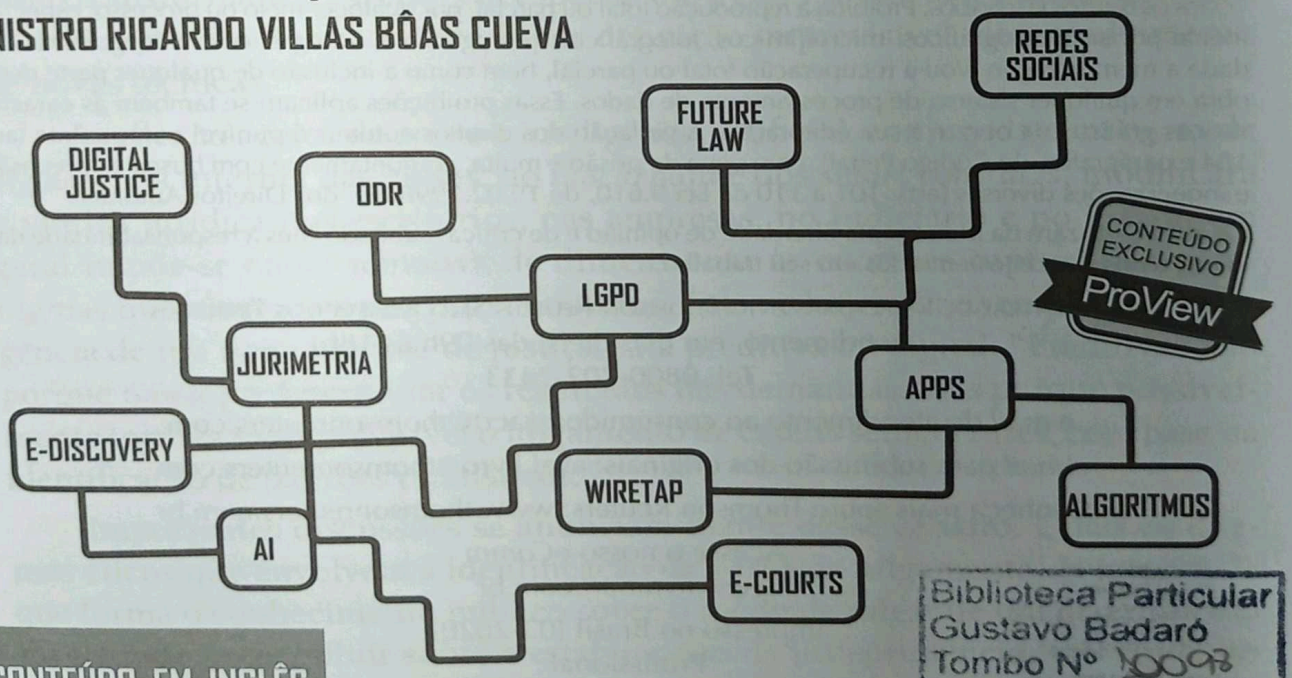
coordenação
PAULO HENRIQUE DOS SANTOS LUCON ▪ ERIK NAVARRO WOLKART ▪
FRANCISCO DE MESQUITA LAUX ▪ GIOVANI DOS SANTOS RAVAGNANI ▪

COLEÇÃO DIREITO E NOVAS TECNOLOGIAS

DIREITO, PROCESSO E TECNOLOGIA

APRESENTAÇÃO
MINISTRO RICARDO VILLAS BÔAS CUEVA



CONTEÚDO EM INGLÊS
- Access to justice and Consumidor.gov case.
- Procedural law and artificial intelligence

THOMSON REUTERS
REVISTA DOS TRIBUNAIS™

FUTURE LAW

Dados digitais: interceptação, busca e apreensão e requisição

Maria Thereza Rocha de Assis Moura

Ministra Vice-Presidente do Superior Tribunal de Justiça. Corregedora-Geral da Justiça Federal. Mestra e Doutora em Direito Processual Penal pela Faculdade de Direito da USP. Professora Doutora de Direito Processual Penal da USP.

Daniel Marchionatti Barbosa

Juiz Auxiliar da Corregedoria-Geral do Conselho da Justiça Federal. Ex-Magistrado Instrutor no Supremo Tribunal Federal. Doutorando pela Universidade de São Paulo (USP). Mestre pela Universidade Federal do Rio Grande do Sul (UFRGS).

1. Generalidades

Em um dia normal, cada um de nós produz grande quantidade de dados digitais. Compartilhar fotos, vídeos, áudios, textos e mensagens faz parte da rotina. Ao mesmo tempo, nossas atividades *on-line* e no mundo real são registradas,

sem que estejamos plenamente conscientes disso. Assim, nossos cliques e buscas na internet e nossa localização no planeta são constantemente captados por empresas de tecnologia.

