VOTO REAJUSTADO

O SENHOR MINISTRO DIAS TOFFOLI (RELATOR):

Conforme relatado, trata-se de recurso extraordinário com agravo, com repercussão geral reconhecida, mediante o qual se questiona a necessidade de prévia autorização judicial para se acessarem a agenda, os registros telefônicos e demais dados contidos no aparelho celular do suposto autor do ilícito penal, o qual foi encontrado pela vítima no local do crime e apreendido pela autoridade policial, com fundamento no art. 6º, inciso II, do CPP.

No caso em apreço, Guilherme Carvalho de Farias foi denunciado como incurso nas penas do art. 157, § 2º, incisos I e II, do Código Penal e condenado, em primeiro grau de jurisdição, à pena de 7 (sete) anos de reclusão e 16 (dezesseis) dias-multa.

O Tribunal de Justiça do Estado do Rio de Janeiro, reconhecendo a ilicitude da prova colhida – determinante para a identificação da autoria delitiva – e, por derivação, da integralidade do aparato probatório constante dos autos, deu provimento ao recurso defensivo, absolvendo o réu com base no art. 386, inciso VII, do Código de Processo Penal.

O fundamento para o juízo de ilicitude da prova foi o de que

> "a identificação do autor do fato se deu a partir do ilícito e desautorizado manuseio, pelos policiais civis, do aparelho de telefonia celular, supostamente de propriedade daquele e que teria caído ao chão durante a fuga do implicado, vindo a ser arrecadado pela vítima e entregue por esta em sede policial" (e-doc. 4, fl. 237).

Segundo registra o voto condutor do acórdão recorrido,

> "[a]pós a vítima ter entregue o aparelho de telefonia celular em sede policial, **o agente da lei MAYKE 'tomou a liberdade' de acessar os dados ali armazenados e referentes não só a fotografias guardadas pelo implicado, como também à agenda de telefones e ao histórico de ligações ali construído e no qual estaria armazenada a última ligação telefônica efetuada por GUILHERME**, que foi para sua namorada, após o que se desenvolveu aquela narrada investigação, que culminou com a identificação do implicado, bem como com a localização, tanto do domicílio do mesmo, quanto de sua namorada e para

> onde rumaram os agentes da lei, acabando por efetuar a prisão do rapinador.
>
> Neste contexto, tem-se por inequívoca a constatação de que a identificação do autor dos fatos foi alcançada unicamente mercê do indevido, desautorizado e ilegal manuseio daquele aparelho de telefonia celular, **o que importou na flagrante e indisfarçável quebra da proteção constitucional incidente sobre a inviolabilidade do sigilo dos dados e das comunicações telefônicas ali existentes**, o que apenas poderia se dar, por exceção, mediante expressa autorização judicial para tanto, mas o que foi ignorado e desrespeitado, muito embora não encerrasse maior dificuldade a observância da exigência legal, bastando para tanto que o policial civil que recebeu o referido aparelho telefônico, de imediato, encaminhasse este ao Delegado de Polícia informando a relevância do objeto, de modo a que tal Autoridade Policial representasse junto ao Plantão Judiciário de modo a obter a autorização para o acesso e verificação dos dados pretendidos" (e-doc. 4, fls. 238-239 – grifo nosso).

Em síntese, o cerne da controvérsia posta nos autos está em saber se é possível acessar, **sem autorização judicial**, dados armazenados eletronicamente em aparelhos celulares encontrados no local do ilícito e apreendidos pela autoridade policial.

Conforme mencionado por ocasião do reconhecimento da repercussão geral, a questão suscitada no recurso extraordinário é dotada de densidade constitucional, visto que envolve, a um só tempo, a invocada "inviolabilidade do sigilo dos dados e das comunicações telefônicas" e a utilização, no processo, de provas supostamente obtidas por meios ilícitos, além de extrapolar o interesse subjetivo das partes, dada sua relevância, não se podendo olvidar, também, a inegável oportunidade e conveniência para se consolidar a orientação do Supremo Tribunal Federal a respeito.

Recordo, outrossim, que o julgamento foi iniciado na sessão do Plenário Virtual realizada de **30/10/20 a 10/11/20**. Naquela assentada, apresentei voto pelo **provimento do agravo e, ato contínuo, do recurso extraordinário** para, **cassando-se o acórdão recorrido**, determinar ao Tribunal de Origem que **prosseguisse no julgamento da apelação criminal**, conforme de direito.

Propus, ainda, a fixação da seguinte tese de repercussão geral:

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

Na sequência, o Ministro **Gilmar Mendes** inaugurou a divergência, ao **negar provimento ao recurso interposto**, fixando a tese de repercussão geral nos seguintes termos:

> "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 XII)."

O Ministro **Edson Fachin** acompanhou a divergência, e o Ministro **Alexandre de Moraes** pediu vista dos autos.

Aproveito, então, a oportunidade para rememorar o caso e para adiantar que, refletindo novamente sobre a matéria de fundo, à luz das valiosas considerações contidas no voto divergente do Ministro **Gilmar Mendes** e das alterações legislativas posteriores, em especial a recente EC nº 115, de 10 de fevereiro de 2022, **revejo meu posicionamento original**, pelas razões que passo a expor.

Primeiramente, destaco que, entre a data dos fatos (21/5/13) e o presente julgamento, transcorreram mais de 10 (dez) anos. Nesse período, aconteceram consideráveis avanços tecnológicos, entre os quais destaco a crescente e massiva utilização de ferramentas de inteligência artificial, inclusive pelos órgãos de persecução penal. Uma revolução tecnológica tão acelerada, como não poderia deixar de ser, ocasionou a transformação completa das formas de vida, trabalho e interação social no país e no mundo. Consequentemente, surgiram novos desafios em todas as áreas e assistimos, ainda hoje, a uma importante alteração da **percepção geral e institucional** sobre **os riscos sistêmicos e ocultos** que **essas tecnologias e suas potencialidades acarretam aos direitos fundamentais**.

Observo também que **os *smartphones* já eram realidade no país em 2013**. Esses aparelhos multifuncionais, além de servirem de instrumento aos serviços ordinários de telefonia móvel, permitem a produção, o armazenamento, a transmissão e a reprodução de arquivos dos mais diversos formatos (textos, imagens, áudios e vídeos) e – **mais que isso** – viabilizam o acesso amplo e irrestrito à internet e, por conseguinte, às redes sociais, aos provedores de **e-mail**, às plataformas bancárias e de **e-commerce**, a uma miríade de **sites** e **blogs** e aos inúmeros aplicativos de mensagens instantâneas, disponíveis, inclusive, gratuitamente. Graças aos **smartphones**, "o mundo passou a caber na palma da mão". Mas, à medida que isso acontecia, as informações pessoais (e não pessoais) – **sabidas e não sabidas** – também se concentraram nos aparelhos celulares. Isso porque todas as suas funcionalidades geram dados e metadados que são registrados na memória física do aparelho, ou "em nuvem", e podem ser facilmente acessados, rastreados e/ou recuperados.

