ARTIGO

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

Rafael Mafei Rabelo Queiroz

Rafael Mafei Rabelo Queiroz, livre-docente em Direito e professor do Departamento de Filosofia e Teoria Geral do Direito da Faculdade de Direito da USP. E-mail: rmqueiroz@usp.br.

Paula Pedigoni Ponce

Paula Pedigoni Ponce, bacharela em Direito e doutoranda na Faculdade de Direito da USP. Email: paula.ponce@usp.br.

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

Palavras-chave
privacidade
sigilo
dados pessoais
Tércio Sampaio Ferraz Jr
Supremo Tribunal Federal

Resumo
Em 1992, Tércio Sampaio Ferraz Júnior escreveu um parecer que foi publicado, no ano seguinte, sob o título de "Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado". Em sucessivos julgamentos, o Supremo Tribunal Federal (STF) incorporou parcialmente o argumento do texto, erigindo com base nele sua doutrina de proteção da privacidade relativa a dados em trânsito (telecomunicações) ou armazenados (sigilo bancário). Passados quase 30 anos da publicação do texto, e diante dos avanços tecnológicos do período, este artigo procura avaliar o que permanece e o que está superado no texto original de Ferraz Júnior. Para tanto, serão apresentados: (i) a estrutura e o argumento do texto; (ii) uma reconstrução histórica do contexto em que o texto foi escrito, a partir de declarações de Ferraz Júnior e reportagens jornalísticas da época; (iii) a maneira como os argumentos de Ferraz Júnior foram incorporados pelo STF; (iv) os pontos da leitura de 1993 que ainda se mostram fundamentais, bem como alguns que devem ser superados. O STF tem ações em curso nos quais terá de revisitar o tema, e a iminente vigência da Lei Geral de Proteção de Dados seguramente levará o tribunal a ter de renovar suas manifestações sobre o direito à proteção de dados. A conclusão do artigo é que há importantes considerações do artigo que permanecem atuais, enquanto outros pontos merecem novas reflexões.

Tércio Sampaio Ferraz Júnior and *Data secrecy: the right to privacy and the limits of the State control:* what remains and what ought to be reconsidered

Keywords
brazil
privacy
secrecy
personal data
Tércio Sampaio Feraz Júnior

Abstract
In 1992, Tércio Sampaio Ferraz Júnior, a leading Brazilian legal philosopher, published the essay "Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado". The essay orients the Brazilian Supreme Federal Court (STF) caselaw on data secrecy and privacy, stating that the constitutional provision on data secrecy only protects data in transit – leaving stored data unguarded. Almost thirty years after its first issue and, given the many techno and sociological changes occurred in the period, this essay aims at evaluating which aspects of the essay stand and which do not. To do so, the article should present: (i) the structure and argument of Ferraz Júnior's text; (ii) a historical reconstruction of the context in which the text was written; (iii) how Ferraz Júnior's arguments were assimilated by the STF; (iv) parts of the 1993 article that are still fundamental, as well as some that must be overcome. The STF is currently analysing cases in which it should revisit its caselaw on data secrecy and privacy, and the imminent General Data Protection Law deem it likely that the Court changes its position. We conclude the essay by stating that there are aspects of the 1993 article still relevant nowadays, whilst some others are in need of further reflexion.

1. Introdução

A Constituição Federal de 1988 introduziu, no artigo 5º, inciso XII, a inviolabilidade do sigilo de dados como direito fundamental. Trata-se de um dos modos de assegurar o direito à privacidade, cujo conteúdo é preenchido por disposições encontradas em outros locais da mesma Constituição (v.g., incisos X e XI do mesmo artigo), assim como na legislação infraconstitucional.

Em 1993, Tércio Sampaio Ferraz Júnior publicou um artigo intitulado "Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado" (doravante, "Sigilo de dados"). Tal artigo serviu de principal fundamentação doutrinária para a interpretação do Supremo Tribunal Federal (STF) acerca do conteúdo e dos limites do direito subjetivo à inviolabilidade da comunicação sigilosa e à proteção de dados pessoais. Em síntese, o STF interpretou que a inviolabilidade do sigilo de dados refere-se apenas aos dados em trânsito–o fluxo de dados do emissor ao receptor da mensagem–durante os instantes da comunicação telefônica e telemática propriamente dita. Ela não se aplicaria aos dados estáticos, já armazenados, ainda que eles tivessem sido objeto de comunicação anterior.[1] Quase trinta anos após sua publicação, por sua reiterada acolhida pelo STF, o texto de Ferraz Júnior é ainda uma importante referência para o debate constitucional brasileiro sobre privacidade, em geral, e proteção de dados pessoais, especificamente. Por um dever de consistência em relação a suas decisões passadas, é esperado que o STF retome a doutrina explicitada naquele artigo para se desincumbir de desafios jurisdicionais análogos que se desenham à frente. São exemplos os debates sobre a constitucionalidade da criptografia forte, celebrizada nos casos de bloqueios ao aplicativo WhatsApp, disputas sobre a validade de provas obtidas por meio de acesso a dados armazenados em celulares sem autorização judicial, assim como as disputas judiciais que seguramente ocorrerão a partir do início da vigência da lei brasileira de proteção de dados pessoais (Lei 13.709/2018).

Dadas as grandes diferenças tecnológicas existentes entre a época de publicação original do artigo e o tempo presente, notadamente no que se refere ao fluxo, à acessibilidade, ao conteúdo, às técnicas de coleta e às facilidades de armazenamento e tratamento de dados, o presente artigo objetiva avaliar a atualidade e pertinência dos argumentos desenvolvidos no clássico texto de Ferraz Júnior. A motivação para esta análise vem da hipótese de que as mudanças nesses pressupostos factuais podem ter impacto sobre a reflexão jurídica acerca do direito à privacidade, em especial na vertente da inviolabilidade de dados armazenados.

O artigo será dividido em quatro seções. Na primeira, é explicitada, em detalhes, a estrutura e o argumento do texto de Ferraz Júnior. Na segunda parte, detalha-se o contexto em que o texto foi escrito. Para tanto, são recuperadas declarações do autor e material de mídia da época. Essa análise é útil para explicitar os tipos de conflitos específicos que Ferraz Júnior mirava àquela altura, o que ajuda a sustentar o argumento de que eles são muito diferentes dos desafios jurídicos atuais quanto à matéria. Na terceira seção, descreve-se a forma como os argumentos de Ferraz Júnior foram incorporados pela jurisprudência do STF. Argumenta-se que o tribunal fez uma incorporação apenas parcial do artigo, implicando proteção insuficiente ao sigilo de dados armazenados. Por fim, a quarta seção identifica quais pontos do texto de Ferraz Júnior são ainda relevantes para uma doutrina efetiva da proteção da privacidade no tocante ao sigilo de dados armazenados–e quais outros, em contrapartida, carecem de complementação, ou mesmo de superação.[2]

2. O texto

"Sigilo de dados" tem como objetivo compreender o conteúdo da previsão constitucional acerca da inviolabilidade do sigilo de dados, bem como os limites que esse conteúdo impõe ao exercício de fiscalizações estatais. O artigo parte de uma distinção entre, de um lado, o direito fundamental à privacidade e, de outro, a garantia da inviolabilidade do sigilo de dados: embora correlatos, um e outro não se confundem (Ferraz Júnior, 1993, p. 439).

O argumento de Ferraz Júnior constrói-se em três etapas: (i) considerações sobre o direito fundamental à privacidade; (ii) considerações sobre a inviolabilidade do sigilo de dados, destacando como ele se aproxima, e como se distancia, do direito à privacidade; por fim, (iii) avaliação sobre os limites da função fiscalizadora do Estado frente aos direitos analisados.

(i) Considerações sobre o direito fundamental à privacidade.

Para Ferraz Júnior, o conteúdo do direito à privacidade é "a faculdade de constranger os outros ao respeito e de resistir à violação do que lhe é próprio, isto é, das situações vitais que, por dizerem a ele só respeito, deseja manter para si, ao abrigo de sua única e discricionária decisão". O objeto desse direito, por sua vez, é "a integridade moral do indivíduo, aquilo que faz de cada um o que é e, desta forma, lhe permite inserir-se na vida social e na vida pública." (Ferraz Júnior, 1993, p. 443).

Ferraz Júnior realiza tais considerações a partir do pano de fundo entre a distinção de público e privado, por ele atribuída a Lafer (1988). Nessa chave de leitura, a privacidade representaria a demarcação da individualidade de um sujeito em face dos outros e do Estado. Tal demarcação permite ao indivíduo se inserir na vida social e pública de sua comunidade, mas sem perder sua individualidade ou o controle daquilo que o representa.

Ferraz Júnior fala em "direitos à privacidade" (1993, p. 442), no plural, os quais incluem intimidade e vida privada, bem como os direitos ao nome, à imagem, à reputação – conforme positivação pelo inciso X do artigo 5º. Todos esses, por sua vez, são regidos pelo princípio da exclusividade, conceito de Hannah Arendt trabalhado por Celso Lafer (1988), que tem como objetivo "assegurar ao indivíduo a sua identidade diante dos riscos proporcionados pela niveladora pressão social e pela incontrastável impositividade do poder político" (Ferraz Júnior, 1993, p. 441). Contudo, o grau de exclusividade é variável entre cada um desses direitos. Por exemplo: nome, imagem e honra possuem um sentido comunicacional, de modo que exigem alguma publicidade, ostentando, consequentemente, um grau menor de exclusividade. Afinal, são feitos para serem conhecidos publicamente. Contudo, não podem se transformar em objeto de apropriação privada (i.e., servir de objeto de trocas de mercado) sem o consentimento de seu titular (Ferraz Júnior, 1993, p. 442). Daí porque seguem privados, ainda que feitos para ganhar publicidade.

(ii) Considerações sobre a inviolabilidade do sigilo de dados e sua comparação com o direito à privacidade.