Como não poderia deixar de ser, essas informações digitais são de grande interesse para o direito. Seu potencial para reconstruir acontecimentos torna-as especialmente interessantes ao processo. Uma infinidade de medidas, mais ou menos invasivas, vem sendo empregada na aquisição dessas informações para o uso em processos judiciais, cíveis ou criminais. Medidas já tradicionais, como a interceptação telemática ou a requisição de informações a terceiros, são somadas a novidades como *roving bug*, cavalo de Troia estatal, busca e apreensão *on-line*, mandado de busca reversa, e inúmeras formas de pesquisar dados privados.

Os ordenamentos jurídicos em geral costumam reconhecer diferentes regimes de quebra de sigilo de dados digitais, conforme a medida é mais ou menos invasiva aos direitos fundamentais do usuário. A maior proteção é reservada ao fluxo telemático. Em seguida, com um grau de proteção um tanto menor, vêm os dados armazenados. Por último, com uma proteção modesta, os dados pessoais – entre estes, os cadastrais são ainda menos tutelados. O direito brasileiro segue essa linha. Curiosamente, por uma série de razões, a relevância prática da quebra de sigilo de dados em processos parece seguir a ordem inversa: requisições de dados pessoais são comuns, a obtenção de dados armazenados é esporádica e a interceptação do fluxo de dados é rara.

Assim, este trabalho analisará cada uma dessas hipóteses de quebra de sigilo de dados digitais, bem como as formas de aquisição desses dados pelo processo judicial.

2. Fluxo telemático

O maior grau de proteção conferido aos dados informáticos pelo ordenamento jurídico brasileiro é quanto ao fluxo telemático, assim considerada a comunicação de dados entre dois dispositivos ou sistemas computacionais. Há, inclusive, controvérsia jurídica relevante sobre a possibilidade de quebra de sigilo desses dados.

O fluxo de dados é protegido pelo inciso XII do art. 5º da CF, segundo o qual "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". O texto constitucional afirma a

inviolabilidade de uma série de comunicações, mas estabelece exceção, permitindo a interceptação, na forma da lei e por ordem judicial. A exceção aplica-se "no último caso". Há quatro linhas de leitura dessa disposição.

Alguns autores defendem que a exegese da norma indica que somente as comunicações telefônicas seriam passíveis de quebra de sigilo, pois a expressão "salvo, no último caso" diria respeito apenas a estas. A correspondência, os dados e as comunicações telegráficas estariam, assim, cobertos por sigilo absoluto.[1]

Outros sustentam que a inviolabilidade absoluta somente albergaria o sigilo das correspondências, não das demais formas de comunicação – telegráfica, de dados e telefônicas.[2] Sob esse enfoque, haveria duas situações de sigilo: de um lado, o das correspondências; de outro, o das comunicações telegráficas, de dados e telefônicas, sendo possível a quebra somente "no último caso", isto é, apenas para o segundo grupo.

Em outro viés, entende-se que a ressalva constitucional abrange todas as hipóteses elencadas no artigo, ou seja, todos os modos de comunicação intersubjetiva previamente elencados, relativizando-se a presunção do sigilo desde que diante da falta de outras medidas menos invasivas.[3]

Finalmente, sustenta-se que a norma constitucional contemplou apenas dois casos: o primeiro, de vedação absoluta de interceptação, abrangendo a correspondência e as comunicações telegráficas; o segundo, enquadrado na exceção do dispositivo, a envolver dados e comunicações telefônicas.[4]

---

1. SILVA, José Afonso. *Curso de direito constitucional positivo*. 36. ed. São Paulo: Malheiros, 2013, p. 440; GRINOVER, Ada Pellegrini; FERNANDES, Antonio Scarance; GOMES FILHO, Antonio Magalhães. *As nulidades no processo penal*. 12. ed. São Paulo: RT, 2011. p. 169.
2. NERY JUNIOR, Nelson; NERY, Rosa Maria de Andrade. *Constituição Federal comentada e legislação constitucional*. São Paulo: RT, 2006. p. 129.
3. MORAES, Alexandre de. *Constituição do Brasil interpretada e legislação constitucional*. 9. ed. São Paulo: Atlas, 2013, p. 179. Pontua o autor que a interpretação do referido inciso deve ser feita de modo a entender que "a lei ou a decisão judicial poderão, excepcionalmente, estabelecer hipóteses de quebra das inviabilidades da correspondência, das comunicações telegráficas e de dados, sempre visando salvaguardar o interesse público e impedir que a consagração de certas liberdades públicas possam servir de incentivo à prática de atividades ilícitas".
4. Cf. STF, QO na Pet 577, Pleno, Rel. Min. Carlos Velloso, j. 25.3.1992, DJ 23.4.1993, voto do Min. Marco Aurélio de Mello. Tendo como ponto de partida esse enfoque, o Ministro rechaçou a possibilidade de se ter o sigilo relativo a "dados" como inafastável. Afirmou, em seu voto: "O sigilo, a meu ver, pode ser afastado mediante a aplicação

O legislador tomou posição pela compatibilidade da quebra de sigilo de dados telemáticos com a CF. As disposições da Lei das Interceptações Telefônicas aplicam-se "à interceptação do fluxo de comunicações em sistemas de informática e telemática" (art. 1º, parágrafo único, da Lei 9.296/1996). Essa disposição foi contestada em Ação Direta de Inconstitucionalidade, a qual aguarda julgamento pelo Pleno do STF.[5] Mais recente, o Marco Civil da Internet afirma o direito do usuário à "inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei" (art. 7º, II, da Lei 12.965/2014).