Nessa esteira, mostra-se de extrema pertinência a advertência do Ministro **Gilmar Mendes**, em seu voto, de que

> "esses aparelhos são capazes de registrar as mais variadas informações sobre os seus usuários, como a sua precisa localização por sistemas de GPS ou estações de rádio-base, as chamadas realizadas e recebidas, os registros da agenda telefônica, os dados bancários dos usuários, informações armazenadas em nuvem, os sites e endereços eletrônicos acessados, lista de e-mail, mensagens por aplicativos de telefone, fotos e vídeos pessoais, entre outros.
>
> Além disso, a conexão de todos esses aparelhos à rede mundial de computadores faz com que estejamos todos integralmente conectados, o tempo todo, fornecendo dados e informações para órgãos públicos e privados".

Acrescenta Sua Excelência que,

> "[a] partir do telefone, pode-se verificar se determinada pessoa esteve ou não em determinado local, qual percurso ela percorreu e que *sites* acessou no caminho. Câmaras de reconhecimento facial integradas à internet possibilitam o reconhecimento instantâneo de suspeitos. Algoritmos podem ser usados para prever e evitar crimes".

Disso conclui o Ministro **Gilmar Mendes** que "[e]sses avanços tecnológicos são importantes e devem ser utilizados para a segurança pública dos cidadãos e a elucidação de delitos". Contudo, Sua Excelência também alerta que se deve ter "**cautela, limites e controles para não transformar o Estado policial em um Estado espião e onipresente**, conforme descrito por George Orwel em seu livro 1984".

De fato, no contexto atual, franquear o acesso ao aparelho celular de alguém implica, na prática, **liberar, autorizar, conceder** – ou, ao menos, **desobstruir** – o acesso a um espectro enorme de dados pessoais (e não pessoais), o que torna possível uma **investigação completa** – e, diga-se de passagem, **muito eficiente** – acerca de suas preferências, de suas relações familiares e interpessoais, de seus afetos, de seus hábitos de vida, trabalho e consumo e, em última análise, de sua forma de pensar, agir e decidir. Isso sem falar, obviamente, das facilidades que esse acesso proporciona para a intrusão indevida e "**para o futuro**", a partir da instalação de **softwares** "espiões".

Por tais motivos, a meu ver, a realidade e a percepção atuais **ampliam e deslocam a discussão original**, centrada pelo próprio recorrente na suposta inviolabilidade do sigilo das comunicações (CF/88, art. 5º, inciso XII), para **a inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas** (CF/88, art. 5º, inciso, X) e, mais precisamente, para o novel "**direito à proteção dos dados pessoais, inclusive nos meios digitais**" (CF/88, art. 5º, inciso LXXIX, incluído pela EC nº 115, de 10/2/22).

Na primeira análise dos autos, compreendi que o caso em apreço se amoldava ao entendimento jurisprudencial formado a partir da análise do RE nº 418.416/SC, Rel. Min. **Sepúlveda Pertence**, julgado pelo Plenário em 2006, identificando-se, sobretudo, com o HC nº 91.867/PA, Rel. Min. **Gilmar Mendes**, julgado pela Segunda Turma em 2012. Todavia, ao revisitar os precedentes da Suprema Corte sobre a matéria e confrontá-los com o panorama fático e jurídico atual, percebo a necessidade de se verticalizar a análise das premissas ali estabelecidas para, só então, enfrentar o caso concreto.

No citado recurso extraordinário, a discussão girava em torno da alegação defensiva de que a condenação por crimes tributários se baseava em prova obtida por meio ilícito, "consubstanciada na decisão que autorizou a busca e apreensão, de cuja execução também teria resultado a violação à proteção constitucional ao sigilo das comunicações de dados".

Embora, no caso, a medida extrema da busca e apreensão tivesse

sido previamente autorizada pelo juízo competente e contivesse autorização expressa para a apreensão de "equipamentos de informática (computadores e disquetes) interessantes à investigação", a defesa sustentava a **impossibilidade de decodificação dos registros contidos no computador apreendido**, invocando como fundamento para tal entendimento o que foi decidido pela Suprema Corte na AP nº 307.

Sobre esse ponto, no voto condutor do acórdão, o Ministro **Sepúlveda Pertence**, então relator do referido recurso extraordinário, ponderou que a **tese da inviolabilidade absoluta de dados contidos em computador não poderia ser tomada como consagrada pelo Colegiado** na aludida ação penal,

> "dada a interferência, naquele caso, de outra razão suficiente para a exclusão da prova questionada - o ter sido o microcomputador apreendido sem ordem judicial e a consequente ofensa da garantia da inviolabilidade do domicílio da empresa - este segundo fundamento bastante, sim, aceito por votação unânime, à luz do art. 5º, XI da Lei Fundamental".

O julgado recebeu a seguinte ementa:

> "I. Decisão judicial: fundamentação: alegação de omissão de análise de teses relevantes da Defesa: recurso extraordinário: descabimento. Além da falta do indispensável prequestionamento (Súmulas 282 e 356), não há violação dos art. 5º, LIV e LV, nem do art. 93, IX, da Constituição, que não exige o exame pormenorizado de cada uma das alegações ou provas apresentadas pelas partes, nem que sejam corretos os fundamentos da decisão; exige, apenas, que a decisão esteja motivada, e a sentença e o acórdão recorrido não descumpriram esse requisito (v.g., RE 140.370, 1ª T., 20.4.93, Pertence, DJ 21.5.93; AI 242.237 - AgR, 1ª T., 27.6.00, Pertence, DJ 22.9.00). II. Quebra de sigilo bancário: prejudicadas as alegações referentes ao decreto que a determinou, dado que a sentença e o acórdão não se referiram a qualquer prova resultante da quebra do sigilo bancário, tanto mais que, dado o deferimento parcial de mandado de segurança, houve a devolução da documentação respectiva. III. Decreto de busca e apreensão: validade. 1. Decreto específico, que somente permitiu que as autoridades encarregadas da diligência selecionassem objetos, dentre aqueles especificados na decisão e na sede das duas empresas