Ferraz Júnior então passa a tratar do sigilo propriamente dito. O sigilo não é, para ele, "o bem protegido", pois "não é o objeto do direito fundamental. Diz respeito à faculdade de agir (manter sigilo, resistir ao devassamento), conteúdo estrutural do direito [à privacidade]" (Ferraz Júnior, 1993, p. 443). Não se

trata, contudo, de uma faculdade exclusiva do indivíduo e a serviço do direito à privacidade: há sigilos que protegem interesses do Estado–melhor dizendo: da comunidade, como são os casos de sigilos impostos em nome da segurança nacional. O sigilo é, portanto, instrumental, não representando um fim em si mesmo. Não há um direito fundamental ao sigilo, e sim circunstâncias nas quais o sigilo é instrumental à proteção de um direito fundamental (à privacidade). Logo, e sempre segundo Ferraz Júnior, enquanto liberdades fundamentais–como é o caso da privacidade–só encontram limites em outras liberdades fundamentais, o sigilo e sua inviolabilidade são marcados pela instrumentalidade (Ferraz Júnior, 1993, p. 445).

De sua leitura do inciso XII do art. 5º, Ferraz Júnior entende que o sigilo ali referido diz respeito estritamente à *comunicação* de dados, e não aos dados em si (1993, p. 446).[3] A partir das simetrias identificadas no texto constitucional, o sigilo de dados seria próximo ao sigilo de correspondência. Recorrendo a Pontes de Miranda (2004, p. 273), o autor conceitua a privacidade, em conjunto com a inviolabilidade de domicílio e correspondência, como uma liberdade de "negação" (1993, p. 443). Ela seria, portanto, uma imunidade[4] contra o pretendido poder de devassa ou intromissão investigativa em certas esferas das vidas privadas de cidadãos. O sigilo, e sua manutenção, efetivariam esse direito, mas sem se confundir com o conteúdo daquilo que protegem. Assim, Ferraz Júnior conclui que o objeto da inviolabilidade do sigilo não são os dados em si, e sim a liberdade de negar acesso ao conteúdo por ele abarcado.

A interceptação de uma mensagem – isto é, a invasão do fluxo entre emissor e receptor, visando a acessar o conteúdo comunicacional que é transmitido – representa violação à proteção conferida pelo sigilo. Por isso ela só deve ser admitida, ainda que com ordem judicial e para fins de interesse público (investigação criminal, por exemplo), nas hipóteses em que o teor da comunicação não puder ser obtido de outra forma. Assim, conclui o autor que a ressalva do artigo 5º, inciso XII, que prevê a interceptação de comunicações por ordem judicial, seja aceita somente nas comunicações telefônicas, nas quais não restam vestígios físicos do conteúdo comunicado, por sua característica de "instantaneidade" (Ferraz Júnior, 1993, p. 447).[5] Houve aqui uma ponderação do constituinte quanto à amplitude do sigilo, o qual sofreu restrição no próprio texto constitucional para permitir, em hipóteses que acabaram definidas em lei posterior,[6] a perenização do conteúdo dessas comunicações instantâneas e não escritas. Por exemplo, diante de uma comunicação por carta, é possível requerer uma busca e apreensão para ter acesso à carta guardada (Ferraz Júnior, 1993, p. 447).

(iii) Limites da função fiscalizadora do Estado.

Por fim, Ferraz Júnior passa a enfrentar um problema prático: quais seriam os limites à função fiscalizadora do Estado em casos de requerimento de acesso a movimentações bancárias? Nessas situações, não estaríamos diante da interceptação de um ato comunicativo entre banco e correntistas, e sim de acesso a dados armazenados nos bancos de dados da instituição financeira. Não sendo comunicação, prossegue o texto, sua proteção não poderia se dar pelo inciso XII do artigo 5º, que diz respeito apenas ao sigilo de comunicações. Contudo, isso não significa que restariam desprotegidos: a tutela jurídica de dados pessoais armazenados fundamentar-se-ia no inciso X do mesmo artigo 5º, por sua inegável pertinência à privacidade dos indivíduos (Ferraz Júnior, 1993, p. 448). Incidiria, neste caso, o princípio da exclusividade, com fundamento no direito à privacidade, genericamente, e não do direito ao sigilo

das comunicações, especificamente.

No caso de dados armazenados, portanto, o intérprete deve se questionar, em face das circunstâncias concretas, em que medida a devassa pretendida sobre os dados é problemática para a integridade moral do indivíduo. Isso variaria, por sua vez, conforme a sensibilidade do dado. Dados que, embora individuais (i.e., pertinentes a um indivíduo), foram feitos para ser públicos, como nome e número de documento, são menos sensíveis; já aqueles que são em princípio feitos para permanecer reclusos do conhecimento público (trocas de cartas privadas, fotografias íntimas) têm maior sensibilidade, dando maior premência ao princípio da exclusividade. Nessa moldura, a intimidade representaria o mais exclusivo dos direitos relacionados à privacidade, uma vez que representa "um âmbito de exclusivo que alguém reserva para si, sem nenhuma repercussão social" (Ferraz Júnior, 1993, p. 442).

3. O contexto

Em 2017, por ocasião dos 25 anos do seu clássico texto, Tércio Sampaio Ferraz Júnior ministrou uma palestra[7] em que relembrou o contexto específico de sua produção. Disse ele:

> "Esse trabalho surgiu de uma coisa muito factual em 1991. Eu, naquela época, era procurador geral da Fazenda e enfrentava um problema de revelação do sigilo, de nomes e de dados identificadores de pessoas que portassem cartões de crédito. A primeira vez que enfrentei essa questão, me lembro de ter feito uma reunião com grandes empresas de bandeiras de cartões de credito, porque elas se recusavam a abrir as suas listas de nomes. [...] Por conta disso eu fui levado a examinar o art. 5º da Constituição, naquela época já vigente, especialmente o inciso XII, que garante a privacidade e o sigilo" (Ferraz Júnior, 2018, p. 20).

Ferraz Júnior foi Procurador-Geral da Fazenda Nacional entre 1991 e 1993.[8] Na época, o Governo Collor debatia medidas de combate a fraudes tributárias e normas de sigilo bancário eram vistas como um entrave à fiscalização (Governo quer o fim do sigilo bancário, para juristas, o plano é inconstitucional, 1991). O chamado "emendão" do Governo Collor, proposta de emenda constitucional que reunia diversas reformas constitucionais, chegou a propor mudanças nas regras de sigilo para fazer frente a essa percebida dificuldade (Projeto de Emenda Constitucional n. 51, 1991; Governo acena com choque se ajuste fracassar, 1991). Nesse contexto, foi editada a Lei Complementar nº 70/91, que permitia à Receita Federal demandar de instituições financeiras no geral, incluindo empresas administradoras de cartão de crédito, informações cadastrais sobre os usuários (nome, afiliação endereço e número do CPF). A operacionalização dessas demandas precisava ser delineada em regulamento específico. Reportagem jornalística de fevereiro de 1992, tratando justamente do regulamento desenhando pelo Ministério da Economia, Fazenda e Planejamento apontava que a Receita Federal poderia utilizar "cruzamentos para identificar números falsos de CPF e CGC, movimentação de caixa 2 e sinais de sonegação de impostos" (Nastari, 1992a).

O Ministério da Economia, Fazenda e Planejamento objetivava emitir duas portarias regulamentares: uma destinada às instituições financeiras e outra às administradoras de cartão de crédito. Segundo declarações de Luís Fernando Wellisch, Secretário da Fazenda Nacional à época, as instituições financeiras não seriam obrigadas a fornecer dados de movimentação das contas dos clientes, pois elas

estariam protegidas pelo sigilo bancário; mas tal restrição não valeria para empresas de cartão de crédito, por não serem "instituições financeiras" no sentido estrito do termo (Folha de São Paulo, 1992).

As administradoras de cartão de crédito, por sua vez, contestavam tal interpretação e defendiam a inconstitucionalidade da medida. Por meio da Associação Brasileira de Cartões de Crédito, prometiam recorrer ao Judiciário contra eventual portaria que demandasse os extratos de seus clientes (Folha de São Paulo, 1992). De fato, o art. 12 chegou a ser regulamentado pela Portaria n° 144, de 25 de fevereiro de 1992, a qual estabelecia a possibilidade de requisição de dados cadastrais de todas as instituições financeiras, a não ser as administradoras de cartão de crédito (Portaria 144/1992, do Ministério da Economia, Fazenda e Planejamento).

O tema continuou a ser debatido entre associações do setor e o Secretário da Fazenda Nacional, que temia contestação judicial das medidas. Em maio de 1992 foi noticiado que, no âmbito das negociações, Tércio Sampaio Ferraz Júnior, na figura de Procurador-Geral da Fazenda, enviou um parecer que fornecia a base legal para a portaria. Com isso, havia a expectativa de que a Procuradoria chegasse a um acordo com as referidas empresas (Nastari, 1992b). Ao que tudo indica, o acordo não se concretizou e nenhuma outra portaria chegou a ser publicada sobre o tema.[9]

Como se vê, o texto era motivado por um problema bastante específico e circunstanciado: o direito de acesso, para um fim específico (fiscalização tributária), a um tipo específico de dado (movimentações de cartão de créditos), que ficava em posse de um pequeno grupo de empresas atuantes em um setor acompanhado de perto por reguladores estatais, as quais tinham, com seus clientes (titulares dos cartões de crédito), relações contratuais estabelecidas. Adicionalmente, vale destacar que, a se permitir a política objetivada pelo governo, os dados seriam transmitidos entre um agente contratualmente obrigado a manter sigilo (as operadoras de cartão de crédito) para outro agente legalmente obrigado a manter sigilo (a Administração Pública tributária). Neste horizonte estreito, a tese do texto foi levada ao STF, a partir de casos relativos à higidez do sigilo financeiro de cidadãos em face da atividade fiscalizadora do Estado.

