COLEÇÃO DIREITO E NOVAS TECNOLOGIAS

DIREITO, PROCESSO E TECNOLOGIA

O não reconhecimento do "anonimato legal" ante a manifestação de um cidadão comum é, muitas vezes, mais nefasto e pernicioso do que para o suposto ofendido, eis que o afastamento do sigilo de dados para manifestações lícitas certamente virá acompanhado de uma série de consequências jurídicas, por exemplo, ações judiciais indenizatórias que possuem um efeito dissuasivo muito poderoso, na medida em que o medo de responsabilização faz calar o cidadão.

Diferentemente de pessoas com grande capacidade financeira, que tem ao seu dispor qualificados corpos de advocacia, o cidadão comum não tem, por via de regra, capacidade para bancar os custos de uma ação judicial, muito menos os honorários de um advogado. Essa, portanto, é apenas uma das razões pelas quais a inaplicabilidade do artigo 22 do Marco Civil da Internet seria mais nociva do que benéfica à sociedade, violando princípios constitucionais de maior significância à coletividade.

Apesar das peculiaridades sociais e jurídicas dos Estados Unidos da América e da Alemanha não se aplicarem literalmente ao ordenamento jurídico brasileiro no que tange ao "anonimato", o texto do artigo 22 da Lei 12.965/2014, em conjunto com a ponderação de outros princípios constitucionais, colocam o "anonimato legal" como a interpretação adequada à regra prevista pelo artigo 5º, IV, da Constituição Federal.

Com efeito, a despeito da Carta de 1988 vedar genericamente o anonimato para o exercício da livre manifestação de pensamento, não fazendo distinção entre a possibilidade de identificação do responsável por manifestações anônimas lícitas e ilícitas, as exigências do parágrafo único do artigo 22 da Lei 12.965/2014, oferecem a melhor interpretação ao artigo 5º, IV, da Constituição Federal, à luz de outros princípios constitucionais de grande relevância, como a privacidade e a liberdade de expressão, o que demonstra a compatibilidade entre o texto legal e constitucional.

O exercício à livre manifestação de pensamento anônimo, desde que materialmente lícito, é essencial, em muitos casos, para garantir a privacidade e a liberdade de crítica de seu responsável.

As quebras de sigilo telemático no processo penal e o paradoxo do acesso irrestrito às comunicações armazenadas

Carina Quito

Mestre em Direito Processual Penal pela Faculdade de Direito da Universidade de São Paulo. Advogada.

Sumário: 1. Generalidades. 2. Quebras de sigilo telemático: natureza jurídica e modalidades. 2.1. Interceptações telemáticas. 2.2. Acesso a comunicações telemáticas armazenadas. 2.3. Apreensão de conteúdos diversos da comunicação. 2.4. Acesso a metadados. 2.5. Acesso a dados cadastrais. 3. Interceptações telemáticas, quebras de sigilo de comunicações armazenadas e seus diferentes níveis de proteção normativa. 4. Afinal, qual sigilo protege o artigo 5º, XII, da CF?. 5. Proposições. 6. Conclusões.

1. Generalidades

O avanço da tecnologia modificou profundamente a forma como nos relacionamos com o mundo e em sociedade. Na sociedade da informação que se desenvolve desde o século XX, a tecnologia marca os mais variados aspectos da vida humana.

Ao uso de computadores domésticos a partir da década de 1980, somaram-se, na década seguinte, a expansão da internet para além das universidades e as comunicações telefônicas por meio de aparelhos celulares. Uma profusão dos *smartphones*, *notebooks* e *tablets* ocorreu em seguida, promovendo verdadeira revolução na forma como nos comunicamos e na forma como armazenamos informações privadas[1].

O uso massivo da tecnologia vem permitindo, recentemente, a coleta e a manutenção das mais variadas informações em dispositivos móveis, computadores e servidores, ampliando de forma significativa as possibilidades de vigilância sobre as atividades humanas.

Como o uso da tecnologia é generalizado nas sociedades modernas, a criminalidade também dele se vale. Assim, é possível dizer que nossos hábitos tecnológicos vêm modificando sensivelmente os mecanismos de investigação criminal e de busca de prova para fins processuais penais, pelo que a tecnologia e a internet estão, atualmente, no centro dos debates sobre o processo penal no Brasil[2], assim como em outros países do mundo.

1. Como refere Denise Provasi Vaz, Provas digitais no processo penal: formulação do conceito, definição das características e sistematização do procedimento probatório. Tese de doutorado apresentada à Faculdade de Direito da Universidade de São Paulo. São Paulo, 2012, p. 19, "os documentos anteriormente redigidos e arquivados em papel tornaram-se eletrônicos; as músicas foram transferidas do disco de vinil e fita cassete para o formato digital; as fotografias deixaram de ser registradas em filme para também assumirem o formato digital; do mesmo modo, a captação de imagens em vídeos; e ainda a comunicação por cartas, bilhetes, telegrama, telefone, foi transmudada em mensagens eletrônicas de texto, e-mails, sistemas VoIP, dentre outros."
2. Por exemplo, em março de 2019, o uso de meios de obtenção de prova digital foi amplamente noticiado e discutido no contexto da investigação do homicídio de Marielle Franco e Anderson Gomes. Em diversas entrevistas concedidas à imprensa, o Delegado de Polícia e as Promotoras de Justiça responsáveis pela investigação afirmaram a importâncias das quebras de sigilo telemático realizadas no âmbito do inquérito policial para se obter indícios de autoria suficientes à decretação das prisões cautelares e ao oferecimento de denúncia contra os suspeitos dos homicídios. A propósito, ver, por todos, <https://g1.globo.com/rj/rio-de-janeiro/noticia/2019/03/21/as-evidencias-para-prisao-dos-dois-suspeitos-de-matar-marielle-e-anderson.ghtml>. Acesso em 22.7.2019.

A despeito de todo o avanço tecnológico, muito pouco se evoluiu no país para a disciplina das provas digitais e dos meios de obtenção de prova em processo penal relacionados à tecnologia e à internet.

A Lei nº 9.296/1996 regulamentou o artigo 5º, XII, parte final, da CF para disciplinar as quebras de sigilo de comunicações telefônicas e telemáticas. Quase vinte anos depois, a Lei nº 12.965/2014 (Marco Civil da Internet) entrou em vigor, passando a tratar das quebras de sigilo de dados cadastrais dos usuários, dos registros de conexão à rede mundial de computadores e dos acessos às aplicações da internet[3], bem como das quebras de sigilo de comunicações armazenadas.

As disposições contidas nas citadas leis não são exaurientes. Ao lado delas, o art. 240 do CPP, que prevê as medidas de busca e apreensão (orginalmente voltadas à arrecadação de coisas que têm existência física), vem sendo aplicado e serve de fundamento para as quebras de sigilo de variados conteúdos armazenados em dispositivos móveis, computadores e servidores que são apreendidos, bem como para justificar o acesso remoto a dados armazenados nos servidores dos provedores de aplicações da internet.

Esse arcabouço normativo é claramente insuficiente, no entanto, para dar conta da complexidade das questões que surgem, no processo penal, a partir do uso crescente da tecnologia. O vazio normativo vem sendo preenchido pelas decisões judiciais tomadas por juízes singulares no âmbito de cada investigação criminal e pelos tribunais, em uma pequena parcela de casos que chegam a ser tratados em instâncias superiores.

Não há uniformidade no tratamento jurisprudencial dado ao tema, o que causa grande insegurança jurídica, além de uso excessivo e abusivo da vigilância estatal em detrimento da proteção à privacidade e ao sigilo das comunicações garantidos constitucionalmente.

À luz desse vazio normativo, faz-se necessário e urgente discutir quais os limites das quebras de sigilo ditas "telemáticas" diante dessas garantias constitucionais.

Neste trabalho, procura-se traçar um breve panorama sobre como são atualmente realizadas, no processo penal, as quebras de sigilo de informações digitais geradas e armazenadas pelo uso das aplicações da internet, distinguindo, para tanto, os diferentes tipos de dados que podem ter seus sigilos levantados.

3. Segundo define o art. 5º, VII, da Lei nº 12.965/2014, aplicações da internet são "o conjunto de funcionalidades que podem ser acessadas por meio de um terminal conectado à internet".

Busca-se analisar, em seguida, as quebras de sigilo de comunicações telemáticas, examinando-se, com especial ênfase, os diferentes níveis de proteção dispensados às comunicações em fluxo e às comunicações armazenadas pelos usuários da rede.