nela indicadas, e que fossem 'interessantes à investigação' que, no caso, tinha pertinência com a prática do crime pelo qual foi efetivamente condenado o recorrente. 2. Ademais, não se demonstrou que as instâncias de mérito tenham invocado prova não contida no objeto da medida judicial, nem tenham valorado qualquer dado resultante da extensão dos efeitos da decisão determinante da busca e apreensão, para que a Receita Federal e a 'Fiscalização do INSS' também tivessem acesso aos documentos apreendidos, para fins de investigação e cooperação na persecução criminal, 'observado o sigilo imposto ao feito'. IV. Proteção constitucional ao sigilo das comunicações de dados - art. 5º, XII, da CF: ausência de violação, no caso. 1. Impertinência à hipótese da invocação da AP 307 (Pleno, 13.12.94, Galvão, DJU 13.10.95), em que a tese da inviolabilidade absoluta de dados de computador não pode ser tomada como consagrada pelo Colegiado, dada a interferência, naquele caso, de outra razão suficiente para a exclusão da prova questionada - o ter sido o microcomputador apreendido sem ordem judicial e a consequente ofensa da garantia da inviolabilidade do domicílio da empresa - este segundo fundamento bastante, sim, aceito por votação unânime, à luz do art. 5º, XI, da Lei Fundamental. 2. Na espécie, ao contrário, não se questiona que a apreensão dos computadores da empresa do recorrente se fez regularmente, na conformidade e em cumprimento de mandado judicial. 3. Não há violação do art. 5º, XII, da Constituição que, conforme se acentuou na sentença, não se aplica ao caso, pois não houve 'quebra de sigilo das comunicações de dados (interceptação das comunicações), mas sim apreensão de base física na qual se encontravam os dados, mediante prévia e fundamentada decisão judicial'. 4. A proteção a que se refere o art. 5º, XII, da Constituição, é da comunicação 'de dados' e não dos 'dados em si mesmos', ainda quando armazenados em computador. (cf. voto no MS 21.729, Pleno, 5.10.95, red. Néri da Silveira - RTJ 179/225, 270). V. Prescrição pela pena concretizada: declaração, de ofício, da prescrição da pretensão punitiva do fato quanto ao delito de frustração de direito assegurado por lei trabalhista (C. Penal, arts. 203; 107, IV; 109, VI; 110, § 2º e 114, II; e Súmula 497 do Supremo Tribunal)" (RE nº 418.416, Rel. Min. **Sepúlveda Pertence**, Tribunal Pleno, julgado em 10/5/06, DJ de 19/12/06).

Vale consignar que, no presente caso, **o acesso ao conteúdo do celular pelos agentes policiais não foi precedido de mandado de busca e apreensão ou de autorização judicial específica para tal finalidade**. Ao contrário. O aparelho foi encontrado fortuitamente pela vítima no local do crime e, ato contínuo, entregue aos agentes policiais, os quais, na sequência, devassaram seu conteúdo em busca de evidências que permitissem estabelecer uma linha investigatória para a elucidação dos fatos, o que, de fato, aconteceu. Como resultado, o celular foi apreendido pela autoridade policial, por interessar à investigação, e as diligências encetadas lograram a identificação do autor do fato e sua prisão em flagrante (flagrante impróprio).

Já o HC nº 91.867, Rel. Min. **Gilmar Mendes**, julgado pela Segunda Turma, **guarda mais semelhança com o caso destes autos.** Nele, discutiu-se a suposta **ilicitude da prova produzida no inquérito policial** em decorrência de **os agentes policiais, após a prisão em flagrante do corréu, terem realizado a análise dos últimos registros telefônicos de dois aparelhos celulares apreendidos**.

Na ocasião, entendeu a Segunda Turma do Supremo Tribunal Federal, **por unanimidade dos votos**, que não estaria configurada a alegada ilegalidade, tendo em vista que "não se confundem comunicação telefônica e registros telefônicos". Reafirmou-se, então, a orientação de que "a proteção constitucional é da comunicação de dados e não dos dados" propriamente ditos, concluindo-se que "a autoridade policial, cumprindo seu mister, buscou, unicamente, colher elementos de informação hábeis a esclarecer a autoria e a materialidade do delito" e que, **ainda que assim não se entendesse, no caso concreto**, "o curso normal das investigações conduziria a elementos informativos que vinculariam os pacientes ao fato investigado".

As razões contidas no voto condutor do acórdão foram sintetizadas na seguinte ementa:

> "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 Williams (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 nº 91.867, Rel. Min. **Gilmar Mendes**, Segunda Turma, julgado em 24/4/12, DJe de 19/9/12).

Ressalto que, apesar de julgado em 2012, **os fatos remontavam ao ano de 2004**, época em que os aparelhos celulares basicamente instrumentalizam os serviços móveis de telefonia, não possuindo tantas funcionalidades quanto os celulares de 2013 (**já *smartphones***, na grande maioria dos casos) e os aparelhos mais atuais.

Ressalto, ainda, que o modo como é feita a análise dos dados porventura extraídos de aparelhos celulares também mudou significativamente desde então, sobretudo em razão da incorporação de ferramentas de inteligência artificial, tornando possível a extração de uma grande quantidade de dados e sua confrontação eficiente, mesmo que possuam naturezas distintas. Diante disso, até mesmo os dados que antes

pareciam não ter nenhuma utilidade ganham potencialidade e permitem **conclusões plausíveis** e **sobre quase tudo**, extrapolando (ou podendo extrapolar facilmente) o objeto da própria investigação.

Apesar de ser possível identificar pontos de divergência e particularidades que distinguem os dois precedentes acima entre si e que também os afastam, de certo modo, do caso ora analisado, é importante realçar que, em ambos os casos, se partiu da premissa comum de que a inviolabilidade do sigilo das comunicações, prevista no art. 5º, inciso XII, do texto constitucional, diz respeito à "**comunicação de dados**", e não aos "dados" **per se** porventura registrados em dispositivos eletrônicos apreendidos.

Antes disso, a mesma premissa havia sido aventada pela Procuradoria-Geral da República, e parcialmente adotada pelo Plenário do Supremo Tribunal Federal no MS nº 21.729. Tratava-se de mandado de segurança impetrado pelo Banco do Brasil contra ato do Procurador-Geral da República, o qual, por ofício, demandou daquela instituição financeira a lista dos beneficiários de recursos públicos destinados ao setor sucroalcooleiro, bem como solicitou dados específicos quanto à existência de débitos e a sua natureza.

Na ocasião, o Vice-Procurador-Geral da República, valendo-se de artigo publicado pelo Professor **Tércio Sampaio Ferraz Júnior** em 1993, sob o título de Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado, sustentou a tese de que **a inviolabilidade do sigilo das comunicações se refere à "comunicação de dados" (isto é, aos "dados em trânsito"), e não aos "dados estáticos" ou armazenados.** O mandado de segurança foi indeferido pelo Supremo Tribunal Federal, **por maioria de 6 votos a 5**. A partir disso, a tese ali sustentada passou a iluminar o exame de casos correlatos.

Contudo, como anotam **Rafael Mafei Rabelo Queiroz e Paula Pedigoni Ponce** em artigo publicado quase trinta anos depois, **só dois dos votos vencedores** no referido julgado fizeram expressa menção ao artigo de **Ferraz Júnior**, enquanto os outros quatro votos vencedores adotaram como razão de decidir a necessidade de se aplicar o princípio da publicidade às operações envolvendo recursos públicos. **Vide** o que dizem os autores:

> "MS nº 21.729/DF: tratava-se de mandado de segurança impetrado pelo Banco do Brasil contra ato do Procurador-Geral da República, que demandava, por ofício, lista de nomes dos

beneficiários de liberação de recursos públicos ao setor sucroalcooleiro, além de dados específicos sobre existência de débitos e naturezas das operações que os originaram. A argumentação do impetrante não chegava a mencionar o artigo 5º, inciso XII, da Constituição, mas limitava-se a insistir na necessidade de ordem judicial para o acesso a tais informações, que equivaleria a quebra de sigilo.

