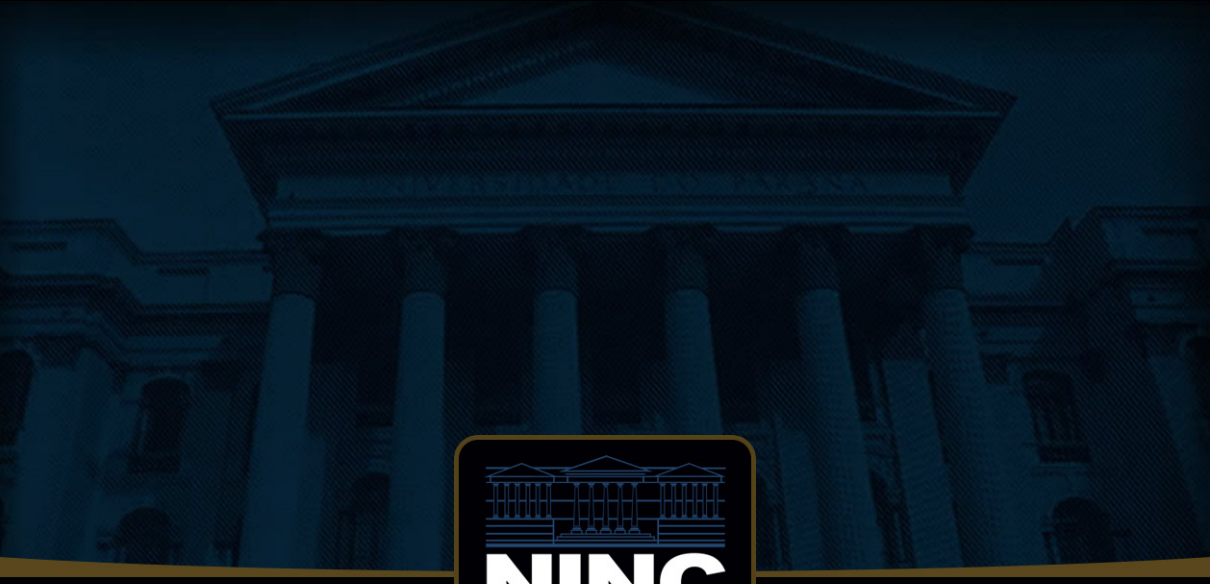

NINC
NÚCLEO DE INVESTIGAÇÕES CONSTITUCIONAIS
UFPR

REVISTA DE INVESTIGAÇÕES CONSTITUCIONAIS

JOURNAL OF CONSTITUTIONAL RESEARCH

VOL. 11 | N. 1 | JANEIRO/ABRIL 2024 | ISSN 2359-5639

Licenciado sob uma Licença Creative Commons
Licensed under Creative Commons

Artigo

Revista de Investigações Constitucionais
ISSN 2359-5639
DOI: 10.5380/rinc.v11i1.89280

Comunicação de dados, não dados em si: origens e problemas do atual paradigma de proteção constitucional do sigilo de dados

Communication of data, not data itself: origins and problems of the current paradigm of constitutional protection of data secrecy

JACQUELINE DE SOUZA ABREU [I, *]

[I] Universidade de São Paulo (São Paulo-SP, Brasil)
jacqueline.abreu@alumni.usp.br
https://orcid.org/0000-0003-0450-4102

Recebido/Received: 27.12.2022 / 27 December 2022
Aprovado/Approved: 15.04.2024 / 15 April 2024

Resumo

Na intersecção entre sigilo telemático e direito processual penal e administrativo, o Supremo Tribunal Federal construiu um argumento prevalente para afastar questões de licitude de certa prova ou meio de obtenção de prova: a Constituição Federal protege "comunicações de dados e não dados em si" - para significar que só protege comunicações em fluxo, e não armazenadas (estáticas) e, hoje também, que só protege conteúdo de comunicações e não outros registros e dados. Por meio de revisão de literatura e de jurisprudência, esse artigo pretende demonstrar como esse argumento surgiu, como é aplicado de forma inconsistente e como anula questões relevantes sobre privacidade na era digital. Sustenta que o STF precisa resgatar uma tese substantiva sobre privacidade e o ônus de fundamentação do Estado no uso da força e que juízes devem olhar para o contexto e nossas práticas sociais ao deliberar sobre tais questões.

Palavras-chave: sigilo; privacidade; dados; Supremo Tribunal Federal; era digital.

Abstract

At the intersection between telematic secrecy and criminal and administrative procedural law, the Brazilian Federal Supreme Court built a prevailing argument to rule out questions of legality of certain evidence or means of obtaining evidence: the Federal Constitution protects "communications of data and not data itself " - to mean that it only protects communications in flow, not stored (static) and, today also, that it only protects communications content and not other records and data. Through a review of literature and case law, this article aims to demonstrate how this argument emerged, how it is applied inconsistently and how it overrides relevant questions about privacy in the digital age. It maintains that the STF needs to rescue a substantive thesis on privacy and reaffirm the State's burden to justify the use of force and that judges should look at the context and our social practices when deliberating on such issues.

Keywords*: secrecy; privacy; data; Brazilian Supreme Federal Court; digital age*

Como citar esse artigo/*How to cite this article*: ABREU, Jacqueline de Souza. Comunicação de dados, não dados em si: origens e problemas do atual paradigma de proteção constitucional do sigilo de dados. **Revista de Investigações Constitucionais**, Curitiba, vol. 11, n. 1, e256, jan./abr. 2024. DOI: 10.5380/rinc.v11i1.89280

[*] Doutora em Direito pela Faculdade de Direito da Universidade de São Paulo (São Paulo-SP, Brasil). Mestra em Direito pela University of California, Berkeley (Berkeley, EUA), com foco em direito e tecnologia, e pela Ludwig-Maximilians-Universität München (Munique, Alemanha), com foco em direitos fundamentais. Foi membro da Comissão de Juristas da Câmara dos Deputados encarregada de elaborar o Anteprojeto de Lei de Proteção de Dados para Segurança Pública e Investigações Criminais Advogada.

SUMÁRIO

1. INTRODUÇÃO

Em 1963, sob a Constituição Federal de 1946, que já garantia ser "inviolável o sigilo da correspondência" (art. 141, § 6º), o Supremo Tribunal Federal (STF) negou provimento a recurso em mandado de segurança impetrado em face de intimação de procuradores da Fazenda para que uma empresa exibisse "papeis existentes em seus arquivos sobre seus negócios comerciais" com outras três empresas.[1] O acórdão entendeu que a então vigente Lei do Sêlo previa que contratos realizados por meio de correspondência não ficam isentos de selo e o art. 58[2] dela autorizaria fiscalização. Dialogando com a garantia constitucional, o voto condutor entendeu que "A inviolabilidade da correspondência assegurada na Constituição não envolve, evidentemente, a correspondência comercial, para efeitos de fiscalização, *quando a carta já chegou ao destinatário*." Como concluiu o relator: "O comerciante tem indiscutível direito a que sua correspondência trafegue pelas repartições postais sem ser violada, mas, uma vez incorporada sua correspondência aos arquivos comerciais, fica ela sujeita à verificação dos agentes fiscais do estado."[3]

O julgado de 60 anos atrás é curioso porque espelha um entendimento que o STF adota até hoje – o de que o inciso XII do art. 5º protege o *fluxo de comunicações*, não os objetos e o teor da comunicação em si. De forma específica ao que este artigo vai tratar, o STF entende que o "sigilo de dados" incluído pela Constituição Federal de 1988 nesse dispositivo protegeria a *comunicação* de dados, e não os dados em si.[4] A

---

1 BRASIL. Supremo Tribunal Federal (Tribunal Pleno). **Recurso em Mandado de Segurança n. 11274/PE**. Relator: Min. Evandro Lins Silva, 27 de novembro de 1963.

2 BRASIL. **Decreto-Lei nº 4.655, de 3 de setembro de 1942**. Dispõe sobre o imposto do selo: "Art. 58. Os estabelecimentos comerciais e industriais, as sociedades civis que revestirem forma comercial, os serventuários de ofício e todos os que são obrigados a manter escrituração não poderão excusar-se, sob pretexto algum, de exibir aos encarregados da fiscalização do selo os papéis e livros de sua escrituração e arquivo."

3 BRASIL. Supremo Tribunal Federal (Tribunal Pleno). **Recurso em Mandado de Segurança n. 11274/PE**, Relator: Min. Evandro Lins Silva, 27 de novembro de 1963.

4 BRASIL. Supremo Tribunal Federal (Tribunal Pleno). **Mandado de Segurança n. 21.729/DF.** Relator: Min. Marco Aurélio, 05 de outubro de 1995 (entendendo que o Banco do Brasil não poderia negar ao MPF informações sobre beneficiários de recursos públicos pela invocação do sigilo bancário). BRASIL. Supremo Tribunal Federal (Tribunal Pleno). **Recurso Extraordinário n. 418.416/SC**. Relator: Min. Sepúlveda Pertence, 10 de maio de 2006 (entendendo que a apreensão de registros contábeis salvos em computador mediante mandado de busca e apreensão não constitui violação à inviolabilidade do sigilo de dados).

tese hoje é atribuída principalmente a Tercio Sampaio Ferraz Junior,[5] que defendeu no início dos anos 1990 que a única maneira de fazer o texto do dispositivo constitucional ter algum sentido é se a inviolabilidade ali resguardada for a do ato de *comunicação,* não das informações comunicadas em si. Informações registradas – física (em cartas e telegramas) ou eletronicamente (dados) – podem ser acessadas mediante busca e apreensão, por exemplo. Mas não o poderiam quando estão em fluxo. Por outro lado, como comunicações telefônicas não deixam registros, o Constituinte teria cuidado de garantir que esse tipo de comunicação, excepcionalmente, fosse "interceptável" para fins de investigações criminais e instruções processuais penais.

Mais recentemente, têm surgido casos – sobretudo colocados pelo avanço tecnológico – que colocam em xeque essa abordagem. De um lado, essa interpretação apresenta uma descontinuidade com como nos relacionamos com mensagens, fotos, arquivos, diários, vídeos – dados *armazenados* em nossos dispositivos eletrônicos. Gera estranhamento a muitos dizer que a Constituição Federal não protege um direito de que pessoas possam manter esses materiais eletrônicos privados, se assim quiserem, só porque estão "estáticos", não em fluxo. Ao mesmo tempo, a criação de um *fluxo de comunicação* não-interceptável – como aqueles viabilizados pela criptografia de ponta-a-ponta, implementada em aplicativos populares como o WhatsApp – deveria ser a realização máxima desse direito a não quebrar o fluxo de comunicação – um caso simples. Apesar disso, o tema gerou enorme controvérsia em tribunais e segue pendente de deliberação no STF.[6]

Nesse contexto, esse artigo pretende demonstrar como a tese ainda hoje reverberada pelo STF é inconsistente e anula questões relevantes sobre privacidade na era digital. Sustenta que precisamos de um desenvolvimento doutrinário e jurisprudencial mais honesto com como nos relacionamos com questões de privacidade – o que deve se estender inclusive em matéria de direito processual penal e direito administrativo policial. Isso significa primeiro reconhecer que questões de privacidade são mais complexas do que apenas determinar se algo é estático ou dinâmico e que a discussão sobre proteção da privacidade em face do Estado não se reduz a um debate sobre a exigência de uma ordem judicial prévia. O teste deve ser trocado por uma avaliação contextual e voltada à análise de critérios materiais de razão e necessidade que resgatem o ônus do Estado de justificar o uso da força contra alguém.