Ao final, são formuladas proposições para sanar o hoje existente descompasso no tratamento das comunicações contemporâneas e das comunicações armazenadas.

2. Quebras de sigilo telemático: natureza jurídica e modalidades

Como explica Ricardo Sidi[4], a palavra "telemática" tem origem na junção dos conceitos de informática e telecomunicação. Refere-se, portanto, às comunicações de dados[5], realizadas através da transmissão de sinais binários, em geral pela rede mundial de computadores[6].

Na prática das investigações criminais, o termo costuma ser utilizado de forma indiscriminada para designar toda informação que tem existência digital e que se gera e se armazena pelo uso da rede mundial de computadores.

Sob essa designação, portanto, são autorizadas judicialmente e executadas medidas diversas, que afastam sigilos protegidos tanto pela garantia constitucional geral à intimidade e à vida privada (artigo 5º, X) quanto o sigilo das comunicações, assegurado pelo artigo 5º, XII – é dizer, autorizam-se quebras para se afastar

4. A interceptação das comunicações telemáticas no processo penal. Belo Horizonte: D'Plácido, 2016, pp. 69-72. Nos termos do autor, "será telemática, portanto, em seu sentido jurídico, a comunicação que se realize de forma digital, ou seja, que se utilize da conversão em séries binárias, seja qual for a estrutura de que se utilize, desde que não se enquadre nas modalidades específicas telefônica e telegráfica".
5. Como explica Ricardo Sidi, A interceptação..., p. 70, mesmo as comunicações humanas, quando realizadas pela via telemática, consistem em comunicações de dados, porque o conteúdo humano é convertido em sinais binários, que trafegam na rede.
6. Augusto Eduardo de Souza Rossini, Informática, telemática e direito penal. São Paulo: Memória Jurídica, 2004, p. 160, observa que a telemática foi o que permitiu a comunicação de uma máquina com a outra, dando origem à chamada Era da Informação, que possui cinco pilares: (i) números são usados para representar todas as informações; (ii) os números são expressos em 0s e 1s; (iii) os computadores transformam a informação ao tratar aritmeticamente esses números; (iv) sistemas de comunicação movem os números e assim transportam a informação e (v) computadores e sistemas de comunicação se combinam para formar redes por onde trafegam os dados, sendo a mais conhecida a internet.

desde o sigilo de comunicações humanas em tráfego, até o sigilo de comunicações e outros conteúdos já armazenados em dispositivos móveis, computadores e em servidores, além de metadados e dados cadastrais.

A confusão terminológica decorre da ausência de definições legais precisas para cada modalidade de quebra e da falta de rigor no emprego de conceitos técnicos.

A despeito do uso indiscriminado do termo para designar coisas diferentes, qualquer que seja o objeto da quebra de sigilo telemático, ela terá a natureza jurídica de meio de obtenção de prova – isto é, instrumento para a investigação de provas, para a colheita de fontes de prova[7-8] – e constituirá, como regra, providência de índole cautelar, uma vez que a eficácia do meio depende do sigilo da medida até que seja executada[9].

Definida a natureza jurídica de meio de obtenção de prova, cumpre analisar as diferentes formas pelas quais vêm sendo atualmente executadas as quebras de sigilo telemático no processo penal.

2.1. Interceptações telemáticas

Por interceptação, entende-se a intromissão, por terceiros não autorizados, no fluxo de comunicações privadas entre duas ou mais pessoas, enquanto elas se realizam.[10] Ao interceptar, esses terceiros não apenas se intrometem de forma

7. Conforme ensina Gustavo Badaró, Processo penal, 5 ed. São Paulo: Revista dos Tribunais, 2017, p. 393, "meios de obtenção de provas, também denominados meios de investigação ou de pesquisa de provas, são instrumentos para a colheita de fontes ou elementos de prova." Segundo o autor, o único meio de obtenção de prova disciplinado pelo CPP é a busca e apreensão, existindo outros meios de obtenção de prova previstos em leis processuais penais especiais, entre eles as interceptações telemáticas, a interceptação ambiental, as quebras de sigilo bancário e fiscal e a infiltração de agentes em organizações criminosas.
8. Sobre as interceptações telemáticas, Ricardo Sidi, A interceptação..., p. 61 afirma que "é uma providência cautelar que constitui um meio de obtenção de prova, sendo o material coletado, via de regra, contido numa mídia, como cd, dvd ou *pendrive*, um meio de prova documental, que será inserido no processo".
9. Nas palavras de Gustavo Badaró, Processo..., p. 394, "justamente por isso, afirma-se que nestes casos o requerimento, a admissibilidade e a efetiva realização de tal meio devem ocorrer sem a ciência da parte investigada, sendo o resultado de tal operação submetido, posteriormente, ao contraditório diferido".
10. Conforme Antonio Scarance Fernandes, Processo penal constitucional, 6. ed. São Paulo: Revista dos Tribunais, 2010, p. 92, "a interceptação consiste na captação da

sub-reptícia no fluxo da comunicação, como o monitoram, para obter acesso ao conteúdo comunicado durante determinado período de tempo.

Conforme descreve Denise Provasi Vaz[11], a medida consiste na captação de dados que estejam em trânsito por uma rede de dispositivos eletrônicos, podendo recair sobre um determinado serviço, como o correio eletrônico, ou sobre a troca de dados a partir de um determinado endereço de IP, caso em que são coletadas todas as mensagens de correio eletrônico bem como as conversas mantidas por meio de comunicadores instantâneos, VoIP etc.

As interceptações telemáticas encontram-se previstas no art. 1°, parágrafo único, da Lei n° 9.296/1996, o qual dispõe que as previsões contidas naquele diploma legal quanto às interceptações telefônicas estendem-se às interceptações de comunicações telemáticas.

Diante da falta de clareza do art. 5°, XII, da CF[12] quanto aos limites da exceção ao sigilo das comunicações, a constitucionalidade do parágrafo único do art. 1° foi intensamente debatida nos anos que sucederam a entrada em vigor da Lei n° 9.296/1996.

Em torno do tema, desenvolveram-se, essencialmente, duas correntes doutrinárias.[13] De acordo com a primeira, estariam tratadas no texto constitucional quatro formas de comunicação (comunicação postal, comunicação telegráfica, comunicação de dados e comunicação telefônica), referindo-se a exceção constitucional ("salvo, no último caso") apenas às comunicações telefônicas, pelo que seriam absolutamente invioláveis as demais formas, entre as quais as comunicações de dados.[14]

---

conversa por um terceiro, sem o conhecimento dos interlocutores (interceptação em sentido estrito) ou com o conhecimento de um deles".

11. Provas..., p. 100.
12. "É inviolável o sigilo da correspondência, e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal".
13. Para uma análise histórica do art. 5°, XII, da CF, ver André Augusto Mendes Machado e André Pires de Andrade Khedi, Sigilo das comunicações e de dados. In: Antonio Scarance Fernandes, José Raul Gavião de Almeida e Maurício Zanoide de Moraes (coord.). Sigilo no processo penal: eficiência e garantismo. São Paulo: Revista dos Tribunais, 2008, pp. 239-266.
14. Nesse sentido posicionaram-se, por exemplo, Ada Pellegrini Grinover, Novas tendências do direito processual penal. Rio de Janeiro: Forense Universitária, 1990, pp. 78-80

Para a segunda corrente, o texto constitucional teria separado as formas de comunicação em dois blocos (comunicação postal e telegráfica, de um lado, e comunicação de dados e telefônica, de outro), de modo que a exceção constitucional seria aplicável ao último, ou seja, às comunicações de dados e telefônicas.[15]

Diante do inevitável avanço da tecnologia, a segunda corrente prevaleceu. Como observa Gustavo Badaró[16], uma interpretação realista da norma constitucional não poderia afastar a possibilidade de interceptação das comunicações telemáticas já que "não se pode considerar uma norma constitucional isolada de seu contexto histórico, social e político, mormente em temas que envolvem a evolução tecnológica".

Esse entendimento doutrinário foi refletido na jurisprudência[17], que se consolidou para admitir essa modalidade de interceptação sob o mesmo regime dos monitoramentos telefônicos. De 1996 para cá, as interceptações de comunicações telemáticas tiveram o seu uso alargado, sendo hoje tão ou mais frequentes do que as próprias interceptações telefônicas.

