V O T O

O Senhor Ministro Gilmar Mendes: Conforme o art. 5º, XII, da CF, é inviolável o sigilo das comunicações telefônicas e de dados, salvo por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal.

Por sua vez, a **inviolabilidade da vida privada e da intimidade** é afirmada pelo art. 5º, X, da Constituição Federal. Como leciona Paulo Gonet Branco, o " *sigilo das comunicações é não só um corolário da garantia da livre expressão de pensamento; exprime também aspecto tradicional do direito à privacidade e à intimidade"* (MENDES, Gilmar F.; BRANCO, Paulo G. G. *Curso de Direito Constitucional*. Saraiva, 2013. p. 293).

Tradicionalmente, a doutrina entendia que a inviolabilidade das comunicações não se aplicava aos dados registrados, adotando uma interpretação mais estrita da norma contida no art. 5º, XII, da CF/88.

Partia-se da compreensão de que os dados em si não eram objeto de proteção, mas somente as comunicações realizadas.

Nesse sentido, vejam-se as distinções realizadas por Tercio Sampaio Ferraz:

> "O sigilo, no inciso XII do art. 5º, está referido à comunicação, no interesse da defesa da privacidade. Isto é feito, no texto, em dois blocos: a Constituição fala em sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações 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 telefônica. 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 defesa do mercado, também não está havendo**

Plenário Virtual - minuta de voto - 02/11/20 13:41

> **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 que não pode ser violada por sujeito estranho à comunicação" (FERRAZ, Tercio S. Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado. *Cadernos de Direito Constitucional e Ciência Política,* n. 1, 1992).

Essa orientação foi incorporada pela jurisprudência do Supremo Tribunal Federal.

No julgamento do **HC 91.867/PA** (Segunda Turma, de minha relatoria, DJe 20.9.2012), destaquei a distinção entre *comunicação telefônica* e *registros telefônicos* , os quais receberiam proteção jurídica distinta.

Naquela oportunidade, defendi que não poderia interpretar-se a cláusula do artigo 5º, XII, da CF no sentido de proteção aos dados enquanto registro, depósito registral. A proteção constitucional seria da comunicação, e não dos dados.

A mesma linha de raciocínio foi adotada no julgamento do RE 418.416 /SC, Tribunal Pleno, DJ 14.12.2007, de relatoria do ilustre Ministro Sepúlveda Pertence, no sentido de estender a proteção da inviolabilidade constitucional à comunicação de dados, e não aos dados propriamente ditos, já que *"tornaria impossível qualquer investigação administrativa, fosse qual fosse"*.

Creio, contudo, que a modificação das circunstâncias fáticas e jurídicas, a promulgação de leis posteriores e o significativo desenvolvimento das tecnologias da comunicação, do tráfego de dados e dos aparelhos *smartphones* , leva, **nos dias atuais, a solução distinta.** Sem dúvidas, cada vez mais, a nossa vida quase inteira está registrada em nossos aparelhos celulares.

Questiona-se se o acesso a informações e dados contidos nos celulares se encontra ou não expressamente abrangido pela cláusula do inciso XII do art. 5º, conforme destacado nos precedentes acima descritos e reforçado pelo ilustre Ministro Relator.

Plenário Virtual - minuta de voto - 02/12/2015 13:41

Trata-se de **questão-problema** extremamente relevante e bem colocada pela doutrina: " *Nesse contexto, o art. 244 do Código de Processo Penal é claro ao dizer que 'a busca pessoal independerá de mandado, no caso de prisão (...). Que o preso em flagrante tenha seu corpo e suas vestes revistadas e apalpadas, está, portanto, autorizado nessas circunstâncias. A questão que se coloca, entretanto, é se é permitido às autoridades policiais estender os limites da busca pessoal do acusado preso 'independentemente de mandado', acessando também dados armazenados no celular por ele portado. A prisão em flagrante autoriza a devassa a tudo que está salvo eletronicamente em dispositivos carregados pelo preso em flagrante, sem que seja necessária ordem judicial?* " (ANTONIALLI, Dennys; ABREU, Jacqueline; MASSARO, Heloisa; LUCIANO, Maria. Acesso de autoridades policiais a celulares em abordagens: retrato e análise da jurisprudência de tribunais estaduais. *Revista Brasileira de Ciências Criminais* , v. 27, n. 154, abr. 2019, p. 191).