---

[5] FERRAZ JUNIOR, Tercio Sampaio. Sigilo de Dados: o direito à privacidade e os limites da função fiscalizadora do Estado. **Revista da Faculdade de Direito da Universidade de São Paulo**, São Paulo, vol. 88, p. 439–59, 1993.

[6] QUEIROZ, Rafael Mafei Rabelo. Privacidade, criptografia e dever de cumprimento de ordens judiciais por aplicativos de trocas de mensagens. In: DONEDA, Danilo (org.). **Caderno Especial - A Regulação da Criptografia no Direito Brasileiro**. São Paulo: Thomson Reuters Brasil, 2018, 13–26.

2. COMUNICAR-SE EM SIGILO: O HISTÓRICO PRÉ-DEBATE JURISPRUDENCIAL

O direito a algum tipo de sigilo está presente em todas as Constituições do Brasil. O mais antigo deles é o que protege cartas, que já se encontrava de algum modo na Constituição Imperial de 1824, junto com alguma proteção ao domicílio.[7] As origens desse direito ao sigilo de correspondência oferecem uma das explicações e um dos argumentos mais fortes para a interpretação hoje dada pelo STF. Afinal, a capacidade de manter a privacidade de cartas trocadas entre pessoas à distância dependia da guarda da confidencialidade de seu teor enquanto estivessem em trânsito: enquanto viajam de uma *casa/domicílio* à outra, de um indivíduo ao outro. Já está aí, portanto, a ideia de garantir um direito específico que proteja uma comunicação *enquanto em fluxo*.

Segundo Neil Richards e Daniel Solove recontam da perspectiva dos Estados Unidos, em tempos coloniais, era difícil *selar* uma carta a ponto de impedir que fosse lida por terceiros.[8] Serviços postais logo então começaram a cobrar esse dever de seus funcionários e surgiram leis ainda em 1710 que impediam a abertura, detenção e atraso de cartas. Pouco a pouco seria atribuída uma noção de objeto "sagrado" às ideias e imagens expressadas por pessoas em cartas – expressões que exigiam respeito.[9] Em 1877, em *Ex parte Jackson,* a Suprema Corte dos Estados Unidos entendeu que "*o fato de que as pessoas dão voluntariamente ao Estado suas cartas para entrega não renuncia a proteção, já que era esperado do Estado que mantenha a confidencialidade*" [10] – não afastando a proteção da Quarta Emenda para tais objetos simplesmente porque tais papéis passavam a ser detidos e transmitidos por órgãos estatais. Mesmo fora do "local privado" da casa, algumas expressões humanas merecem um "espaço privado".[11]

Após as cartas, vieram as preocupações em garantir que novos órgãos públicos e sobretudo empresas encarregadas de viabilizar comunicações à distância respeitassem a inviolabilidade de correspondências. As invenções do telégrafo e do telefone

---

7 BRASIL. **Constituição Política do Império do Brazil, de 25 de março de 1824**:VII. Todo o Cidadão tem em sua casa um asylo inviolavel. De noite não se poderá entrar nella, senão por seu consentimento, ou para o defender de incendio, ou inundação; e de dia só será franqueada a sua entrada nos casos, e pela maneira, que a Lei determinar. XXVII. O Segredo das Cartas é inviolável. A Administração do Correio fica rigorosamente responsavel por qualquer infracção deste Artigo.

8 SOLOVE, Daniel; RICHARDS, Neil. Privacy's Other Path: Recovering the Law of Confidentiality. **The Georgetown Law Journal**, Washington, vol. 96, p. 123-182, 2007, p. 141–42.

9 SOLOVE, Daniel; RICHARDS, Neil. Privacy's Other Path: Recovering the Law of Confidentiality. **The Georgetown Law Journal**, Washington, vol. 96, p. 123-182, 2007, p. 142–43. Era reforçada ainda, segundo os autores, por doutrinas de *direitos autorais* pelo qual "expressões não publicadas [fixadas] em cartas" seriam protegidas contra publicação involuntária: não precisavam ser íntimas a ponto de ferir sentimentos de autor – a própria noção de propriedade veiculava esse interesse e essa proteção.

10 *Ex parte Jackson,* 96 US 727 (1877).

11 SHAPIRO, Stuart. Places and Spaces: The Historical Interaction of Technology, Home, and Privacy. **The Information Society,** vol. 14, n. 4, p. 275-284, nov. 1998. https://doi.org/10.1080/019722498128728. p. 278–79.

foram objeto de apropriação social e respostas regulatórias semelhantes às cartas.[12] No Brasil, passaram a ter referência constitucional na cláusula de direitos a partir da Constituição Federal de 1967.[13] Em 1988, "por exigência da nossa época"[14], o dispositivo constitucional passou a também incluir a menção aqui estudada de proteção a dados: "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" (inciso XII).

Curiosamente, a intenção legislativa, que nunca se pode dizer única, nem clara, nem resolvida, pelo menos a princípio passa longe do que depois se transformaria a discussão constitucional. De forma específica, a primeira menção a "dados" no contexto Constituinte apareceu no "Substitutivo 2" do Relator, ao que se permite extrair dos arquivos da Assembleia Nacional Constituinte, acolhendo emenda de Artur da Távola (PMDB/RJ) de que o "sigilo clássico" deveria agora abranger também a hipótese de "comunicação de dados", "no mundo contemporâneo". A redação dada no substitutivo foi: "É inviolável o sigilo da correspondência e das comunicações telegráficas, telefônicas e de dados, salvo por ordem judicial, nos casos e na forma que a lei estabelecer, para fins de instrução processual". Na fase final de redação, foi aprovada sugestão de Hélio Braun (PMDB/RS) de que o que se deve "fixar é a inviolabilidade do sigilo de dados e não precipuamente o sigilo das comunicações de dados", acolhida na versão aprovada e promulgada, após intercessão de Ricardo Fiuza (PFL) no Plenário explícita para este fim.[15] Isto é, se hoje a leitura que prevalece é restritiva, não foi isso que vocalizavam constituintes que lutaram pela redação final do dispositivo.

---

12 SOLOVE, Daniel; RICHARDS, Neil. Privacy's Other Path: Recovering the Law of Confidentiality. **The Georgetown Law Journal**, Washington, DC, vol. 96, p. 123-182, 2007, p. 144–45. SHAPIRO, Stuart. Places and Spaces: The Historical Interaction of Technology, Home, and Privacy. **The Information Society,** vol. 14, nº 4, p. 275-284, nov. 1998, pp. 280, https://doi.org/10.1080/019722498128728.

13 BRASIL. **Constituição da República Federativa do Brasil de 24 de janeiro de 1967**. Art. 150 - A Constituição assegura aos brasileiros e aos estrangeiros residentes no Pais a inviolabilidade dos direitos concernentes à vida, à liberdade, à segurança e à propriedade, nos termos seguintes:§ 9º - São invioláveis a correspondência e o sigilo das comunicações telegráficas e telefônicas. § 10 - A casa é o asilo inviolável. do indivíduo. Ninguém pode penetrar nela, à noite, sem consentimento do morador, a não ser em caso de crime ou desastre, nem durante o dia, fora dos casos e na forma que a lei estabelecer.

14 Palavras do Constituinte Adolfo Oliveira (PFL), defendendo o Substitutivo 2. Ver ASSEMBLEIA NACIONAL CONSTITUINTE. **Diário da Assembléia Nacional Constituinte (Suplemento 'C')**, Brasília, 1987, p. 186, https://www.senado.leg.br/publicacoes/anais/constituinte/9b_Sistematizacao.pdf.

15 Ver CÂMARA DOS DEPUTADOS. **A construção do artigo 5º da Constituição de 1988**. Brasília: Câmara dos Deputados. Edições Câmara, 2013, p. 79-82;1545;1751; ASSEMBLEIA NACIONAL CONSTITUINTE. **Diário da Assembléia Nacional Constituinte (Suplemento 'B')**. Brasília, 1988, p. 213, http://imagem.camara.gov.br/Imagem/d/pdf/307anc23set1988SUPB.pdf.

3. A CONSTRUÇÃO DA JURISPRUDÊNCIA DO STF

Um olhar na jurisprudência do STF sobre o "sigilo de dados" mostra que tanto o aparente objetivo legislativo de conferir uma abrangente proteção a dados quanto a fundamentação possível para destacar a proteção de comunicações em fluxo perderam o rumo. Nesse item, reconstruo essa história em quatro atos – quatro julgados: (i) o primeiro ainda firmando essa proteção, mas já com ressalvas que depois voltariam a assombrar; (ii) o segundo, que escancara a controvérsia, sem decidi-la; (iii) o terceiro, em que o recorte da proteção é feito; (iv) o quarto, que revela como essa proteção foi replicada.[16]

O primeiro precedente do STF relevante para a jurisprudência de sigilo de dados é a Ação Penal 307, de 1994, em que o ex-Presidente da República Fernando Collor de Mello figurava como réu principal.[17] Nela se suscitava a inadmissibilidade de gravações feitas por Sebastião Curió de conversas telefônicas tidas com o ex-tesoureiro de campanha Paulo César Farias e o ex-Ministro Bernardo Cabral (mas sem conhecimento deles) e obtenção de memória de computadores por busca e apreensão domiciliar no escritório da empresa de PC Farias. A parte relevante neste artigo é o tratamento de computadores.

O relator Ministro Ilmar Galvão relata que os computadores foram inicialmente apreendidos por agentes da Receita Federal durante diligência de natureza fiscal e depois encaminhados à Polícia Federal, onde foram degravados.[18] Em contraste com o que antes ocorria, afirma então que a Constituição Federal de 1988 não admite o ingresso em domicílio durante o dia mesmo de agentes do Fisco no exercício de sua função sem autorização judicial prévia. Este seria, portanto, um vício de origem.[19] De todo modo, ainda que essa diligência tivesse ocorrido de forma regular, o acesso à memória do computador não poderia:

> *a Polícia Federal não poderia ter-se apropriado dos dados contidos naquele micro-computador, para mandar decodifica-los ao seu alvedrio, como fez, acobertados que se achavam pelo sigilo, o qual, conquanto se possa ter por corolário da inviolabilidade do próprio recinto dos escritórios da empresa, acha-se especificamente contemplado no*

[16] Realizei pesquisa sobre julgados do STF sobre privacidade em face do Estado originalmente para a tese de doutorado, onde faço alongada exposição e reconstrução histórica: ABREU, Jacqueline de Souza. **Privacidade, segurança e tecnologia**. Tese (Doutorado em Direito) – Faculdade de Direito da Universidade de São Paulo. São Paulo, 2022. Os quatro casos aqui destacados foram selecionados a partir de sua relevância e influência para a construção da jurisprudência detectada nesta pesquisa anterior.

[17] BRASIL. Supremo Tribunal Federal (Tribunal Pleno). **Ação Penal n. 307/DF**. Relator: Min. Ilmar Galvão, 13 de dezembro de 1994. Diário de Justiça, 13 de outubro de 1995.

[18] BRASIL. Supremo Tribunal Federal (Tribunal Pleno). **Ação Penal n. 307/DF**. Relator: Min. Ilmar Galvão, 13 de dezembro de 1994. Diário de Justiça, 13 de outubro de 1995, p. 2179.

[19] BRASIL. Supremo Tribunal Federal (Tribunal Pleno). **Ação Penal n. 307/DF**. Relator: Min. Ilmar Galvão, 13 de dezembro de 1994. Diário de Justiça, 13 de outubro de 1995, p. 2187.