Os requisitos e a forma de execução desse meio de obtenção de prova encontram-se tratados na Lei n° 9.296/1996, daí por que se diz que as interceptações telemáticas correspondem a um meio de obtenção de prova típico.

---

e Vicente Greco Filho, Interceptação telefônica: (considerações sobre a Lei n. 9.296, de 24 de julho de 1996), 2. ed. São Paulo: Saraiva. 2005, pp. 13-19.

15. Nesse sentido, Tércio Sampaio Ferraz Jr., Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado. Revista da Faculdade de Direito da Universidade de São Paulo, vol. 88, 1993, pp. 439-459; Lenio Luiz Streck, As interceptações telefônicas e os direitos fundamentais: Constituição, cidadania, violência: a Lei 9.296/96 e seus reflexos penais e processuais penais. 2. ed. Porto Alegre: Livraria do Advogado, 2001, pp. 45-49; Antonio Scarance Fernandes, Processo..., p. 96 e Gustavo Badaró, Interceptação de comunicações telefônicas e telemáticas: limites ao avanço da tecnologia. Disponível em <http://www.badaroadvogados.com.br/?p=321>. Acesso em 16.04.2014.
16. Idem. Gustavo Badaró defende a constitucionalidade das interceptações telemáticas com ressalvas. Para o autor, que parte da leitura do art. 5°, XII, da CF proposta por Tércio Sampaio Ferraz Jr., as comunicações telemáticas apenas podem ser interceptadas se por algum motivo não puderem ser apreendidas uma vez que tenham sido armazenadas.
17. Observe-se que desde muito pouco tempo depois da entrada em vigor da Lei n° 9.296/1996, os tribunais passaram a se posicionar favoravelmente a essa modalidade de quebra de sigilo. A propósito, conferir STF, Tribunal Pleno, ADI MC 1.488/SC, rel. Min. Néri da Silveira, j. un. 07.11.1996, *DJ* 26.11.1999. No STJ, ver, por todos, RHC 25.268/DF, 6ª Turma, rel. Min. Vasco Della Giustina (Des. Convocado do TJRS), j. 27.03.2012, *DJe* 11.04.2012.

O art. 2º traça requisitos estritos[18] que traduzem em termos legais critérios de proporcionalidade[19], sem os quais não podem ser autorizadas as interceptações: (i) devem estar presentes indícios razoáveis de autoria ou participação em infração penal; (ii) deve haver demonstração da imprescindibilidade do meio para a obtenção da prova da infração penal, e (iii) o fato investigado deve constituir infração penal punida com reclusão.

O art. 3º, por sua vez, prevê legitimação ativa para requerer a medida às autoridades policiais e representantes do Ministério Público, fazendo referência, ainda, à possibilidade de os juízes determinarem a sua execução de ofício.

O art. 4º trata do conteúdo do requerimento (que pode ser escrito ou oral, em caso de extrema urgência, a teor do § 1º), prevendo que, de modo a atender os requisitos traçados no art. 2º, o pedido deverá conter a demonstração da necessidade do emprego do meio de obtenção de prova e a indicação dos meios a serem empregados.

Já o art. 5º dispõe que a decisão que autorizar a medida deverá ser fundamentada, sob pena de nulidade, indicando também a forma de execução da diligência, que não poderá exceder o prazo de quinze dias, renovável por igual tempo, uma vez demonstrada a indispensabilidade do meio de obtenção de prova.

Quanto ao prazo da medida, também muito já se discutiu acerca da constitucionalidade de prorrogações sucessivas, que ampliariam demasiadamente o período de quinze dias originalmente previsto na lei. Enquanto parte da doutrina posicionou-se por uma leitura restritiva do art. 5º, segundo a qual o limite temporal insuperável seria de trinta dias (correspondente, portanto, a dois períodos de quinze dias)[20], o entendimento majoritário e que prevaleceu na

18. Os requisitos são negativos. Diz o artigo 2º que as interceptações não serão autorizadas se não preenchidas as condições referidas nos incisos.

19. Conforme leciona Luís Roberto Barroso, Curso de direito constitucional contemporâneo, 8. ed. São Paulo: Saraiva, 2019, p. 512, a proporcionalidade, também referida na doutrina como princípio, máxima ou postulado, evoluiu como um mecanismo instrumental para aferir a legitimidade das restrições a direitos fundamentais em três etapas, nas quais se vai verificar: "(i) a adequação de uma medida para produzir determinado resultado (idoneidade do meio para realizar o fim visado), (ii) a necessidade da providência, sendo vedado o excesso (se houver meios menos gravosos para atingir o mesmo fim é ilegítimo o emprego do meio mais gravoso e (iii) a proporcionalidade em sentido estrito, pela qual se afere se o fim justifica o meio, vale dizer, se o que se ganha é mais valioso do que aquilo que se sacrifica".

20. A propósito, ver Geraldo Prado. Limite às interceptações telefônicas e a jurisprudência do Superior Tribunal de Justiça. 2. ed. Rio de Janeiro: Lumen Juris, 2006, p. 40 e André Augusto Mendes Machado e André Andrade Pires Khedi, Sigilo..., pp. 255-257.

jurisprudência é de que as renovações podem ocorrer por sucessivos períodos de quinze dias, sem limitação, desde que demonstrada a imprescindibilidade das extensões e desde que sejam devidamente fundamentadas as decisões que as autorizam[21].

Os artigos 8º[22] e 9º preveem, respectivamente, que as interceptações devem correr em autos apartados dos autos de investigação (ou da ação penal), preservando-se o sigilo das diligências e do conteúdo obtido, e que o material colhido que seja estranho ao objeto da persecução criminal deverá ser inutilizado, por decisão judicial, a requerimento do Ministério Público ou da parte interessada.

O artigo 10[23] – cuja redação foi recentemente alterada pela Lei nº 13.964/2019 – tipifica como crime (apenado com dois a quatro anos de reclusão e multa) realizar interceptações ou escutas ambientais, ou quebrar segredo de justiça, sem autorização judicial ou com objetivos não definidos em lei. O recém incluído parágrafo único desse artigo tipifica, por sua vez, a conduta do magistrado que ordena a execução de interceptação ou de escuta com objetivo não autorizado em lei, ficando o agente sujeito às mesmas penas do *caput*.

Embora o procedimento probatório esteja relativamente bem delineado na Lei nº 9.296/1996 no tocante às interceptações telefônicas, a lei não previu forma específica para a execução das interceptações telemáticas. Na prática, convencionou-se determinar aos provedores de *e-mails* (ou de outras aplicações de trocas de mensagens *on-line*) a criação de contas espelho[24] em que devem ser replicados,

21. O STJ consolidou esse entendimento, que se encontra refletido, por exemplo, nos seguintes precedentes: STJ, 5ª Turma, AgRg no REsp 1345926/ES, rel. Min. Jorge Mussi, j. un. 19.11.2015, *DJe* 25.11.2015; STJ, 5ª Turma, AgRg no REsp 1541305/SC, rel. Min. Reynaldo Soares da Fonseca, j. un. 02.05.2017, *DJe* 05.05.2017 e STJ, 5ª Turma, AgRg no AREsp 564035/SP, rel. Min. Jorge Mussi, j. un. 13.06.2017, *DJe* 30.06.2017. No STF, mesma orientação é refletida no seguinte precedente: STF, 1ª Turma, RHC 117467/SP, rel. min. Dias Toffoli, j. un. 05.11.2013, *DJe* 22.11.2013.

22. A Lei nº 13.964/2019 inseriu na Lei nº 9.296/1996 o artigo 8º-A, que tipifica meio de obtenção de prova diverso, qual seja, a captação ambiental de sinais eletromagnéticos, ópticos ou acústicos.

23. O texto da Lei nº 9.296/1996 conta agora com o artigo 10-A, também incluído pela Lei nº 13.964/2019, o qual tipifica a realização de captação ambiental (de sinais eletromagnéticos, ópticos ou acústicos) sem autorização judicial, quando exigida, prevendo pena de reclusão de dois a quatro e multa anos ao agente.

24. Helena Regina Lobo da Costa e Marcel Leonardi, Busca e apreensão e acesso remoto a dados em servidores, *Revista Brasileira de Ciências Criminais*, ano 19, n. 88, jan./fev. 2011, pp. 216-217, ao tratarem das quebras de sigilo de comunicações em servidores para divulgação de dados de terceiros, transcrevem ordem judicial em que se determina:

em tempo real[25], os fluxos de mensagens dos investigados, de modo que seus conteúdos possam ser acessados pelas autoridades encarregadas das investigações.