Contudo, ainda que se conclua pela não inclusão na referida cláusula, **entendo que tais dados e informações encontram-se abrangidos pela proteção à intimidade e privacidade, constante do inciso X do mesmo art. 5º.**

Tratando sobre o direito à intimidade, José Adércio Leite Sampaio defende que:

> "Em geral, define-se o direito à intimidade como uma espécie de editoria das informações pessoais ou como um genérico 'direito a ser deixado em paz'. Ele é mais do que isso e mais bem se apresenta como um direito à liberdade, marcado por um conteúdo mais determinado ou determinável, conjugado a um complexo de princípios constitucionais, que nada mais são do que suas manifestações concretas. [...] **Afirmar que o ser humano é livre exige, não como seu pressuposto, mas como consectário, reconhecer seu domínio ou controle sobre os inputs e outputs de informação** . Esse sentido natural da liberdade de traduz, no mundo jurídico, na liberdade 'informacional' próxima ao que o Tribunal Constitucional Federal alemão chamou de *Informationelle Selbsstbestimmung,* ou autodeterminação em matéria de informação, que conjuga o aspecto negativo de não impedimento ao positivo, de controle" (In: CANOTILHO, J. J. Gomes; MENDES, Gilmar; SARLET, Ingo; STRECK, Lênio Luiz. *Comentários à Constituição do Brasil,* p. 292-293).

Plenário Virtual - minuta de voto - 02/12/2020 13:41

No âmbito infraconstitucional, as normas do art. 3º, II, III; 7º, I, II, III, VII; arts. 10 e 11 da Lei 12.965/2014 – o marco civil da internet –, estabelecem diversas proteções à privacidade, aos dados pessoais, à vida privada, ao fluxo de comunicações e às comunicações privadas dos usuários da *internet* .

A norma do art. 7º, III, da referida lei é elucidativa ao prever a inviolabilidade e sigilo das **comunicações privadas armazenadas (dados armazenados)** , *"salvo por ordem judicial".*

Percebe-se, portanto, que a legislação infraconstitucional avançou para possibilitar a proteção dos dados armazenados em comunicações privadas, os quais só podem ser acessados mediante prévia decisão judicial – matéria submetida à reserva de jurisdição.

Entendo que o avanço nesse importante tema da proteção do direito à intimidade e à vida privada deve ser considerado na interpretação do alcance das normas do art. 5º, X e XII, CF.

Mais importante que a alteração do contexto jurídico, **a impactante transformação das circunstâncias fáticas joga novas luzes sobre o tema.**

Nesse sentido, houve um incrível desenvolvimento dos mecanismos de comunicação e armazenamento de dados pessoais em *smartphones* e telefones celulares na última década.

Nos dias atuais, esses aparelhos são capazes de registrar as mais variadas informações sobre os seus usuários, como a sua precisa localização por sistema 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.

Conforme noticiado pelos meios de comunicação, os celulares são a principal forma de acesso dos brasileiros e cidadãos do país à *internet.* Esse

plenário virtual - minuta de voto - 02/11/2013 13:11

motivo, por si só, já seria suficiente para concluir pela incidência das normas acima descritas no que toca à proteção dos dados, fluxos de dados e demais informações contidas nesses dispositivos.

Afirma-se que " *a utilização habitual das novas tecnologias torna necessária a obtenção de prova de tipo tecnológico que, embora contribua para aprimorar a eficácia estatal na persecução dos delitos, em igual medida aumentará o risco de lesividade ao direito fundamental à autodeterminação informativa das pessoas investigadas* " (PÉREZ ESTRADA, Miren J. La protección de los datos personales en el registro de dispositivos de almacenamiento masivo de información. *Revista Brasileira de Direito Processual Penal* , vol. 5, n. 3, set./dez. 2019, p. 1308, tradução livre).