> *inciso XII, do mesmo artigo, ao lado da correspondência e das comunicações telegráficas e telefônicas.*[20]

Referia-se ao sigilo de dados. Continuou:

> *Aliás, nos tempos modernos, em que todos os aparelhos datilográficos das empresas é realizado por meio de digitação, a invasão da memória dos computadores implica fatalmente a quebra do sigilo não apenas dos dados em geral, desde os relativos a simples agenda até os relacionados a fórmulas e cálculos, mas também de toda correspondência, epistolar e telegráfica, em relação aos quais o manto constitucional é de natureza absoluta, já que não deixou espaço reservado ao trabalho normativo do legislador ordinário, como se fez com as comunicações telefônicas.*[21]

O revisor Min. Moreira Alves adota a mesma linha de raciocínio: além do mesmo vício de origem já pontuado (ausência de autorização judicial prévia para ingressar no domicílio), entendeu que "com relação aos dados em geral – e, consequentemente, os constantes de computador que pode armazenar as mais sigilosas informações de seu proprietário – estão eles cobertos pela garantia do disposto no inciso XII do artigo 5º da Constituição"[22]. Não dá, entretanto, o mesmo ar de proteção absoluta que o relator, apesar de ressaltar a necessidade de regulamentação:

> *Pelos termos em que está redigido esse dispositivo, é possível sustentar que as demais inviolabilidades só admitem sejam afastadas por texto constitucional expresso. Mas, ainda quando se admita que possam ser postas de lado nas hipóteses e na forma prevista na lei, o que é certo é que não há lei que disponha a respeito no concernente – que é o que importa no momento – à inviolabilidade dos dados aludidos no citado texto constitucional.*[23]

Os min. Carlos Velloso, Celso de Mello, Néri da Silveira, Sepúlveda Pertence, Sidney Sanchez e Octavio Gallotti concordam quanto à ilegalidade da prova obtida pela degravação da memória de computar, sobretudo por ter sido obtida por busca e apreensão domiciliar sem autorização judicial.[24] O Min. Sepúlveda Pertence ressalva que

---

[20] BRASIL. Supremo Tribunal Federal (Tribunal Pleno). **Ação Penal n. 307/DF**. Relator: Min. Ilmar Galvão, 13 de dezembro de 1994. Diário de Justiça, 13 de outubro de 1995 p. 2187.

[21] BRASIL. Supremo Tribunal Federal (Tribunal Pleno). **Ação Penal n. 307/DF**. Relator: Min. Ilmar Galvão, 13 de dezembro de 1994. Diário de Justiça, 13 de outubro de 1995 p. 2188.

[22] BRASIL. Supremo Tribunal Federal (Tribunal Pleno). **Ação Penal n. 307/DF**. Relator: Min. Ilmar Galvão, 13 de dezembro de 1994. Diário de Justiça, 13 de outubro de 1995 p. 2440-1.

[23] BRASIL. Supremo Tribunal Federal (Tribunal Pleno). **Ação Penal n. 307/DF**. Relator: Min. Ilmar Galvão, 13 de dezembro de 1994. Diário de Justiça, 13 de outubro de 1995, p. 2441.

[24] Não participaram os Ministros Marco Aurélio, Francisco Rezek e Maurício Corrêa.

> *Basta-me aí a ilegalidade quanto à apreensão, à vista do inciso XI, da Constituição. Não me comprometo, por ora, consequentemente, com o problema do que se chamou "sigilo de dados": continuo um tanto perplexo, no que toca a saber se, no art. 5º, inciso XII, da Constituição, o que se protegeu foi o sigilo de qualquer dado armazenado por alguém ou o sigilo da comunicação de dados, uma vez que se trata naquele inciso, de diversas formas de comunicação intersubjetiva e não do sigilo de arquivos. Basta-me, portanto, a ilicitude da apreensão, à falta de autorização judicial à diligência dos agentes do Fisco.*[25]

Em 1996, a discussão que chegou ao STF foi a constitucionalidade da previsão de interceptação telemática, estabelecida no parágrafo único do art. 1º da Lei nº 9.296/96 (Lei de Interceptações).[26] Nesse caso, o segundo aqui destacado, a controvérsia seria reconhecida explicitamente. A Associação dos Delegados de Polícia do Brasil propôs a ADI 1.488, com pedido liminar para suspender o dispositivo – por "atentar contra a inviolabilidade do sigilo das comunicações no âmbito do processamento de dados (art. 5º, inciso XII, C.F.), inadmissível como prova (art. 5º, inciso LVI, C.F.)". O receio era de que essa possibilidade "resultará em laudos de degravação de computadores que, no caso concreto, ocorrerá sempre ao arrepio da garantia de inviolabilidade da intimidade das pessoas (art. 5º, inciso X, C.F.)". O pedido liminar foi julgado pelo Plenário no mesmo ano.

O relator Min. Néri da Silveira reconhece que existe uma controvérsia relativa à interpretação apropriada do inciso XII do art. 5º e a qual grupo de comunicações/objetos se referiria a exceção que admite o afastamento do sigilo "no último caso". A defender a possibilidade cravada na Lei nº 9.296/96 estaria o entendimento segundo o qual "comunicações de telemática e informática" estariam abrangidas em "comunicações telefônicas", o que seria a realidade "no estágio atual do desenvolvimento tecnológico". Nessa linha, o relator cita trabalho de Ivan de Lira Carvalho para o qual a Constituinte teria admitido interferência em *informes em tráfego* – inclusive das comunicações de dados que se dão através de linha telefônica. Avançando para ponto que depois geraria distinções duradouras, o relator também registra a defesa deste autor de que, se a Constituição admitiu a interferência para tanto, também o fez sobre "dados estáticos" parados em computador ("se pode mais, pode menos", era a lógica). Daí recorda o entendimento do STF na AP 307 "no sentido da inviolabilidade de dados constantes de

---

[25] BRASIL. Supremo Tribunal Federal (Tribunal Pleno). **Ação Penal n. 307/DF**. Relator: Min. Ilmar Galvão, 13 de dezembro de 1994. Diário de Justiça, 13 de outubro de 1995, p. 2637.

[26] BRASIL, Supremo Tribunal Federal (Tribunal Pleno). **Medida Cautelar na Ação Direta de Inconstitucionalidade n. 1488/DF**. Relator: Min. Néri da Silveira, 07 de novembro de 1996. BRASIL, **Lei n. 9.296, de 24 de julho de 1996**. Regulamenta o inciso XII, parte final, do art. 5º da Constituição Federal: "Art. 1º A interceptação de comunicações telefônicas, de qualquer natureza, para prova em investigação criminal e em instrução processual penal, observará o disposto nesta Lei e dependerá de ordem do juiz competente da ação principal, sob segredo de justiça. Parágrafo único. O disposto nesta Lei aplica-se à interceptação do fluxo de comunicações em sistemas de informática e telemática."

computador". A ação proposta carregaria, então, "fundamentos relevantes". O acórdão fecha, entretanto, com julgamento unânime de que não haveria "periculum in mora" a justificar a suspensão da norma. O pedido de mérito nunca foi a julgamento e ação teve seguimento negado por razões formais posteriormente. Apesar dos "fundamentos relevantes", eles não viriam a ser enfrentados.

O Min. Sepúlveda Pertence retomaria a discussão sobre sigilo telemático de computadores exatamente de onde ela parou na AP 307. É nesse terceiro ato que a discussão posta é finalmente enfrentada. No Recurso Extraordinário 418.416, de 2006, abre esclarecendo que o caso foi afetado ao Plenário após insistência do advogado, pelo qual o seu voto no caso estaria em desacordo com o entendimento firmado na AP do Collor.[27] O ministro sustenta que nunca houve entendimento pacificado de que o sigilo de dados seria absoluto – muito embora esse pareça ter sido o entendimento do relator ministro Ilmar Galvão naquele caso e, em alguma medida, também do revisor Moreira Alves. A maioria focou na ausência de mandado de busca e apreensão *domiciliar* e os que concordaram com relator e revisor não se manifestaram explicitamente quanto à compreensão sobre sigilo de dados. É nesse caso que o Min. Sepúlveda Pertence vai proferir o voto que mais marcará a jurisprudência do STF sobre esse tema.

Tratava-se de busca e apreensão feita em sede de empresa para apuração de crimes fiscais. Diferente do que ocorreu na Ação Penal, aqui a apreensão de computadores se deu mediante cumprimento de mandado judicial de busca e apreensão relativamente específico – no sentido de que ao menos continha a previsão de que equipamentos informáticos poderiam ser apreendidos e selecionados aqueles "interessantes à investigação" – criminal. Nesse sentido, não se colocava a questão de violação a domicílio (art. 5º, XI), que esteve no fundo do caso anterior. Aqui, sendo o mandado específico para incluir esses objetos, era válido, e a prova, em tese lícita. Nesse contexto, sobrava saber se a apreensão da mídia em si representava uma violação.

Neste ponto, o ministro retomará entendimento a que já sinalizava em votos anteriores – nos mais diversos contextos, e notadamente no MS 21.729, de 1995, que tratava de sigilo bancário de beneficiários de recursos públicos. Para ele:

> *na espécie, 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 de comunicações de dados (interceptação das comunicações), mas sim apreensão de base física na qual se encontravam os dados, mediante prévia e fundamentada decisão judicial.*[28]

---

[27] BRASIL. Supremo Tribunal Federal (Tribunal Pleno). **Recurso Extraordinário n. 418.416/SC**. Relator: Min. Sepúlveda Pertence, 10 de maio de 2006. Diário de Justiça eletrônico, 02 de fevereiro de 2007.

[28] BRASIL. Supremo Tribunal Federal (Tribunal Pleno). **Recurso Extraordinário n. 418.416/SC**. Relator: Min. Sepúlveda Pertence, 10 de maio de 2006. Diário de Justiça eletrônico, 02 de fevereiro de 2007, p. 1264.

Ampara-se em trabalho de Tercio Sampaio Ferraz Jr. para a distinção.[29]

O Plenário acompanha o ministro na tese. Em seus comentários na convergência, o Min. Cezar Peluso diz ser pouco razoável entender-se que a Constituição Federal trataria de sigilo *dos dados*. Nessa linha "bastaria que a prova do crime fosse sempre registrada no computador, o que tornaria inviável a persecução criminal"[30]. Também o Min. Gilmar Mendes: "entendo que não se pode interpretar essa cláusula do artigo 5º, XII, no sentido de proteção aos dados enquanto registro, depósito registral." O contrário reforçaria uma ideia de "um tipo de paraíso da impunidade ou da criminalidade"[31] Os intérpretes parecem recear que reconhecer a proteção de sigilo de dados no inciso XII signifique conferir uma proteção absoluta a todo tipo de dado.

Nos debates, o Min. Sepúlveda Pertence ressalvaria que "o que merece proteção está protegido sobre o outro inciso, o que protege a intimidade"[32], ponto que o Min. Lewandowski também faria. É do Min. Carlos Ayres Britto, também concordando com Pertence, as observações mais elaboradas sobre privacidade e como aquela discussão se encaixava diante das proteções dos incisos X, XI e XII do art. 5º da CF/88:

> *A matéria está toda imbricada, não é a toa que a Constituição cuida dos três incisos assim, um atrás do outro - só faço uma distinção: a Constituição não confunde privacidade com intimidade. Tanto que usa de duas palavras diferentes, ligando uma à outra pela conjunção aditiva 'e'. Privacidade, para mim, é uma comunicação reservada entre pessoas, digamos, 'en petit comité'. É a pessoa se relacionando com seus amigos, com seus parentes. Ao passo que a intimidade é a pessoa consigo mesma, sozinha. Exemplo: alguém escrevendo um diário - está no uso de sua intimidade. (...)*
>
> *Os três círculos da doutrina europeia. Ao passo que uma comunicação por 'e-mail' já é privacidade; uma carta já é privacidade. Porém um diário, não; é absolutamente intimidade. Quando a pessoa está consigo mesma, é intimidade; quando está com os seus - amigos, parentes -, aí se dá a privacidade. Agora tanto a intimidade como a privacidade têm o seu locus, o seu habitat na casa em que se mora ou em que se trabalha. Vejam como os três incisos se entrelaçam. E a interpretação do Ministro Sepúlveda Pertence*

---

29 FERRAZ JUNIOR, Tercio Sampaio. "Sigilo de Dados: o direito à privacidade e os limites da função fiscalizadora do Estado". **Revista da Faculdade de Direito da Universidade de São Paulo**, São Paulo, vol. 88, p. 439–59, 1993.