Cumpre anotar, contudo, que a criação de conta espelho não tem previsão na Lei nº 9.296/1996, nem mesmo na Resolução nº 59/2008 do Conselho Nacional de Justiça, que disciplina e uniformiza rotinas visando ao aperfeiçoamento do procedimento de interceptação de comunicações telefônicas e em sistemas de informática e telemática nos órgãos jurisdicionais do Poder Judiciário. Trata-se da forma convencional de se requisitar a execução da medida, que não exclui a possibilidade de se acessar o fluxo das comunicações por outros meios técnicos igualmente eficazes.

2.2. Acesso a comunicações telemáticas armazenadas

O acesso às comunicações telemáticas armazenadas não foi previsto na Lei nº 9.296/1996. Não obstante, o levantamento do sigilo de comunicações pretéritas tem sido uma constante em investigações criminais.

Como observam Jacqueline de Souza Abreu e Dennys Antonialli,[26] a legislação infraconstitucional trata o assunto em duas leis diferentes. Quando o acesso a essas comunicações depende de um intermediário (em geral os provedores de aplicações da internet que detêm os dados), incide o disposto no artigo 7º, III, do Marco Civil da Internet, o qual determina que o acesso ocorra mediante ordem judicial, sem, contudo, prever requisitos substantivos de padrão probatório. Quando o acesso se dá diretamente nos dispositivos móveis, computadores ou servidores fisicamente apreendidos, seu fundamento legal é o artigo 240 do CPP, que trata das medidas de busca e apreensão.

"(i) o desvio eletrônico de todo o conteúdo de dados telemáticos intercambiados com terceiros via internet, pelo prazo de quinze dias, a contar da efetiva implementação; (ii) os dados cadastrais do responsável pela conta; (iii) os IPs e terminais telefônicos utilizados para conexão pelo responsável pela conta; (iv) todas as pastas e arquivos e conteúdos da referida conta; (v) todos os *logs* de acesso à conta ou outros *logs* referentes à conta; (vi) informações de outra conta porventura existente em nome do mesmo usuário; (vii) criação de um e-mail espelho para o desvio do conteúdo do endereço eletrônico monitorado".

25. Ou o mais perto disso que se possa chegar. Como discorreremos em seguida, de um ponto de vista técnico, é praticamente impossível se precisar qual é de fato o momento do tráfego das comunicações digitais.

26. Vigilância sobre as comunicações no Brasil: interceptações e quebras de sigilo, infiltrações e seus limites constitucionais. São Paulo: InternetLab, 2017, p. 25.

Diferentemente do que ocorre em relação às quebras de sigilo de comunicações telemáticas em tráfego, as quebras de sigilo de comunicações já armazenadas encontram-se apenas nomeadas no Marco Civil da Internet, carecendo de disciplina específica.

Ao condicionar o acesso às mensagens armazenadas em servidores dos provedores de aplicações da internet apenas à existência de ordem judicial, sem qualquer outro requisito ou limite temporal, a Lei nº 12.965/2014 cria o paradoxo que será posteriormente tratado neste artigo: comunicações armazenadas – muitas vezes por anos a fio – acabam por receber, na prática das investigações criminais, menor grau de proteção do que as comunicações telemáticas em fluxo[27], cuja violação depende do preenchimento de requisitos previstos na Lei nº 9.296/1996, e se condiciona, em princípio, ao prazo exíguo de quinze dias.

Ainda que a Lei nº 12.956/2014 tenha deixado de instituir requisitos próprios para essas quebras, como toda a restrição a direito fundamental, o acesso ao conteúdo de comunicações armazenadas deveria ser pautado por critérios de proporcionalidade, isto é, pelos subprincípios da proporcionalidade[28], o que deixa de acontecer com frequência na prática.

2.3. Apreensão de conteúdos diversos da comunicação

Além de *e-mails* armazenados, sob a nomenclatura "quebra de sigilo telemático" são comumente afastados os sigilos de outros tipos de dados que repousem em dispositivos móveis, computadores ou servidores.

Trata-se de informações como listas de contatos, agendas de compromissos, fotos, arquivos de texto, vídeo e áudio, planilhas, dados de localização e de deslocamentos feitos pelos usuários, histórico de navegação, histórico de pesquisas, lista de aplicativos baixados, informações sobre compras *on-line*, entre outras – enfim, toda sorte de informações que possam ser armazenadas nos próprios dispositivos móveis dos alvos ou nos servidores de provedores de aplicações da internet.

27. A existência desse paradoxo foi constatada e abordada por Dennys Antonialli, Francisco Brito Cruz e Mariana Giorgetti Valente, Smartphones: baús de tesouro da Lava Jato. In: Jacqueline de Souza Abreu e Dennys Antonialli (eds.), Direitos fundamentais e processo penal na era digital: doutrina e prática em debate, vol. I. São Paulo: InternetLab, 2018, pp. 58-63.

28. Vide nota 19.

A não ser pelo acesso a dados de localização em determinadas circunstâncias bastante específicas, previstas no art. 13-B do CPP[29], o levantamento de sigilo desses dados não recebe disciplina específica, não tendo sido sequer nomeado no Marco Civil da Internet. Com efeito, o acesso é também realizado com fundamento no art. 240 e seguintes do CPP, que tratam das medidas de busca e apreensão.

Como o instituto concebido pelo CPP o foi para a apreensão de coisas que têm existência física, ele serve de fundamento para o acesso a esses dados quando armazenados em dispositivos móveis, computadores e servidores cuja apreensão física seja devidamente autorizada por decisão fundamentada e refletida em mandado judicial específico[30].

Já em relação aos dados a serem acessados remotamente nos servidores das empresas provedoras de aplicações da internet, as autoridades encarregadas das investigações e o Poder Judiciário costumam utilizar o art. 240 do CPP para fundamentar as ordens de quebra, ao argumento de que as informações constantes desses bancos de dados corresponderiam, em última análise, a documentos, sendo passíveis, portanto, de apreensão remota (ou imprópria).

Aqui, novamente, a ausência de disciplina específica faz que o afastamento de sigilo de tais dados, que são protegidos pela garantia geral do art. 5º, X, da CF, dependa, na prática, apenas de ordem judicial, qualquer que seja a finalidade de sua arrecadação e sem limite temporal.

É forço convir que, com a evolução da tecnologia, os *smartphones* são muito mais do que aparelhos utilizados para fazer chamadas telefônicas e enviar mensagens de texto. São computadores pessoais portáteis, verdadeiras extensões da

29. O artigo 13-B do CPP, introduzido ao estatuto processual em 2016 pela Lei nº 13.344/2016 prevê que, se necessário à prevenção e à repressão de crimes relacionados ao tráfego de pessoas, o membro do Ministério Público ou o delegado de polícia poderão requisitar, mediante autorização judicial, às empresas prestadoras do serviço de telecomunicações e/ou telemática que disponibilizem imediatamente os meios técnicos adequados – como sinais, informações e outros – que permitam a localização da vítima ou dos suspeitos do delito em curso. O dispositivo legal é, a nosso ver, inconstitucional, uma vez que permite restrição à garantia inscrita no art. 5º, X, independentemente de apreciação do Poder Judiciário.

30. Como observam Helena Regina Lobo da Costa e Marcel Leonardi, Busca..., pp. 207-209, o mandado de busca deve contar a indicação precisa do local da busca e a delimitação também precisa de seu objeto, não se admitindo interpretações ampliativas, tampouco ampliação do objeto do mandado durante sua execução.

personalidade, que possibilitam o armazenamento de dados que são um retrato muito íntimo e fiel de seus donos[31].

Embora esses dados não correspondam ao conteúdo humano de comunicações, é evidente que o levantamento de seus sigilos pode acarretar profunda vulneração à intimidade, pois tem aptidão para revelar todo tipo de preferências e hábitos. Não por outro motivo, o Poder Judiciário deve atuar com extrema cautela e observância estrita aos subprincípios da proporcionalidade em cada uma das quebras a serem decretadas, de modo a aferir, em cada caso, a efetiva adequação e necessidade do acesso aos dados (limitando-o ao mínimo necessário), e a existência de justa medida entre o grau de violação à privacidade e os objetivos de cada investigação individualmente considerada.

2.4. Acesso a metadados

O acesso a aplicações da internet gera registros de data, hora, local e *internet protocol* (IP). Essas informações são chamadas de metadados,[32] sendo tratadas no artigo 5º, VI e VIII, da Lei nº 12.965/2014.