4. A incorporação do texto pelo STF

Com o objetivo de compreender a repercussão, divulgação e "herança" do artigo de 1993, buscou-se identificar e avaliar criticamente a forma como o STF o incorporou à sua jurisprudência. Isto é, procurou-se mensurar qual foi o efetivo papel do texto nas decisões escolhidas, em que medida a argumentação o utilizou como recurso e, por fim, se a tese associada a ele passou a integrar a *ratio decidendi* do Tribunal.[10]

4.1. Casos em que o argumento do texto foi invocado

A jurisprudência do STF acerca da proteção constitucional ao sigilo de dados, notadamente a tese que "para o STF, o sigilo garantido pelo art. 5º, XII, da CF refere-se apenas à comunicação de dados, e não aos dados em si mesmos" (Mendes & Branco, 2012, p. 421), foi destacadamente construída em dois casos[11]: o Mandado de Segurança nº 21.729/DF, e o Recurso Extraordinário 418.416/SC. Para compreender de que modo o "Sigilo de dados" foi incorporado à jurisprudência da Corte, serão apresentados brevemente os dois casos, com

atenção ao peso de "Sigilo de dados" na posição finalmente encampada do STF.

(i) MS nº 21.729/DF: tratava-se de mandado de segurança impetrado pelo Banco do Brasil contra ato do Procurador-Geral da República, que demandava, por ofício, lista de nomes dos beneficiários de liberação de recursos públicos ao setor sucroalcooleiro, além de dados específicos sobre existência de débitos e naturezas das operações que os originaram. A argumentação do impetrante não chegava a mencionar o artigo 5º, inciso XII, da Constituição, mas limitava-se a insistir na necessidade de ordem judicial para o acesso a tais informações, que equivaleria a quebra de sigilo.[12]

A autoridade coatora prestou informações, confirmando os fatos e alegando que havia questionamentos quanto à autoridade do Ministério Público para requerer os dados em questão. Alegaram suspeitar de violação tanto da Lei Complementar (LC) nº 75/1993, quanto do art. 129, inciso VI, da Constituição Federal. Em extenso parecer, o Vice Procurador Geral da República introduziu a discussão sobre o inciso XII, juntamente com trecho[13] do artigo de Ferraz Júnior (Vice Procuradoria Geral da República, 1994). Foi a primeira aparição de "Sigilo de dados" nos autos do caso. O parecer da PGR argumentava que o sigilo bancário não teria guarida constitucional, nem a partir de interpretação do artigo 5º, inciso X, nem a partir do inciso XII. Nesse sentido, sem natureza constitucional, as exceções estabelecidas ao sigilo bancário seriam válidas enquanto motivadas pela salvaguarda de interesses constitucionalmente protegidos – como seria o caso do art. 8º da LC 75, em sintonia com o art. 129, inciso VI da Constituição Federal. Segundo o parecer, o inciso XII do art. 5º não protegia o sigilo bancário, porque blindaria, através do sigilo, apenas as comunicações de dados – e não os dados em si, uma vez recebidos e armazenados.

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

Os votos vencidos, quais sejam, os Ministros Marco Aurelio, Maurício Corrêa, Celso de Mello, Ilmar Galvão e Carlos Velosos, de forma geral, argumentaram que o sigilo bancário teria status constitucional em decorrência dos incisos X e XII do artigo 5º e que, portanto, sua quebra necessitaria de ordem judicial. Os votos dos Ministros Sepúlveda Pertence e Francisco Rezek[14] foram os únicos a se contrapor a tal afirmação, recuperando o texto de Ferraz Júnior e indicando que entendiam que o sigilo de dados ali mencionado se referia tão somente ao sigilo da comunicação de dados e que, consequentemente, não seria aplicável ao sigilo bancário. É curioso notar que os votos vencidos, embora não tenham invocado o texto de Ferraz Júnior, poderiam ter igualmente se valido dele para amparar seu argumento: afinal, "Sigilo de dados" é explícito em afirmar que dados armazenados, embora não acobertados pelo sigilo do inc. XII do art. 5º, podem ser protegidos pela regra geral da privacidade, quando fosse o caso.[15] Mas não o fizeram.

(ii) RE nº 418.416-SC: tratava-se de Recurso Extraordinário impetrado por Luciano Hang, empresário proprietário da rede de lojas de departamento Havan, contra decisão do TRF-4 que confirmara sua condenação por crimes tributários. O objetivo do RE era obter a anulação da condenação, que seria fundada em prova

obtida por meio ilícito: argumentava-se que a decisão que autorizou a busca e apreensão também teria resultado em violação à proteção constitucional do sigilo de dados. Por mais que o mandado de busca e apreensão mencionasse a apreensão de equipamentos de informática, a defesa argumentava que isso não implicava possibilidade de decodificação dos registros armazenados em computador apreendido (o que efetivamente havia ocorrido).

A defesa de Hang destacava a decisão do Plenário do STF na Ação Penal nº 307 (1994) (Caso Collor). Na oportunidade, o tribunal havia decidido que era ilícita a decodificação dos registros de computador apreendidos na sede de uma empresa. Contudo, havia uma diferença fundamental: no caso da AP no 307, ao contrário do que ocorrera no RE nº 418.416-SC, tal apreensão fora feita sem mandado judicial. A partir dos argumentos da defesa, sob pena de contrariar decisão anterior do Plenário, a Primeira Turma decidiu afetar o caso para julgamento pelo Tribunal Pleno.

Em 10 de maio de 2006, na sessão plenária de julgamento, o Ministro Sepúlveda Pertence (relator) destacou a existência de mandado judicial específico no 2° caso. Quanto à alegação de violação ao sigilo de dados, afirmou que a norma do inc. XII do art. 5º não se aplicava àquela situação, 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" (RE n° 418.416-SC, 2006, pp. 1252-1253). Quando retomou considerações que fizera no MS 21.729, Pertence invocou "Sigilo de dados" em tom elogioso: "trabalho preciso sobre o tema do d. Tércio Ferraz, do qual extraio essa síntese magnífica, que não tenho dúvidas em subscrever" (RE n° 418.416-SC, 2006, p. 1254).

Os demais membros do Plenário acompanharam o voto do Relator.[16] O Ministro Cezar Peluso acrescentou que interpretação diversa daquela—i.e., que estendesse o sigilo a dados armazenados – levaria a absurdos: dados de registro (como uma anotação em papel) não seriam invioláveis em si, mas passariam a sê-lo se fossem armazenados em computadores. Para impedir a atuação fiscalizadora estatal, então, bastaria que o indivíduo movesse dados de outros meios de armazenamento para o computador, garantindo-lhes o *status* de sigilosos.

4.2. Incorporação seletiva

Como conclusão preliminar, temos que, a despeito de o MS nº 21.729 por vezes ser indicado como precedente, a tese sobre o sigilo de dados referir-se à comunicação de dados e não aos dados em si não compôs a *ratio decidendi* do Tribunal naquela ocasião. Representou, entretanto, um primeiro passo nesse sentido. O Ministro Sepúlveda Pertence, que já se mostrara convencido pela tese naquela oportunidade, foi responsável por recuperá-la no RE nº 418.416, na condição de relator. Nessa oportunidade, o tema foi abertamente discutido e referendado pelo Tribunal Pleno como um todo. Desse modo, foi a partir desse caso em que se deu a efetiva incorporação da tese do texto à jurisprudência do STF.

A incorporação de "Sigilo de dados" pelo STF, contudo, foi seletiva.[17] A obra só foi citada nos trechos em que se caracterizava a proteção constitucional do "sigilo de dados" presente no artigo 5º, inciso XII—isto é, firmando o entendimento de que esta proteção se volta à comunicação de dados e não aos dados em si. Se essa não chega a ser uma leitura equivocada do artigo, pois a distinção entre dados em trânsito e dados armazenados de fato está nele, ela deixa de fora, ao mesmo tempo, um ponto relevante do argumento completo do autor: para além da distinção entre dados armazenados ou em trânsito comunicativo, Ferraz Júnior também

afirmava que, embora a proteção constitucional do sigilo (inc. XII do art. 5º) não alcançasse dados armazenados, o acesso a eles seria balizado pela guarida constitucional da privacidade (inc. X do mesmo artigo). Isto é, seria relevante avaliar em que medida o acesso aos dados armazenados no *hard disk* violaria a intimidade do indivíduo: mesmo que eles não pudessem ser chamados de "sigilosos", nada impedia que fossem considerados, por exemplo, "íntimos", e contassem com proteção condizente a esse *status*. A despeito disso, considerações sobre intimidade e potencial violação ao art. 5º, inciso X não integraram a análise do STF em qualquer um desses casos. A recuperação de considerações desse tipo mostra-se, hoje, mais necessária do que nunca. A essa tarefa, dedica-se a seção final do artigo.

5. Privacidade e proteção de dados: desafios atuais e caminhos da tutela jurídica

Em 1993, Ferraz Júnior já traçava paralelos entre a proteção do sigilo de dados e a intimidade do indivíduo. Em quase trinta anos, o conceito de privacidade passou por importantes alterações. A proteção de dados pessoais se consolida como categoria decorrente dessa evolução.

Após desenvolvimentos germinais na disciplina legal do direito à proteção de dados pessoais,[18] chegamos à atual geração legislativa nesta matéria. Nela destacam-se o Regulamento Geral de Proteção de Dados Pessoais (RGPD)[19] da União Europeia; e, localmente, a recém aprovada Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709, de 14 de agosto de 2018 ou LGPD). Se antes a proteção jurídica contra violações a dados pessoais estava disponível somente para quem estivesse disposto a arcar com os custos econômicos e sociais de um litígio, a geração atual de leis de proteção de dados busca elevar o padrão coletivo dessa tutela. Esse objetivo é perseguido a partir de variadas estratégias. Doneda (2011, p. 98) destaca, entre outras, o fortalecimento da posição do indivíduo frente às entidades que coletam e processam seus dados, tornando seu controle mais efetivo; da decisão de consentimento individual, limitando-a, por exemplo, no que diz respeito a dados pessoais sensíveis; criação de autoridades independentes responsáveis por garantir a observância das normas.

