Federal).

Conforme destaquei na decisão recorrida,

"[…] o inciso XII do Texto Maior proclama que 'é inviolável o 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 processual penal'.

A jurisprudência desta Suprema Corte tem afirmado reiteradamente que o inciso XII do art. 5º da Carta Magna protege o sigilo das comunicações em fluxo (troca de dados e mensagens). Assenta também que o sigilo das comunicações armazenadas, como depósito registral, é tutelado pela previsão constitucional do direito à privacidade, na forma do inciso X do art. 5º, CF (cito o HC 91.867/PA, relator Ministro Gilmar Mendes). No campo infraconstitucional, o Marco Civil da Internet (Lei 12.965/2014) traça os princípios aplicáveis em nosso ordenamento, enumerados no art. 3º, tal como o da proteção da privacidade e dos dados pessoais, assegurando, outrossim, a inviolabilidade e sigilo do fluxo de suas comunicações e sigilo de suas comunicações privadas armazenadas, ressalvada ordem judicial de sua quebra (art. 7º da mencionada lei)". (págs. 8-9 do documento eletrônico 48)

Nesse ponto, no âmbito acadêmico e com apoio na doutrina de Tercio Ferraz, o Ministro Alexandre de Moraes leciona que:

"A inviolabilidade do sigilo de dados (art. 5º, XI) complementa a previsão ao direito à intimidade e vida privada (art. 5º, X), sendo ambas as previsões de **defesa da privacidade** regidas pelo **princípio da exclusividade**, que pretende assegurar ao indivíduo, como ressalta Tercio Ferraz, a

> 'sua identidade diante dos riscos proporcionados pela niveladora pressão social e pela incontrastável impositividade do poder político. Aquilo que é exclusivo é o que passa pelas opções pessoais, afetadas pela subjetividade do indivíduo e que não é guiada nem por normas nem por padrões objetivos. No recôndito da privacidade se esconde, pois, a intimidade. A intimidade não exige publicidade porque não envolve direitos de terceiros. **No âmbito da privacidade, a intimidade é o mais exclusivo dos seus direitos**'.

Dessa forma, a defesa da privacidade deve proteger o homem contra: (a) a interferência em sua vida privada, familiar

> e doméstica; (b) a ingerência em sua integridade física ou mental , ou em sua liberdade intelectual e moral; (c) os ataques à sua honra e reputação; (d) sua colocação em perspectiva falsa; (e) comunicação de fatos relevantes e embaraçosos relativos à sua intimidade; (f) o uso de seu nome, identidade e retrato; (g) a espionagem e a espreita; (h) a intervenção na correspondência; (i) a má utilização de informações escritas e orais; (j) a transmissão de informes dados ou recebidos em razão do segredo profissional." *(Direito Constitucional*. 33. ed. São Paulo: Atlas, 2017. p. 74; grifei)

Ao contrário do que afirmado pelos agravantes, a decisão impugnada afastou, sobejamente, a premissa de que o art. 13, § 2º, da Lei 12.965/2014 supostamente autorizaria a autoridade policial ou o Ministério Público a implementarem medidas semelhantes ao que fez o órgão acusatório do Paraná, ao fazer - insisto – a clara e objetiva diferenciação entre os conceitos técnicos conferidos pela legislação. Naquele *decisum* descrevi, minuciosamente, a diferença entre: (i) acesso aos **registros de conexão** (conjunto de informações referentes à data e hora de início e término de uma conexão à internet, sua duração e o endereço IP utilizado pelo terminal para o envio e recebimento de pacotes de dados); e (ii) utilização/preservação/congelamento dos **dados telemáticos** de qualquer investigado (conteúdo de *e-mail*, *iMessages*/*hangout*s, fotos, contatos, históricos, dentre outros).