O art. 5º, VI, define os chamados "registros de conexão" como conjunto de informações referentes à data e hora de início e término de uma conexão à internet, sua duração e o endereço de IP utilizado para o envio e recebimento do pacote de dados. Já o inciso VIII define os "registros de acesso", a eles se referindo como o conjunto de informações referentes à data e hora de uso de uma determinada aplicação da internet, a partir de um determinado número de IP.

31. Cf. Dennys Antonialli e Jacqueline de Souza Abreu, O conto do baú do tesouro: a expansão da vigilância pela evolução e popularização de celulares no Brasil. Disponível em <lavits.org/wp-content/uploads/2018/04/33-Jacquelie-de-Souza-Abreu-e-Dennys-Antonialli.pdf>. Acesso em 21.06.2019.

32. O conceito de metadados pode variar. Jacqueline de Souza Abreu e Dennys Antonialli, Vigilância..., p. 23, no relatório publicado pelo InternetLab em 2017, tratam como metadados "todos os dados e registros gerados a partir de uma comunicação e que não constituam o seu conteúdo em si, como, por exemplo, data, hora e duração da comunicação, remetente, destinatários, eventuais dados de localização geográfica do dispositivo (como Estação de Rádio Base), códigos de identificação de dispositivos (como IMEI), etc.". Já Ricardo Sidi, As interceptações..., p. 294, refere-se a tais dados como dados de tráfego, que englobam a identificação do remetente e do destinatário das mensagens, horário de envio, a locação dos interlocutores através de Estações de Rádio Base, a quantidade de *bytes* transmitidos, volume do áudio (em caso de transmissão de áudio), duração dos diálogos, IPs gerados e o custo da comunicação".

O art. 10 do Marco Civil da Internet dispõe que tanto a guarda quanto o acesso aos registos ali definidos devem atender à preservação da intimidade, da vida privada, da honra e da imagem das pessoas – em clara referência à garantia inscrita no art. 5º, X, da CF –, e estabelece aos provedores de conexão e de acesso a obrigação de manter esses registros pelo prazo de um ano e seis meses, respectivamente, ou por tempo superior, a pedido das autoridades policiais ou membros do Ministério Público, quando maior período for necessário à obtenção de ordem judicial para as correspondentes quebras de sigilo.

Sendo esses dados indissociáveis de comunicações e de outras atividades concretas dos usuários na rede, considera-se que os metadados integram a intimidade, ficando o afastamento de seus sigilos condicionado à cláusula de reserva de jurisdição, como consignado expressamente no texto legal (art. 13, § 5º e art. 15, § 3º).

O Marco Civil da Internet, em seu art. 22, parágrafo único, cuidou de estabelecer requisitos para que a parte interessada peça ao Poder Judiciário o afastamento do sigilo de registros de conexão e de acesso para formar conjunto probatório, seja em processo judicial cível ou criminal. Logo, esses requerimentos devem conter (i) fundados indícios da ocorrência do ilícito; (ii) justificativa motivada da utilidade dos registros solicitados para fins de investigação ou instrução probatória e (iii) identificação do período ao qual se referem.

Ainda que não tão rigorosos quanto aqueles traçados na Lei nº 9.296/1996, os requisitos do art. 22 também refletem no texto legal critérios de proporcionalidade (necessidade, adequação e equilíbrio entre a restrição e o fim a que se destina) para a mitigação da garantia constitucional à intimidade e à vida privada.

2.5. Acesso a dados cadastrais

A exemplo dos registros de conexão e de acesso a aplicações da internet, a Lei nº 12.965/2014, em seu art. 10, previu que o acesso aos dados cadastrais dos usuários da rede deve observar, como regra, a garantia inscrita no artigo 5º, X, da CF.

O Decreto nº 8.771/2016 (Regulamento do Marco Civil da Internet) definiu, no art. 11, § 2º, I a III, os elementos que integram o conceito de dados cadastrais, sendo eles a filiação; o endereço e a qualificação pessoal do usuário – esta entendida como nome, prenome, estado civil e profissão. Já o § 1º do art. 11 dispensou os provedores que não coletam esses dados de fornecê-los às autoridades, desde que informem tal circunstância a quem faz a requisição.

Muita controvérsia existe acerca da possibilidade de acesso direito a esses dados por autoridades policiais e membros do Ministério Público independentemente de ordem judicial prévia.

O art. 10, *caput*, do Marco Civil da Internet previu que a disponibilização de dados pessoais deve atender à preservação da intimidade, da vida privada, da honra e da imagem das pessoas. Trata-se essa da regra, excepcionada pelo § 3º, segundo o qual o disposto no *caput* não impede o acesso a dados cadastrais, pelas autoridades administrativas que detenham competência legal para a sua requisição. No mesmo sentido, o artigo 11 do Decreto nº 8.771/2016 dispõe que as autoridades administrativas a que se refere o artigo 10, § 3º, da Lei nº 12.965/2014 indicarão o fundamento legal de competência expressa para o acesso direito aos dados cadastrais.

A nosso ver, a cláusula de reserva de jurisdição deverá ser a regra para a disponibilização desses dados, e o acesso direito excepcional, autorizado apenas nas hipóteses taxativamente previstas em lei para a investigação de determinados crimes que, por sua gravidade, justificam maior grau de eficiência na persecução em detrimento da garantia constitucional.

As exceções legais estão previstas no art. 17-B da Lei nº 9.613/1998 (incluído pela Lei nº 12.683/2012), que dispõe sobre os crimes de lavagem de dinheiro; no art. 15 da Lei nº 12.850/2013, que dispõe sobre os crimes praticados por organizações criminosas, e no art. 13-A do CPP, que cuida da requisição de dados cadastrais na investigação dos crimes tipificados nos arts. 148, 149 e 149-A, 158, § 3º e 159 do CP e no art. 239 do Estatuto da Criança e do Adolescente[33].

Tratando-se de previsões excepcionais, entendemos que, à luz da garantia inscrita no artigo 5º, X, da CF, tais leis devem ser lidas restritivamente, limitando-se o acesso direito a dados cadastrais à investigação dos crimes tratados nesses diplomas legais[34].

---

33. Os artigos 13-A e 13-B, como anteriormente referido, foram incluídos no CPP pela Lei nº 13.344/2016, que buscou conferir às investigações criminais maior eficiência quando apurados os crimes de sequestro e cárcere privado; redução a condição análoga à de escravo; tráfico de pessoas e extorsão mediante sequestro – crimes mais graves e cuja característica comum é a restrição permanente à liberdade de locomoção das vítimas.

34. Jacqueline de Souza Abreu e Dennys Antonialli, Vigilância... cit., pp. 33-34 destacam que as normas que previram a desnecessidade de ordem judicial para o acesso a dados cadastrais são fruto de recentes reformas legislativas que atendem a pressões das autoridades administrativas para ter acesso direto aos dados, visando ao aumento da eficácia dos procedimentos investigativos, sobretudo em termos de rapidez. Ressaltam os autores que, antes mesmo das modificações legislativas, essas autoridades administrativas já defendiam o acesso direto aos dados cadastrais, ao argumento de que tais informações não receberiam a proteção constitucional do artigo 5º, X ou XII. Sob

3. Interceptações telemáticas, quebras de sigilo de comunicações armazenadas e seus diferentes níveis de proteção normativa

Como se pode perceber a partir do panorama anteriormente traçado, os mecanismos de quebra de sigilo telemático distinguem-se em função da natureza das informações cujo sigilo é afastado, o que acarreta limitação a diferentes garantias constitucionais, em maior ou menor grau.

Caso utilizássemos uma escala decrescente para medir o nível de limitação às garantias constitucionais alcançado por cada modalidade de quebra, partiríamos, necessariamente, das interceptações telemáticas e quebras de sigilo de comunicações armazenadas – que, a nosso ver, encontram-se no mesmo patamar, conforme discorreremos a seguir –, passando, sucessivamente, pelas apreensões de conteúdos armazenados diversos do conteúdo humano de comunicações – as quais, a depender da natureza e da quantidade de informações obtidas, podem, de certa forma, equiparar-se às primeiras – , pelo acesso aos metadados e, finalmente, pelas quebras de dados cadastrais[35].

Se o artigo 5º, X, da CF enuncia uma cláusula geral de proteção à intimidade e à vida privada, o inciso XII, a seu turno, contém proteção adicional: tutela-se, ali, além da intimidade, a liberdade de manifestação de pensamento, daí por que as comunicações telemáticas situar-se-iam no início da escala anteriormente mencionada.