Na LGPD, destacam-se princípios para o tratamento dos dados pessoais, quais sejam (art. 6º): (i) finalidade, ideia de que o tratamento deve ser realizado apenas para propósitos legítimos, específicos, explícitos e informados ao titular; (ii) adequação, que determina que o tratamento seja compatível com as finalidades informadas ao titular; (iii) necessidade, exigência de que o tratamento se limite ao mínimo necessário para a realização de suas finalidades. Com o objetivo de possibilitar ao titular o controle sobre seus dados pessoais e as formas de tratamento destes, a lei estabelece ainda: (iv) livre acesso aos dados e às formas de tratamento; (v) direito dos titulares de garantir a qualidade de dados, atualizando-os ou pedindo sua correção; e (vi) transparência com relação às práticas de tratamento utilizadas. A lei, pauta-se, ainda, pelos princípios da (vii) segurança e (viii) prevenção, estimulando a adoção de medidas técnicas e administrativas para a proteção de dados pessoais. Por fim, a LGPD (ix) veda qualquer tratamento para fins discriminatórios ilícitos ou abusivos e (x) estabelece que os agentes deverão adotar medidas aptas a comprovar a observância e o cumprimento das normas de proteção de dados pessoais, bem como a eficácia dessas medidas.

Tais princípios buscam possibilitar o controle do titular sobre seus dados pessoais e as formas

de tratamento empregadas. Com a "ubiquidade da tecnologia da informação" (Mendes, 2014, pp. 78-79), usos de dados pessoais com potencial danoso à intimidade e integridade moral do indivíduo ganham espaço. Esses dados podem ser obtidos por meio de práticas invasivas aos limites de uma privacidade classicamente concebida (i.e., como um bloqueio), mas também por uma garimpagem, cada vez mais barata e acessível tecnologicamente, de rastros deixados a partir do uso de redes sociais, páginas de Internet e aplicativos para *smartphones*. Longe de olhares, há intensa mercância de dados pessoais, às vezes mediante autorizações genéricas e irrefletidas concedidas por seus titulares, que servem para ranqueamentos, perfilhamentos, classificações de perfil, tendo, por isso, impacto direto sobre as vidas de indivíduos. A elas somam-se invasões, furtos de dados, práticas de vigilância e monitoramento, bem como estratégias publicitárias e comerciais abusivas.

Todas essas mudanças, amplamente reconhecidas por filósofos e juristas do presente, e confirmadas pela atual onda legislativa para a proteção de dados pessoais, impõem a "Sigilo de dados" um desafio quanto a sua atualidade. Na parte final deste artigo, apresenta-se o que nele permanece atual, e o que se encontra carente de atualização, com vistas aos desafios jurídicos do presente.

a. O que permanece?

(i) A centralidade da dignidade humana como parâmetro normativo que dá sentido ao direito à privacidade e à proteção de dados pessoais.

Em "Sigilo de dados", como já apresentado, Ferraz Júnior é explícito em apontar a integridade moral do indivíduo como uma variável relevante para o equacionamento de conflitos jurídicos que tensionam o direito à privacidade e à proteção de dados. Trata-se, no limite, de avaliação relacionada ao princípio da dignidade humana. A privacidade, com os instrumentos jurídicos à sua disposição–dentre os quais o sigilo–serve para garantir aos cidadãos espaços de autonomia indispensáveis ao florescimento humano individual. Sem esses espaços de autonomia, corre-se o risco de aniquilamento do indivíduo, que tenderá a sucumbir à pressão irresistível de um poder ("político", na qualificação de Ferraz Júnior) nivelador e aniquilador de personalidades e liberdades.

A ancoragem da discussão sobre sigilo de dados e privacidade no princípio da dignidade humana não era trivial àquela altura, razão pela qual convém destacar este ponto do argumento de Ferraz Júnior. A violação de sigilo privado é, afinal, indolor e silenciosa; para a vasta maioria dos cidadãos, ela é imperceptível, dado que apenas uma fração pequena das pessoas devassadas tende a experimentar problemas com as autoridades. Por que haveria risco à dignidade humana neste caso? Se a dignidade humana tem a ver com o tratamento mínimo ao qual fazemos jus por nosso *status* de humanidade,

a investigação de dados–indolor e silenciosa–seria mesmo *indigna*? Não deveríamos guardar esse rótulo para outras práticas notoriamente imorais, como a tortura investigativa, a prisão de familiares para forçar confissões, ou devassas domiciliares sem ordem judicial? Nessa linha, não estaria a dignidade, ao contrário, a recomendar justamente a devassa discreta de dados, para nos poupar dos constrangimentos, incômodos e dores da vigilância e fiscalização ostensiva, sensível e espalhafatosa aos olhos de todos?

Ao relacionar dados pessoais à privacidade, e ao mesmo tempo reconhecer a importância desse valor para a dignidade humana, Ferraz Júnior foi importante em desenhar a moldura axiomática dentro da qual os debates sobre proteção e acesso a dados pessoais devem ser pensados. Ainda que indolor, silencioso e discreto, o acesso a dados pessoais pode trazer graves implicações à privacidade, afetando, por consequência, a dignidade dos sujeitos. Nessa linha, "Sigilo de dados" reconhece que há uma dimensão das vidas privadas cujo simples acesso não autorizado por terceiros, por mais discreto de seja, é incompatível com o próprio *status* humano. É intrinsecamente humano e, portanto, valoroso enquanto característica indissociável da humanidade, guardar espaços de nossa intimidade em relação aos quais se decide, sem interferências ostensivas ou sorrateiras, quem deles pode participar. Compartilhar segredos mais recônditos e intimidades mais reclusas apenas com quem se escolhe é uma forma de expressar confiança, amizade e amor. Não reconhecer este espaço de exclusividade, eliminando, em consequência, a possibilidade do exercício desses julgamentos afetivos, implica violação a algo inerentemente humano e valoroso, mesmo quando tal devassa se dá de modo discreto e imperceptível.

(ii) O reconhecimento de que dados importam à privacidade individual, e os limites que essa relação impõe para a função fiscalizadora do Estado.

Conforme apontado no item 4.2 (retro), o STF fez uma incorporação parcial de "Sigilo de dados". Se é verdade que o texto afirmava que apenas dados em trânsito eram protegidos pelo sigilo imposto pelo art. 5º, inc. XII, da Constituição, é verdade também que Ferraz Júnior afirmava que os dados armazenados caíam sob a proteção do inc. X do mesmo artigo. Se não eram blindados por sigilo, continuavam, não obstante, protegidos pelo direito fundamental à privacidade, se fossem relevantes à intimidade, vida privada, honra e imagem do cidadão. Diz o texto: "informações, em termos de *privacy*, constitutivas da integridade moral da pessoa"; [...] "dados que a pessoa guarda para si e que dão consistência à sua pessoalidade – dados de foro íntimo, expressões de autoestima, avaliações personalíssimas com respeito a outros, pudores, enfim dados que, quando constantes de processos comunicativos, exigem do receptor extrema lealdade e alta confiança, e que, se devassados, desnudariam a personalidade, quebrariam a consistência psíquica, destruindo a integridade moral do sujeito"; [dados que] "envolvam relações de convivência privada"; "dados que envolvam avaliações (negativas) do comportamento que, publicadas, podem ferir o bom nome do sujeito, isto é, o modo como ele supõe e deseja ser visto pelos outros"; dados que alguém fornece a alguém e não deseja ver explorados (comercialmente, por exemplo) por terceiros"(-Ferraz Júnior, 1993, pp. 448-449).

Todos esses dados, embora não acobertados pelo sigilo do inc. XII (exceto quando estiverem em fluxo comunicativo), seguem protegidos,

segundo Ferraz Júnior, pela dimensão da privacidade.

Esta questão importa para um debate teórico hoje existente: a crescente quantidade de informações íntimas armazenadas em servidores de *e-mails* e aplicações de troca de mensagens tem forçado à interpretação de que a distinção entre dados em trânsito e dados armazenados, para fins de proteção à privacidade, perderia sentido (Quito, 2018; Sidi, 2016). Se é verdade que Ferraz Júnior guardava a característica da inviolabilidade aos dados em trânsito, a integralidade do argumento exposto em "Sigilo de dados" mostra que é possível dar proteção a dados armazenados pelo reconhecimento de sua pertinência à privacidade–e até mesmo à intimidade–dos indivíduos. O dilema entre a inviolabilidade dos dados em trânsito e a vulnerabilidade dos dados armazenados, na leitura de Ferraz Júnior, é falso: mesmo reconhecendo a distinção entre dados em fluxo de comunicação e dados estáticos, esses últimos podem estar abarcados com proteção máxima à intimidade de seu titular.

Partindo dessa leitura, é forçoso reconhecer que os limites que a intimidade e a privacidade do indivíduo colocam à atividade fiscalizadora do Estado valem também para dados armazenados. Assim, quando o conteúdo desses dados potencialmente contenha informações relevantes à intimidade de um cidadão, elas devem merecer grau elevado de proteção contra devassas investigativas, mediante rígida avaliação de adequação, estrita necessidade e proporcionalidade.

(iii) A distinção entre as comunicações que deixam vestígios físicos e aquelas que não deixam como parâmetro permissivo para a interceptação de comunicações.

Contra uma interpretação expansiva do inc. XII do art. 5º da Constituição, "Sigilo de dados" oferece uma interpretação consistente e fiel à letra e ao espírito constitucional que merece ser defendida.