A autoridade coatora prestou informações, confirmando os fatos e alegando que havia questionamentos quanto à autoridade do Ministério Público para requerer os dados em questão. Alegaram suspeitar de violação tanto da Lei Complementar (LC) nº 75/1993, quanto do art. 129, inciso VI, da Constituição Federal. Em extenso parecer, o Vice Procurador Geral da República introduziu a discussão sobre o inciso XII, juntamente com trecho do artigo de Ferraz Júnior (Vice Procuradoria Geral da República, 1994). Foi a primeira aparição de 'Sigilo de dados' nos autos do caso. O parecer da PGR argumentava que o sigilo bancário não teria guarida constitucional, nem a partir de interpretação do artigo 5º, inciso X, nem a partir do inciso XII. Nesse sentido, sem natureza constitucional, as exceções estabelecidas ao sigilo bancário seriam válidas enquanto motivadas pela salvaguarda de interesses constitucionalmente protegidos – como seria o caso do art. 8º da LC 75, em sintonia com o art. 129, inciso VI da Constituição Federal. Segundo o parecer, o inciso XII do art. 5º não protegia o sigilo bancário, porque blindaria, através do sigilo, apenas as comunicações de dados – e não os dados em si, uma vez recebidos e armazenados.

Por maioria de 6 a 5, o STF indeferiu o mandado de segurança. A tese encampada pela PGR, da inviolabilidade do sigilo de comunicações, mas não dos dados armazenados, elaborada com apoio no texto de Ferraz Júnior, sagrou-se vencedora. Em dois votos vencedores, dos Ministros Sepúlveda Pertence e Francisco Rezek, o texto foi expressamente citado. A *ratio* comum da maioria do Tribunal, entretanto, extraída dos votos dos Ministros Octavio Gallotti, Sidney Sanches, Néri da Silveira, Moreira Alves e Sepúlveda Pertence, fundamentou-se na aplicação do princípio da publicidade às operações envolvendo recursos públicos. Tratava-se, afinal, de um caso envolvendo financiamentos rurais concedidos pelo Banco do Brasil.

Os votos vencidos, quais sejam, os Ministros Marco

> Aurélio, Maurício Corrêa, Celso de Mello, Ilmar Galvão e Carlos Velosos, de forma geral, argumentaram que o sigilo bancário teria status constitucional em decorrência dos incisos X e XII do artigo 5º e que, portanto, sua quebra necessitaria de ordem judicial. Os votos dos Ministros Sepúlveda Pertence e Francisco Rezek foram os únicos a se contrapor a tal afirmação, recuperando o texto de Ferraz Júnior e indicando que entendiam que o sigilo de dados ali mencionado se referia tão somente ao sigilo da comunicação de dados e que, consequentemente, não seria aplicável ao sigilo bancário. É curioso notar que os votos vencidos, embora não tenham invocado o texto de Ferraz Júnior, poderiam ter igualmente se valido dele para amparar seu argumento: afinal, 'Sigilo de dados' é explícito em afirmar que dados armazenados, embora não acobertados pelo sigilo do inc. XII do art. 5º, podem ser protegidos pela regra geral da privacidade, quando fosse o caso. Mas não o fizeram" (QUEIROZ, Rafael Mafei Rabelo; PONCE, Paula Pedigoni. Tércio Sampaio Ferraz Júnior e sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado: o que permanece e o que deve ser reconsiderado. **Revista Internet & Sociedade**, n. 1, v. 1, fevereiro de 2020, p. 64-90).

Seja como for, fato é que, gradualmente, a jurisprudência do Supremo Tribunal Federal acabou encampando, ao menos em parte, o texto seminal do Professor **Tércio Sampaio Ferraz Júnior**, para quem, "[o] sigilo, no inciso XII do art. 5º, está referido à *comunicação*, no interesse da defesa da privacidade".

Conforme explica referido autor,

> "[i]sto é feito, no texto, em dois blocos: a Constituição fala em sigilo 'da correspondência e das comunicações telegráficas, de dados e das comunicação telefônicas'. Note-se, para a caracterização dos blocos, que a conjunção *e* une correspondência com telegrafia, segue-se uma vírgula e depois, a conjunção de dados com comunicações telefônicas. Há uma simetria nos dois blocos. Obviamente o que se regula é *comunicação* por correspondência e telegrafia, *comunicação* de dados e telefonia. O que fere a liberdade de omitir pensamento é, pois, entrar na *comunicação* alheia, fazendo com que o que devia ficar entre sujeitos que se comunicam privadamente passe

> ilegitimamente ao domínio de um terceiro. Se alguém elabora para si um cadastro sobre certas pessoas, com informações marcadas por avaliações negativas, e o torna público, poderá estar cometendo difamação, mas não quebra sigilo de dados. Se estes dados, armazenados eletronicamente, são transmitidos, privadamente, a um parceiro, em relações mercadológicas, para a defesa do mercado, também não estará havendo quebra de sigilo. Mas se alguém *entra nesta transmissão*, como um terceiro que nada tem a ver com a relação comunicativa, ou por ato próprio ou porque uma das partes lhe cede o acesso indevidamente, estará violado o sigilo de dados.
>
> A distinção é decisiva: o objeto protegido no direito à inviolabilidade do sigilo não são os dados em si, mas a sua comunicação restringida (liberdade de negação). A troca de informações (comunicação) *privativa* é questão que não pode ser violada por sujeito estranho à comunicação. Doutro modo, se alguém, não por razões profissionais, ficasse sabendo legitimamente de dados incriminadores relativos a uma pessoa, ficaria impedido de cumprir o seu *dever* de denunciá-los!" (JÚNIOR, Tércio Sampaio Ferraz. Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado. **Revista da Faculdade de Direito**, Universidade de São Paulo, v. 88, p. 439-459, 1993).