30 BRASIL. Supremo Tribunal Federal (Tribunal Pleno). **Recurso Extraordinário n. 418.416/SC**. Relator: Min. Sepúlveda Pertence, 10 de maio de 2006. Diário de Justiça eletrônico, 02 de fevereiro de 2007, p. 1275.

31 BRASIL. Supremo Tribunal Federal (Tribunal Pleno). **Recurso Extraordinário n. 418.416/SC**. Relator: Min. Sepúlveda Pertence, 10 de maio de 2006. Diário de Justiça eletrônico, 02 de fevereiro de 2007, p. 1314.

32 BRASIL. Supremo Tribunal Federal (Tribunal Pleno). **Recurso Extraordinário n. 418.416/SC**. Relator: Min. Sepúlveda Pertence, 10 de maio de 2006. Diário de Justiça eletrônico, 02 de fevereiro de 2007, p. 1289.

> *não só nos possibilita conhecer o conteúdo e o alcance do inciso XII, como nos auxilia a conhecer o conteúdo e o alcance dos incisos imediatamente anteriores.*[33]

Apesar do cenário desenhado sobre privacidade e o entrelaçamento entre dispositivos, de modo que a discussão não se encerraria no art. 5º, XII, essa ideia não permaneceria, isto é, não seria transportada a outros julgados. É na síntese do Min. Marco Aurélio que se vê a ideia que repercutiria, suprimindo-se o "no caso": "comungo inteiramente com a afirmação dos colegas de não haver, no caso, a proteção quanto a dados armazenados."[34] O único que não se posicionou sobre o tema foi o Min. Joaquim Barbosa – concordando no resultando, mas destacando outros aspectos no acórdão: para ele a decisão era fundamentada, teve origem em documentos nos quais se vislumbrou a possível prática de sonegação de tributos e na verificação de uma série de discrepâncias entre declarações e faturas.[35]

No Habeas Corpus 91.867, de 2012, a 2ª Turma apreciou a licitude de provas obtidas pela verificação do histórico de chamadas de dois celulares apreendidos com preso em flagrante – os fatos são de 2004.[36] Nesse caso vemos a força do entendimento fixado sobre dados armazenados, aqui aplicado às mais corriqueiras atividades policiais. Isto é, desconectada de outras proteções de fundo, como a inviolabilidade do domicílio, e de investigações sobre fatos específicos já ocorridos. O voto do relator Min. Gilmar Mendes, em linha com o que se viu até aqui, abre com um "destaque" que na verdade se refere a duas postulações distintas, mas cujo sentido se mesclaria no voto e na jurisprudência formada a partir daí: a *primeira,* de que "não se confundem *comunicação telefônica* e os *registros telefônicos*, recebendo, inclusive, proteção jurídica distinta"[37]. Reporta-se ao fato de que o teor de conversas pode ser distinguido de (meta)dados relativos ao histórico de chamadas recebidas e efetuadas. A seguir, no entanto, a distinção ganha outra conotação: consigna que "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 os 'dados'."[38] Cita jurisprudência que afirma essa interpretação e a clássica obra de Tercio Sampaio Ferraz Junior.

---

[33] BRASIL. Supremo Tribunal Federal (Tribunal Pleno). **Recurso Extraordinário n. 418.416/SC**. Relator: Min. Sepúlveda Pertence, 10 de maio de 2006. Diário de Justiça eletrônico, 02 de fevereiro de 2007, p. 1303-4.

[34] BRASIL. Supremo Tribunal Federal (Tribunal Pleno). **Recurso Extraordinário n. 418.416/SC**. Relator: Min. Sepúlveda Pertence, 10 de maio de 2006. Diário de Justiça eletrônico, 02 de fevereiro de 2007, p. 1317.

[35] BRASIL. Supremo Tribunal Federal (Tribunal Pleno). **Recurso Extraordinário n. 418.416/SC**. Relator: Min. Sepúlveda Pertence, 10 de maio de 2006. Diário de Justiça Eletrônico, 02 de fevereiro de 2007, p. 1306.

[36] BRASIL. Supremo Tribunal Federal (2. Turma). **Habeas Corpus n. 91.867/PA**. Relator: Min. Gilmar Mendes, 24 de abril de 2012. Diário de Justiça Eletrônico, 20 de setembro de 2012.

[37] BRASIL. Supremo Tribunal Federal (2. Turma). **Habeas Corpus n. 91.867/PA**. Relator: Min. Gilmar Mendes, 24 de abril de 2012. Diário de Justiça Eletrônico, 20 de setembro de 2012, p. 9.

[38] BRASIL. Supremo Tribunal Federal (2. Turma). **Habeas Corpus n. 91.867/PA**. Relator: Min. Gilmar Mendes, 24 de abril de 2012. Diário de Justiça Eletrônico, 20 de setembro de 2012, p. 10.

Após a abertura, recorre aos argumentos de que (i) "a autoridade policial que, ao prender em flagrante delito o corréu, tomou a cautela de colher todo material com potencial interesse para investigação" agiu segundo prescreve o art. 6º do CPP[39]; (ii) "os números — registros de ligação no aparelho — estavam acessíveis à autoridade policial, mediante simples exame do objeto apreendido, circunstância que, de fato, diferencia do acesso a informações registradas na empresa de telefonia"; e (iii) o exame teria indicado apenas um número de telefone, dado que não se conectaria a nenhum valor constitucionalmente protegido nem teria de per se nenhum significado. Procede a um conjunto de perguntas retóricas ante à conclusão:

> *Ad argumentadum, abstraindo-se do meio material em que o dado estava registrado (aparelho celular), indago: e se o número estivesse em um pedaço de papel no bolso da camisa usada pelo réu no dia do crime, seria ilícito o acesso pela autoridade policial? E se o número estivesse anotado nas antigas agendas de papel ou em um caderno que estava junto com o réu no momento da prisão? Ademais, impende lembrar que a Constituição Federal excepcionou a inviolabilidade domiciliar na hipótese de flagrante delito (art. 5º, XI). A própria liberdade sofre restrição no flagrante delito. Um aparelho de celular receberia proteção diversa? A obviedade que resulta da resposta a essas indagações, denota que, não raras vezes, na construção argumentativa desvia-se o foco da tutela constitucional. A proteção jurídica à intimidade, à vida privada, não me parece que tenha o alcance pretendido pelo impetrante."*[40]

Nesse contexto, conclui que a atitude dos policiais foi "perfeitamente razoável, não havendo que se falar de lesão à intimidade ou privacidade" dos corréus. Não deixa de também registrar um chavão típico, "Não há direitos e garantias fundamentais de

---

[39] BRASIL. **Decreto-Lei nº 3.689, de 3 de outubro de 1941**. Código de Processo Penal:
Art. 6º Logo que tiver conhecimento da prática da infração penal, a autoridade policial deverá: I - dirigir-se ao local, providenciando para que não se alterem o estado e conservação das coisas, até a chegada dos peritos criminais; (Redação dada pela Lei nº 8.862, de 28.3.1994) II - apreender os objetos que tiverem relação com o fato, após liberados pelos peritos criminais; (Redação dada pela Lei nº 8.862, de 28.3.1994) III - colher todas as provas que servirem para o esclarecimento do fato e suas circunstâncias; IV - ouvir o ofendido; V - ouvir o indiciado, com observância, no que for aplicável, do disposto no Capítulo III do Título VII, deste Livro, devendo o respectivo termo ser assinado por duas testemunhas que lhe tenham ouvido a leitura; VI - proceder a reconhecimento de pessoas e coisas e a acareações; VII - determinar, se for caso, que se proceda a exame de corpo de delito e a quaisquer outras perícias; VIII - ordenar a identificação do indiciado pelo processo datiloscópico, se possível, e fazer juntar aos autos sua folha de antecedentes; IX - averiguar a vida pregressa do indiciado, sob o ponto de vista individual, familiar e social, sua condição econômica, sua atitude e estado de ânimo antes e depois do crime e durante ele, e quaisquer outros elementos que contribuírem para a apreciação do seu temperamento e caráter. X - colher informações sobre a existência de filhos, respectivas idades e se possuem alguma deficiência e o nome e o contato de eventual responsável pelos cuidados dos filhos, indicado pela pessoa presa. (Incluído pela Lei nº 13.257, de 2016)

[40] BRASIL. Supremo Tribunal Federal (2. Turma). **Habeas Corpus n. 91.867/PA**. Relator: Min. Gilmar Mendes, 24 de abril de 2012. Diário de Justiça Eletrônico, 20 de setembro de 2012, p. 14.

caráter absoluto, sendo certo, também, que esses não podem, a qualquer pretexto, servir de manto protetor de práticas escusas."[41] O julgamento foi unânime.

4. A REVERBERAÇÃO E OS PROBLEMAS DO TESTE FIXADO

Assim, há anos prevalece no STF a noção de que apenas o "processo de comunicar" é protegido pelo art. 5º, XII, CF/88 – e reverbera o efeito cadeia da síntese de que a "proteção constitucional é da comunicação 'de dados' e não os 'dados'" em julgados de todo país.

A influência do teste – dados em fluxo ou dados estáticos – chega a ser tanta que obscurece discussões sobre direitos à privacidade que poderiam recorrer a outros dispositivos constitucionais (proteção da intimidade, da vida privada), ou que se assentam na inviolabilidade do domicílio. É o que se vê dos casos acima que já versavam sobre (dados estáticos em) computadores e celulares. Até seria possível dizer que o STF não entendeu que nunca são protegidos, apenas que naqueles contextos (apreensão mediante mandado de busca específico no âmbito de investigação criminal ou busca incidente a uma prisão em flagrante, respectivamente), condições aplicáveis para acesso foram satisfeitas. Mas nuances se perderam. O paradigma de proteção constitucional reduzido a um teste binário do que está em fluxo ou não acaba por fundamentalmente facilitar a obtenção e uso dessas informações nos mais diversos contextos, dispensando até a exigência de observâncias a requisitos materiais – como discussão sobre indícios e causa provável – e a parâmetros de proporcionalidade vinculados a uma análise do contexto.[42] Torna novas e inovadoras medidas de investigação, nunca tratadas em lei, uma não-questão, como se não merecessem maior debate.[43] Na prática, isso significa uma erosão de direitos à privacidade.

---

41 BRASIL. Supremo Tribunal Federal (2. Turma). **Habeas Corpus n. 91.867/PA**. Relator: Min. Gilmar Mendes, 24 de abril de 2012. Diário de Justiça Eletrônico, 20 de setembro de 2012, p. 16-7.