Ao insistir na inviolabilidade do fluxo de dados em trânsito ("comunicação"), Ferraz Júnior distingue dois tipos de comunicação: há, de um lado, formas de comunicação marcadas por "instantaneidade", como a comunicação telefônica, que "só é enquanto ocorre" (Ferraz Júnior, 1993, p. 447); e há, de outro, aquelas que deixam vestígios físicos, sendo, portanto, suscetíveis de investigação sem necessitar da medida extrema da interceptação. No caso dessas últimas,

> é possível realizar investigações e obter provas com base em vestígios que a comunicação deixa: a carta guardada, o testemunho de quem leu o nome do endereçado e do remetente, ou de quem viu a destruição do documento, o que vale também para o telegrama, para o telex, para o telefax, para a recepção da mensagem de um computador para outro, etc. (Ferraz Júnior, 1993, p. 448).

Esta distinção ganhou grande relevância contemporânea em razão da proliferação de aplicativos de trocas de mensagem. Como se valem de dados telemáticos para a transmissão de suas comunicações, tais aplicativos têm sofrido pressões para cooperar com autoridades

com o fim de permitir interceptação de mensagens. Tal iniciativa baseia-se em uma leitura abrangente do inc. XII do art. 5º (bem como no parágrafo único do art. 1o da Lei 9.296/1996), que, ao contrário da interpretação de Ferraz Júnior, permitiria interceptação de qualquer espécie de comunicação – não apenas das comunicações "instantâneas", de que a comunicação telefônica seria exemplar.

A interpretação de "Sigilo de dados", por outro lado, não admite essa leitura ampliativa: uma vez que as mensagens deixam vestígios na ponta emissora e receptora da comunicação, investigações que se interessem pelo teor das mensagens trocadas devem recorrer a outras técnicas de investigação – notadamente, a apreensão de aparelhos e a perícia de seu conteúdo. Em caso de mensagens trocadas e armazenadas em servidores ("na nuvem"), cabe também lembrar de sua proteção pela regra geral da privacidade, independentemente de não se tratar de comunicação em curso. Afinal, o teor dessas comunicações armazenadas como regra abrange elementos de intimidade, honra e imagem, recomendando cautela exemplar no acesso a seu conteúdo, e sendo vedadas, à primeira vista, devassas indiscriminadas quanto ao intervalo de tempo, os interlocutores e o assunto das mensagens.

Além disso, a distinção lança luz sobre outro debate contemporâneo relacionado ao sigilo de dados: a possibilidade de emprego de tecnologias de criptografia forte por parte de aplicativos de troca de mensagens instantâneas.[20] O argumento de órgãos de persecução penal de que as empresas de tecnologia têm o dever de possibilitar a interceptação de mensagens trocadas não se sustenta a partir de consideração que o grosso das mensagens trocadas por estas plataformas deixam vestígios (Queiroz, 2018, p. 21).

Em um contexto no qual a informatização é regra, e a quantidade de dados armazenados em bancos de dados informáticos será cada vez maior, "Sigilo de dado", desde que não seja lido de modo seletivo, oferece balizas que seguem úteis à proteção da privacidade dos cidadãos em face da conveniência investigativa estatal.

b. O que está superado

(i) "Privacidade", no tocante a nossos dados pessoais, não pode mais ser conceituada apenas como um direito que se defende passivamente, por resistência a intromissões ou devassas.

Conforme já exposto na parte 2 deste texto, a concepção de privacidade adotada em "Sigilo de dados" é de um direito de bloqueio ou resistência (Ferraz Júnior, 1993, p. 443), que daria a seu titular a faculdade de impedir intromissões indevidas ou devassas nas esferas de exclusividade de sua vida privada. Essa concepção, embora siga válida, não mais esgota a dimensão que o direito à privacidade assume nos dias de hoje.

Como bem destaca Doneda, novas dinâmicas associadas à informação, propulsionadas pela tecnologia e a intensificação dos fluxos de informação, afetam de forma inédita a relação entre dados pessoais e privacidade (2006, p. 6). Nesse cenário, o direito à privacidade não mais se estrutura em torno do isolamento do indivíduo. Ele deve, isto sim, oferecer meios adequados para a proteção de uma esfera privada do indivíduo de maneira funcional em um contexto de "vida em relação" (Doneda, 2006 p. 2).

Para fazer frente a esse desafio, a privacidade não pode se reduzir a uma liberdade negativa

– ou "liberdade de negação", nas palavras de Ferraz Júnior (1993, p. 443). Ao contrário, deve ampliar-se para incluir também a dimensão de uma liberdade positiva[21] (Bioni, 2019, pp. 96-97; Antonialli, 2010, pp. 13-14). Retomando os termos de Hohfeld (1913), clássicos para uma analítica dos direitos subjetivos: ela deixa de ser apenas uma imunidade (de resistência ao poder ou à liberdade de terceiros) e transforma-se agora também em um poder, com dimensão ativa–de exigir, por exemplo, conhecimento, controle e disposição de dados relativos à individualidade, que estejam em poder de terceiros e sejam capazes de afetar autonomia e liberdades de indivíduos.[22]

(ii) A proteção de dados pessoais não deve mais ser pensada de modo individualista, na esteira da concepção tradicional de privacidade, mas sim relacional.

"Sigilo de dados" conceitua o direito à privacidade, ao menos em suas esferas maiores de exclusividade ("intimidade"), a partir da perspectiva de um indivíduo por oposição à sociedade que o ameaça devassar, sobretudo por força do abuso inoponível e nivelador do poder político. Como já exposto em maiores detalhes pouco atrás, esta concepção é derivada do pensamento de Hannah Arendt, na leitura que dela faz Celso Lafer. Nos cânones do direito à privacidade, tal concepção de privacidade é aquela notoriamente forjada por Warren e Brandeis, em texto seminal do final do século XIX: um direito de ser "deixado em paz", derivado, por extensão, do direito consuetudinário de propriedade privada, que garantia a seu titular exclusividade de um bem em face de terceiros (Warren & Brandeis, 1890).

A massificação da produção, coleta, armazenamento, tratamento e compartilhamento de dados pessoais desafia esta concepção individualista de privacidade: ela não mais se limita à garantia de não intrusão, mas deve se espraiar, para que seja efetiva, por todo o feixe de relações do indivíduo. Embora se possa discutir a natureza autônoma do direito de dados pessoais com relação à privacidade, parece inquestionável que essa nova matéria, embora dotada de um campo prático de atuação cada vez mais autônomo, mantém-se ao menos em parte fortemente relacionada com a privacidade, mas em via de mão dupla: da mesma forma que recebe da privacidade a preocupação com a preservação da esfera de autonomia e individualidade dos cidadãos, a disciplina jurídica da proteção de dados pessoais informa a doutrina da privacidade sobre a natureza relacional e difusa desses objetos merecedores de proteção.

Essa compreensão modificada da privacidade se impõe em face de novos modos de existência social, nas quais a conectividade informática é uma realidade cada vez mais incontornável: locomover-se, entreter-se, fazer pagamentos, acessar contas bancárias ou usufruir de serviços públicos e privados são práticas cada vez mais dependentes de interação em rede. Essa conectividade compulsória resulta em dispersão atomizada de dados pessoais, inclusive dados sensíveis, por toda esfera de relações (públicas e privadas) dos cidadãos. Warren e Brandeis desenvolveram a doutrina clássica do direito à privacidade como reação a ameaçadoras inovações tecnológicas de suas épocas: câmeras fotográficas de longo alcance e aparelhos gravadores de voz, capazes de expor os segredos mais recônditos dos cidadãos–especialmente das elites políticas e econômicas cujas vidas privadas eram objeto de interesse da imprensa e do público. Se os desafios tecnológicos agora são outros, não há razão para manter-se preso a um ideal de privacidade forjado em fins do século XIX.[23] Pode-se, assim, avançar

rumo a uma concepção relacional e positiva da privacidade.

(iii) Distinção rígida entre dados em trânsito e dados armazenados como critério para maior ou menor proteção contra intromissões.

Se é verdade, como dito há pouco, que a distinção entre dados estáticos e dados em fluxo não precisa acarretar desconsideração à sensibilidade de dados armazenados para fins de proteção da privacidade, é também verdade que, talvez pela recepção apenas parcial de "Sigilo de dados" pelo STF, essa clivagem, que está de fato presente no texto, tem sido utilizada para negligenciar a devida proteção a dados armazenados.

Isso é sem dúvida um problema e merece superação. Já não faz sentido distinguir entre dados em trânsito e dados estáticos como critério para maior ou menor proteção à privacidade: o barateamento do armazenamento de dados e a migração das comunicações humanas para serviços providos pela Internet, com opções de armazenamento de segurança em servidores ("*backups* na nuvem"), torna o conjunto de dados armazenados sobre um indivíduo, por seu considerável volume e abrangência temporal, mais sensível à sua intimidade do que conversas telefônicas interceptadas. A hierarquia protetiva que coloca dados em trânsito acima de dados armazenados simplesmente é anacrônica diante das mudanças na tecnologia e nas práticas comunicativas desde 1993 até os dias atuais (Sidi, 2016; Quito, 2018).

Se não é possível ignorar a distinção entre os incisos X e XII do art. 5º da Constituição, tampouco há razão para impor uma proteção menos efetiva à nossa intimidade apenas porque estejam em dados armazenados, e não em trânsito. Essa particular leitura de "Sigilo de dados", que não é a única possível de ser feita do texto e nem é necessariamente a melhor, deve ser descartada em favor de outra que equalize a proteção de dados armazenados e dados em trânsito pelo critério que substantivamente importa: o grau de exclusividade que se deve reconhecer às informações contidas nos dados e seu impacto sobre a privacidade de seu titular. O inc. X, art. 5º, da Constituição dá conta desta fundamentação sem dificuldades.

Em julgamento recente, uma das turmas do STF parece ter iniciado interpretação nesse sentido.[24]

(iv) Dados menos exclusivos não necessariamente são menos relevantes para a integridade moral do indivíduo.