Considerando essa nova realidade e defendendo a necessidade de decisão judicial para acesso aos dados contidos em aparelhos telefônicos, assenta-se na doutrina que:

> " **Do direito fundamental à privacidade protegido constitucionalmente extrai-se como princípio básico, que quanto mais grave for a intervenção, maiores devem ser os requisitos para a intervenção nesse direito e mais específica deve ser a lei que prevê tal interferência** . Essa regra, deduzida do princípio da proporcionalidade, está presente também no inciso XII, do art. 5° da Constituição Federal, que exige a reserva legal qualificada para a intervenção na garantia da inviolabilidade do sigilo das comunicações telegráficas, de dados e das comunicações telefônicas, ao prescrever o requisito 'da ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal'.
>
> **Se o STF no RE 418.416/SC já entendeu que a garantia da inviolabilidade de sigilo art. 5°, XII, referia-se à comunicação de dados e não aos dados em si, é porque certamente o cenário dos riscos ao cidadão era bastante diverso tendo em vista as tecnologias então existentes** . Afinal, usualmente os dados sofrem maior risco de interceptação durante o processo de comunicação – isto é, no tráfego – e não enquanto eles estão armazenados. Ocorre que com o advento da internet e dos aparelhos pessoais conectados em rede, a constelação de riscos alterou-se radicalmente e os programas espiões são o maior exemplo do risco de acesso clandestino e de manipulação dos dados armazenados em sistemas pessoais, que na vida moderna, guardam praticamente todas as informações a respeito de seu usuário. Nesse contexto, a efetividade da garantia constitucional da inviolabilidade

Plenário Virtual - minuta de voto - 04/11/2020 13:41

> do sigilo pressupõe que ela alcance também os dados armazenados em sistemas informáticos pessoais – tais como computadores, smartphones e agendas eletrônicas – cujo acesso passa a ser possível por meio desses programas e que podem acarretar riscos gravíssimos de monitoramento e vigilância ao cidadão sem que ele tome sequer conhecimento a respeito." (MENDES, Laura Schertel. **Uso de softwares espiões pela polícia: prática legal?** Disponível em: <//www.jota.info/opiniao-e-analise/artigos/uso-de-softwares-espioes-pela-policia-pratica-legal-04062015>. Acesso em 4.6.2015).

Os casos citados no referido artigo são paradigmáticos. Há, nos dias atuais, a possibilidade de inserção de *softwares* espiões em aparelhos celulares (MENDES, Carlos Hélder. *Tecnoinvestigação.* Entre a proteção de dados e a infiltração por software. JusPodivm, 2020; CAPRIOLI, Francesco. Il "captatore informatico" come strumento di ricerca della prova in Italia. *Revista Brasileira de Direito Processual Penal* , v. 3, n. 2, 2017).

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. Câmeras de reconhecimento facial integradas à internet possibilitam o reconhecimento instantâneo de suspeitos. Algorítimos podem ser usados para prever e evitar crimes (GUIMARÃES, Rodrigo C. A Inteligência Artificial e a disputa por diferentes caminhos em sua utilização preditiva no processo penal. *Revista Brasileira de Direito Processual Penal* , v. 5, n. 3, 2019; PEDRINA, Gustavo M. Consequências e perspectivas da aplicação de inteligência artificial a casos penais. *Revista Brasileira de Direito Processual Penal* , v. 5, n. 3, 2019).

Esses avanços tecnológicos são importantes e devem ser utilizados para a segurança pública dos cidadãos e a elucidação de delitos (SOARES, Gustavo T. *Investigação criminal e inovações técnicas e tecnológicas.* D' Plácido, 2016). Contudo, **deve-se ter cautela, limites e controles para não transformar o Estado policial em um Estado espião e onipresente** , conforme descrito por George Orwell em seu livro 1984.