42 Essa colocação tem uma dimensão empírica mais abrangente não só sobre o que foi visto no STF, mas sobre o que se vê da jurisprudência do STJ e em tribunais estaduais ao redor do país que surge daí. Como muitos processos em que são proferidas ordens de quebra de sigilo tramitam em segredo de justiça e, as que são questionadas, são publicizadas muito excepcionalmente já a nível de discussão em tribunais superiores (quando o são), a realização de pesquisa empírica abrangente enfrenta desafios. Para uma visão do impacto dessa jurisprudência em casos de buscas de dispositivos eletrônicos em torno de prisões em flagrante, ver ANTONIALLI, Dennys; ABREU, Jacqueline de Souza; MASSARO, Heloísa; LUCIANO, Maria. Acesso de Autoridades Policiais a Celulares Em Abordagens e Flagrantes: Retrato e Análise Da Jurisprudência de Tribunais Estaduais. **Revista Brasileira de Ciências Criminais,** São Paulo, vol. 154, p. 177–214, 2019. Para relatos de advogados que atuam na área, ver AZEREDO, João Fábio A. Sigilo das Comunicações Eletrônicas Diante do Marco Civil da Internet. In: DE LUCCA, Newton; SIMÃO Filho, Adalberto; LIMA, Cíntia Rosa Pereira de (Coord.). **Direito & Internet III - Tomo II: Marco Civil da Internet (Lei n. 12.965/2014).** São Paulo: Quartier Latin, 2015. p. 211–32. p. 227–28; QUITO, Carina Acesso a Comunicações Eletrônicas Armazenadas na Prática Judiciária". In: ANTONIALLI, Dennys; ABREU, Jacqueline de Souza (Org.). **Direitos Fundamentais e Processo Penal na Era Digital: Doutrina e Prática em Debate**. Vol. I. São Paulo: InternetLab, 2018. p. 100–107.

43 BRASIL. Superior Tribunal de Justiça (6. Turma). **Agravo Regimental no Recurso Especial n. 1.760.815/PR**. Relator: Min. Laurita Vaz, 23 de outubro de 2018. Diário de Justiça Eletrônico, 13 de novembro de 2018

Com a emergência e popularização de tecnologias digitais, em que todas as nossas atividades se tornam dados eletrônicos,[44] a implicação daí extraída seria que a infinidade de "dados armazenados" não estaria protegida: nossas atividades, características, pensamentos, obras e bens que se traduzem em dados "estáticos" não seriam protegidas. Por conta da estranheza que isso causa, quando muito, argumenta-se que *conteúdo* de comunicações *armazenadas* suscita uma proteção constitucional pelo art. 5º, X, CF/88 ou que hoje já existe uma proteção infralegal no Marco Civil da Internet (art. 7º, III).[45] Recentemente, voto do Min. Gilmar Mendes no HC 168052 da 2ª Turma do STF sinalizou mudança de compreensão nessa linha, justamente em atenção aos novos hábitos de comunicação e às capacidades de celulares.[46] O caso foi, entretanto, de resultado apertado (3x2) e, no Pleno, casos que recolocam o problema ainda estão em aberto (como o ARE 1042075), com risco de reafirmação desses critérios simplificadores antigos ou de supostos novos testes que já nascem antigos – ponto a que retornarei adiante.

A jurisprudência precisa ser redirecionada e nesse item desenvolvo as razões: sua incoerência interna com a própria jurisprudência do STF e a pobreza da teoria da privacidade que representa.

4.1. Inconsistências internas

Em primeiro lugar, a jurisprudência sobre sigilo de dados que enfatiza dados em fluxo é incoerente internamente à própria jurisprudência do STF. Como visto no item anterior, o teste ainda hoje aplicado pelo STF e exportado para tribunais Brasil a fora surgiu a partir de um receio de que, não fosse assim, a proteção constitucional a dados teria de ser considerada absoluta na CF/88. Essa posição pressupõe que apenas o processo de comunicar de comunicações telefônicas pode ser quebrado por conta

(entendendo que a quebra de sigilo de todos os registros de ligações e envio de SMS de uma torre de rádio é válida pois afeta unicamente dados estáticos); BRASIL. Superior Tribunal de Justiça (3. Seção). **Recurso em Mandado de Segurança n. 60.698/RJ**. Relator: Min. Rogerio Schietti Cruz, 26 de agosto de 2020. Diário de Justiça Eletrônico, 04 de setembro de 2020 (entendendo que a quebra de sigilo do conjunto desconhecido de pessoas que tenha buscado por certas palavras-chave em serviços de pesquisa não viola a Constituição Federal, entre outras razões, porque envolve dados estáticos).

44 FERGUSON, Andrew Guthrie. Structural Sensor Surveillance. **Iowa Law Review**, Iowa, vol. 106, p. 47–112, 2021.

45 Na doutrina, o descompasso que essa jurisprudência possui numa era com diversas comunicações *armazenadas* já vem sendo denunciada e criticada há um tempo. Ver SIDI, Ricardo. A interceptação de e-mails e a apreensão física de e-mails armazenados. **Revista Fórum de Ciências Criminais**, Belo Horizonte, vol. 4, p. 101-121, jul./dez. 2015, p. 112; AZEREDO, João Fábio A. Sigilo das Comunicações Eletrônicas Diante do Marco Civil da Internet. In: DE LUCCA, Newton; SIMÃO Filho, Adalberto; LIMA, Cíntia Rosa Pereira de (Coord.). **Direito & Internet III - Tomo II: Marco Civil da Internet (Lei n. 12.965/2014).** São Paulo: Quartier Latin, 2015, p. 226–30.

46 "STF: Suspenso julgamento sobre validade de provas obtidas no WhatsApp sem autorização", **Migalhas,** 12 de junho de 2019, https://www.migalhas.com.br/Quentes/17,MI304267,21048-STF+Suspenso+julgamento+-sobre+validade+de+provas+obtidas+no+WhatsApp.

da linguagem de *inviolabilidade* e da exceção contida no próprio texto constitucional: "XII - 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;".

Ocorre que, para que essa leitura e receio fossem minimamente plausíveis, o STF teria que admitir apenas quebra de sigilo de fluxo de interceptações telefônicas, por conta da exceção contida no texto, restando os demais "fluxos" protegidos de forma absoluta. Ao contrário disso, o STF admite tanto (i) interceptações de dados (interceptações telemáticas), tendo deixado de enfrentar definitivamente a discussão sobre a Lei nº 9.296/96 e deixando vingar uma autorização legal de já 25 anos para interceptações do tipo, como se viu, quanto (ii) interceptações mesmo de correspondências (quando há previsão legal ou ordem judicial). Reporto-me a quando o STF teve de decidir se prova obtida por meio de abertura de pacote postado nos Correios viola o sigilo de correspondência. O relator, Min. Marco Aurélio, entendeu que o sigilo de comunicações protege comunicações entre pessoas, independentemente do meio pelo qual ocorre (se carta ou pacote). Havendo suspeita, deveria ter sido buscada autorização judicial para intervir. A maioria, no entanto, e para fins de tese fixada, aderiu ao voto-vogal do Min. Fachin, pelo qual, não havendo autorização judicial, nem existindo hipótese legal em que se insira esse tipo de acesso na legislação que trata de serviços postais, houve violação do sigilo de correspondência.[47] O Min. Alexandre de Moraes restou vencido: para ele, seria possível o acesso sem autorização judicial prévia quando verificados fundados indícios da prática de atividades ilícitas. Como se vê, o fato de que a correspondência estava *em fluxo* nem fez parte da discussão. Ninguém invocou uma proteção absoluta ao processo de comunicar-se. A suposição de que há algo completamente absoluto/inviolável no art. 5º, XII simplesmente não se sustenta na prática judicial do próprio STF.

Em segundo lugar, dados bancários são dados estáticos – e hoje "eletrônicos", insertos em bancos de dados que compõem o sistema financeiro como um todo e o sistema interno de bancos – e a qualidade de dados estáticos nunca foi justificativa para descartar discussões constitucionais sobre o tema. O STF sempre falou em privacidade ao deliberar sobre sigilo bancário.[48] De uma perspectiva básica de coerência, no mínimo, tudo isso deveria ensejar a mesma postura para dados "telemáticos" em geral: serem estáticos não é suficiente para encerrar qualquer outra análise sobre privacidade nem os minimizar.

---

[47] BRASIL. Supremo Tribunal Federal (Tribunal Pleno). **Recurso Extraordinário n. 1116949/PR**. Relator: Min. Marco Aurélio. Relator p/ acórdão Min. Edson Fachin, 18 de agosto de 2020.

[48] NIGRI, Tânia. **O Sigilo Bancário e a Jurisprudência do Supremo Tribunal Federal**. São Paulo: IASP, 2016; ÁVILA, Ana Paula Oliveira; WOLOSZYN, André Luis. A tutela jurídica da privacidade e do sigilo na era digital: doutrina, legislação e jurisprudência. **Revista de Investigações Constitucionais**, Curitiba, vol. 4, n. 3. p. 167-200, set./dez. 2017. DOI: 10.5380/rinc.v4i3.51295.

Dois exemplos de envergadura histórica ilustram como o reconhecimento da proteção constitucional é relevante. Em 25 de março de 1992, o STF negou petição de Delegado da Polícia Federal que buscava autorização judicial para a quebra de sigilo do ex-Ministro do Trabalho Antonio Rogério Magri, demitido em janeiro daquele ano pelo Presidente Fernando Collor de Mello em meio a acusações de corrupção.[49] O pedido para fornecimento de extratos bancários de 1991 e 1992 dele e da esposa se baseava unicamente em publicação na imprensa segundo a qual cintas de dinheiro teriam sido encontradas no lixo de sua residência. O relator, Min. Carlos Velloso, na mesma linha que o parecer da Procuradoria-Geral da República, entendeu que "o sigilo bancário protege interesses privados. É ele espécie de direito à privacidade, inerente à personalidade das pessoas e que a Constituição consagra (C.F., art. 5º, X), além de atender 'a uma finalidade de ordem pública, qual seja a de proteção do sistema de crédito' (...)". Dito isso, "não é ele um direito absoluto, devendo ceder, é certo, diante do interesse público, do interesse da justiça, do interesse social, conforme, aliás, tem decidido essa Corte". Em tese, portanto, não haveria dúvidas da possibilidade em tese de quebra de sigilo bancário com autorização judicial. Ocorre aqui que o pedido não estaria instruído "com os elementos de prova mínimos de autoria de delito, aptos a justificar a autorização judicial pretendida". "Aliás, não há notícia do delito que teria sido praticado". Não havia, portanto, suspeita individualizada suficiente a autorizar o deferimento da medida. Isto é, dentro de uma análise judicial prévia sobre a possibilidade de acesso aos dados, houve espaço para uma discussão sobre requisitos materiais. Bastante diferente do que teria ocorrido se a discussão morresse com a constatação de que extratos bancários não constituem comunicação de dados e encerrado a discussão por aí.

Reconhecer a proteção constitucional da privacidade também permite discussão sobre recursos, procedimentos, *standards* de defesa. A autorização judicial prévia sempre serviu de contrapartida para restrições da privacidade sobre informações financeiras, até que seus limites fossem testados em 2019, no âmbito de discussões sobre transferências de dados de autoridades administrativas como a Receita Federal e o COAF (Conselho de Controle de Atividades Financeiras) para o Ministério Público, para fins de investigação criminal.[50] O STF reafirmou um direito à privacidade sobre informações bancárias, mas nesse contexto dispensou a autorização judicial prévia, desde que realizada na forma prevista em legislação – que reservaria tais transferências aos materiais relativos a representações fiscais para fins penais elaboradas pelo Fisco (art.

[49] BRASIL. Supremo Tribunal Federal (Tribunal Pleno). **Petição (Questão de Ordem) n. 577/DF**. Relator: Min Carlos Velloso, 25 de março de 1992. Diário de Justiça, 23 de abril de 1993.

[50] BRASIL. Supremo Tribunal Federal (Tribunal Pleno). **Recurso Extraordinário n. 1.055.941/SP**. Relator: Min. Dias Toffoli, 04 de dezembro de 2019.