"Sigilo de dados" faz uma importante distinção entre tipos diferentes de dados pessoais, segundo a sua "exclusividade". Alguns dados, diz Ferraz Júnior, são mais exclusivos, porque não foram feitos para sair da esfera de segredos de seu titular: "dados de foro íntimo, expressões de autoestima, avaliações personalíssimas com respeito a outros, pudores, enfim dados que, quando constantes de processos comunicativos, exigem do receptor extrema lealdade e alta confiança, e que, se devassados, desnudariam a personalidade, quebrariam a consistência psíquica, destruindo a integridade moral do sujeito" (Ferraz Júnior, 1993, pp. 448-449).

Outros, prossegue o texto, são feitos para a atividade comunicativa e relacional inerente à vida em sociedade:

> pelo sentido inexoravelmente comunicacional da convivência, a vida

> privada compõe, porém, um conjunto de situações que, usualmente, são informadas sem constrangimento. São dados que, embora privativos–como o nome, endereço, profissão, idade, estado civil, filiação, número de registro público oficial, etc.–condicionam o próprio intercâmbio humano em sociedade, pois constituem elementos de identificação que tornam a comunicação, possível, corrente e segura (Ferraz Júnior, 1993, p. 449).

Esses últimos dados, sempre segundo o autor, "só são protegidos quando compõem relações de convivência privativas: a proteção é para elas, não para eles" (op. cit.). A exclusividade desses dados é menor, e não faria sentido protegê-los de modo mais intenso por seu papel eminentemente comunicacional.

Atualmente, contudo, é disseminada a compreensão de que esse tipo de dado pode servir como critério e base para práticas profícuas de perfilização de cidadãos, embora não sejam íntimos e exclusivos. Vale dizer, o dado, mesmo que não seja íntimo, pode ser relevante para a integridade moral do indivíduo. Um nome é capaz de revelar, por exemplo, origem racial ou étnica, ou a (presumível) orientação religiosa da pessoa: basta que pensemos em nomes marcadamente orientais, árabes ou judaicos. O fato de a legislação reconhecer tais marcadores como dados sensíveis[25] revela como práticas de perfilização, ainda que possam se valer de dados menos exclusivos, podem cruzar a linha da individualidade do sujeito. O modo de se vestir, embora seja igualmente pensado para situações de interação com outros seres humanos, pode denunciar preferências políticas (uma camiseta com mensagens políticas) ou religiosas (o uso de adornos). Tudo isso mostra que o grau de "exclusividade" fixo e inerente ao dado em si é um critério imperfeito para medir o grau de proteção que ele merece a título de tutela de privacidade e dignidade humana: mesmo dados inerentemente comunicativos, feitos para a interação humana, podem ser coletados e tratados de modo prejudicial àqueles valores.

(v) Em uma economia de dados, a atividade fiscalizadora estatal não é mais a única grande ameaça à privacidade.

Até mesmo pelo problema específico que motivou sua redação – a questão do acesso a dados de operadoras de cartão de crédito, bem exposta no início deste artigo – "Sigilo de dados" tem o Estado como antípoda do direito à privacidade. Embora o texto não seja comprometido *a priori* com a proposição de que apenas o Estado ameaça a privacidade de indivíduos, ele certamente apresenta-o como o agente principal, quase que exclusivo, desses riscos, pela clivagem que faz entre o privado (como âmbito onde se situa a privacidade) e público (como âmbito do poder político que a ameaça). Esse retrato não corresponde à realidade do presente. Conforme o retrato detalhado e impactante feito no recente livro de Shoshana Zuboff (2019), o "capitalismo de vigilância" tem hoje uma força incomparável a de três décadas atrás. Nele, dados relativos a vidas privadas e intimidades são matéria prima essencial para atividades econômicas diversas, fundando, no limite, uma nova ordem econômica. Não apenas o "poder político", mas também o poder econômico são ameaças à privacidade e à dignidade que ela ajuda a proteger.

Embora grande parte da preocupação com a atuação dessas empresas esteja em suas práticas comerciais, o que juridicamente se situa no direito antitruste ou no direito do consumidor, não é menos verdade que muitos modelos de

negócios na economia de dados representam riscos à privacidade e ao pleno exercício da autonomia de indivíduos. Conforme bem mostra O'Neill (2018), a forma de atuação de muitos negócios que usam dados pessoais como matérias primas frequentemente vale-se de classificações e perfilhamentos imperfeitos, a partir de algoritmos opacos e incompreensíveis em sua operação. Esses dados pessoais, muitas vezes coletados em circunstâncias desconhecidas e inauditáveis, são tratados para gerar julgamentos, veredictos e ranqueamentos determinados em aspectos centrais da vida humana (emprego, moradia, crédito, justiça criminal, entre muitos outros), mas atuam por uma lógica misteriosa, compreensível apenas por quem programou os algoritmos que tomam as decisões. A opacidade e falta de regulação os torna, na prática, inapeláveis; tornam-se, de fato, oráculos do destino de massas de cidadãos. Tanto quanto a devassa de nossos segredos mais exclusivos, essas práticas empresariais negam aos sujeitos afetados o direito a algo que seu *status* humano exige: o direito de conhecer, compreender, corrigir e apelar contra decisões que os massificam em dados, perfis e rótulos ("bom pagador", "trabalhador eficiente", "criativo", "saudável"), marcando seu destino em aspectos essenciais da existência humana (consumidor, profissional etc.).

A geração atual de leis de proteção de dados pessoais quer fazer frente não apenas ao poder estatal, mas também ao poder privado das empresas da economia da informação. Nesses casos, o Estado, ao menos pela via legislativa, atuou como regulador da economia dos oráculos de dados, agindo para disciplinar práticas abusivas e permitir aos cidadãos o exercício do controle sobre seus dados e, nesse contexto, seus destinos.

6. Considerações finais

Neste artigo, realizou-se uma leitura detida de "Sigilo de dados", texto seminal na doutrina do direito à privacidade e proteção de dados no Brasil, para avaliar sua atualidade em face dos desafios atuais que o tema impõe.

Após recuperar o argumento do texto e o contexto de sua produção, analisou-se o modo de sua incorporação pelo STF. Conforme demonstrado, essa incorporação foi apenas parcial: se, por um lado, a distinção entre dados armazenados e dados em trânsito foi efetivamente apropriada pelo Tribunal, não houve, por outro lado, guarida explícita ao argumento, igualmente contido no texto, de que dados armazenados importam ao direito à privacidade e devem ser objeto de cauteloso sopesamento antes de sua devassa, uma vez que o conteúdo desses últimos pode ser íntimo e, portanto, protegido por um grau maior de exclusividade.

Finalmente, avaliou-se os pontos do texto que se mostram ainda atuais, bem como aqueles que exigem uma reflexão atualizadora, em face dos desafios presentes. Como pontos ainda atuais, destacam-se: (i) a centralidade do princípio da dignidade humana como parâmetro normativo que dá sentido ao direito à privacidade e à proteção de dados pessoais, orientando a aplicação desses direitos; (ii) o reconhecimento de que dados importam à privacidade individual, impondo limites à atuação fiscalizadora do Estado—conforme imprimido no próprio título do texto seminal; e (iii) a distinção entre as comunicações que deixam vestígios físicos e aquelas instantâneas como critério de interpretação da exceção constitucional ao sigilo de comunicações – isto é, para a identificação de quais tipos de interceptação são permitidos. Já como pontos que merecem reflexão atualizadora, destacam-se os seguintes: (i) o direito à privacidade não mais se estrutura como uma liberdade de negação, por meio da proteção de

dados pessoais, ela se reveste de um aspecto positivo de controle dos próprios dados pessoais; (ii) a proteção de dados pessoais deve ser pensada em uma perspectiva relacional, em detrimento da natureza individualista associada à concepção tradicional de privacidade; (iii) a distinção rígida entre dados em trânsito e dados armazenados não mais se sustenta como critério de interpretação da inviolabilidade do sigilo de dados veiculada por meio do artigo 5°, inciso XII da Constituição Federal; e (iv) na sociedade da informação, a atividade fiscalizadora do Estado não é mais a grande ameaça à privacidade–alinhando-se a agentes privados.

Nesse sentido, este trabalho se coloca como esforço de superação de dificuldades para interpretação e aplicação de conceitos e teorias tradicionais do direito às questões jurídicas na era digital (Kira, 2019). Demonstra, ainda, que olhar para o passado, representado aqui por texto seminal da década de 90, pode ser tarefa produtiva para tal empreitada – quando devida e cuidadosamente conduzida.

Referências

Abreu, J. D. S. (2018). *Passado, presente e futuro da criptografia forte: desenvolvimento tecnológico e regulação*. Revista Brasileira de Políticas Públicas, 7(3), pp. 24-42.

Ação Penal nº 307 (1994, 13 de dezembro). Relator: Ilmar Galvão. Acesso em 18 de novembro de 2019, disponível em: http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=AC&docID=324295.

Agravo Regimental no Habeas Corpus n° 124322/RS (2016, 19 de dezembro). Relator: Roberto Barroso. Acesso em 18 de novembro de 2019, disponível em: http://portal.stf.jus.br/processos/downloadPeca.asp?id=310980619&ext=.pdf. Antonialli, D. M. (2010). *Privacy and International Compliance: When Differences Become an Issue*. In 2010 AAAI Spring Symposium Series.

Avolio, L. F. T. (2003). *Provas ilícitas: interceptações telefônicas, ambientais e gravações clandestinas*. Editora Revista dos Tribunais.

Aristides estuda ação no caso dos cartões de crédito (1992, 11 de março). *O Estado de São Paulo*, Caderno Economia e Negócios, página 1.

Badaró, G. H. R. I. (2010). Interceptação de comunicações telefônicas e telemáticas: limites ante o avanço da tecnologia. In Lima, J. C., & Casara, R. R., Temas para uma perspectiva crítica do direito: homenagem ao Professor Geraldo Prado. Rio de Janeiro: Lumen Juris, 483-499.