Destaque-se que essas recentes ressignificações do direito à privacidade e à intimidade também têm sido objeto de intenso debate em outros países.

Em 2018, por exemplo, o Tribunal Constitucional alemão declarou a inconstitucionalidade da lei de proteção da Constituição do Estado de Nordrhein-Westfalen (NRW-VSG), que permitia à polícia daquela unidade

Plenário Virtual - minuta de voto - 02/11/2020 13:41

da federação a realização de buscas ou investigações secretas e remotas em computadores de pessoas suspeitas de cometer ilícitos criminais, autorizando, ainda, o monitoramento de todas as atividades de suspeitos na internet (MENKE, Fabiano. *In:* MENDES, Gilmar Ferreira; SARLET, Ingo Wolfgang; COELHO, Alexandre Zavaglia P. *Direito, Inovação e Tecnologia,* p. 215-216).

Nesse julgamento, a Corte construiu o conceito do denominado direito fundamental da garantia da confidencialidade e integridade dos sistemas técnico-informacionais (*Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme*).

Ou seja, decidiu a Corte alemã que os dados pessoais dos indivíduos não podem ser acessados de forma indiscriminada, devendo existir sistemas, procedimentos e instrumentos de controle contra esses acessos indevidos (GRECO, Luís; GLEIZER, Orlandino. A infiltração online no processo penal – Notícia sobre a experiência alemã. *Revista Brasileira de Direito Processual Penal* , vol. 5, n. 3, p. 1483-1518, set./dez. 2019).

A Europa também possui uma avançada legislação sobre a proteção de dados (*General Data Protection Regulation* - GDPR) recentemente aprovada, que dispõe sobre o livre consentimento no compartilhamento de dados e informações pessoais, a privacidade dos usuários e até mesmo a portabilidade das informações fornecidas.

Embora voltada para as relações entre os usuários da internet e as grandes empresas de comunicação, a legislação em questão evidencia a importância da proteção aos dados nos dias atuais.

Nos Estados Unidos, o precedente marcante da Suprema Corte se deu em **Riley V. Califórnia** , de 2014, em que se decidiu, à unanimidade, que uma busca de conteúdos digitais em um celular durante uma prisão seria inconstitucional se não houvesse autorização judicial. No caso, afirmou-se que a autorização de busca pessoal durante uma prisão tem as funções de garantir a segurança dos policiais e de preservar a prova e, nesse sentido, o celular, por si só, não acarretaria qualquer risco ou dano, de modo que poderia ser retido para que então se buscasse a autorização judicial.

Passando à análise da questão colocada neste agravo em recurso extraordinário, **entendo ser possível o acesso aos dados contidos em**

Plenário Virtual - minuta de voto - 02/11/20 13:41

aparelhos celulares, uma vez que não há uma norma absoluta de proibição da visualização do seu conteúdo, conforme se poderia extrair a partir de uma interpretação literal da norma contida no art. 5º, XII, da Constituição da República.

Não obstante, a proteção à intimidade e à vida privada, contida no art. 5º, X, da CF/88, e a exigência da observância ao princípio da proporcionalidade nas intervenções estatais nesses direitos impõem a revisão de meu posicionamento anterior, para que **o acesso seja condicionado à prévia decisão judicial.** (GLOECKNER, Ricardo J.; EILBERG, Daniela D. Busca e apreensão de dados em telefones celulares: novos desafios diante dos avanços tecnológicos. *Revista Brasileira de Ciências Criminais* , , v. 27, n. 156, p. 353-393, jun. 2019).

As normas do art. 3º, II, III; 7º, I, II, III, VII; art. 10 e 11 da Lei 12.965/2014 e as significativas alterações no contexto fático subjacente evidenciam se tratar de verdadeiro caso de mutação constitucional na interpretação do âmbito de proteção dos direitos estabelecidos no art. 5º, X e XII, da CF.