Ao proteger o fluxo de comunicações de dados digitais, o direito está protegendo a comunicação em si, independentemente de seu conteúdo. Gustavo Badaró bem observa que a proteção "trata da liberdade de comunicação entre os indivíduos", e não diretamente da privacidade do conteúdo comunicado.[6] Quaisquer dados que estejam sendo comunicados de forma privada, enquanto estão sendo comunicados, são protegidos. Estão incluídos não apenas dados que correspondem a uma comunicação humana imediatamente perceptível ao usuário, como mensagens de texto, voz ou imagens, *e-mails* enviados ou recebidos, mas também quaisquer dados que estejam sendo trocados entre sistemas computacionais. Assim, dados que o usuário nem sempre tem plena consciência de que está trocando, como atualizações automáticas de *software*, ou comandos em *sites* abertos na *world wide web*.

Além do conteúdo comunicado, a comunicação produz outros dados, denominados dados de tráfego. Eles são gerados em virtude da comunicação, mas não correspondem ao seu conteúdo. A Convenção de Budapeste sobre Crimes

---

do que se contém na parte final do preceito, conforme a expressão: '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'." Embora o Ministro, em relação ao primeiro caso, tenha afirmado a inviolabilidade do sigilo da correspondência, o STF já se manifestou no sentido de que a quebra do sigilo da correspondência para deslindar a prática de homicídio não é ilícita: HC 70814, 1ª Turma, Rel. Min. Celso de Mello, j. 1º.3.1994, DJ 24.06.1994. De igual modo decidiu o STJ: HC 203371, 5ª Turma, Rel. Min. Laurita Vaz, j. 03.05.2012, DJe 17.9.2012.

5. ADI 4.112, Rel. Min. Gilmar Mendes. A ação foi incluída em pauta pelo relator em setembro de 2016 e está aguardando data no calendário de julgamento do Pleno.
6. BADARÓ, Gustavo Henrique Righi Ivahy. Interceptação de comunicações telefônicas e telemáticas: limites ante o avanço da tecnologia. In: LIMA, José Corrêa de; CASARA, R.R. Rubens. (coord). *Temas para uma perspectiva crítica do direito*: homenagem ao Professor Geraldo Prado. 2. ed. Rio de Janeiro: Lumen Juris, 2012. p. 467-482.

Cibernéticos (*Budapeste Convention on Cybercrime*) os define como "quaisquer dados de computador relativos à comunicação por meio de sistema de computador, gerado por sistema de computador que seja parte na cadeia de comunicação, indicando a origem, destino, rota, horário, data, tamanho ou duração da comunicação, ou tipo do sistema" (artigo 1, "d").[7]

No Brasil, há jurisprudência consolidada relativa aos dados de tráfego telefônico, no sentido de que não há aplicação do art. 5º, XII, da CF, sendo possível a quebra de sigilo por Comissão Parlamentar de Inquérito.[8] O mesmo raciocínio vale para os dados de tráfego telemático. Nosso direito enquadra os dados de tráfego telemático no gênero dos dados pessoais.[9]

O termo interceptação designa a quebra do fluxo de dados digitais nos principais diplomas normativos acerca do tema.[10]

Uma característica importante da interceptação é ocorrer em tempo real, recaindo sobre o fluxo de comunicações. Se os mesmos dados são adquiridos após armazenados em um dispositivo computacional, não haverá interceptação, mas quebra de sigilo de dados armazenados, a qual poderá ocorrer por busca e apreensão digital ou requisição a terceiros.[11] Assim é a previsão da Convenção de Budapeste, na qual a interceptação pode ser definida como a "coleta ou gravação de dados de conteúdo, em tempo real, por meio de um sistema de computador" (artigo 21).

No caso do Brasil, ao aplicar à interceptação telemática as normas sobre a interceptação telefônica, o legislador seguiu os limites constitucionais aplicáveis a esta. Restou indubitável que a interceptação telemática exige autorização judicial, previsão legal e só pode ser usada para a investigação criminal ou instrução processual penal. Não é possível decretar a interceptação em causas

---

7. Elaborada no âmbito do Conselho da Europa, com a participação ativa de Canadá, Japão, Filipinas, África do Sul e Estados Unidos, a Convenção foi ratificada por 63 países, vários deles fora da Comunidade Europeia. O Brasil não é signatário.
8. MS 23.652, Rel. Min. Celso de Mello, Plenário, julgado em 22.11.2000.
9. Ainda que não represente o entendimento dominante, importante destacar a consistência dos argumentos de Ricardo Sidi, para quem os dados de tráfego têm a mesma proteção do conteúdo da comunicação, especialmente se a quebra de sigilo ocorrer em tempo real, ou se os dados estiverem ligados a uma comunicação concreta. Ver: SIDI, Ricardo. *A interceptação de comunicações telemáticas no processo penal*. Belo Horizonte: D'Placido, 2016. p. 298.
10. Na Alemanha, a interceptação é denominada *Telekommunikationsüberwachung* (monitoramento de telecomunicação, § 100a, do StPO).
11. Ver *infra*, capítulo 3.

cíveis ou usar aplicações intrusivas para, mediante vigilância em massa (*mass surveillance*), prevenir ataques à ordem pública ou a prática de crimes graves.