Em obra dedicada ao tema, Adriano Marteleto Godinho e Wilson Furtado Roberto ponderam o seguinte:

> "Da análise do texto dos incisos VI e VIII do art.5º, constata-se que o propósito do art. 13 do Marco Civil da Internet consiste em disciplinar, de forma exclusiva, a manutenção dos registros de conexão, **que abarcam apenas informações relativas ao termo inicial e final de uma conexão - e, consequentemente, sua duração - e o endereço IP, isto é, o endereço de protocolo da internet**, qualificado como 'o código atribuído a um terminal de uma rede para permitir sua identificação, definido segundo parâmetros internacionais' pelo inciso III do mesmo art. 5º. **A disponibilização dos registros de conexão, pois, não revela dados pessoais do usuário responsável pelo acesso à rede, tais como nome, endereço e informações de identificação (CPF, RG e outras) - cabendo**

> **salientar, a propósito, que o Marco Civil da Internet sequer especifica quais dados cadastrais devem ser cobrados pelo utente no momento da contratação do serviço de acesso à Internet junto ao provedor**. Ademais, da guarda de registros de acesso a aplicações de Internet cuidam os arts. 14 e 15 da Lei, ficando sua análise à margem do escopo central deste capítulo, destinado a investigar de que modo se dará a guarda exclusiva de registros de conexão e o eventual requerimento judicial para o fornecimento de tais dados."(GODINHO, Adriano Marteleto e ROBERTO, Wilson Furtado, *in* LEITE, George Salomão e LEMOS, Ronaldo, Coord. *Marco Civil da Internet*. 2 ed. São Paulo: Atlas. 2015, págs. 744-745, grifei).

Os mesmos autores demonstram certa perplexidade com o risco de interpretações ampliativas dos poderes dados às autoridades públicas para requererem a preservação de dados sem que haja autorização judicial a este respeito, *litteris*:

> "Há, todavia, certos aspectos nebulosos relativamente ao modo que a lei regulamentou, em particular, a guarda dos registros de conexão. Sabe-se, do teor do já analisado art. 13 do Marco Civil, que a obrigação de manutenção destes dados perdura por um período de um ano, estabelecendo o § 2º do próprio dispositivo que tanto a autoridade policial ou administrativa quanto o Ministério Público podem requerer cautelarmente que os registros de conexão fiquem armazenados sigilosamente por lapso temporal mais extenso. E, para já, surgem algumas indagações acerca dos exatos contornos para a solicitação em questão. **Salta aos olhos a possibilidade de não apenas o órgão ministerial, como também a autoridade policial ou administrativa virem a solicitar a ampliação do aludido prazo**. E, à falta de previsão legal específica, resta indagar: **quem seria a tal 'autoridade administrativa' competente para tais fins? Diante da omissão legislativa, resta ainda questionar: por quanto tempo os dados continuariam a ser preservados? Não se estaria, afinal, conferindo amplíssima margem ao Estado para intervir nos domínios da internet?**" (*Op. Cit.*, pág. 751, grifei)

Outrossim, foi devidamente elucidado que – de acordo com o firme entendimento desta Suprema Corte - a privacidade alcança "[…] o direito

de manter o controle sobre a sua própria informação e de determinar a maneira de construir sua própria esfera pública". (pág. 11 do documento eletrônico 48). Desse modo, o congelamento de dados telemáticos, na extensão buscada pela acusação, seja para utilização atual ou futura em processo crime, não pode se dar sem prévia autorização judicial.

E mais, o supracitado art. 10, § 1º, do Marco Civil da Internet, ao tratar de forma específica da proteção aos registros, dados pessoais e comunicações privadas, é claro quanto à possibilidade de fornecimento de informações de acesso (registro de conexão e registro de acesso a aplicações de internet), **desde que sejam requisitados por ordem de um juiz**.

