A bondade dos bons não protege nossos dados armazenados

A vida em sociedade nas últimas décadas está condicionada pela tecnologia, que forjou um novo modo de comunicar e interagir, de se informar e se expressar, de trabalhar, e, *por assim dizer, de exercer livremente a personalidade*. Dentro dessa dinâmica, a crescente carga de informação relacionada às mencionadas atividades deixa de se materializar por meios físicos e se converte em um massivo volume de dados que alimentam *hard drives* e *smartphones*, além da imaterial e etérea *nuvem* — metáfora pela

ı de armazenamento por meio de rede global de servidores. Seja por meio dos servidores de internet, seja nos próprios dispositivos pessoais, a verdade é que a conveniência que essas tecnologias proporcionam faz com que se concentre nesses meios uma quantidade significativa de dados que muito revelam sobre a vida privada dos usuários. E a violação da esfera íntima da privacidade está em risco maior na medida em que *"o computador, supremo regente da apressada vida moderna, passa a exercer a função de verdadeiro cofre de nossos sentimentos e disposições mais pessoais"* [1]. A discussão ganha dimensões e contornos importantes quando se analisa a problemática que envolve a natureza e o regime de proteção dos dados armazenados, especialmente quando esses dados refletem o conteúdo de comunicações privadas.

O novo paradigma de vida digital delineado nas últimas décadas impõe que se assegure uma adequada tutela da privacidade nesse contexto, de modo a reconsiderar a compreensão que se tem sobre o âmbito de proteção de direitos substanciais que com ela se relacionam, a exemplo do sigilo das comunicações.

As comunicações privadas se realizam cada vez mais pela via digital, por meio de dados, cujo conteúdo segue sucessivamente armazenado após o fim do processo comunicativo. Essa dinâmica leva a que se disponha de bancos de dados que contemplam anos de comunicações armazenadas, capazes de revelar as mais íntimas informações particulares decorrentes das interações sociais de uma pessoa, mas pela circunstância de estarem armazenadas e não em fluxo, não gozariam da proteção atribuída ao sigilo das comunicações. Isso decorre do caráter restritivo da interpretação que se atribui ao conteúdo da proteção constitucional inserida no artigo 5º, XII, CF, pela qual o sigilo das comunicações tem como objeto a própria ação comunicativa, mas os dados comunicados [2]. Tal compreensão acaba por levar a que se proteja menos substancialmente o sigilo do conteúdo das comunicações privadas armazenadas, entendidas como aquelas que já alcançaram o destinatário e superaram o caráter da contemporaneidade. Sustenta-se que estas estariam abrangidas pelo artigo 5º, X, CF, situando-se no âmbito da garantia da privacidade.

O entendimento de que a intromissão no processo comunicativo com vistas a conhecer seu conteúdo representa violação de maior gravidade, levou a uma regulamentação específica para a medida de interceptação telefônica. Desse modo, se para a investigação criminal interessa a quebra do sigilo das comunicações armazenadas mediante a requisição de disponibilização desses dados por provedores de aplicações de internet, seu deferimento não dependerá do atendimento aos requisitos mais estritos da Lei 9.296/96, tais como a presença de indícios de autoria ou participação em crimes apenados com reclusão; a inexistência de meios menos invasivos para a produção da prova e a delimitação temporal para a duração da medida.

O fundamento seria, por outro lado, os artigos 7º, III, e 10º, §2º, da Lei 12.965/14, que instituiu o Marco Civil da Internet, o qual, apesar de estabelecer a necessidade de autorização judicial para que os provedores disponibilizem o acesso às comunicações armazenadas, nada diz quanto aos limites formais e materiais para a decretação de tal medida invasiva. A ausência dessa regulamentação específica fez despontar, na prática judiciária, grave descompasso entre o grau de proteção conferido às comunicações em fluxo em comparação às comunicações eletrônicas armazenadas, potencialmente mais invasivas [3], deixando esse conteúdo vulnerável e suscetível a violações cada vez mais amplas e injustificadas [4].

Há de se questionar, em primeiro lugar, a coerência ou razoabilidade de se retirar as comunicações armazenadas do âmbito de proteção do artigo 5º, XII, CF, ou ao menos de se exigir condições menos restritivas para autorizar o acesso ao seu conteúdo para fins de investigação criminal.

Inclusive, como destaca Sidi [5], em relação à interceptação de e-mails, do ponto de vista tecnológico sequer seria possível distinguir o que se concebe como mensagens em trânsito e mensagens armazenadas, já que sua captação sempre se dará a partir de algo armazenado, como foi ponderado no caso Konop v. Hawaiian Airlines, Inc (2002), destacando que o armazenamento é um estágio obrigatório da transmissão das mensagens. Por outro lado, ainda que a medida não caracterize uma interceptação propriamente dita pela falta do requisito contemporaneidade, *"é inegável que a preservação de seu conteúdo humano e demais detalhes ligados a ela não podem ser dissociados da expressão constitucional 'sigilo das comunicações', dotada de tão claro sentido linguístico"* [6].