198, Código Tributário Nacional[51]). Também definiu que relatórios de inteligência sobre operações suspeitas elaborados pelo COAF podem ser repassados sem autorização judicial prévia (art. 15 da Lei nº 9.613/98[52]) quando presentes indícios de ilícitos. Para fins de tese de repercussão geral, ficou definido que deve ser resguardado o "sigilo das informações em procedimentos formalmente instaurados e sujeitos a posterior controle jurisdicional". Podem ser feitos "unicamente por meio de comunicações formais, com garantia de sigilo, certificação do destinatário e estabelecimento de instrumentos efetivos de apuração e correção de eventuais desvios". Isto é, reconhecendo a proteção constitucional e apesar de dispensando a ordem judicial, foram buscados instrumentos regulatórios alternativos de proteção – ainda que alguns possam criticar a solução,[53] é completamente oposta do resultado que existiria se dados bancários passassem a não ter mais qualquer proteção constitucional simplesmente porque estáticos.

Como se vê dos dois casos, a afirmação de um direito à privacidade sobre dados bancários tende a levar a discussão para outras searas: desde requisitos materiais que devem ser atendidos a exigências e condicionantes procedimentais. O sigilo de dados, telemático, perde muito quando nem chega a esse nível de discussão, que é hábil a garantir mecanismos de responsabilização e controle do exercício do poder investigativo pelo Estado.

---

51 BRASIL. **Lei nº 5.172, de 25 de outubro de 1966** (Código Tributário Nacional). Dispõe sobre o Sistema Tributário Nacional e institui normas gerais de direito tributário aplicáveis à União, Estados e Municípios: "Art. 198. Sem prejuízo do disposto na legislação criminal, é vedada a divulgação, por parte da Fazenda Pública ou de seus servidores, de informação obtida em razão do ofício sobre a situação econômica ou financeira do sujeito passivo ou de terceiros e sobre a natureza e o estado de seus negócios ou atividades. § 1o Excetuam-se do disposto neste artigo, além dos casos previstos no art. 199, os seguintes: I – requisição de autoridade judiciária no interesse da justiça; II – solicitações de autoridade administrativa no interesse da Administração Pública, desde que seja comprovada a instauração regular de processo administrativo, no órgão ou na entidade respectiva, com o objetivo de investigar o sujeito passivo a que se refere a informação, por prática de infração administrativa. § 2o O intercâmbio de informação sigilosa, no âmbito da Administração Pública, será realizado mediante processo regularmente instaurado, e a entrega será feita pessoalmente à autoridade solicitante, mediante recibo, que formalize a transferência e assegure a preservação do sigilo. § 3o Não é vedada a divulgação de informações relativas a: I – representações fiscais para fins penais; II – inscrições na Dívida Ativa da Fazenda Pública; III – parcelamento ou moratória."

52 BRASIL. **Lei nº 9.613, de 3 de março de 1998**. Dispõe sobre os crimes de "lavagem" ou ocultação de bens, direitos e valores; a prevenção da utilização do sistema financeiro para os ilícitos previstos nesta Lei; cria o Conselhor de Controle de Atividades Financeiras – COAF, e dá outras providências: "Art. 15. O COAF comunicará às autoridades competentes para a instauração dos procedimentos cabíveis, quando concluir pela existência de crimes previstos nesta Lei, de fundados indícios de sua prática, ou de qualquer outro ilícito."

53 ESTELLITA, Heloisa. O RE 1.055.941: um pretexto para explorar alguns limites à transmissão, distribuição, comunicação, transferência e difusão de dados pessoais pelo COAF. **Direito Público**, Brasília, vol. 18, nº 100, p. 606–36, 2021. https://doi.org/10.11117/rdp.v18i100.5991.o Supremo Tribunal Federal, ao julgar o Recurso Extraordinário 1.055.941, decidiu que o COAF poderia revelar informações sigilosas (financeiras

4.2. Falta de teoria substantiva

As necessidades de revisitar a tese não param na incoerência interna da jurisprudência do STF. Um teste baseado no caráter "dinâmico" ou "estático" de um dado para identificar a proteção de direito constitucional à privacidade é, no mínimo, insuficiente e, no máximo, completamente equivocado. A doutrina hoje replicada é vazia de fundamentação convincente.[54] A que tipo de fundamento a exclusão de dados estáticos da proteção constitucional ou a redução a priori de sua importância poderia apelar? Não guardamos o que entendemos relevante guardar? Não fazemos isso com cartas e documentos e diversos outros bens que valorizamos? Nossas práticas sociais não resguardam respeito a esse material pessoal? Como isso poderia contaminar pleitos de privacidade?

Comecei este artigo sugerindo que uma perspectiva genealógica do tema pode e deve reconhecer um tipo de vínculo entre a proteção do inciso XII e o "processo de comunicar-se". Como visto, olhando para casos anteriores a 1988 e pondo em perspectiva as origens internacionais históricas desse tipo de garantia de sigilo, temos que a proteção buscava garantir a possibilidade de se comunicar à distância ainda *em* privacidade, sem que canais de comunicação como os Correios fossem subvertidos e explorados por terceiros, pelas empresas e pelo próprio Estado para atravessar a privacidade dos comunicantes. Mesmo porque, fora desse contexto de fluxo, cartas trocadas estavam em geral "armazenadas" na *casa* de alguém (protegidas pelo domicílio) e, quando não à distância, pessoas conversam presencialmente umas com as outras, em que, então, também podia se pressupor haver privacidade, se não houvesse outras pessoas por perto ou se fossem, no máximo, estranhos desinteressados e com memória seletiva. A proteção de um processo de comunicação nunca quis dizer, portanto, que o que estava guardado junto a bens de alguém ou foi dito sob expectativas de privacidade inerentes a uma relação social não merecia proteção. Pelas mesmas razões, no equivalente eletrônico dessas experiências, nunca poderia significar que "dados estáticos" não seriam protegidos de modo algum, que a eles pode haver acesso facilitado ou mesmo livre. O próprio Min. Sepúlveda Pertence, em um dos julgados históricos que originaram essa distinção, visto acima, usou essa leitura do art. 5º, XII apenas para afastar o argumento de que mídias eletrônicas, obtidas dentro de um lar junto e por conta de uma busca e apreensão domiciliar autorizada judicialmente, não poderiam nunca ser acessadas. E só.[55]

---

[54] Para contraste, ver a amplitude e densidade de discussões sobre doutrina interpretativa em torno da Quarta Emenda à Constituição dos Estados Unidos e artigos e livros acadêmicos discutindo diferentes concepções de privacidade e qual a que melhor expressa o valor desse conceito e como deve ser traduzido em proteções jurídicas: COHEN, Julie E. What privacy is for. **Harvard Law Review**, Cambridge, vol. 126, p. 1904–33, 2013; GRAY, David. **The Fourth Amendment in an Age of Surveillance**. Cambridge: Cambridge University Press, 2017; RICHARDS, Neil.**Why Privacy Matters**. Oxford: Oxford University Press, 2021.

[55] Para uma desconstrução também da utilização que artigo do professor Tercio Sampaio Ferraz Jr. recebeu ao longo dos anos para suportar essa visão, ver PONCE, Paula Pedigoni; QUEIROZ, Rafael Mafei Rabelo. Tércio

A razão substantiva que podemos imputar à proteção jurídica tradicional à confidencialidade de comunicações privadas parece muito mais relacionada a resguardar uma prerrogativa de privacidade que está enraizada em nossas práticas sociais que prestigiam a autonomia pessoal sobre a acessibilidade que damos a outras pessoas sobre aspectos da vida de relevância pessoal sob certo contexto. Nós tendemos a respeitar esses limites pessoais e quem não o faz é criticado. Se é assim, devemos nos questionar se outros tipos de privacidades que valorizamos, igualmente enraizada em nossas práticas sociais, não necessitam de proteção em nossas práticas jurídicas. Isso passa por uma leitura integrada de todos os dispositivos constitucionais que revelam um compromisso com direitos à privacidade.

5. UMA PROPOSTA

Nesse ponto, uma interpretação concorrente poderia sustentar que, no lugar do teste binário dinâmico x estático, coloquemos um teste binário que distinga se é conteúdo ou se é informação cadastral e/ou metadados. Isto é, que abandone a discussão em torno do art. 5º, XII e diga que, pelo inciso X, que protege a intimidade e a vida privada, conteúdo está protegido e outros tipos de dados não. É essa hoje proposta aventada por doutrinadores, como antecipei acima, e colocada em voto no STF – como o ARE 1042075, tema 977 de repercussão geral do STF.

Trata-se de caso em que a autoridade policial acessou – sem autorização judicial prévia – números de telefone e fotos de dispositivo encontrado na cena de um crime (roubo na saída de agência bancária, com celular caído na fuga) e assim identificou o suposto dono, que fora acusado. Aplicando o entendimento de sempre, como visto, não haveria problema algum, já que os dados estáticos não seriam protegidos. Mas dizer que não temos uma prerrogativa de privacidade sobre o celular causa enorme estranheza. Nesse contexto, o relator Min. Dias Toffoli propõe manter as distinções entre dados em fluxo e dados estáticos, mas reformulando-a para uma distinção entre conteúdo de comunicações e outros dados e permitindo o acesso direto aos segundos, de modo que a tese a prevalecer no caso seria: 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). O Min. Gilmar Mendes abriu a divergência, já acompanhado do Min. Edson Fachin, com a tese "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

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. **Internet & Sociedade**, São Paulo, vol. 1, nº 1, 64–90, fev. 2020.

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)". O julgamento foi interrompido após pedido de vista do Min. Alexandre de Moraes.

O Superior Tribunal de Justiça (STJ) também já trilha essa via. Esse Tribunal, em 2016, no RHC 51.531[56], foi que primeiro enxergou o descompasso normativo que a interpretação tradicional do STF acarreta: não havendo proteção constitucional para dados telemáticos estáticos, teriam de julgar que ninguém possui direito à privacidade sobre informações salvas em celulares. No caso, isso significaria que a polícia basicamente teria livre acesso a celulares: não haveria problema algum em que a autoridade policial acessasse celular de quem quisesse em abordagens e flagrantes. Foi então afirmado que deveria ser reconhecida proteção a conteúdo de celulares, tornando necessária autorização judicial prévia e sendo ilícita a prova obtida sem essa ordem anterior. Mais recentemente, no entanto, o STJ começou a calibrar essa interpretação para autorizar acesso a "agenda de contatos e histórico de ligações" pela autoridade policial sem ordem judicial, reservando proteção apenas a conteúdo de comunicações.[57] Isto é, pondo no lugar da distinção entre dados em fluxo e dados estáticos uma distinção entre conteúdo de comunicações, de um lado, e outros tipos de dados, de outro.

Essa alternativa tampouco supera os problemas apontados.

De um ponto de vista da jurisprudência do STF, seria igualmente inconsistente tentar selecionar *quais dados* são protegidos ou não. Isso porque o contexto sempre importa. Por exemplo, vejamos "dados cadastrais". Informações para contato são aquelas que provocaram a definição de novo marco para a jurisprudência do STF sobre proteção de dados pessoais. Em 2020, o STF julgou pedido de medida cautelar em cinco ações diretas de inconstitucionalidade no STF (ADI 6387, 6388, 6389, 6390 e 6393) contra a Medida Provisória 954 de 2020, que dispôs que "as empresas de telecomunicação prestadoras do STFC [Serviço Telefônico Fixo Comutado] e do SMP [Serviço Móvel Pessoal] deverão disponibilizar à Fundação IBGE, em meio eletrônico, a relação dos nomes, dos números de telefone e dos endereços de seus consumidores, pessoas físicas ou jurídicas" (art. 2º).