Prossegue **Ferraz Júnior**, detalhando o âmbito de proteção da inviolabilidade do sigilo das comunicações telefônicas no texto constitucional:

> "(...) toma seu correto sentido o disposto no inciso XII do art. 5º da CF, quando ali se admite, apenas para a comunicação telefônica e, assim mesmo, só para fins de investigação criminal ou instrução processual penal, por ordem judicial, a quebra do sigilo. Conquanto haja quem caminhe para uma interpretação literal deste texto, não nos parece razoável aceitá-la na sua inteira singeleza. Note-se, antes de mais nada, que dos quatro meios de comunicação ali mencionados – correspondência, telegrafia, dados, telefonia – só o último se caracteriza por sua instantaneidade. Isto é, a comunicação telefônica só é *enquanto ocorre.* Encerrada, não deixa vestígios no que se refere ao relato das mensagens e aos sujeitos comunicadores. É apenas possível, *a posteriori,* verificar qual unidade telefônica ligou para outra. A gravação de conversas telefônicas por meio chamado

> 'grampeamento' é, pois, uma forma sub[-]reptícia de violação do direito ao sigilo da comunicação, mas, ao mesmo tempo, é a única forma tecnicamente conhecida de preservar a ação comunicativa. Por isso, no interesse público (investigação criminal ou instrução processual penal), é o único meio de comunicação que exigiu, do constituinte, uma ressalva expressa. Os outros três não sofreram semelhante ressalva porque, no interesse público, é possível realizar investigações e obter provas com base em vestígios que a comunicação deixa: a carta guardada, o testemunho de quem leu o nome do endereçado e do remetente, ou de quem viu a destruição do documento, o que vale também para o telegrama, para o telex, para o telefax, para a recepção da mensagem de um computador para outro, etc.
>
> Como isto é tecnicamente possível, o constituinte não permitiu absolutamente a entrada de terceiros, ainda que em nome do interesse público.
>
> Esta proibição, porém, não significa que, no interesse público, não se possa ter acesso *a posteriori* à identificação dos sujeitos e ao relato das mensagens comunicadas. Por exemplo, o que se veda é uma autorização judicial para interceptar correspondência, mas não para requerer busca e apreensão de documentos" (JÚNIOR, Tércio Sampaio Ferraz. Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado. **Revista da Faculdade de Direito**, Universidade de São Paulo, v. 88, p. 439-459, 1993).

Isso não significa que, para o Professor **Tércio Sampaio Ferraz Júnior**, o texto constitucional asseguraria proteção jurídica apenas e tão somente para a "comunicação de dados", isto é, para o "fluxo comunicacional", ou para os "dados em trânsito". Os "dados estáticos", ou armazenados, segundo ele, também são passíveis de proteção jurídica e, embora **não** se revistam **sempre e incondicionalmente** de caráter sigiloso, **podem alcançar essa qualidade, em diferentes níveis, a depender das circunstâncias**, quando, por exemplo, digam respeito à intimidade, à vida privada, à honra e à imagem, encontrando guarida, portanto, no disposto no art. 5º, inciso X, do texto constitucional.

Nessa esteira, explica o autor que,

> "[n]o que tange à intimidade, é a informação daqueles dados que a pessoa guarda para si e que dão consistência à sua

pessoalidade - dados de foro íntimo, expressões de auto-estima, avaliações personalíssimas com respeito a outros, pudores, enfim, dados que, quando constantes de processos comunicativos, exigem do receptor extrema lealdade e alta confiança, e que, se devassados, desnudariam a personalidade, quebrariam a consistência psíquica, destruindo a integridade moral do sujeito. Em termos do princípio da exclusividade, diríamos que esta é, nesses casos, de grau máximo. Em consequência, o emissor pode comunicar tais dados, se o desejar, mas a ninguém é dado exigir dele a informação transmitida, salvo em casos especialíssimos em que a intimidade de alguém venha a interferir na intimidade de outrem: o direito de não ser obrigado a revelar situações íntimas é limitado pelo direito de o receptor recusar informações íntimas que lhe firam a própria intimidade. Por isso, em processos que versem situações íntimas, a lei garante o sigilo. A inexigibilidade desses dados, salvo quando alguém se vê por eles ferido na sua própria intimidade, faz deles um limite ao direito de acesso à informação (art. 5º, XIV, da CF.).

No que diz respeito à vida privada, é a informação de dados referentes às opções da convivência, como a escolha de amigos, a frequência de lugares, os relacionamentos civis e comerciais, ou seja, de dados que, embora digam respeito aos outros, não afetam, em princípio, direitos de terceiros (exclusividade da convivência). Pelo sentido inexoravelmente comunicacional da convivência, a vida privada compõe, porém, um conjunto de situações que, usualmente, são informadas sem constrangimento. São dados que, embora privativos - como o nome, endereço, profissão, idade, estado civil, filiação, número de registro público oficial, etc. -, condicionam o próprio intercâmbio humano em sociedade, pois constituem elementos de identificação que tornam a comunicação possível, corrente e segura. Por isso, a proteção desses dados em si, pelo sigilo, não faz sentido. Assim, a inviolabilidade de dados referentes à vida privada só tem pertinência para aqueles associados aos elementos identificadores usados nas relações de convivência, as quais só dizem respeito aos que convivem. Dito de outro modo, os elementos de identificação só são protegidos quando compõem relações de convivência privativas: a proteção é para elas, não para eles. Em consequência, simples cadastros de elementos identificadores (nome, endereço, R.G., filiação, etc.) não são protegidos. Mas cadastros que envolvam relações de

> convivência privadas (por exemplo, nas relações de clientela, desde quando é cliente, se a relação foi interrompida, as razões pelas quais isto ocorreu, quais os interesses peculiares do cliente, sua capacidade de satisfazer aqueles interesses, etc.) estão sob proteção. Afinal, o risco à integridade moral do sujeito, objeto do direito à privacidade, não está no nome, mas na exploração do nome, não está nos elementos de identificação que condicionam as relações privadas, mas na apropriação dessas relações por terceiros a quem elas não dizem respeito. Pensar de outro modo seria tornar impossível, no limite, o acesso ao registro de comércio, ao registro de empregados, ao registro de navio, etc, em nome de uma absurda proteção da privacidade.
>
> Por último, a honra e a imagem. A privacidade, nesse caso, protege a informação de dados que envolvam avaliações (negativas) do comportamento que, publicadas, podem ferir o bom nome do sujeito, isto é, o modo como ele supõe e deseja ser visto pelos outros. Repita-se que o direito à privacidade protege a honra, o direito à inviolabilidade do sigilo de dados protege a comunicação referente a avaliações que um sujeito faz sobre outro e que, por interferir em sua honra, comunica restritivamente, por razões de interesse pessoal. É o caso, por exemplo, de cadastros pessoais que contêm avaliações negativas sobre a conduta (mau pagador, devedor impontual e relapso, etc). No tocante à imagem, para além do que ela significa de boa imagem, assimilando-se, nesse sentido, à honra, a proteção refere-se a dados que alguém fornece a alguém e não deseja ver explorada (comercialmente, por exemplo) por terceiros" (JÚNIOR, Tércio Sampaio Ferraz. Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado. **Revista da Faculdade de Direito**, Universidade de São Paulo, v. 88, p. 439-459, 1993).

Também é verdade que o artigo de **Tércio Sampaio Ferraz Júnior** se referia a um contexto muito diferente do delineado nos autos. Investigavam-se os limites da atuação fiscalizatória dos agentes estatais, tendo em vista a recorrente solicitação de dados pela Receita Federal a instituições financeiras públicas e privadas e a administradoras de cartão de crédito, mantenedoras de bancos de dados, para fins de verificação da regularidade tributária.