Como analisamos no item 2.1., ao longo dos anos que seguiram a promulgação do texto constitucional em 1988, calorosos debates ocorreram em torno do alcance da garantia ao sigilo das comunicações e da constitucionalidade das interceptações telemáticas.

O entendimento que prevaleceu na doutrina, assim como na jurisprudência, tem origem na interpretação conferida ao art. 5º, XII, da CF, em artigo

a mesma lógica, autoridades administrativas pretendem ampliar a possibilidade de acesso direto aos dados cadastrais para quaisquer investigações. O assunto ainda não foi enfrentado de forma definitiva pelos tribunais brasileiros, conquanto se observe na jurisprudência certa tendência à flexibilização da garantia constitucional nesse tema.

35. Nesse mesmo sentido, Ricardo Sidi, As interceptações..., p. 295, tratando das interceptações telemática, igualmente estabelece uma diferenciação entre grupos de dados que, de acordo com o conceito de *expectation of privacy* do direito norte-americano, são merecedores de diferentes níveis de proteção. Segundo o autor, o primeiro e mais caro indivíduo, logo o destinatário de maior *expectation of privacy*, será o conteúdo humano das comunicações. Logo abaixo dele virão os dados de tráfego e, no último nível, estão alocados os dados cadastrais.

publicado no ano de 1993 por Tércio Sampaio Ferraz Jr.[36]. Naquele trabalho, o autor defendeu que o sigilo das comunicações assegurado constitucionalmente não recai sobre o conteúdo comunicado, mas sobre o fluxo da comunicação, garantindo a liberdade de comunicação sem a intervenção de terceiros:

> "(...) O que fere a liberdade de omitir pensamento é, pois, entrar na *comunicação* alheia, fazendo com que o que devia ficar entre sujeitos que se comunicam privadamente passe ilegitimamente ao domínio de um terceiro. (...)
>
> A distinção é decisiva: o objeto protegido no direito à inviolabilidade do sigilo não são os dados em si, mas a sua comunicação restringida (liberdade de negação). A troca de informações (comunicação) *privativa* é que não pode ser violada por sujeito estranho à comunicação."[37-38]

Embora tenha considerado que o art. 5º, XII, da CF distinguiu dois blocos – de um lado as comunicações por carta e telegrama e, de outro, as comunicações de dados e telefônicas –, e que a exceção constitucional estaria relacionada ao último, Tércio Sampaio Ferraz Jr. concluiu que: (i) os fluxos de comunicação são sempre invioláveis, conquanto possam ser apreendidos os resultado das comunicações já realizadas e (ii) a exceção à regra de inviolabilidade do fluxo, prevista na parte final do artigo 5º, XII, diz respeito unicamente às comunicações telefônicas, as quais, por sua natureza, não deixam registros.

A instantaneidade dos contatos telefônicos justificaria, portanto, a intervenção do Estado no próprio processo de comunicação para desviar fluxos e copiá-los, viabilizando a colheita de provas para as investigações e processos criminais.

36. Sigilo..., pp. 439-459.

37. Sigilo..., p. 447.

38. Esse entendimento doutrinário vem sendo refletido há anos na jurisprudência dos tribunais brasileiros. No julgamento do RE 418.416/SC, pelo STF, o relator, Ministro Sepúlveda Pertence, valeu-se do trabalho de Tércio Sampaio Ferraz Jr. para assentar a premissa de que a Constituição protege a comunicação (fluxo) de dados e não os dados em si, razão pela qual não se poderia considerar ilegal a apreensão de dados digitais em base física na qual se encontravam os dados armazenados. Mais de dez anos depois, em 2016, o STJ, no âmbito da Operação Lava Jato, com base nessa mesma premissa (já antes utilizada em outros julgamentos) declarou serem perfeitamente legais as quebras de sigilo de comunicações pretéritas armazenadas em dispositivo móvel apreendido com um dos réus, porque as mensagens já armazenadas estariam excluídas do âmbito de proteção do art. 5º, XII, da CF (STJ, 5ª Turma, RHC 75.800/PR, rel. Min. FElix Fischer, j. un. 15.09.2016, *DJe* 26.09.2016).

Ao reconhecerem a constitucionalidade do artigo 1º, parágrafo único, da Lei nº 9.296/1996, os tribunais brasileiros passaram a admitir, para fins penais, a intromissão de agentes do Estado também no fluxo de comunicações telemáticas, condicionando esse meio de obtenção de prova aos mesmos requisitos das interceptações telefônicas – por sua vez pautados em critérios de proporcionalidade (adequação, necessidade de proporcionalidade em sentido estrito)[39] – *e à limitação temporal de quinze dias, ainda que tal prazo seja prorrogável por decisão motivada que demonstre a necessidade de se estender a medida.*

Como visto, no cotidiano das investigações criminais as quebras de sigilo de comunicações telemáticas não se restringem ao monitoramento futuro do fluxo de mensagens, recaindo, frequentemente, sobre o conteúdo de comunicações armazenado nas contas dos usuários investigados, não raro sobre todo o conteúdo das caixas de mensagens, o que pode equivaler a anos de conversas arquivadas, mas resguardadas do conhecimento de terceiros[40].

Como observa Ricardo Sidi[41], os provedores de e-mail servem-se, na atualidade, de tecnologia *imap* (*internet message access protocol*), que permite aos usuários manter com as empresas a totalidade de seus *e-mails* (enviados, recebidos e rascunhos) para acessá-los de qualquer lugar e de qualquer dispositivo. Por conta das características dessa tecnologia, na prática, a totalidade das mensagens pode corresponder a muitos anos, quiçá décadas de mensagens trocadas, que acabam tendo seus sigilos levantados.

39. Como observam Ana Paula Oliveira Ávila e André Luis Woloszyn, A tutela jurídica da privacidade e do sigilo na era digital: doutrina, legislação e jurisprudência. Revista de Investigações Constitucionais, vol. 4., n.3, Curitiba, set./dez, 2017. Disponível em <http://dx.doi.org/10.5380/rinc.v4i3.51295>. Acesso em 07.07.2019., "a regulação da matéria opta, claramente, por um critério de proporcionalidade na utilização do meio (escuta telefônica) restritivo da privacidade do indivíduo, à medida que implica o emprego excepcional da escuta, i.e., somente para crimes mais graves, assim considerados aqueles punidos com pena de reclusão, e somente quando outros meios não forem suficientes para a prova da autoria ou participação em atividade criminosa. Não poderia ser de outro modo: tratando-se a privacidade e o correlato sigilo das comunicações telefônicas de um direito fundamental, sua restrição deve operar-se na estrita medida necessária (princípio da proibição de excesso) e de modo adequado, necessário e proporcional em sentido estrito (princípio da proporcionalidade)".

40. Por exemplo, Ricardo Sidi, As interceptações..., p. 303, dá notícia de decisão judicial proferida no âmbito da Operação Lava Jato (autos nº 5049597-93.2013.4047000/PR, de 26.11.2013) obrigando a Microsoft do Brasil a franquear acesso à integralidade das mensagens armazenadas nas contas e *e-mail* dos investigados.

41. As interceptações..., p. 302.

Por mais que a observância aos subprincípios da proporcionalidade fosse de rigor na tomada de qualquer decisão que importe restrição a direitos fundamentais, constata-se, na prática, uma tendência à flexibilização do acesso às comunicações armazenadas sob a justificativa de que, no texto da lei, não há maiores restrições a essa modalidade de quebra. Não há dúvida de que medidas desse tipo acarretam profunda violação ao sigilo das comunicações e à intimidade, afrontando claramente o postulado da proporcionalidade.

A ausência de limitação temporal na Lei nº 12.965/2014 é causa de evidente excesso no meio empregado (quebra de sigilo telemático) para a consecução do fim (investigação de fato determinado e limitado no tempo). Esse excesso já foi declarado pelo STJ, no julgamento do HC nº 315.220/RS[42], em setembro de 2015, quando a 6ª Turma discutiu a legalidade de quebra de sigilo de *e-mails* armazenados no período compreendido entre 2004 e 2014, por indivíduo investigado na Operação Revelação.

A relatora, Ministra Maria Thereza de Assis Moura, considerou que não haveria proporcionalidade, pois não demonstrada a imprescindibilidade da quebra de sigilo das mensagens de correio eletrônico pelo exorbitante período de dez anos. Embora não unânime o julgamento[43], o STJ acabou por conceder a ordem para anular a prova colhida.