A interceptação telemática adquire os dados que estão sendo comunicados entre dois pontos. Os dados digitais são comunicados por meio de telecomunicação, definida como transmissão, emissão ou recepção de informação de qualquer natureza (art. 60, § 1º, da Lei 9.472/1997). A transmissão da comunicação à distância pode usar qualquer suporte. Os sinais podem ser confinados a fios, utilizar radiocomunicação – art. 162, § 1º, da Lei 9.472/1997 – ou qualquer outra tecnologia.

A interceptação envolve a aquisição dos dados e a sua decodificação. Para que uma comunicação de dados seja juridicamente protegida, ela precisa apresentar restrição ao acesso público em algum desses aspectos. Uma rádio digital, por exemplo, que transmita seu sinal por radiocomunicação usando um protocolo público, poderá ser captada e ouvida com o uso de meios disponíveis para qualquer pessoa. Não será, por isso, uma comunicação de dados protegida contra a interceptação.[12]

Vários meios de transmissão de dados envolvem o uso de radiocomunicação, tornando a aquisição dos pacotes de dados relativamente simples. Uma rede *wi-fi*, por exemplo, pode ter os sinais captados por qualquer antena nas proximidades. No entanto, o uso de técnicas de encriptação pode tornar a mensagem incompreensível. Com isso, a aquisição dos dados será inútil.

De outro lado, redes que usam cabos tornam a aquisição dos dados bem mais difícil, visto que será necessário o acesso físico à infraestrutura da rede. Mesmo que não trafeguem codificados, a proteção constitucional da comunicação de dados é aplicável.

A interceptação pode ser executada com apoio de terceiros ou diretamente pelas autoridades. No direito brasileiro, a ordem judicial é sempre imprescindível e deve indicar a forma de execução da diligência (art. 5º da Lei das Interceptações Telefônicas).

A lei menciona que será possível requisitar "serviços e técnicos especializados às concessionárias de serviço público" (art. 7º da Lei das Interceptações Telefônicas).[13] A despeito da falta de uma previsão legal específica, pensamos

12. Nos Estados Unidos, a legislação usa o conceito de "prontamente acessível ao público em geral" (*readily accessible to the general public*), para excluir as regras de proteção à privacidade das comunicações (18 U.S. Code § 2510. 16).

13. Em verdade, as concessionárias de serviço público dificilmente têm a contribuir com a interceptação telemática. O acesso à internet não é um serviço de telecomunicações,

que qualquer terceiro que tem acesso ao fluxo de comunicações pode ser chamado a apoiar a medida. Em regra, os provedores de conexão e os provedores de aplicações de internet são esses intervenientes.

Os provedores de conexão costumam colaborar com as ordens judiciais. Normalmente, são sociedades empresárias brasileiras que também atuam no mercado de telefonia, habituadas ao procedimento de interceptação. No entanto, por razões de ordem prática, a interceptação com apoio dos provedores de serviço é pouco produtiva.[14]

Os provedores de aplicações de internet, por sua vez, costumam ser bastante resistentes a colaborar com interceptações. Normalmente, são empreendimentos que fazem da privacidade do usuário um ativo. As aplicações mais sensíveis, como os aplicativos de trocas de mensagens, investem em criptografia forte, tornando impossível, ao próprio provedor, decodificar o conteúdo das mensagens. É o caso, por exemplo, do WhatsApp, aplicativo de mensagens mais usado no Brasil, que adotou a criptografia de ponta a ponta.

Na execução direta, os investigadores usam seus próprios meios para adquirir e decodificar os sinais, contornando os sistemas de segurança eventualmente existentes. No entanto, *independentemente do grau de resistência que os sistemas envolvidos ofereçam, a autorização judicial faz-se necessária para a interceptação.*

Um exemplo de execução direta ocorreu em um caso concreto analisado pelo STJ. Após apreender o aparelho celular, os investigadores habilitaram o recurso WhatsApp Web, com autorização do juízo, e restituíram o telefone. Com isso, passaram a acessar todas as mensagens trocadas pelo usuário no aplicativo de mensagens WhatsApp. O STJ reputou ilícita a prova. As razões de decidir

---

muito embora, via de regra, use um serviço de telecomunicações como suporte, entrando no conceito de serviço de valor adicionado (art. 61 da Lei 9.472/1997). São vários os serviços de telecomunicações que servem como suporte ao acesso à internet – serviço telefônico fixo comutado, serviço móvel pessoal (telefonia móvel), TV a cabo etc. Entre o universo de prestadores desses diversos serviços, apenas algumas das operadoras de telefonia fixa – Serviço Telefônico Fixo Comutado (STFC) – são concessionárias de serviço público. Os demais serviços são prestados em regime privado, sob o regime da autorização (arts. 63 e 64 da Lei 9.472/1997).