Da mesma forma, **não** se mostra viável conferir **acesso parcial às informações** contidas nos aparelhos celulares, uma vez que tal posicionamento acarretaria o enfraquecimento do grau de proteção que deve ser conferido a partir das normas constitucionais e legais aplicáveis ao caso, possibilitando abusos e acessos indevidos que poderiam ser inclusive escamoteados.

Destaco, por último, que a permissão do acesso direto, pelas autoridades policiais, pode estimular que pressões indevidas sejam exercidas sobre os acusados para o fornecimento de senhas de acesso a informações confidenciais.

Não é incomum ouvir relatos de investigados que forneceram "voluntariamente" senhas de acesso a celulares ou prestaram depoimentos informalmente no momento da prisão e, posteriormente, na fase judicial do processo, afirmam que, em realidade, foram pressionados a isso.

Desta feita, o acesso direto pode conflitar, ainda, com o direito fundamental à não autoincriminação (art. 5º, LVII, da CF/88). Penso, portanto, que o **acesso aos aparelhos telefônicos deve ser submetido a**

Plenário Virtual - minuta de voto - 02/12/2020 13:41

prévia decisão judicial, na qual seja demonstrado, *in concreto* , a necessidade, adequação e proporcionalidade do acesso aos dados e informações requeridos.

Trata-se de medida fundamental para resguardar os direitos individuais e evitar buscas genéricas (*fishing expedition*). Isso porque a necessidade de controle judicial impõe a demonstração da necessidade da medida e da sua justa causa, além de possibilitar o estabelecimento de limites aos dados a serem coletados.

Ressalta-se que **nada impede a atuação da polícia no momento do flagrante para apreender o aparelho celular, respeitados os requisitos legais para tanto** (haver fundada suspeita de que existam provas em sua memória) **e a cadeia de custódia** , para posterior representação ao juízo para que autorize o acesso aos dados. Contudo, vale destacar que tal apreensão não pode se tornar uma atitude automática, visto que depende da constatação de fundada suspeita e potencial relevância probatória, o que será submetido a posterior controle judicial.

Ademais, pode-se aventar hipótese em que o acesso aos dados do celular possa se mostrar extremamente urgente , como para localizar uma pessoa sequestrada ou evitar um ataque terrorista. Por óbvio, em tais casos excepcionais, a ponderação dos valores em jogo poderia eventualmente justificar o acesso mesmo antes da autorização judicial (ZILLI, Marcos. A prisão em flagrante e o acesso de dados em dispositivos móveis. Nem utopia, nem distopia, apenas racionalidade. In: ANTONIALLI, ABREU (ed.). *Direitos fundamentais e processo penal na era digital* . Internetlab, 2018. p. 64-99). Contudo, por óbvio, trata-se de situação extremamente excepcional, a ser posteriormente controlada pelo juízo, sob pena de ilicitude probatória se injustificada.

Por fim, entendo ainda que o STF poderia caminhar para uma formulação semelhante a uma Miranda *clause* , no qual o acesso indevido a dados pessoais ou a obtenção de informações sem a observância das garantias fundamentais do processo leve à inutilização dos elementos de prova obtidos, ante a proibição das provas ilícitas contida no art. 5º, LVI, da CF.

Por esses motivos, **divirjo do eminente relator** e **voto pelo desprovimento do recurso interposto** e proponho a fixação da seguinte **tese** , em sede de repercussão geral:

Plenário Virtual - minuta de voto - 02/11/2018 13:41

"O acesso a registro telefônico, agenda de contatos e demais dados contidos em aparelhos celulares apreendidos no local do crime atribuído ao acusado **depende de prévia decisão judicial que justifique**, com base em elementos concretos, a necessidade e a adequação da medida e delimite a sua abrangência à luz dos direitos fundamentais à intimidade, à privacidade e ao sigilo das comunicações **e dados** dos indivíduos (CF, art. 5º, X e XX)."

É como voto.

Plenário Virtual - minuta de voto - 02/11/20 13:41