A possibilidade de o cidadão administrar e dispor sobre o conteúdo pessoal de *e-mails*, mensagens, contatos e históricos de localização é uma garantia individual enrijecida pelo direito à preservação da intimidade, da vida privada, da honra e da imagem das pessoas (art. 5º, X e XII, da Constituição Federal), e somente pode ser mitigada sob a ótica constitucional nos casos expressamente autorizados por lei e, no que importa no caso concreto, nos limites estritos dessa autorização. Entendimento diverso permitiria que autoridades de investigação, independentemente de decisão judicial, realizassem a busca e apreensão prévia de conteúdos e seu congelamento, para posterior formalização da medida por ordem judicial, em prática vedada por qualquer *stantard* que se extraia da ordem constitucional vigente.

Por fim, vale registrar que a submissão da medida requerida pelo Ministério Público do Estado do Paraná à prévia autorização judicial não conflita com os arts. 16º, item 1, e art. 18º, item 1, **b**, da Convenção de Budapeste. Eis o teor dos dispositivos:

> "Art. 16º – Conservação expedita de dados informáticos armazenados
>
> 1. Cada parte adotará as medidas legislativas e outras que se revelem necessárias para permitir às suas autoridades competentes exigir ou obter de uma outra forma a conservação expedita de dados informáticos específicos, incluindo dados relativos ao tráfego, armazenados por meio de um sistema informático,

> nomeadamente nos casos em que existem motivos para pensar que os mesmos são susceptíveis de perda ou alteração."
>
> "Art. 18 – Injunção
> 1. Cada Parte adotará as medidas legislativas e outras que se revelem necessárias para habilitar as suas autoridades competentes para ordenar:
> […]
> b) a um fornecedor de serviços que preste serviços no território da Parte, que comunique os dados na sua posse ou sob seu controlo, relativos aos assinantes e respeitantes a esses serviços."

Conforme se verifica, referidas normas, por mais que se esforce o intérprete, não afastam ou restringem a incidência da cláusula pétrea da reserva de jurisdição na hipótese.

Ante o quadro, considerando o modelo constitucional vigente e a venerável tradição jurídica pátria, não há como cogitar, como alegam os agravantes, que a submissão judicial prévia para acesso ou preservação de dados acobertadas pelo direito à intimidade, à imagem e à vida privada signifique prejuízo ao combate da criminalidade, bastando, para tanto, que as autoridades investigativas guardem reverência aos limites constitucionais de sua atuação.

Portanto, caberá ao juízo *a quo* indicar, precisamente, a prova ora declarada inválida e que tenha sido arrecadada na investigação, ou seja: (i) todo e qualquer material, seja ele qual for, que seja anterior a 3/12/2018, pois ultrapassado o prazo de 1 ano (art. 13, *caput*, da Lei 12.965/2014), contado do dia em que deferida judicialmente a quebra do sigilo, ou seja, 3/12/2019 (doc. eletrônico 4); e (ii) todo material que não se enquadre no conceito de "registros de conexão" (art. 5º , VI, da Lei 12.965/2014) no período compreendido entre 3/12/2018 e 3/12/2019.

Na forma do art. 157 do CPP, as provas ilícitas deverão ser desentranhadas dos autos, não podendo ser mantidas sob o fundamento de validade daquele conteúdo precisamente identificado como ilícito, nos exatos termos dessa decisão.

Em seguida, o magistrado de origem deverá reavaliar, após o devido contraditório das partes, quanto à existência de justa causa para o prosseguimento da ação penal, abstendo-se a acusação, ainda, de fazer uso de tais elementos em quaisquer outros procedimentos investigatórios porventura existentes.

Por fim, no que tange ao pleito formulado por Marcelo Alvarenga Panizzi (documento eletrônico 55), tratando-se de coautoria, aplica-se ao caso justamente o art. 580, do CPP, de modo a permitir que a decisão prolatada neste *habeas corpus,* estritamente quanto às provas consideradas inválidas, estenda-se ao peticionante, por não ter sido baseada em motivos de caráter exclusivamente pessoal.

Em face do exposto, nego provimento aos agravos regimentais.

É como voto.