14. Um mesmo usuário usa provedores diversos em seus deslocamentos (uma rede em casa, outra no trabalho, a rede móvel no aparelho telefônico, acessos via *wi-fi* em cafés etc.). Interceptando-se apenas um dos provedores, grande parte da comunicação ficará perdida. Além disso, os provedores de aplicações de internet vêm oferecendo criptografia das comunicações sensíveis, tornando a aquisição de dados inútil.

foram a impossibilidade de assegurar a integridade da prova – as mensagens poderiam ser enviadas ou excluídas pelos próprios investigadores, sem que houvesse registro – e a traição à confiança do investigado, que teve o telefone devolvido sem ser advertido da habilitação do aplicativo Web.[15]

A primeira dificuldade poderia ser contornada com o uso de um *software* que, em separado, registre as atividades dos investigadores no computador. A segunda é bem mais profunda: remete aos limites éticos do uso dos meios ocultos de investigação,[16] os quais, por definição, envolvem algum grau de traição de confiança. Os tribunais brasileiros são tímidos no estabelecimento de parâmetros gerais para aceitação dessas técnicas de investigação, preferindo uma abordagem caso a caso.

Uma alternativa de execução tecnicamente viável é o uso de programas espiões pelos agentes de investigação: *software* controlado pelo Estado, instalado de forma oculta no dispositivo do investigado. Há uma infinidade de ferramentas usadas para *hackear* sistemas computacionais, geralmente empregadas para fins maliciosos, que podem ser adaptadas para essa finalidade – cavalo de Tróia (*Trojan horse*), *keyloger*, *spyware*, etc.

Caso a execução da medida se valha de *software* instalado no sistema computacional invadido, o Estado deve levar em conta a segurança do sistema invadido e dos sistemas de terceiros. No caso brasileiro, não há parâmetro legal ou precedentes que permitam afirmar que uma medida semelhante é admissível, ainda que com ordem judicial. Caso se entenda pela viabilidade, os riscos técnicos devem ser informados ao magistrado, que os considerará em seu indispensável juízo de admissibilidade.

A invasão não deve colocar em risco o funcionamento do sistema invadido. Outra preocupação é com a afetação a terceiros: vírus e *software* malicioso podem ter a habilidade de se propagar em rede, o que poderia afetar a terceiros não investigados. O programa invasor não deve produzir danos colaterais desnecessários.

A invasão do sistema do alvo abre portas teóricas para várias possibilidades investigativas. Uma delas é o controle de aparelhos (câmeras e microfones de computadores e aparelhos telefônicos) para captar e transmitir sinais de áudio e vídeo de forma sub-reptícia. O uso da técnica, conhecida como *roving bug*, é

15. RHC 99.735, Rel. Min. Laurita Vaz, Sexta Turma, julgado em 27.11.2018.

16. Além da interceptação telemática, a legislação brasileira menciona a interceptação telefônica, a captação ambiental, a infiltração de agentes e a ação controlada (art. 3º da Lei 12.850/2015).

aceita pelo direito em alguns países.[17] Importante notar que, de acordo com o direito brasileiro, o uso dessa técnica não constituiria interceptação telemática, mas captação ambiental (art. 3º, II, da Lei 12.850/2013).[18]

Outra medida que não se confunde com a interceptação telemática, a despeito de ocorrer em ambiente virtual, é a infiltração de agentes de investigação na internet. Nesse caso, deve-se observar a diferença entre interceptação e gravação, tradicional na doutrina brasileira.[19] A interceptação ocorre sem o conhecimento dos interlocutores. Na escuta e na gravação, ao menos um dos interlocutores sabe da captação – e ao menos um a desconhece. A diferença reside na pessoa que executa a medida. A escuta é executada por terceiro. A gravação é realizada por um dos interlocutores. Na infiltração de investigadores na internet, busca-se obter provas de crimes e de suas autorias mediante a interação *on-line* dos investigadores com os investigados. O registro dessa interação é usado como prova. A medida poderia ser classificada como escuta ou gravação, não como interceptação. O direito brasileiro prevê o uso dessa técnica no Estatuto da Criança e do Adolescente, para apuração de crimes ligados à pedofilia e de invasão de dispositivo informático.[20]

Como a interceptação telemática se vale das normas sobre a interceptação telefônica, há extensa bibliografia sobre o procedimento respectivo que pode ser observada.[21]

Como visto, o fluxo de dados é o estado mais protegido dos dados digitais. A interceptação dos dados telemáticos ocorre em tempo real e adquire todo o conteúdo comunicado, pelo que é muito custosa à privacidade e só pode ser adotada mediante autorização judicial, com o objetivo de apurar crimes graves.