Nos Estados Unidos, onde o *Stored Communications Act* estabelece limites menos restritivos para o acesso às comunicações eletrônicas que já estejam armazenadas nos provedores há mais de 180 dias, compreende-se que por estarem armazenadas as comunicações não estariam contempladas no âmbito da Quarta Emenda à Constituição, tal como as contemporâneas, para as quais se exige requisitos mais severos como a demonstração de causa provável. Nesse contexto, a irrazoabilidade da diferença de tratamento entre as duas situações fora reconhecida em meio ao caso *United States v. Warshak* (2010). A corte considerou, no caso, que se o e-mail é análogo ao telefone e à carta, não se pode acessar seu conteúdo sem a observância da Quarta Emenda, cujo objetivo fundamental é proteger a privacidade e a segurança dos indivíduos contra invasões arbitrárias por funcionários do governo. Nesse sentido, seria uma questão de "bom senso" entender que existe uma expectativa razoável de privacidade no e-mail armazenado, equivalente à de chamadas telefônicas e correio postal, especialmente na medida em que o e-mail desempenha um "papel vital" na vida profissional e pessoal dos cidadãos.

O fato é que, como se vem observando por meio da prática judiciária, a ausência de disciplina específica quanto às condições para a decretação da medida de quebra de sigilo do conteúdo de comunicações armazenadas, como os e-mails, leva a que ela seja concebida, quando muito, como hipótese de busca e apreensão, dando margem a verdadeiras devassas à privacidade dos investigados e permitindo que se vasculhe o conteúdo de décadas de comunicações armazenadas.

Como alertado por Orin Kerr, o Direito Processual Penal evoluiu no sentido de regular os mecanismos comuns à investigação de crimes materiais, valendo-se de elementos físicos de prova, de modo que as normas existentes são naturalmente moldadas para se adequarem às necessidades da investigação e à tutela da privacidade dentro desse contexto. A prova digital é colhida de formas tão particulares que as normas atualmente disponíveis não fazem sentido nesse novo contexto. As regras que bem equilibram privacidade e segurança pública na busca por provas físicas costumam produzir resultados indesejáveis quando aplicados aos meios de investigação de provas digitais — eis que acabam concedendo poderes extremamente invasivos ao Estado [7].

Tendo isso em vista, importa discutir possíveis caminhos para a definição de *standards* para a autorização judicial da quebra de sigilo das comunicações privadas armazenadas em provedores de aplicações de internet. Por se tratar, de todo modo, de medida cautelar probatória, deve ter seu deferimento condicionado aos requisitos de cautelaridade que a justifiquem [8], sendo imperioso, fundamentalmente, demonstrar a presença de indícios razoáveis de autoria ou participação nos fatos investigados; indicar lapso temporal determinado, pertinente ao fato apurado; e justificar a proporcionalidade da medida invasiva.

Para além disso, os parâmetros aplicados para a medida de busca e apreensão não são adequados para dar conta do peculiar contexto dos dados digitais, na linha do sustentado por Kerr. O contexto extremamente físico e material inerente à busca domiciliar se opõe fortemente ao contexto do armazenamento de documentos digitais. Basta que se faça uma comparação mental do volume de documentos físicos passíveis de serem encontrados em um determinado espaço físico, frente ao volume de suas versões digitais que um servidor é capaz de armazenar.

É preciso cautela na transposição automática do conceito de domicílio para o contexto digital para fins de individualização do campo dentro do qual se realizará a busca, não bastando a mera indicação de um endereço de e-mail para que se possa acessar indiscriminadamente todo o seu conteúdo armazenado. Ao contrário, o caráter peculiar da quebra de sigilo das comunicações eletrônicas exige que a adequada individualização do campo destinado à quebra de sigilo compreenda, além do endereço de e-mail, também um lapso temporal determinado

— como pressuposto de sua proporcionalidade.

Não há como se considerar minimamente aceitável, nesse sentido, ordens judiciais que determinem a disponibilização, pelos provedores de aplicações de internet, da integralidade do conteúdo de e-mails armazenados nas contas dos usuários, enviados e recebidos, desde sua criação [9] — sem a delimitação de um lapso temporal razoável, vinculado ao objeto da investigação. O silêncio da Lei 12.965/14 não pode implicar a completa vulnerabilidade do conteúdo desses dados de comunicação, sendo necessária a observância de parâmetros específicos para lidar com as complexidades da prova digital, os quais sejam consentâneos com a adequada tutela do direito à privacidade.

Valendo-se do disposto no inciso II do artigo 240, CPP, é possível dizer que a determinação dos motivos e dos fins da medida de quebra de sigilo dos dados deve contemplar tanto a fixação do lapso temporal a condicionar o acesso, quanto a identificação precisa do que pode ser alcançado pela busca, conforme o objeto da investigação. Ambos os requisitos devem constar da fundamentação da autorização judicial, de modo a definir estritamente os limites da medida.