Mas a assimetria entre as interceptações telemáticas e as quebras de sigilo de comunicações armazenadas vai além da questão atinente ao limite temporal anteriormente tratado, tocando o próprio fim almejado pela medida.

Ao estabelecer que a exceção ao sigilo das comunicações servirá única e exclusivamente à persecução criminal, o art. 5º, XII, da CF observou critério de proporcionalidade em sentido estrito, reforçado pelo art. 2º, III, da Lei nº. 9.296/1996, no qual se previu que apenas a persecução de crimes objetivamente considerados mais graves pelo legislador (os crimes punidos com "reclusão"[44-45]) justificaria a restrição excepcional ao sigilo.

42. STJ, 6ª Turma, HC 315.220/RS, rel. Min. Maria Thereza de Assis Moura, j. m.v. 15.09.2015, *DJe* 09.10.2015.

43. O revisor, Ministro Rogério Schietti Cruz, negava a ordem baseando-se na mesma ideia de que as restrições postas no art. 2º da Lei nº 9.296/1996 aplicam-se exclusivamente à intromissão no fluxo da comunicação.

44. Como observa Luiz Regis Prado, Curso de direito penal brasileiro, vol. I, 15. ed. São Paulo: Revista dos Tribunais, 2017, p. 351, não existe distinção ontológica entre as modalidades de pena privativa de liberdade, de modo que "a diferença entre reclusão e detenção é meramente quantitativa, fundada basicamente na maior gravidade da primeira".

45. Antonio Scarance Fernandes, Processo..., p. 97, pondera que a limitação imposta pelo art. 2º, III quanto à natureza do crime objeto de persecução criminal é falha. Isso

A redação do Marco Civil da Internet, por sua vagueza, acaba por permitir que extensos registros de comunicação passada sejam vasculhados para instruir investigações e processos de crimes punidos com detenção – logo reputados menos graves –, muitos dos quais sequer justificariam a propositura de ações penais, porque suscetíveis de transação penal ou de suspensão condicional processo.[46] Do mesmo modo, permite que extensos períodos de comunicações passadas sejam acessados para a instrução de processos cíveis, o que é de todo incompatível com a finalidade antevista no art. 5º, XII, da CF.

Enfim, o tratamento legal dispensado ao acesso às comunicações armazenadas na Lei nº 12.965/2014 cria o seguinte paradoxo: enquanto em tráfego, as mensagens trocadas são protegidas com rigor; no instante seguinte ao seu armazenamento – momento esse que sequer pode ser precisado[47] –, o rigor desaparece, viabilizando acesso praticamente irrestrito aos registros de conteúdos comunicados, desde que haja, para tanto, autorização judicial.

4. Afinal, qual sigilo protege o artigo 5º, XII, da CF?

A evolução da tecnologia e de novas formas de comunicação impõe urgente reexame das premissas em que foi assentada a interpretação do art. 5º, XII, da

porque, se há certo exagero em se admitir interceptações para todos os crimes de reclusão, por outro lado a investigação de crimes de injúria e ameaça praticados por meios eletrônicos pode depender de interceptações telemáticas para viabilizar a formação do conjunto probatório. Assim, argumenta o autor que o melhor seria que a lei tivesse criado um rol taxativo de crimes para os quais as interceptações seriam permitidas, a exemplo do que se fez no Projeto Miro Teixeira. No mesmo sentido argumentam André Augusto Mendes Machado e André Pires de Andrade Khedi, Sigilo..., p. 253. Concordamos com Antonio Scarance Fernandes acerca da necessidade de um rol taxativo de crimes, mas discordamos de que crimes de menor potencial ofensivo possam compor esse rol. Entendemos que a apuração desses crimes, por mais que mereçam ser investigados, não se encontra em razoável proporção com a devassa de comunicações privadas que pode decorrer das medidas de interceptação.

46. É o que se verifica em relação à persecução dos crimes contra a honra (calúnia, difamação e injúria), reputados de menor potencial ofensivo (art. 61 da Lei nº 9.099/1995), que afetam bens personalíssimos e que seriam passíveis de transação penal (art. 76 da Lei nº 9.0995/1995) porque recebem pena máxima inferior a dois anos.

47. Ricardo Sidi, As interceptações..., p. 301, esclarece que, do ponto de vista tecnológico, nem mesmo seria possível distinguir as mensagens em trânsito daquelas armazenadas, dado que o armazenamento é um estágio obrigatório da transmissão de *e-mails*, que são armazenados em diversos computadores entre o momento em que o remetente escreve a mensagem e o destinatário a lê.

CF, a fim de se harmonizar o tratamento dado aos diferentes métodos de quebra de sigilo de comunicações telemáticas.

O entendimento que até hoje prevalece quanto ao âmbito de proteção da garantia do sigilo das comunicações é produto de interpretação do texto constitucional indissociável de um momento histórico em que as comunicações eram essencialmente telefônicas e a internet sequer tinha ainda uso doméstico.

No ano de 2017, o tema foi revisitado por Tércio Sampaio Ferraz Jr. durante o "I Congresso de Direitos Fundamentais e Processo Penal na Era Digital", promovido pelo InternetLab com o apoio institucional da Faculdade de Direito da Universidade de São Paulo[48]. Na ocasião, ao discorrer novamente sobre as noções de fluxo da comunicação e resultado da comunicação, o autor observou que a dificuldade hoje existente, no mundo digital, está em lidar separadamente com as noções de fluxo e resultado da comunicação, como se fossem coisas totalmente distintas e dissociadas. Isso porque, segundo o autor, a armazenagem no mundo virtual, ao contrário do mundo físico, não é diferente do próprio fluxo.

Juliano Maranhão, em palestra proferida no mesmo Congresso[49], também analisou a garantia inscrita no art. 5º, XII, da CF à luz do avanço da tecnologia. Afirmando que o objeto de proteção constitucional é a liberdade de pensamento – isto é, a liberdade que tem cada indivíduo de se expressar sem receio de que seu pensamento venha a ser conhecido por um terceiro estranho à comunicação –, o autor conclui que o importante não seria propriamente o tempo da transmissão da comunicação, mas a espontaneidade em comunicar-se, o que dificulta a separação das noções de fluxo e resultado da comunicação anteriormente proposta.

De fato, como observa Ricardo Sidi[50], não há como se transpor a distinção entre fluxo e resultado – que sequer é mencionada no texto constitucional – ao tempo presente, em que as comunicações eletrônicas passam por diversos estágios de armazenamento entre o envio pelo remetente e seu recebimento pelo destinatário. Para o autor, o objeto de proteção do art. 5º, XII, da CF é o conteúdo das comunicações, sem distinção entre comunicações contemporâneas e

48. Sigilo de dados, o direito à privacidade e os limites do poder do Estados: 25 anos depois. In: Jacqueline de Souza Abreu e Dennys Antonialli (eds.), Direitos..., pp. 20-40.

49. O que é dado não é comunicado? In: Jacqueline de Souza Abreu e Dennys Antonialli (eds.), Direitos..., pp. 44-55.

50. As interceptações..., p. 302.

armazenadas, afinal, a preservação de seu conteúdo humano e demais detalhes não pode ser dissociada do sigilo[51].

Concordamos integralmente com Juliano Maranhão e Ricardo Sidi. Para além da questão tecnológica que inviabiliza a delimitação precisa do momento em que a comunicação telemática está de fato em fluxo, entendemos que o exame sobre o objeto de proteção do art. 5º, XII, da CF passa pelo questionamento sobre a finalidade do sigilo, que é manter algo em segredo[52]. E o que se quer manter em segredo, resguardado do conhecimento de terceiros, é, naturalmente, o conteúdo comunicado. Sem isso o sigilo não teria qualquer razão de ser.

Se a Constituição busca resguardar, além da intimidade, a liberdade de se dizer aquilo que se pensa sem que pessoas não autorizadas tomem conhecimento do que foi dito, será forçoso convir que o conteúdo das comunicações, esteja ele já comunicado ou armazenado na esfera íntima de seu titular, é o objeto da garantia constitucional.