---

17. Nos Estados Unidos, ver U.S. v. OLIVA. United States Court of Appeals, Ninth Circuit. Nos. 10-30126, 10-30134. July 20, 2012.
18. Não há captação de dados comunicados pelo usuário, mas a captação de imagens ou de áudio em um ambiente e a criação de um fluxo de comunicação para transmitir o material captado às autoridades. Tratar-se-ia de uma medida particularmente invasiva, cuja constitucionalidade, mesmo com autorização judicial, seria duvidosa.
19. A classificação é baseada nas lições de Ada Pellegrini Grinover, em GRINOVER, Ada Pellegrini. *Provas ilícitas, interceptações e escutas*. Brasília: Gazeta Jurídica, 2013. p. 262-263.
20. Arts. 190-A a 190-E da Lei 8.069/1990, introduzidos pela Lei 13.441/2017.
21. De autoria da primeira autora deste trabalho, ver: MOURA, Maria Thereza Rocha de Assis. Interceptação telefônica e telemática na jurisprudência brasileira. In: Kai Ambos; Eneas Romero. (Org.). *Crime Organizado – Análise da Lei 12.850/2013*. 1. ed. São Paulo: Marcial Pons; CEDPAL, 2017, v. 1, p. 163-191.

A interceptação pode ser executada diretamente, pelos próprios policiais, ou envolver requisição a terceiros – normalmente, provedores de acesso ou de aplicações de internet.

3. Dados armazenados

Os dados digitais armazenados em dispositivos locais ou em nuvem também são protegidos, mas de forma menos intensa do que o fluxo de dados.

O art. 5º, XII, da CF não se aplica à quebra de sigilo de dados armazenados. O *leading case* dessa interpretação, de 2006, foi estabelecido pelo STF em caso em que computador fora apreendido e acessado o seu disco rígido pelas autoridades.[22]

O precedente sedimentou o direito à inviolabilidade da intimidade e da vida privada, mencionado no art. 5º, X, da CF, como fundamento constitucional da proteção aos dados armazenados.[23]

O direito à privacidade ou à vida privada está contemplado em várias declarações de direito, como o artigo 17, 1, do Pacto Internacional sobre Direitos Civis e Políticos, artigo 11, 2, do Pacto de San José da Costa Rica, artigo 8º da Convenção Europeia de Direitos Humanos e artigo XXII da Declaração Islâmica Universal dos Direitos Humanos.

No Brasil, o texto constitucional traçou uma distinção de difícil compreensão, ao consagrar a inviolabilidade da intimidade e da vida privada (art. 5º, X). De acordo com Tércio Sampaio Ferraz Júnior, há um "diferente grau de

---

22. RE 418.416, Tribunal Pleno, rel. Min. Sepúlveda Pertence, DJ de 19.12.2006.

23. Curiosamente, em seu caso marco sobre o tema, o Tribunal Constitucional Alemão preferiu afastar o direito à privacidade e invocar o direito geral da personalidade – articulação do direito ao livre desenvolvimento da personalidade (artigo 2, 1, da Lei Fundamental) com a dignidade da pessoa humana (artigo 1, 1, da Lei Fundamental). Do direito geral da personalidade, o Tribunal derivou a "garantia de confidencialidade e de integridade" dos sistemas de tecnologia da informação. Essa garantia protege contra "acessos secretos" às informações do sistema, ou contra captações de informações do sistema por outros sistemas independentes – § 205 –, aplicável independentemente do grau de dificuldade para as autoridades públicas conseguirem invadir o sistema – § 206. A Corte também negou retirar a proteção de cláusulas que parecem mais próximas para uma abordagem por analogia, como a inviolabilidade das telecomunicações (artigo 10 da Lei Fundamental), a inviolabilidade da residência (artigo 13 da Lei Fundamental) e a autodeterminação informacional – §§ 167-169 da decisão (BVerfG, 1 BvR 370/07, 27-2-2008). A Constituição brasileira não menciona expressamente o direito ao livre desenvolvimento da personalidade, o que dificulta a aproximação da fundamentação do Tribunal Alemão.

exclusividade" entre intimidade e privacidade. A intimidade seria "o âmbito do exclusivo que alguém reserva para si, sem nenhuma repercussão social, nem mesmo ao alcance de sua vida privada que, por mais isolada que seja, é sempre um viver entre os outros (na família, no trabalho, no lazer em comum)". O autor dá os seguintes exemplos: "o diário íntimo, o segredo sob juramento, as próprias convicções, as situações indevassáveis de pudor pessoal, o segredo íntimo cuja mínima publicidade constrange". Por sua vez, a vida privada envolveria "a proteção de formas exclusivas de *convivência*", ou seja, situações em que há comunicação entre sujeitos, da qual estão excluídos terceiros.[24] Portanto, de acordo com essa definição, a intimidade diz respeito a informações que não são comunicadas, ao passo que a privacidade diz respeito à comunicação restrita de informações.