Além do mais, o panorama geral era outro. Nas duas últimas

décadas, a popularização dos **smartphones** e a ampliação do acesso a internet por meio de tais aparelhos eletrônicos, além do surgimento de novas tecnologias digitais e de novas aplicações para as já existentes, a partir do desenvolvimento e da aplicação de ferramentas de inteligência artificial, levaram à intensificação da transformação digital. Em razão disso, passamos a testemunhar uma hiperconectividade que não passou desapercebida pelo Poder Constituinte Derivado.

Em 2022, o Congresso Nacional promulgou a **Emenda Constitucional nº 115/22**, a qual introduziu no art. 5º da Constituição o inciso LXXIX, segundo o qual "**é assegurado, nos termos a lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais**".

Na doutrina, já havia vozes nesse sentido mesmo antes da referida emenda constitucional. **Rafael Mafei Rabelo Queiroz e Paula Pedigoni Ponce**, por exemplo, há algum tempo defendem que "[j]á não faz sentido distinguir entre dados em trânsito e dados estáticos como critério para maior ou menor proteção à privacidade". Para os autores,

> "o barateamento do armazenamento de dados e a migração das comunicações humanas para serviços providos pela Internet, com opções de armazenamento de segurança em servidores ('*backups* na nuvem'), torna o indivíduo, por seu considerável volume e abrangência temporal, mais sensível à sua intimidade do que conversas telefônicas interceptadas. A hierarquia protetiva que coloca dados em trânsito acima de dados armazenados simplesmente é anacrônica diante das mudanças na tecnologia e nas práticas comunicativas deste 1993 até os dias atuais (Sidi, 2016; Quito, 2018)" (QUEIROZ, Rafael Mafei Rabelo; PONCE, Paula Pedigoni. Tércio Sampaio Ferraz Júnior e sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado: o que permanece e o que deve ser reconsiderado. **Revista Internet & Sociedade**, n. 1, v. 1, fevereiro de 2020, p. 64-90).

Concluem **Rafael Mafei** e **Paula Pedigoni** que,

> "[s]e não é possível ignorar a distinção entre os incisos X e XII do art. 5º da Constituição, tampouco há razão para impor uma proteção menos efetiva à nossa intimidade apenas porque estejam em dados armazenados, e não em trânsito. Essa particular leitura de 'Sigilo de dados', que não é a única possível de ser feita do texto e nem é necessariamente a melhor,

> deve ser descartada em favor de outra que equalize a proteção de dados armazenados e dados em trânsito pelo critério que substantivamente importa: o grau de exclusividade que se deve reconhecer às informações contidas nos dados e seu impacto sobre a privacidade de seu titular. O inc. X, art. 5º, da Constituição dá conta desta fundamentação sem dificuldades" (QUEIROZ, Rafael Mafei Rabelo; PONCE, Paula Pedigoni. Tércio Sampaio Ferraz Júnior e sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado: o que permanece e o que deve ser reconsiderado. **Revista Internet & Sociedade**, n. 1, v. 1, fevereiro de 2020, p. 64-90).

A argumentação dos autores foi premonitória, sobretudo quando se considera o uso acentuado de aplicativos de mensagens instantâneas, com o envio e a recepção de mensagens de voz ou em vídeo, em substituição ao serviço telefônico convencional. Vivemos tempos de comunicação assíncrona, a qual, em regra, deixa vestígios em equipamentos eletrônicos. Como assegurar menor proteção constitucional a esse tipo de comunicação?

Não se pode olvidar, outrossim, que **a transformação digital leva, necessária e inevitavelmente, à evolução do direito**. Esse é um processo contínuo, que se retroalimenta e enseja a atuação das instituições de Estado.

Antes mesmo da citada Emenda Constitucional nº 115/22, o Poder Legislativo deu o primeiro passo ao editar a **Lei nº 12.695, de 23 de abril de 2014**, apelidada de "Marco Civil da Internet", para estabelecer princípios, garantias, direitos e deveres para o uso da internet no país e, ao fazê-lo, assumindo protagonismo no cenário jurídico internacional por algum tempo, elevou ao patamar de direito dos respectivos usuários "a inviolabilidade e sigilo de suas **comunicações privadas armazenadas, salvo por ordem judicial**" e o "não fornecimento a terceiros de seus dados pessoais, **inclusive registros de conexão, e de acesso a aplicações de internet**, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei" (art. 7º, incisos III e VII).

Por oportuno, transcrevo na íntegra o art. 7º da Lei nº 12.695/14:

> "Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:
>
> I - inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente

de sua violação;

II - inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei;

III - inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial;

IV - não suspensão da conexão à internet, salvo por débito diretamente decorrente de sua utilização;

V - manutenção da qualidade contratada da conexão à internet;

VI - informações claras e completas constantes dos contratos de prestação de serviços, com detalhamento sobre o regime de proteção aos registros de conexão e aos registros de acesso a aplicações de internet, bem como sobre práticas de gerenciamento da rede que possam afetar sua qualidade;

VII - não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei;

VIII - informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que:

a) justifiquem sua coleta;

b) não sejam vedadas pela legislação; e

c) estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet;

IX - consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais;

X - exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei e na que dispõe sobre a proteção de dados pessoais; (Redação dada pela Lei nº 13.709, de 2018)

XI - publicidade e clareza de eventuais políticas de uso dos provedores de conexão à internet e de aplicações de internet;

XII - acessibilidade, consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, nos termos da lei; e

XIII - aplicação das normas de proteção e defesa do consumidor nas relações de consumo realizadas na internet."

Conquanto referidos direitos criem, em contrapartida e imediatamente, obrigações diretas para os provedores de internet, não se pode ignorar que carregam normatividade suficiente para se imporem a outros atores, incluindo-se nesse universo os agentes do próprio Estado, em especial os órgãos de fiscalização e de persecução penal.

Assim, se nem mesmo para esses agentes e mediante requisição formal estariam os provedores legitimados a entregar dados protegidos **independentemente de ordem judicial ou do consentimento livre e expresso do(s) usuário(s) envolvido(s), ou, ainda, fora das hipóteses legais**, como admitir que agentes estatais possam contornar o óbice legal por seus próprios meios, acessando o conteúdo armazenado **(e legalmente protegido)** do aparelho telefônico encontrado fortuitamente na cena do crime e apreendido com fundamento no art. 6º, inciso II, do CPP?

Também antes da Emenda Constitucional nº 115/22, a Lei nº 13.709, de 14 de agosto de 2018, conhecida como Lei Geral de Proteção de Dados Pessoais (LGPD) e nitidamente inspirada na **General Data Protection Regulation (GDPR)** (Regulamento 2016/679 da União Europeia), parece alçar os "dados pessoais" **a uma categoria dotada de autonomia com relação aos direitos à privacidade e à intimidade**, previstos no art. 5º, inciso X, da Constituição Federal, mas por ser emanação da personalidade do indivíduo, e estar a esses direitos intrinsecamente relacionada, seria merecedora de proteção jurídica diferenciada. Afinal, protegendo-se os dados, protege-se a informação neles contida, assegurando-se a privacidade ou a intimidade de seu detentor.