Em síntese, a limitação da proteção constitucional ao fluxo, além de anacrônica (pois ignora o avanço da tecnologia e a realidade sensível), amplia demasiadamente a vigilância do Estado sobre as comunicações, contrariando toda a sistemática de proteção aos direitos fundamentais. A adequada proteção do sigilo de que trata o art. 5º, XII dependerá, portanto, de se alterar gradativamente as posições doutrinárias e a orientação da jurisprudência para se reconhecer que o conteúdo humano comunicado é o que se deve manter sob segredo para se assegurar a espontaneidade das comunicações entre pessoas.

5. Proposições

Como demonstrado, qualquer tentativa de se harmonizar o tratamento dispensado às comunicações telemáticas em fluxo e àquelas armazenadas dependerá do reconhecimento de que toda e qualquer forma de comunicação telemática insere-se no âmbito de proteção constitucional do artigo 5º, XII.

A fim de se alcançar segurança jurídica, qualquer tentativa de se uniformizar esse tratamento passará necessariamente, também, pela promoção de alterações legislativas visando instituir, seja no Marco Civil da Internet, seja em outro

51. As interceptações..., p. 300.

52. André Augusto Mendes Machado e André Pires Andrade Khedi, Sigilo..., p. 240, em alusão a Tércio Sampaio Ferraz Jr., distinguem segredo e sigilo, anotando que segredo é o conteúdo estrutural do direito, aquilo que se quer proteger, ao passo que o sigilo diz respeito à faculdade de agir que protege o segredo.

diploma legal, uma disciplina própria das quebras de sigilo de comunicações armazenadas, semelhante ao regime das interceptações de comunicações telemáticas.

Para que haja observância ao sigilo das comunicações tal como disposto no art. 5º, XII, da CF a nova regulamentação deverá prever, em primeiro lugar, que as quebras de sigilo de comunicações armazenadas terão finalidade processual penal e dependerão da existência de indícios razoáveis de autoria ou participação no crime investigado.

Deverá condicionar, ainda, as quebras de sigilo de comunicações telemáticas pretéritas à demonstração da indispensabilidade do meio de obtenção de prova, limitando o acesso das autoridades estatais à menor quantidade de dados possível. Para tanto, a lei poderá condicionar as quebras de sigilo de comunicações armazenadas à adequada delimitação temporal dos fatos investigados pelas autoridades encarregadas das apurações, a fim de balizar os magistrados quanto à pertinência do período que deverá ser o objeto de quebra.

De igual modo, seria de todo recomendável que se estabelecesse no texto legal um intervalo de tempo máximo a ser observado em cada autorização judicial de quebra (por exemplo, os trinta dias anteriores à data do fato investigado), passível de ampliação, a requerimento da parte interessada, mediante comprovação da necessidade de se abranger período maior.

A fim de evitar que o meio empregado seja excessivo, seria de rigor que as ampliações dos intervalos de quebras fossem autorizadas uma a uma, mediante decisões devidamente justificadas.

Para assegurar, por fim, o equilíbrio entre o meio empregado (quebra de sigilo de comunicações armazenadas) e o fim almejado (investigação criminal), entende-se que a lei deveria estabelecer critério objetivo de proporcionalidade estrita, tal como o fez a Lei nº 9.296/1996. Diferentemente do que se previu naquela lei, contudo, entendemos que a nova regulamentação poderia contar com um rol taxativo de crimes, a exemplo do que sugeria o Anteprojeto apresentado em 2003 pela comissão composta por Ada Pellegrini Grinover, Antônio Carlos de Castro, Antonio Magalhães Gomes Filho, Antonio Scarance Fernandes e Luiz Guilherme Vieira, de uma nova lei de interceptações telefônicas[53].

53. Cf. André Augusto Mendes Machado e André Pires Andrade Khedi, Sigilo..., pp. 250-254. Segundo os autores, o Anteprojeto previu o seguinte rol: (i) tráfico de substâncias entorpecentes e drogas afins; (ii) tráfico de seres humanos e subtração de incapazes; (iii) tráfico de armas, munições e explosivos; (iv) tráfico de espécimes da fauna silvestre; (v) lavagem de dinheiro; (vi) crimes contra o sistema financeiro nacional; (vii)

A propósito, concordamos com a observação feita por Antonio Scarance Fernandes[54] de que a distinção hoje existente na Lei nº 9.296/1996 dá margem a distorções. Exemplo disso são os crimes previstos na Lei nº 8.666/1993, que, sendo apenados com detenção, não autorizam a interceptação de comunicações telefônicas ou telemáticas.

Uma alternativa à construção de um rol taxativo de crimes seria a indicação de um critério objetivo de pena, que observasse o limite máximo de pena abstratamente cominada ao delito investigado, a justificar a medida.

Mesmo que não sobrevenha uma disciplina própria, ou até que isso aconteça, os próprios requisitos negativos estabelecidos no art. 2º, I a III, da Lei nº 9.296/1996 devem ser observados também nas quebras de sigilo de comunicações telemáticas armazenadas. Afinal, como concluímos anteriormente, o objeto da proteção constitucional deve ser considerado único: o conteúdo da comunicação humana que se quer preservar.

Porquanto os requisitos contidos no art. 2º correspondem a critérios de proporcionalidade para o monitoramento futuro de comunicações, esses mesmos critérios devem ser observados para o acesso às comunicações armazenadas, assim como deve ser observado o prazo estabelecido no art. 5º, ainda que se considere viável ampliá-lo, justificadamente, conforme vêm admitindo os tribunais brasileiros para o monitoramento de comunicações contemporâneas.

6. Conclusões

1. O avanço da tecnologia modificou a forma como nos comunicamos e armazenamos dados pessoais. Essa modificação traz reflexos para o processo penal, que cada vez mais se vale de meios de obtenção de provas digitais para a investigação de crimes e posterior formação de conjunto probatório em processo judicial.

2. A legislação processual não acompanhou o avanço tecnológico, tendo sido o vazio legislativo suprido por decisões judiciais que não são uniformes,

crimes contra a ordem econômica e tributária; (viii) crimes contra a administração pública; (ix) falsificação de moeda ou a ela assimilados; (x) roubo, extorsão simples, extorsão mediante sequestro, sequestro e cárcere privado; (xi) homicídio doloso; (xii) ameaça quando cometida por telefone; (xiii) crimes praticados por organizações criminosas e (xiv) decorrentes de ações de terrorismo.

54. Processo..., p. 97.

tampouco restritivas, acarretando exacerbado nível de vigilância estatal sobre as atividades humanas em rede.

3. Quebra de sigilo telemático é expressão utilizada para designar, na prática das investigações criminais, meios de obtenção de prova que têm por objeto o levantamento de sigilo de informações de diferentes espécies. Dada a natureza dessas informações, cada modalidade de quebra de sigilo importa restrição a diferentes garantias fundamentais, em diferentes níveis.

4. As modalidades de quebra de sigilo telemático atualmente em uso no processo penal são: interceptações telemáticas; quebras de sigilo de comunicações armazenadas; apreensão de conteúdos diversos das comunicações humanas; acesso a metadados, e acesso a dados cadastrais.

5. Em uma escala, as comunicações telemáticas receberiam maior nível de proteção constitucional em relação às demais formas de quebra de sigilo de dados, em virtude da proteção constitucional diferenciada prevista no art. 5º, XII, que resguarda a intimidade e a liberdade de expressão do pensamento.

6. Embora a doutrina e a jurisprudência tenham consolidado o entendimento de que ao art. 5º, XII, da CF protege o fluxo das comunicações e não o conteúdo comunicado, tal entendimento não se sustenta diante do avanço da tecnologia, conduzindo a um descompasso no tratamento dado às comunicações em fluxo e às comunicações armazenadas, que acabam sendo menos protegidas.

7. O segredo protegido pelo sigilo constitucional é o conteúdo próprio de comunicações humanas, sem distinção entre as comunicações em fluxo e armazenadas, não se justificando o sigilo se não para manter resguardado de terceiros o próprio conteúdo comunicado.

8. Para se alcançar segurança jurídica e uniformidade no tratamento dispensado às diferentes formas e momentos de acesso às comunicações telemáticas, seria necessário que a lei traçasse disciplina própria para as quebras de sigilo de comunicações telemáticas armazenadas, que são atualmente apenas referidas no Marco Civil da Internet.

9. Essa disciplina não deve destoar do regime jurídico das interceptações telemáticas.

10. Caso essa nova disciplina não sobrevenha, ou até que venha a existir, devem ser aplicadas às quebras de sigilo de comunicações telemáticas armazenadas as previsões da Lei nº 9.296/1996, quanto aos requisitos das quebras e prazo da medida.