Dados íntimos ou privados armazenados em formato digital são invioláveis por força da própria Constituição, ainda que não tenham sido comunicados (dados íntimos) e ainda que estejam armazenados em dispositivos não ligados à internet. A proteção é aplicável independentemente do local em que os dados estão armazenados. Dados armazenados no dispositivo do usuário ou em nuvem – em servidores dos provedores de aplicações de internet – estão igualmente protegidos. Dispositivos ligados em redes internas ou mesmo sem conexão, como discos rígidos de computadores pessoais, *pen drives* ou outras mídias portáteis, são igualmente invioláveis. Em parte, o Marco Civil da Internet e a legislação penal apenas desenvolvem sua defesa.

O Marco Civil da Internet confere ao usuário o direito à "inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial" (art. 7º, III). A norma qualifica os dados protegidos, ao falar em "comunicações privadas armazenadas". Com isso, está restringindo seu escopo apenas aos dados comunicados – privados. Em tese, dados produzidos e armazenados localmente – no próprio computador do usuário, por exemplo – estão fora do escopo do dispositivo legal – ainda que inseridos na proteção constitucional.

A legislação penal contém disposição que protege dados armazenados localmente. O art. 154-A do Código Penal criminaliza a invasão não autorizada de "dispositivo informático", "mediante violação indevida de mecanismo de segurança".

À proteção dos dados armazenados não se aplicam as restrições constantes do art. 5º, XII, da CF e da Lei das Interceptações Telefônicas. Em tese, é possível

24. FERRAZ JÚNIOR, Tércio Sampaio. Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado. In *Revista da Faculdade de Direito*, Universidade de São Paulo, v. 88. p. 441-442.

levantar o sigilo de dados em casos cíveis ou em casos envolvendo crimes sujeitos às penas de detenção.

A legislação não dispõe exaustivamente sobre os parâmetros e o meio de execução da quebra de sigilo de dados armazenados. No âmbito da internet, o Marco Civil limita-se a exigir a ordem judicial para afastar a inviolabilidade e o sigilo – "inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial" (art. 7º, III). O Marco Civil fala em ordem judicial para quebrar sigilo de dados, mas é específico para os dados de registro (art. 22) e pessoais (art. 10, § 1º). Portanto, a ordem judicial para a quebra de sigilo de dados armazenados não é especificada nessa lei.

Na falta de disposições legais próprias, resta aplicar, por analogia, as normas procedimentais mais próximas, na forma do art. 4º da LINDB e do art. 3º do CPP. A analogia pode ser buscada no art. 240, § 1º, do CPP, no art. 22, parágrafo único, do Marco Civil da Internet e no art. 2º da Lei das Interceptações Telefônicas.

O art. 240, § 1º, do CPP trata da busca e apreensão domiciliar, exigindo "fundadas razões" a autorizarem a medida. A aquisição de dados digitais é uma medida bastante semelhante a busca e apreensão e, inclusive, recebe esse nome em alguns diplomas normativos. A Convenção Europeia sobre o Cibercrime usa a expressão "busca e apreensão de dados de computadores armazenados" (*Search and seizure of stored computer data*, art. 19). O Código de Processo Penal Alemão fala em busca e apreensão *on-line* (*Online-Durchsuchung*, § 100b, StPO). Portanto, serão necessárias "fundadas razões".

O art. 22, parágrafo único, do Marco Civil da Internet exige a demonstração de "fundados indícios da ocorrência do ilícito"; a apresentação de "justificativa motivada da utilidade dos registros solicitados para fins de investigação ou instrução probatória"; e a especificação do "período ao qual se referem os registros". O primeiro requisito desenvolve o que se deve entender por "fundadas razões" a justificar a medida. Além disso, deve ser demonstrado que a medida tem potencial de comprovar o ilícito e especificar, com a maior precisão possível, os dados a serem buscados ou requisitados.

A Lei das Interceptações Telefônicas estabelece outros parâmetros relevantes para um meio de obtenção de prova tão invasivo (art. 2º). Em primeiro lugar, exige indícios de que o próprio alvo tenha contribuído para o ilícito (I). No caso dos dados armazenados, também é possível cogitar, em hipóteses excepcionais devidamente justificadas, a quebra de sigilo de terceiros, especialmente da vítima ausente ou falecida. Em segundo lugar, a norma estabelece uma subsidiariedade do meio de obtenção de prova, a ser usado apenas se a prova não puder ser feita por outro meio menos invasivo (II). Por fim, indica um juízo de

proporcionalidade em sentido estrito, tendo por parâmetro a gravidade do fato em apuração (III).

Não se deve admitir a quebra de sigilo de dados armazenados para fazer provas em demandas cíveis ou para a apuração de crimes punidos com detenção. A interceptação telemática só é admissível se "o fato investigado constituir infração penal punida, no máximo, com pena de detenção" (art. 2º, III). O mesmo parâmetro deve ser adotado para a quebra de sigilo de dados armazenados, visto que ambas as medidas redundam no acesso ao conteúdo de informações íntimas ou privadas. A legislação andou mal ao não deixar clara essa questão. Na falta de norma expressa, não é impossível que uma medida tão invasiva acabe sendo utilizada de forma abundante em ações acerca de relações próximas, como causas de família, sucessões ou contratuais. Importante lembrar que, em causas cíveis, a busca e apreensão é comum como medida de execução, mas bem rara como meio de obtenção de provas.