Bioni, B. R. (2019). Proteção de dados pessoais: A função e os limites do consentimento. Rio de Janeiro: Forense.

Doneda, D. (2006). Da privacidade à proteção de dados pessoais. Rio de Janeiro: Renovar.

Doneda, D. (2011). A proteção dos dados pessoais como um direito fundamental. Espaço Jurídico Journal of Law [EJJL], 12(2), pp. 91-108.

Ferraz Júnior, T. S. (1993). Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado. *Revista da Faculdade de Direito*, Universidade de São Paulo, 88, pp. 439-459.

Ferraz Júnior, T. S. (2001). A liberdade como autonomia recíproca de acesso à informação. In Martins, I. G. D. S., & Greco, M. A., *Direito e Internet: relações jurídicas na sociedade informatizada*. São Paulo: Revista dos Tribunais, pp. 241-7.

Ferraz Júnior, T. S. (2018). Sigilo de dados, o direito à privacidade e os limites do poder do Estado: 25 anos depois. In Abreu, J. D. S., & Antonialli, D., *Direitos Fundamentais e Processo Penal na Era Digital: Doutrina e Prática em Debate*. Vol. I. São Paulo: InternetLab, pp. 18-41.

Governo acena com choque se ajuste fracassar (1991, 23 de agosto). *Folha de São Paulo*, Caderno Brasil, p. 1.

Governo quer o fim do sigilo bancário, para juristas, o plano é inconstitucional (1991, 2 de fevereiro). *Folha de São Paulo*, Caderno de Economia, p. 1.

Greco Filho, V. (2015). *Interceptação telefônica: considerações sobre a Lei nº 9.296*. São Paulo: Saraiva.

Habeas Corpus n° 91867/PA (2013, 26 de novembro). Relator: Marco Aurélio. Acesso em 18 de novembro de 2019, disponível em: http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=5426785.

Hohfeld, W. N. (1913). Some Fundamental Legal Conceptions as Applied in Judicial Reasoning. Yale Law Journal, v. 23, pp. 16-59. Acesso em 25 de junho de 2019, disponível em https://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=2324&context=ylj

Igo, S. E. (2018). The known citizen. A history of privacy in modern America. Cambridge: Harvard University Press.

Kira, B. (2019). "O Direito Na Era Digital: Ensino, Teoria, e Prática Em Face Das Novas Tecnologias de Informação e Comunicação." In Poder Judiciário, Concorrência e Regulação, AJUFE.

Queiroz, R. M. R. (2018). Privacidade, criptografia e dever de cumprimento de ordens judiciais por aplicativos de trocas de mensagens. Revista dos Tribunais, v. 998, pp. 13-26.

Macedo Júnior, R. P. (2009). O método de leitura estrutural. Working Paper. Disponível em http://bibliotecadigital.fgv.br/dspace/handle/10438/2814

Mandado de Segurança 21.729-DF (2001, 19 de outubro). Relator: Marco Aurélio. Acesso em 18 de novembro de 2019, disponível em:: http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=AC&docID=85599.

Miranda, F. C. P. de. (2004). *Tratado de Direito Privado–Tomo 07*. Bookseller, IBooks.

Mendes, G. F., & Branco, P. G. G. (2012). *Curso de direito constitucional*. 7 ed. rev. Saraiva Educação SA.

Mendes, L. S. (2014). *Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental*. Saraiva.

Nastari, J. (1992a, 18 de fevereiro). Receita terá dados de clientes de bancos. *O Estado de São Paulo*, Brasília, Caderno de Economia, p. 3.

Nastari, J. (1992b, 05 de maio). Receita vai exigir dados de cartões de crédito. *O Estado de São Paulo*, Caderno Economia, p. 5.

Lafer, C. (1988). Público e Privado: o direito à informação e o direito à intimidade. *A reconstrução dos direitos humanos*. São Paulo, Companhia das Letras, pp. 237-274.

O'NEIL, C. (2018). *Weapons of math destruction: How big data increases inequality and threatens democracy*. London: Penguin Books.

Pocock, J. G. A., Miceli, S., & Fernandez, F. (2003). *Linguagens do ideário político*. São Paulo: EDUSP.

Prado, G. (2006). *Limite às interceptações telefônicas e a Jurisprudência do Superior Tribunal de Justiça*. Rio de Janeiro: Lumen Juris.

Projeto de Emenda Constitucional n. 51, de 1991 (da Presidência da República) (1991). *Altera dispositivos da Constituição da República Federativa do Brasil*. Disponível em http://www.camara.gov.br/proposicoesWeb/prop_mostrarintegra?codteor=1243014&filename=Dossie+-PEC+51/1991

Quito, C. (2018). Acesso a comunicações armazenadas na prática judiciária. In Abreu, J. D. S., & Antonialli, D., *Direitos Fundamentais e Processo Penal na Era Digital: Doutrina e Prática em Debate*. Vol. I. São Paulo: InternetLab, pp. 102-107.

Receita Federal vai ter acesso a extratos de cartões de crédito (1992, 19 de fevereiro). *Folha de São Paulo*, Brasília, Caderno Dinheiro, p. 2.

Recurso Extraordinário n° 418.416-SC (2006, 10 de maio). Relator: Sepúlveda Pertence. Acesso em 18 de novembro de 2019, disponível em http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=AC&docID=395790.

Recurso Ordinário em Habeas Corpus n° 132062/RS (2016, 29 de novembro). Relator: Marco Aurélio. Acesso em 18 de novembro de 2019, disponível em http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=13902497.

Rodriguez, J. R. (2013). *Como Decidem as Cortes? Para Uma Crítica Do Direito (Brasileiro)*. 1a edição. Rio de Janeiro, RJ, Brasil: FGV Editora.

Sidi, R. (2016). *A interceptação das comunicações telemáticas no processo penal*. Belo Horizonte: Editora Plácido.

Suspenso julgamento de HC que discute validade provas obtidas em conversas de Whatsapp sem autorização judicial (2019, 11 de junho). *Notícias STF*. Acesso em 18 de novembro de 2019, disponível em http://www.stf.jus.br/portal/cms/verNoticiaDetalhe.asp?idConteudo=413786.

Warren, S., & Brandeis, L. (1890). The Right to Privacy. *Harvard Law Review*, 4(5), pp. 193–220.

Vice Procuradoria Geral da República. *Parecer* (1994, 26 de setembro). Dispõe sobre o Mandado de Segurança nº 21.729-DF, pp. 40-66.

Vojvodic, A. de M., Machado, A. M. F., & Cardoso, E. L. C. C. (2009). *Escrevendo Um Romance, Primeiro Capítulo: Precedentes e Processo Decisório No STF*. Revista Direito GV 5(1): pp. 21–44.

Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. New York: PublicAffairs.

Notas finais

1 Excluídas as decisões monocráticas, temos: Mandado de Segurança n° 21.729-DF (2001) , Agravo Regimental no Habeas Corpus n° 124322/RS (2016), Recurso Ordinário em Habeas Corpus n° 132062/RS (2016), Habeas Corpus n° 91867/PA (2013) e Recurso Extraordinário n° 418.416-SC (2006).

2 Em razão do objetivo amplo da presente pesquisa, cada uma das seções contou com metodologia própria e, em certo sentido, independente das demais. Na primeira seção, empregou-se o método de leitura estrutural para leitura e apresentação do caminho argumentativo do texto (Macedo Júnior, 2009). Na segunda seção, guardadas as devidas proporções, pretende-se fazer uma espécie de "história do discurso político" – na qual se busca compreender a linguagem, o contexto, interlocutores e posição ocupada pelo autor quando da autoria do texto (Pocock, Micely & Fernandez, 2003), a partir – principalmente, de declarações do autor e matérias jornalísticas da época. Na terceira seção, a descrição da incorporação pelo STF das teses do autor se deu, principalmente, a partir das metodologias apresentadas em: Hübner Mendes (2010) e Vojvodic, Machado, e Cardoso (2009). Por fim, a quarta e última seção partiu de reflexão autoral à luz de literatura recente sobre o tema.

3 Olhando para o texto constitucional, Ferraz Júnior identifica dois blocos em que o termo comunicação seria um elemento de destaque: "da correspondência e das comunicações telegráficas" e "de dados e das comunicações telefônicas". Essa interpretação decorre da existência da conjunção 'e' adotada nos dois momentos e da vírgula que os separa. Trata-se de interpretação atualmente disputada, conforme explorado mais a frente no artigo.

4 A conceituação é de W. N. Hohfeld, para quem a imunidade, enquanto direito subjetivo, é o oposto do poder (também enquanto direito subjetivo): "poder é o 'controle' afirmativo de uma pessoa, em uma determinada relação jurídica, em relação a outra pessoa; enquanto a imunidade é a liberdade, por parte de uma pessoa, do poder legal ou 'controle' de outra pessoa, em uma relação jurídica (Hohfeld, 1913, p. 55. Tradução nossa).

5 Deve-se destacar que a Lei nº 9.296/96 (Lei de Interceptações) prevê, em seu artigo 1º, a possibilidade de interceptação do "fluxo de comunicações em sistemas de informática e telemática". Ocorre que se trata de artigo de constitucionalidade disputada, inclusive alvo de ações diretas de inconstitucionalidade no STF (ADI nº 1.488-9/DF e ADI n° 4.112/DF). De um lado, argumenta-se que o dispositivo constitucional possuiria dois blocos, separados por uma vírgula e, portanto, a expressão "no último caso" referir-se-ia a comunicações de dados e telefônicas (narram a existência dessa posição: Grinover, 1997, p. 25; Sidi, 2016, p. 221). De outro, defende-se uma interpretação gramatical do artigo 5º, inciso XII, no sentido de que a expressão "no último caso" só seria referente a comunicações telefônicas (nesse sentido, ver: Avolio, 2010, p. 170; Greco Filho, 2015, pp. 15-17). Mais recentemente, observa-se um esforço de recuperação do "Sigilo de dados" para auxílio na interpretação do dispositivo constitucional. De um lado, os teóricos Badaró (2010) e Prado (2006) argumentam que as premissas de Ferraz Júnior permanecem válidas (isto é, que a interceptação só seria possível quando caracterizada pela instantaneidade), mas a leitura adequada do dispositivo constitucional frente à realidade tecnológica é que este só possibilitaria

a interceptação em casos que não for possível a apreensão posterior desses dados. De outro, Queiroz (2018) observa que a inconstitucionalidade do art. 1º da Lei de Interceptações decorre de uma interpretação literal e hermenêutica da norma constitucional, a última a partir da distinção de Ferraz Júnior entre as comunicações que deixam vestígios e aquelas que não deixam. Além disso, argumenta que se vive um contexto de hipervulnerabilidade de informações pessoais sensíveis da internet, onde a proteção da privacidade merece ser privilegiada.