No que se refere ao lapso temporal, trata-se de verdadeira individualização do campo dentro do qual a medida se realizará. Analogicamente à busca domiciliar, a determinação do lapso temporal dentro do qual a quebra do sigilo está autorizada representa, juntamente com o endereço de e-mail, a identificação do domicílio no qual se realiza a busca e apreensão. Desse modo, acessar dados de comunicação não abrangidos pelo lapso temporal seria o mesmo que realizar a busca e apreensão fora dos limites físicos do domicílio indicado no mandado. Trata-se, pois, de limite objetivo que deve restringir e condicionar o acesso.

Um outro limite se refere à indicação do objeto da medida — relacionado ao motivo e aos fins da diligência — e servirá como parâmetro a nortear a busca no campo delimitado temporalmente, de modo a determinar o que é de interesse para a investigação em questão. Nesse caso, trata-se de critério subjetivo que depende de análise e filtragem do conteúdo, o que destaca a imprescindibilidade de que se determine, o mais precisamente possível, o fato investigado e o que se pretende demonstrar por meio das comunicações — a fim de evitar que se legitime, com base em decisões genéricas, as práticas de *fishing expedition* [10].

Diante de tal demarcação, importante insistir, portanto, que o lapso temporal que define o material objeto da quebra do sigilo configura-se como limitação objetiva que condiciona o acesso do conteúdo pelos órgãos persecutórios. Desse modo, cabe ao provedor de internet selecionar os dados respectivos que integram o objeto da autorização judicial para apresentá-los à autoridade solicitante.

A exemplo do que se discutiu acima, cogitar de disponibilização de acesso integral ao conteúdo das comunicações eletrônicas privadas e esperar que os órgãos persecutórios se autolimitarão no sentido de somente acessarem e utilizarem o conteúdo relacionado aos fatos investigados é manter a porta aberta para a prática de *fishing expedition*. A relevância do direito constitucional tutelado (aliado a outro de ainda maior relevo, qual seja, a presunção de inocência), exige uma proteção que não dependa desta expectativa de boa-fé.

"Do contrário, ficaremos sempre na circularidade ingênua de quem, acreditando na 'bondade dos bons' (Agostinho Ramalho Marques Neto), presume a legitimidade de todo e qualquer ato de poder, exigindo que se demonstre (cabalmente, é claro) uma conduta criminosa e os 'motivos' pelos quais uma 'autoridade' manipularia uma prova… Eis a postura a ser superada" [11].

[1] PRADO, Geraldo. *Limite às Interceptações Telefônicas e a Jurisprudência do Superior Tribunal de Justiça.* 2ª ed. Rio de Janeiro: Lumen Juris, 2012.

[2] FERRAZ JUNIOR, Tercio Sampaio. Sigilo de Dados: O Direito à Privacidade e os Limites à Função Fiscalizadora do Estado. *Cadernos de Direito Constitucional e Ciência Política.* Nº 1, pp. 76-90, 1992.

[3] QUITO, Carina. Acesso a comunicações eletrônicas armazenadas na prática judiciária. *In:* ANTONIALLI, Dennys; ABREU, Jacqueline de Souza. *Direitos Fundamentais e Processo na Era Digital.* São Paulo: Internetlab, 2018, p. 103.

[4] Sobre o tema, ver também: ABREU, Jacqueline de Souza; ANTONIALLI, Dennys. *Vigilância sobre as comunicações no Brasil.* 2ª ed. Internetlab, 2017. Disponível em: https://www.internetlab.org.br/wp-content/uploads/2017/05/Vigilancia_sobre_as_comunicacoes_no_Brasil_2017_InternetLab.pdf.

[5] SIDI, Ricardo. SIDI, Ricardo, A interceptação de e-mails e a apreensão física de e-mails armazenados. *In:* Revista Fórum de Ciências Criminais, n.4, pp. 101-21, julho/dezembro 2015.

[6] *Idem.*

[7] Trad. livre. KERR, Orin S. Digital Evidence and the new Criminal Procedure. *In: Columbia Law Review*. v. 105, 2005, pp. 279-318.

[8] STJ, 6ª Turma, Habeas Corpus nª 315.220, rel. Min. Maria Thereza Rocha de Assis Moura, j. 15.09.2015.

[9] *Cf.* SIDI, Ricardo, *op. cit.*, notas 48 e 49; QUITO, Carina, *op. cit.*, p. 103.

[10] ROSA, Alexandre Morais da. *Guia do Processo Penal Estratégico.* Florianópolis, Emais, 2021, p.

619.

[11] LOPES JR., Aury. MORAIS DA ROSA, Alexandre. A importância da cadeia de custódia para preservar a prova penal. Disponível em: https://www.conjur.com.br/2015-jan-16/limite-penal-importancia-cadeia-custodia-prova-penal.

Date Created
24/09/2021