O voto da relatora Min. Rosa Weber, desde a suspensão liminar – referendada pelo Plenário[58], assentou, de forma paradigmática, que também os dados que foram objeto do pedido são protegidos constitucionalmente e que a medida, com escopo

---

[56] BRASIL. Superior Tribunal de Justiça (6. Turma). **Recurso em Habeas Corpus n. 51.531/RO**. Relator: Min. Néfi Cordeiro, 19 de abril de 2016. Diário de Justiça Eletrônico, 09 de maio de 2016.

[57] BRASIL. Superior Tribunal de Justiça (5. Turma). **Recurso Especial n. 1.782.386/RJ**. Relator: Min. Joel Ilan Paciornik, 15 de dezembro de 2020. Diário de Justiça Eletrônico, 18 de dezembro de 2020.

[58] BRASIL. Supremo Tribunal Federal (Tribunal Pleno). **Referendo da Medida Cautelar nas Ações Diretas de Inconstitucionalidade n. 6387, 6388, 6389, 6390 e 6393**/DF. Relatora: Min. Rosa Weber, 07 de maio de 2020. Diário de Justiça Eletrônico, 12 de novembro de 2020.

ambíguo e alcance excessivo, não poderia ser admitida. A finalidade declarada – "produção de estatística oficial" – seria inespecífica, o que comprometeria também a avaliação sobre o atendimento do princípio da necessidade. Ademais, não teria sido elencada qualquer indicação da necessidade de uma coleta massiva de todos os dados, principalmente para pesquisas que, segundo o próprio IBGE declarou, seriam feitas por amostragem. Nesse aspecto, sinalizou que as principais pesquisas já estavam sendo realizadas remotamente, por dados já existentes. Por fim, também observou que não foram previstas medidas de segurança. Todos esses problemas seriam potencializados pela ausência de uma autoridade de controle e supervisão – visto que a Autoridade Nacional de Proteção de Dados prevista na Lei nº 13.709/18 ainda não havia sido criada – e pelo adiamento da entrada em vigor da Lei Geral de Proteção de Dados. A relatora foi seguida pela maioria. Como se vê, os dados em si não podem ser suficientes para afastar discussões – cada contexto suscita uma discussão sobre competências, finalidade, base legal, necessidade, e outras exigências de justiça e devido processo.

Também em 2020, o STF barrou a elaboração de dossiês de informações de servidores públicos integrantes do movimento "antifascista" pela Secretaria de Operações Integradas do Ministério da Justiça por ter como único critério o posicionamento político. O tal dossiê reunia típicos "dados cadastrais": nomes e, em certos casos, fotos e endereços de perfis de redes sociais. Para a relatora da medida cautelar referendada no Plenário, "O uso – ou o abuso – da máquina estatal para a colheita de informações de servidores com postura política contrária ao governo caracteriza desvio de finalidade."[59] Um relatório com esse escopo, ainda que tenha sido feito para "inteligência", seria incompatível com a democracia. É um caso que reforça que mesmo dados simples e comuns podem despertar a proteção de um direito à privacidade se o contexto permitir dizer que é um que a pessoa tem: ninguém deve ser catalogado pelo Estado por suas opiniões políticas, mesmo que isso só envolva "dados estáticos" – mesmo os de tipo cadastral. Sendo assim, propor um novo teste que olhe para certos tipos de dados e diga ou dê margem para que se diga que não há proteção constitucional é incoerente com o que já fez o STF em outros casos recentes. Quando muito, se for para dizer que nesses cenários havia proteção e em outros não há, isso significa admitir que o cenário contextual é relevante para a avaliação – que não pode se perder só olhando ao tipo de dados ou à estaticidade deles. Significa se engajar no empreendimento de elaborar a justificativa para a ação estatal e que conjunto de circunstâncias a autorizam.

De uma perspectiva de teoria da privacidade, o novo teste aventado para definir a proteção constitucional – trocar a distinção entre fluxo e estático por conteúdo e o resto – também é fraco. Os "metadados" podem estar atrelados a exercícios bastante

[59] BRASIL. Supremo Tribunal Federal (Tribunal Pleno). **Medida Cautelar na Arguição de Descumprimento de Preceito Fundamental n. 722/DF**. Relator: Min. Cármen Lúcia, 20 de agosto de 2020. Diário de Justiça Eletrônico, 22 de outubro de 2020.

valiosos de privacidade e reunir informações sobre pessoas que ninguém espera estarem disponíveis para análise de terceiros e sobre as quais legitimamente temos expectativas de privacidade enraizadas em nossas práticas sociais: ninguém sabe quais foram as últimas pessoas a quem alguém telefonou e todos os sites que visitou na internet, senão a própria pessoa – é certo que temos expectativas de privacidade sobre essas informações, que não fazem parte do campo de conhecimento de nenhuma outra pessoa. Ainda que compartilhemos a quem ligamos e de onde ligamos com empresas de telefonia, fazemos isso no contexto de uma relação comercial. Espera-se cuidado com relação ao que é feito com essas informações. Ademais, a própria arquitetura do serviço é uma em que o público em geral não fica sabendo – isso mantém a expectativa de privacidade em face de terceiros.

O fato de que hoje o teste binário aplicado pelo STF está longe da forma como pensamos e protegemos concepções de privacidade no domínio telemático no direito penal é sintomático da necessidade de reconsideração – e o que ensaiam por no lugar não supre essa falha. Quando um hacker acessou dados *estáticos* de celulares de autoridades públicas, esse aspecto nunca foi suficiente para deixar de condenar a ação da perspectiva de violação à privacidade.[60] Suspeito ainda que se o hacker tivesse acessado não o conteúdo de comunicações, mas todos os demais dados – metadados das comunicações, fotos, histórico de ligações, agenda de contatos, histórico de localização, histórico de websites acessados – ou mesmo só a lista de chamadas, também ainda teriam visto problema de privacidade em sua ação. Precisamos de uma perspectiva mais honesta sobre como experimentamos privacidades na era tecnológica e as expectativas legítimas que carregamos nesses usos. Os testes binários fluxo/estático e conteúdo/metadado não capturam a dimensão normativa sobre como nos engajamos e valorizamos privacidade, nem dão conta da variedade de preocupações e riscos que a conduta estatal em questão pode ensejar e que precisa ser justificada.

Uma maneira de pensar se há expectativas relevantes de privacidade em jogo merecedoras de proteção constitucional é imaginar um terceiro comum do povo no lugar de autoridades públicas no contexto em questão – chamo isso de modelo do

[60] O descompasso normativo dessa postura de que essas informações não são protegidas por um direito à privacidade pode ser ilustrado por um episódio que veio à tona no Brasil quando autoridades de investigação foram alvo de ataque criminoso que envolveu acesso a comunicações armazenadas em celulares. Refiro-me a revelações do portal The Intercept Brasil, que supostamente recebeu de hacker histórico de mensagens trocadas entre membros da Lava Jato, notadamente o procurador da República Deltan Dallagnol, e ex-juiz e agora também ex-ministro da Justiça Sergio Moro. Ver MARTINS, Rafael Moro; SANTI, Alexandre de; e GREENWALD, Glenn. 'Não é muito tempo sem operação?' Exclusivo: chats revelam colaboração proibida de Sergio Moro com Deltan Dallagnol na Lava Jato. **The Intercept Brasil,** 9 de junho de 2019, https://theintercept.com/2019/06/09/chat-moro-deltan-telegram-lava-jato/. Só é possível dizer que há violação da privacidade nesse caso se, em primeiro lugar, se admitir que dados constantes em celulares são protegidos por um tal direito, mesmo que sejam "estáticos". Em termos de teoria da privacidade, é incoerente e contraditório que o valor da privacidade em questão seja reconhecido no âmbito da tutela penal, mas não enquanto garantia válida também a acusados.

"terceiro malicioso"[61]. Nossas práticas sociais sustentam a observação de que é legítimo que se recuse um pedido de alguém estranho para acessar nosso celular na rua em uma abordagem (incluindo apenas para ver histórico de ligações e fotos) e que é legítimo criticar e condenar terceiros que hackeiem nosso computador, ou mesmo um funcionário de uma empresa de telecomunicações ver para seus próprios fins nossas informações pessoais. Isso significa que há algo de valioso – que em geral chamamos de "privacidade" – e que devemos considerar quando o Estado almeja se engajar em condutas semelhantes. Nós autorizamos agentes do Estado a se engajarem em condutas que seriam ofensivas – e ilícitas – não fosse pela fundamentação constitucional que as autoriza – e que precisa existir no caso concreto.[62]

Nesse sentido, além do abandono de testes binários para tratar da proteção constitucional, deve ser resgatada a noção de que o ônus de fundamentação para agir é do Estado, que precisa justificar que não está atuando arbitrariamente, descuidadamente, nem em excesso. Isso vale mesmo no combate ao crime – ser fundamentado, dentro das prerrogativas de um estado constitucional, afinal, é o que autoriza o monopólio do Estado do uso da força. O que pode ser feito em situações de normalidade ou de urgência, em um flagrante no policiamento ostensivo, na apreensão de objeto largado em cena de crime, no âmbito de uma medida cautelar em uma grande investigação, diretamente pelas autoridades ou por meio de empresas, para implementação de uma política pública, pode variar. A medida do que consideramos mais ou menos grave e interventivo e quais cuidados e protocolos requer, também. Os contextos importam. Nossas respostas regulatórias devem responder às preocupações com arbitrariedades, negligências e excessos de cada um deles: autorizações judiciais prévias que controlem a justa causa e o limite de restrição são, em muitos casos, vocacionadas a garantir salvaguardas, mas não necessariamente são aptas a lidar com todos os contextos ou a lidar com todas as preocupações. Na era da vigilância baseada em coleta massiva de dados, de políticas de segurança cada vez mais preventivas e preditivas, outras ferramentas voltadas a embutir salvaguardas e limites também terão de ser consideradas[63], ao lado do resgate do papel da reserva legal.

Direitos específicos à privacidade não são os únicos que balizam a atuação do Estado, mas certamente reforçam limites e condições de forma especial em certos

---

[61] Ver também ABREU, Jacqueline de Souza. **Privacidade, segurança e tecnologia**. Tese (Doutorado em Direito) – Faculdade de Direito da Universidade de São Paulo. São Paulo, 2022.

[62] Entendo que, quando não é sequer possível imaginar um "terceiro malicioso" – como em um exemplo que envolva o uso de ferramentas de vigilância sequer disponíveis a clientes não-governamentais –, a impossibilidade de encontrar qualquer comparativo em nossas práticas é um sinal de alerta adicional do exercício de poder a ser justificado e da necessidade de atenção regulatória.

[63] Tratando da diversificada "caixa de ferramentas" para regular atividades de vigilância do Estado, ver OHM, Paul. The Surveillance Regulation Toolkit: Thinking Beyond Probable Cause. In: GRAY, David; HENDERSON, Stephen (org.). **The Cambridge Handbook of Surveillance Law**. Cambridge: Cambridge University Press, 2017, 491–508.

momentos. A exigência de suspeita individualizada para meios de obtenção de prova em geral está imbricada com exigências de fundamentação de um tratamento desigual e seletivo do Estado sobre alguém e que envolve risco de dano moral. Isto é, risco de que o Estado *erre* e alguém sofra uma restrição de seus direitos equivocadamente, sem na verdade ser culpado de nada. As noções de justiça que vedam medidas inadequadas e desnecessárias estão também embutidas a toda atuação do Estado, como é paradigmático no direito administrativo. A interpretação jurídica não só dos dispositivos que versam sobre privacidade deve urgentemente se reconectar com os princípios morais e políticos subjacentes que justificam essas proteções. Hoje, dizer que não se protegem dados estáticos é só atalho para deixar de enfrentar nuances contextuais e de elaborar razões jurídicas – a autorização para agir só existe pelas condições materiais e formais específicas que foram atendidas pelo Estado e que o desautorizam quando não existentes.