6 Lei Geral de Interceptações–Lei nº 9.296, de 24 de julho de 1996.

7 Em maio de 2017, o Internetlab, centro independente de pesquisa sobre direito e sociedade, organizou o I Congresso Internacional Direitos Fundamentais e Processo Penal na Era Digital, que contou com a palestra "Sigilo de dados, o direito à privacidade e o poder do Estado: 25 anos depois" ministrada por Ferraz Júnior. Ver: Ferraz Júnior, T. S. (2018). Sigilo de dados, o direito à privacidade e os limites do poder do Estado: 25 anos depois. In Abreu, J. D. S., & Antonialli, D., Direitos Fundamentais e Processo Penal na Era Digital: Doutrina e Prática em Debate. Vol. I. São Paulo: InternetLab, pp. 18-41.

8 Informação consta na biografia disponibilizada em seu site pessoal: http://www.terciosampaioferrazjr.com.br/?q=biografia. Acesso em: 15 de junho de 2019.

9 Essa foi a última notícia ou portaria encontrada sobre o assunto. Foram consultadas as bases de dados do Acervo do Estado de São Paulo e Acervo da Folha de São Paulo, bem como os Diários Oficiais da Imprensa Nacional. O arrefecimento da discussão pode ser explicado pelo período político tenso que seguiu a esse momento, considerando que a denúncia de Pedro Collor na Revista Veja foi realizada no mês de maio de 1992.

10 Tal análise foi realizada a partir da metodologia explorada em Hübner Mendes (2010) e Vojvodic, Machado e Cardoso (2009).

11 Foi realizada pesquisa na Plataforma de jurisprudência do STF com os termos chave "sigilo de dados e XII". Foram encontrados 14 acórdãos, 427 decisões monocráticas, 44 informativos. Analisamos as ementas e indexações dos referidos acórdãos. Destes, dez eram impertinentes, tratando de assuntos diversos relacionados ao inciso XII. Os outros quatro [HC-AgR 124322/RS (2016), RHC 132062/RS (2016), HC 91867/PA (2016) e RE 418416/SC (2006) empregavam a tese de Sampaio Ferraz acerca da proteção do sigilo de dados se referir aos dados em trânsito e citavam, expressamente, o MS N° 21.729/DF (2001). O mais antigo dos quatro, o RE 418.416/SC (2006), foi referenciado nos outros três julgados desse grupo.

12 O mandado de segurança argumentava, em resumo, que: (i) o pedido violava o sigilo bancário concedido a suas operações, que só poderia ser quebrado mediante ordem judicial, de acordo com o art. 38 da Lei nº 4.595/1964; (ii) a exceção de quebra de sigilo a respeito de documentos e informações preceituada no art. 8º, §2º da Lei Complementar nº 75/1993 (Estatuto do Ministério Público) só valeria para autoridades públicas, e o Banco do Brasil não representaria uma no caso; e (iii) apesar de a privacidade, representada no art. 5º, inc. X, e sigilo bancário não serem absolutos, estes só poderiam ser quebrados mediante decisão judicial.

13 A reconstrução dos dois casos se deu por meio da leitura do acórdão. Entretanto, diante da indicação no acórdão de que o parecer da

Vice Procuradoria havia tratado do o sigilo de dados, o documento foi solicitado via Lei de Acesso à Informação à Seção de Arquivo do STF para a consulta de seu conteúdo.

14 Como mencionado, os demais votos vencedores se limitaram a apontar o caráter público dos recursos em questão.

15 "Assim, por exemplo, solicitar ao juiz que permita à autoridade acesso à movimentação bancária de alguém não significa pedir para interceptar suas ordens ao banco (sigilo da comunicação) mas acesso a dados armazenados (sigilo da informação). A primeira solicitação– salvo se o meio for o telefone é inadmissível; já a segunda é possível. Em que limites? 10. A análise do inciso X do art. 5º da Constituição nos orienta a resposta: são aquelas informações, em termos de privacy, constitutivas da integridade moral da pessoa." (Ferraz Júnior, 1993, p. 448).

16 Com exceção do Ministro Marco Aurélio, que opôs vício de procedimento nas razões do Recurso Extraordinário, mas mencionou concordar com a tese da proteção ao sigilo de comunicação de dados.

17 Essa leitura aproxima-se de diagnóstico de José Rodrigo Rodriguez no sentido de que a invocação de autoridades é modelo preponderante de raciocínio jurídico no Brasil. Pode-se destacar trecho nesse sentido: "As cortes brasileiras citam, com muita frequência, doutrinadores e teóricos do direito (além de 'jurisprudências') sem reconstruí-los em uma linha de argumentação racional, ou seja, sem explicar o porquê de cada autor (ou caso) ser relevante para a solução final, de acordo com a sua reconstrução sistemática das fontes do direito". (Rodriguez, 2013, p. 81)

18 Para uma reconstrução completa das gerações de proteção de dados pessoais, ver: Mendes, 2014, pp. 37-44; Doneda, 2006, pp. 203-217; Bioni, 2019, pp. 117-121.

19 Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados).

20 A denominação "criptografia forte" se refere aos casos em que a tecnologia não oferece mecanismos de acesso aos dados – mesmo em casos de respeito ao devido processo legal. No caso dos aplicativos de troca de mensagens, coloca-se como sinônimo para "criptografia de ponta a ponta". Para descrição completa do debate, ver: Abreu (2018).

21 A distinção entre liberdade negativa e liberdade positiva vem de "Two Concepts of Liberty" conhecido ensaio de Isaiah Berlin (1992). "Liberdade negativa" diz respeito à área mínima de não intrusão que uma pessoa, para que possa ser considerada livre (e não coagida ou escravizada), deve preservar (cit., p. 169); já a "Liberdade positiva" diz respeito à garantia da liberdade por ações positivas, por uma conduta ativa (e não por mera não interferência), que garanta ao sujeito que ele se mova por suas próprias "razões e propósitos conscientes", e não por "causas que [o] afetem externamente" (cit., p. 178). Embora o conceito de liberdade positiva de Berlin construa-se em oposição à heteronomia (logo, de preservação de autonomia, no sentido da capacidade de dar a si mesmo suas próprias máximas de conduta, ao invés de tê-las impostas por terceiros), ele é de todo utilizável neste caso. A distinção entre "ser livre de" (liberdade negativa) e "ser livre para" (liberdade positiva) é inteiramente útil à

distinção que ora fazemos para o direito à privacidade, para o qual a dimensão positiva, no tocante ao direito protetivo de dados pessoais, é sumamente relevante.

22 É interessante apontar que Ferraz Júnior (2001) já voltou a analisar como o desenvolvimento tecnológico coloca novas questões para a proteção da intimidade do indivíduo. Neste, lidava com cenários hipotéticos sobre o futuro de sociedades informatizadas: os cenários de "big brother" (Estado policial forte) e "little sister" (Estado enfraquecido). Enquanto o primeiro seria marcado por uma redução da esfera privada em razão do agigantamento do Estado de vigilância, este guiado pelo combate à criminalidade, o segundo derivaria do fortalecimento de redes de comunicações privadas e bancos de dados inacessíveis ao Estado, por exemplo, a partir de criptografia. Para o autor, trata-se de embate entre liberdade (na figura da sua espontaneidade individual resguardada pelo sigilo) e interesse público (nas figuras da transparência, direito à informação e repressão ao abuso de poder) (2001, p. 134). Esses cenários convidariam a uma nova reflexão sobre a operação da liberdade. Em detrimento da liberdade individual, operada a partir da oposição indivíduo/sociedade, estaríamos diante da liberdade em reciprocidade. A proteção de dados não seria um direito no sentido de domínio absoluto (propriedade do indivíduo sobre seus dados), mas sim um direito à autodeterminação informacional, objetivando possibilitar a cada um sua liberdade de comunicação – isto é, um exercício de sua liberdade em reciprocidade. Trata-se de nova roupagem para o direito à liberdade que, antes individual, passa a ser exercido em rede. Nessa argumentação, Ferraz Júnior reitera sua interpretação sobre o sigilo de dados–faria sentido, então, que a proteção fosse referia à comunicação de dados–e não aos dados em si (2001, p. 139).

23 Para uma detalhada visão da evolução histórica do conceito de privacidade à luz das mudanças sociais e tecnológicas de cada período da história dos EUA, v. Igo, 2018.

24 Trata-se do HC n° 168052/SP, ver: Suspenso julgamento de HC que discute validade provas obtidas em conversas de Whatsapp sem autorização judicial (2019, 11 de junho). Notícias STF. Disponível em http://www.stf.jus.br/portal/cms/verNoticiaDetalhe.asp?idConteudo=413786. O tema também é objeto de análise pelo STF no ARE n° 1042075, no qual foi declarado repercussão geral.

25 "Dado sensível" é uma categoria disseminada na atual legislação de proteção de dados pessoais. Na lei brasileira, é definido no art. 5º, II, como "dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente a saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural".

Recebido em 04/07/2019
Aceito em 18/12/2019