Destaco os arts. **1º, 2º e 6º** do aludido diploma legal, cuja redação transcrevo:

> "Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, **inclusive nos meios digitais**, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.
>
> Parágrafo único. As normas gerais contidas nesta Lei são de interesse nacional e devem ser observadas pela União, Estados, Distrito Federal e Municípios" (Incluído pela Lei nº 13.853, de 2019).
>
> "Art. 2º A disciplina da proteção de dados pessoais tem

como fundamentos:

I - o respeito à privacidade;

II - a autodeterminação informativa;

III - a liberdade de expressão, de informação, de comunicação e de opinião;

IV - a inviolabilidade da intimidade, da honra e da imagem;

V - o desenvolvimento econômico e tecnológico e a inovação;

VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e

VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais."

"Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:

I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;

II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;

III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;

IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;

V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;

VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;

VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de

> destruição, perda, alteração, comunicação ou difusão;
>
> VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;
>
> IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;
>
> X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas."

Ressalto, ainda, que a LGPD excluiu de sua disciplina, **expressa e propositalmente, a regulação do tratamento de dados para fins de segurança pública e de atividades de persecução e repressão de infrações penais**, a qual deverá ser objeto de legislação específica, que

> "deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular previsto nesta lei" (art. 4º, **caput** e inciso III, alíneas **a** e **d**, c/c o § 1º).

Há, ainda, um outro ponto que gostaria de destacar. Apesar de relativamente recente, o direito à privacidade passou (e ainda passa) por considerável ressignificação. A princípio, a doutrina o definia como o direito de estar só (**the right to be let alone***)* e, mais recentemente, a ele passou se referir à possibilidade de se proceder ao "controle informacional" a respeito dos dados que dizem respeito à própria pessoa, porque consistiriam, em última instância, em manifestação de sua personalidade. De toda sorte, há sempre uma tênue linha divisória entre privacidade (ou vida privada) e intimidade.

Nesse sentido, explica **Mikhail Vieira de Lorenzi Cancelier** o seguinte:

> "Nascido em berço burguês, o direito à privacidade, de maneira geral, permaneceu restrito às suas origens até o final da primeira metade do século XX. Tal cenário começa a alterar-se de forma mais contundente no decorrer da década de 1960 motivado, sobretudo, pelo crescimento da circulação de informações, consequência do desenvolvimento exponencial da

tecnologia de coleta e sensoriamento, resultando em uma 'capacidade técnica cada vez maior de recolher, processar e utilizar a informação' (DONEDA, 2006, p. 12). Para além do fator informacional, como já visto anteriormente, do decorrer do século XX, a relação do indivíduo e da sociedade com os espaços público e privado também experimentam mudanças significativas, promovendo a democratização do interesse pela tutela da privacidade, assim como de seu exercício. Dessa forma, e com velocidade considerável, o direito à privacidade vai expandindo suas fronteiras, alcançando novos sujeitos, englobando diferentes objetos e tornando-se presente em locais com ele antes incompatíveis.

No Brasil, tanto o constituinte quanto o legislador ordinário, ao elaborarem a Constituição 1988 e o Código Civil de 2002 (Lei nº 10.406) optaram por não fazer uso do termo privacidade, mas das expressões vida privada e intimidade, sem oferecer conceitos a nenhuma delas. Na Constituição de 1988 fala-se, também, em sigilo (de correspondência, das comunicações telegráficas, de dados e das comunicações telefônicas) e na inviolabilidade da casa. Fica claro que é possível fazer uso de qualquer um dos termos para referenciar a mesma situação. Por exemplo, fala-se em vida privada ou vida íntima para tratar do mesmo espaço da vida sobre a qual se fala. Algo secreto, sigiloso ou íntimo pode ser relacionado ao mesmo aspecto que se deseja manter em segredo. O privado pode ser íntimo, o íntimo pode ser secreto, o secreto pode ser privado. Ao mesmo tempo, cada um deles poderá assumir - de forma bastante subjetiva - a depender do sujeito da fala, um significado específico. Assim, nem sempre o íntimo será secreto ou o assunto sigiloso será privado. O que se quer dizer é que o significado do discurso irá variar conforme quem o profere, possibilitando cada um dos termos aqui apresentados usos variados. Juridicamente, a mesma possibilidade é aventada. Privacidade, então, deve ser vista antes de tudo como exercício de uma liberdade da pessoa, uma necessidade humana. Parte-se para uma visão da privacidade que é interna ao sujeito, faz parte dele, formando-o como ser humano. Seja trabalhando a privacidade como o estar só ou numa perspectiva mais contemporânea de controle informacional, não se pode perder o vínculo com a pessoa, como forma de manifestação da personalidade. Ter privacidade é fundamental ao indivíduo, não apenas em oposição ao público, mas numa relação interna,

visto que não será possível a assunção de seus desejos sem a construção de seu espaço íntimo.

Lafer (1988, p. 239), fazendo uso da expressão 'direito à intimidade', caracteriza-o como '[...] direito do indivíduo de estar só e a possibilidade que deve ter toda pessoa de excluir do conhecimento de terceiros aquilo que a ela só se refere e que diz respeito ao seu modo de ser no âmbito da vida privada'. Malta (2007, p. 28) acompanha a corrente que vê no direito à intimidade a proteção dos pensamentos e emoções mais restritos da pessoa. Machado (2014, p. 73) aponta a intimidade como o 'núcleo essencial da pessoa'. Zanon (3013, p. 48), sem a intenção de cravar uma definição absoluta, situa a intimidade num local exclusivo que o sujeito reserva a si mesmo. Ardenghi (2012, p. 238) coloca o direito à intimidade como o poder conferido à pessoa de se resguardar de intromissões ao espaço mais reservado de sua existência, assim como 'a faculdade de fazer concessões nesse terreno'.

Para nós, apesar de considerar importante a diferenciação entre os termos privacidade e intimidade, não se enxerga impedimentos no uso da expressão direito à privacidade para tratar do direito à intimidade, afinal este está inserido naquele. Ademais, acompanha-se o entendimento de Cabral (2012, p. 116-117) no sentido de que o 'grau de proteção da intimidade em uma dada situação poderá variar de acordo com elementos objetivos casuísticos'. Assim, o '[...] resguardo da reserva varia na medida em que os fatos situem-se no ciclo de sigilo, de resguardo ou de publicidade da vida do indivíduo. Tudo depende de tudo. Das pessoas, de cada pessoa, da sua sensibilidade e das suas circunstâncias; nas necessidades e exigências da sociedade relativas ao conhecimento e à transparência da vida em comum (CABRAL, 2012, p. 116-117)'" (CANCELIER, Mikhail Vieira de Lorenzi. O direito à privacidade hoje: perspectiva histórica e o cenário brasileiro. **Sequência**, nº 76, v. 38, Florianópolis, setembro de 2017, p. 213-239).

Feitas essas considerações, registro que a Suprema Corte Brasileira, como prenuncia o voto divergente do Ministro **Gilmar Mendes** no presente caso, não está alheia aos novos tempos e a seus desafios específicos.