6. CONCLUSÃO

Esse artigo buscou explorar o paradigma interpretativo desenvolvido pelo Supremo Tribunal Federal para analisar questões de sigilo de dados: a tese de que a Constituição Federal, no seu art. 5º, inciso XII, protege a comunicação de dados, e não dados em si. Comecei mostrando a relação do dispositivo que protege o sigilo de comunicações com o *processo* de comunicar-se e como o sigilo de dados foi incluído no clássico dispositivo constitucional, a princípio com uma pretensão de proteção expansiva. Pouco depois, o STF viria a desenvolver uma jurisprudência sobre o tema que se tornou bastante restritiva: começou com certos ruídos entre um caso e outro, dentro de um contexto de acesso a computadores dentro de domicílios em investigações, que resultou em regra de ouro – uma simplificação – arrastada para diversos contextos de atuação policial e que se torna particularmente vazia diante do avanço tecnológico, de um mundo lotado de "dados estáticos".

O ponto crítico do teste aí criado é que ele não é coerente com a interpretação do próprio STF em outros casos, o que resulta na aplicação de um critério arbitrário. Também não carrega em si uma teoria da privacidade, isto é, uma tese substantiva de por que a privacidade é protegida em certos casos e não em outros. Diante desses problemas, discuti e descartei o que tem sido aventado como uma solução – tentar selecionar alguns tipos de dados que ainda mereceriam proteção constitucional. No lugar, comecei a desenhar algumas premissas básicas para um novo caminho a ser percorrido pelo STF: um reconhecimento maior de que são nossas práticas sociais e os contextos que no fim importam em discussões de privacidade e que discussões sobre requisitos materiais, previsão legal, e procedimentos devem ser resgatadas.

7. REFERÊNCIAS

ABREU, Jacqueline de Souza. **Privacidade, segurança e tecnologia**. Tese (Doutorado em Direito) – Faculdade de Direito da Universidade de São Paulo. São Paulo, 2022.

ANTONIALLI, Dennys; ABREU, Jacqueline de Souza; MASSARO, Heloísa; LUCIANO, Maria. Acesso de Autoridades Policiais a Celulares Em Abordagens e Flagrantes: Retrato e Análise Da Jurisprudência de Tribunais Estaduais. **Revista Brasileira de Ciências Criminais**, São Paulo, vol. 154, p. 177–214, 2019.

ASSEMBLEIA NACIONAL CONSTITUINTE. **Diário da Assembleia Nacional Constituinte (Suplemento 'C')**. Brasília, 1987. Disponível em: https://www.senado.leg.br/publicacoes/anais/constituinte/9b_Sistematizacao.pdf. Acesso em: 25 de dezembro de 2022.

ASSEMBLEIA NACIONAL CONSTITUINTE. **Diário da Assembleia Nacional Constituinte (Suplemento 'B')**. Brasília, 1988. Disponível em: http://imagem.camara.gov.br/Imagem/d/pdf/307anc23set1988SUPB.pdf. Acesso em: 25 de dezembro de 2022.

ÁVILA, Ana Paula Oliveira; WOLOSZYN, André Luis. A tutela jurídica da privacidade e do sigilo na era digital: doutrina, legislação e jurisprudência. **Revista de Investigações Constitucionais**, Curitiba, vol. 4, n. 3. p. 167-200, set./dez. 2017. DOI: 10.5380/rinc.v4i3.51295.

AZEREDO, João Fábio A. Sigilo das Comunicações Eletrônicas Diante do Marco Civil da Internet. In: DE LUCCA, Newton; SIMÃO Filho, Adalberto; LIMA, Cíntia Rosa Pereira de (Coord.). **Direito & Internet III - Tomo II: Marco Civil da Internet (Lei n. 12.965/2014).** São Paulo: Quartier Latin, 2015. p. 211–32.

BRASIL. Superior Tribunal de Justiça (6. Turma). **Agravo Regimental no Recurso Especial n. 1.760.815/PR**. Relator: Min. Laurita Vaz, 23 de outubro de 2018. Diário de Justiça Eletrônico, 13 de novembro de 2018.

BRASIL. Superior Tribunal de Justiça (6. Turma). **Recurso em Habeas Corpus n. 51.531/RO**. Relator: Min. Néfi Cordeiro, 19 de abril de 2016. Diário de Justiça Eletrônico, 09 de maio de 2016.

BRASIL. Superior Tribunal de Justiça (3. Seção). **Recurso em Mandado de Segurança n. 60.698/RJ**. Relator: Min. Rogerio Schietti Cruz, 26 de agosto de 2020. Diário de Justiça Eletrônico, 04 de setembro de 2020.

BRASIL. Superior Tribunal de Justiça (5. Turma). **Recurso Especial n. 1.782.386/RJ**. Relator: Min. Joel Ilan Paciornik, 15 de dezembro de 2020. Diário de Justiça Eletrônico, 18 de dezembro de 2020.

BRASIL. Supremo Tribunal Federal (Tribunal Pleno). **Ação Penal n. 307/DF**. Relator: Min. Ilmar Galvão, 13 de dezembro de 1994. Diário de Justiça, 13 de outubro de 1995.

BRASIL. Supremo Tribunal Federal (2. Turma). **Habeas Corpus n. 91.867/PA**. Relator: Min. Gilmar Mendes, 24 de abril de 2012. Diário de Justiça Eletrônico, 20 de setembro de 2012.

BRASIL. Supremo Tribunal Federal (Tribunal Pleno). **Mandado de Segurança n. 21.729/DF.** Relator: Min. Marco Aurélio, 05 de outubro de 1995.

BRASIL, Supremo Tribunal Federal (Tribunal Pleno). **Medida Cautelar na Ação Direta de Inconstitucionalidade n. 1488/DF**. Relator: Min. Néri da Silveira, 07 de novembro de 1996.

BRASIL. Supremo Tribunal Federal (Tribunal Pleno). **Referendo da Medida Cautelar nas Ações Diretas de Inconstitucionalidade n. 6387, 6388, 6389, 6390 e 6393**/DF. Relatora: Min. Rosa Weber, 07 de maio de 2020. Diário de Justiça Eletrônico, 12 de novembro de 2020.

BRASIL. BRASIL. Supremo Tribunal Federal (Tribunal Pleno). **Medida Cautelar na Arguição de Descumprimento de Preceito Fundamental n. 722/DF**. Relator: Min. Cármen Lúcia, 20 de agosto de 2020. Diário de Justiça Eletrônico, 22 de outubro de 2020.

BRASIL. Supremo Tribunal Federal (Tribunal Pleno). **Petição (Questão de Ordem) n. 577/DF**. Relator: Min Carlos Velloso, 25 de março de 1992. Diário de Justiça, 23 de abril de 1993.

BRASIL. Supremo Tribunal Federal (Tribunal Pleno). Recurso em Mandado de Segurança n. 11274/PE. Relator: Min. Evandro Lins Silva, 27 de novembro de 1963.

BRASIL. Supremo Tribunal Federal (Tribunal Pleno). **Recurso Extraordinário n. 1.055.941/SP**. Relator: Min. Dias Toffoli, 04 de dezembro de 2019.

BRASIL. Supremo Tribunal Federal (Tribunal Pleno). **Recurso Extraordinário n. 1116949/PR**. Relator: Min. Marco Aurélio. Relator p/ acórdão Min. Edson Fachin, 18 de agosto de 2020.

BRASIL. Supremo Tribunal Federal (Tribunal Pleno). **Recurso Extraordinário n. 418.416/SC**. Relator: Min. Sepúlveda Pertence, 10 de maio de 2006. Diário de Justiça Eletrônico, 02 de fevereiro de 2007.

CÂMARA DOS DEPUTADOS. **A construção do artigo 5º da Constituição de 1988**. Brasília: Câmara dos Deputados. Edições Câmara, 2013.

COHEN, Julie E. What privacy is for. **Harvard Law Review**, Cambridge, vol. 126, p. 1904–33, 2013

FERGUSON, Andrew Guthrie. Structural Sensor Surveillance. **Iowa Law Review**, Iowa, vol. 106, p. 47–112, 2021.

FERRAZ JUNIOR, Tercio Sampaio. Sigilo de Dados: o direito à privacidade e os limites da função fiscalizadora do Estado. **Revista da Faculdade de Direito da Universidade de São Paulo**, São Paulo, vol. 88, p. 439–59, 1993.

GRAY, David. **The Fourth Amendment in an Age of Surveillance**. Cambridge: Cambridge University Press, 2017.

MARTINS, Rafael Moro; SANTI, Alexandre de; e GREENWALD, Glenn. 'Não é muito tempo sem operação?' Exclusivo: chats revelam colaboração proibida de Sergio Moro com Deltan Dallagnol na Lava Jato. **The Intercept Brasil**, 9 de junho de 2019, https://theintercept.com/2019/06/09/chat-moro-deltan-telegram-lava-jato/.

NIGRI, Tânia. **O Sigilo Bancário e a Jurisprudência do Supremo Tribunal Federal**. São Paulo: IASP, 2016.

OHM, Paul. The Surveillance Regulation Toolkit: Thinking Beyond Probable Cause. In: GRAY, David; HENDERSON, Stephen (org.). **The Cambridge Handbook of Surveillance Law**. Cambridge: Cambridge University Press, 2017, p. 491–508.

PONCE, Paula Pedigoni; QUEIROZ, Rafael Mafei Rabelo. 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. **Internet & Sociedade**, São Paulo, vol. 1, nº 1, 64–90, fev. 2020. https://revista.internetlab.org.br/tercio-sampaio-ferraz-junior-e-sigilo-de-dados-o-direito-a-privacidade-e-os-limites-a-funcao-fiscalizadora-do-estado-o-que-permanece-e-o-que-deve-ser-reconsiderado/.

QUEIROZ, Rafael Mafei Rabelo. Privacidade, criptografia e dever de cumprimento de ordens judiciais por aplicativos de trocas de mensagens. In: DONEDA, Danilo (org.). **Caderno Especial - A Regulação da Criptografia no Direito Brasileiro**. São Paulo: Thomson Reuters Brasil, 2018, 13–26.

QUITO, Carina Acesso a Comunicações Eletrônicas Armazenadas na Prática Judiciária". In: ANTONIALLI, Dennys; ABREU, Jacqueline de Souza (Org.). **Direitos Fundamentais e Processo Penal na Era Digital: Doutrina e Prática em Debate**. Vol. I. São Paulo: InternetLab, 2018. p. 100–107.

RICHARDS, Neil. **Why Privacy Matters**. Oxford: Oxford University Press, 2021.

SHAPIRO, Stuart. Places and Spaces: The Historical Interaction of Technology, Home, and Privacy. **The Information Society,** vol. 14, n· 4, p. 275-284, nov. 1998. https://doi.org/10.1080/019722498128728.

SIDI, Ricardo. A interceptação de e-mails e a apreensão física de e-mails armazenados. **Revista Fórum de Ciências Criminais**, Belo Horizonte, vol. 4, p. 101-121, jul./dez. 2015.

SOLOVE, Daniel; RICHARDS, Neil. Privacy's Other Path: Recovering the Law of Confidentiality. **The Georgetown Law Journal**, Washington, vol. 96, p. 123-182, 2007.

INFORMAÇÕES ADICIONAIS

ADDITIONAL INFORMATION

Editores responsáveis	
Editor-chefe	Daniel Wunder Hachem
Editor-adjunto	Luzardo Faria