A factibilidade de se acessar, por meio de aparelhos celulares, **bem mais que metadados relativos à comunicação telefônica havida a partir**

de terminal específico introduz na discussão travada nos autos, inevitavelmente, a questão da inviolabilidade da intimidade, da vida privada, da honra e da imagem (CF/88, art. 5º, inciso X), agora reforçada pelo direito à proteção dos dados pessoais, inclusive nos meios digitais (CF/88, art. 5º, inciso LXXIX), introduzido pela EC nº 115, de 2022. São esses fatos empíricos e normativos, supervenientes ao julgamento do HC nº 91.867, que justificam e conferem proteção jurídica especial aos dados armazenados, o que enseja a superação do precedente e a construção de uma solução distinta para o caso concreto, mais condizente com a nova realidade.

Por tudo isso, revendo meu posicionamento original, **concluo pela inadmissibilidade de se permitir à autoridade policial a devassa do conteúdo de aparelhos celulares apreendidos independentemente de prévia autorização judicial**. Nas hipóteses como a dos autos, de apreensão de aparelhos celulares com fundamento no art. 6º do CPP, a autoridade policial deverá requerer ao juízo competente, justificadamente, autorização para acessar os dados ali contidos. O requerimento formal possibilitará ao juízo sopesar, diante das peculiaridades e circunstâncias do caso concreto, a adequação, a necessidade e a proporcionalidade em sentido estrito da medida, estabelecendo a abrangência da extração e da análise dos dados coletados **e, especialmente, assegurará a lisura da cadeia de custódia das provas porventura obtidas a partir daí**, como determinam o art. 158-A e seguintes do CPP, inseridos pela Lei nº 13.964, de 2019.

Registro, por último, que o Superior Tribunal de Justiça, há algum tempo,

> "vem enfatizando, em sucessivos julgados, que é ilícita a tomada de dados, bem como das conversas de WhatsApp, obtidas diretamente pela autoridade policial em aparelho celular apreendido no flagrante, sem prévia autorização judicial" (STJ, HC nº 674.185/MG, Rel. Min. **Sebastião Reis Júnior**, Sexta Turma, julgado em 17/8/21, DJe de 20/8/21).

Assim, para aquele Tribunal Superior, dados constantes de aparelhos celulares somente são admitidos como prova lícita no processo penal quando há prévio mandado de busca e apreensão expedido por juiz competente, ou autorização judicial para o acesso aos dados dos celulares apreendidos, ou, ainda, quando há autorização voluntária para esse

acesso pelo interlocutor da conversa (**v.g.**, REsp nº 1.675.501/MG, Rel. Min. **Sebastião Reis Júnior**, Sexta Turma, DJe de 27/10/17; AgRg no HC nº 646.771/PR, Rel. Min. **João Otávio de Noronha**, Quinta Turma, DJe de 13/8/21; AgRg no HC nº 773.03/SP, Rel. Min. **Laurita Vaz**, Sexta Turma, DJe de 19/10/23; AgRg no AREsp nº 2.347.064/SC, Rel. Min. **Reinaldo Soares da Fonseca**, Quinta Turma, DJe de 30/10/23; AgRg na PET no HC nº 768.319/SP, Rel. Min. **Messod Azulay Neto**, Quinta Turma, DJe de 20/12/23).

No caso concreto, como muito bem consignado no voto condutor do acórdão recorrido,

> "[a]pós a vítima ter entregue o aparelho de telefonia celular em sede policial, **o agente da lei MAYKE 'tomou a liberdade' de acessar os dados ali armazenados e referentes não só a fotografias guardadas pelo implicado, como também à agenda de telefones e ao histórico de ligações ali construído e no qual estaria armazenada a última ligação telefônica efetuada por GUILHERME**, que foi para sua namorada, após o que se desenvolveu aquela narrada investigação, que culminou com a identificação do implicado, bem como com a localização, tanto do domicílio do mesmo, quanto de sua namorada e para onde rumaram os agentes da lei, acabando por efetuar a prisão do rapinador.
>
> Neste contexto, tem-se por inequívoca a constatação de que a identificação do autor dos fatos foi alcançada unicamente mercê do indevido, desautorizado e ilegal manuseio daquele aparelho de telefonia celular, **o que importou na flagrante e indisfarçável quebra da proteção constitucional incidente sobre <u>a inviolabilidade do sigilo dos dados e das comunicações telefônicas ali existentes</u>**, o que apenas poderia se dar, por exceção, mediante expressa autorização judicial para tanto, mas o que foi ignorado e desrespeitado, muito embora não encerrasse maior dificuldade a observância da exigência legal, bastando para tanto que o policial civil que recebeu o referido aparelho telefônico, de imediato, encaminhasse este ao Delegado de Polícia informando a relevância do objeto, de modo a que tal Autoridade Policial representasse junto ao Plantão Judiciário de modo a obter a autorização para o acesso e verificação dos dados pretendidos" (fl. 238 e-STJ – grifo nosso).

É irrepreensível a solução dada pelo Tribunal *a Quo* ao entender

pela **ilicitude do acesso não autorizado judicialmente ao conteúdo do aparelho celular e da prova daí resultante**, já que a estratégia investigativa – da qual resultou a elucidação do fato criminoso e de sua autoria, a prisão em flagrante do recorrido e sua posterior condenação pelo delito de roubo – só foi definida a partir desse acesso e das informações por esse meio obtidas, contaminando todo o acervo probatório angariado.

Ante o exposto, alterando meu entendimento original, **nego provimento ao recurso extraordinário com agravo**.

Tendo em vista o julgamento do presente recurso, **dou por prejudicados os requerimentos constantes das Petições/STF nº 38.990/18 e nº 77.244/17**, as quais continham pedido de suspensão de processos que tramitam em instâncias ordinárias.

Por fim, aderindo à proposta do Ministro **Gilmar Mendes**, à qual **acresço** a necessidade de **atuação célere e diligente dos órgãos de persecução penal** na busca da necessária autorização judicial, bem como a necessidade de se conferir **prioridade à tramitação e à apreciação** de pedidos dessa natureza, inclusive em regime de plantão judiciário, fixo a tese de repercussão geral nos seguintes termos:

> "1. O acesso a registro telefônico, agenda de contatos e demais dados contidos em aparelhos celulares apreendidos no local do crime atribuído ao acusado depende de prévia decisão judicial que justifique, com base em elementos concretos, a necessidade e a adequação da medida e delimite sua abrangência à luz dos direitos fundamentais à intimidade, à privacidade, ao sigilo das comunicações e à proteção dos dados pessoais, inclusive nos meios digitais (CF, art. 5º, incisos X, XII e LXXIX).
>
> 2. Em tais hipóteses, a celeridade se impõe, devendo a autoridade policial atuar com a maior rapidez e eficiência possível e o Poder Judiciário conferir tramitação e apreciação prioritárias aos pedidos dessa natureza, inclusive em regime de plantão."

É como voto.