Dessa forma, para a quebra de sigilo de dados armazenados são necessários os seguintes requisitos:

a) prova da existência de um crime punido com reclusão;

b) indícios de responsabilidade pelo ilícito, pelo titular dos dados. Muito excepcionalmente, pode-se cogitar da adoção da medida contra terceiros, como a vítima falecida;

c) identificação, o mais precisa possível, dos dados a serem buscados ou requisitados;

d) impossibilidade de obter a prova por outro meio menos gravoso;

e) adequação da medida para provar o fato a ser apurado;

f) proporcionalidade em sentido estrito da medida, levando em conta, especialmente, o custo aos direitos individuais que a ela representa.

O Superior Tribunal de Justiça considerou desproporcional a quebra de sigilo de *e-mails*, na qual foram requisitadas todas as mensagens referentes a um período de dez anos, "sem que se declinasse adequadamente a necessidade da medida extrema ou mesmo os motivos para o lapso temporal abrangido".[25]

A quebra de sigilo de dados armazenados pode ser executada de duas formas: mediante busca e apreensão de dados ou mediante requisição.

A busca e apreensão de dados ocorre quando os dados são acessados e copiados pelas próprias autoridades.

25. HC 315.220, Rel. Min. Maria Thereza de Assis Moura, Sexta Turma, julgado em 15.9.15.

O meio menos sofisticado é a apreensão física do dispositivo no qual os dados estão gravados, com o subsequente acesso direto. Há, no entanto, situações bem mais complexas.

Normalmente, os sistemas ligados a rede são dotados de segurança, como senhas e padrões de acesso. A aquisição pode ser realizada pelos próprios agentes estatais, mediante invasão do sistema, burlando a segurança. Seria o caso, por exemplo, de quebra da senha por força bruta, ou de seu achado no curso das investigações. O bom trabalho policial para obter meios para superar a segurança não dispensa a autorização judicial para execução da medida. Ou seja, ainda que os agentes estatais tenham possibilidade técnica de adquirir os dados, a autorização judicial é necessária.[26]

Assim como ocorre no fluxo de dados, teoricamente a execução direta da busca e apreensão pode se valer de *software* instalado no sistema do investigado. As mesmas preocupações quanto a danos colaterais aos sistemas do alvo e de terceiros se aplicam.[27]

Outra forma de aquisição de dados digitais é a requisição, a qual pode ser direcionada ao próprio titular dos dados ou a terceiro.[28]

Em causas cíveis, é juridicamente viável requisitar os dados ao próprio titular dos dados, aplicando-se as regras sobre a exibição de documento, arts. 396 a 400 do CPC.

Em causas criminais, há dificuldade em compatibilizar a intimação do investigado ou do réu para produzir provas em seu desfavor com o direito à não autoincriminação. Além disso, o interessado poderia excluir os dados incriminatórios. Assim, a intimação do imputado para produzir os dados em seu desfavor é, em princípio, indevida.

---

26. Nesse sentido, ver MENDES, Gilmar. *Curso de Direito Constitucional*. 13. ed. São Paulo: Saraiva, 2018. pp. 610-611.

27. Ver, *supra*, capítulo 2. Como referido, não há parâmetro legal ou precedentes que permitam afirmar que uma medida semelhante é admissível, ainda que com ordem judicial. Caso se entenda pela viabilidade, os riscos técnicos devem ser informados ao magistrado, que os considerará em seu indispensável juízo de admissibilidade.

28. Em tese, seria possível direcionar a busca e apreensão contra o terceiro que controla os dados. Por razões de conveniência, essa medida não é a preferencial, devendo ser observada apenas em caso de resistência à requisição ou de risco à integridade dos dados. Nos Estados Unidos, a preferência pela requisição também é explicada porque ela está sujeita a requisitos probatórios menos exigentes do que a busca e apreensão digital. Esta é regida pela Quarta Emenda, que "demanda causa provável". No Brasil, os requisitos para ambas as medidas são idênticos.

A requisição ao terceiro pode ocorrer em causas cíveis ou criminais. O terceiro será aquele que tem o controle dos dados, normalmente um provedor de aplicações de internet.

Nem sempre os provedores de serviços armazenam o conteúdo das informações de seus usuários. Em alguns casos, armazenam sob criptografia, com o propósito de impedir o acesso por seus próprios agentes. A impossibilidade de acesso ao conteúdo pode ser uma estratégia deliberada para tornar o serviço mais interessante aos usuários. É o caso, por exemplo, do serviço de mensagens WhatsApp, que elimina de seus servidores as mensagens entregues e adota criptografia ponta a ponta.

Em nossa opinião, na falta de disposição legal em sentido contrário, os provedores não estão obrigados a reter ou adotar estrutura de sistema que permita o acesso por agentes públicos. Aplica-se o princípio da legalidade – art. 5º, II, da CF. Logo, a intimação para a retenção ou decriptação de mensagens, tendo em vista a estratégia de negócios do provedor, só pode ser exigida se embasada em determinação legal específica.

Portanto, os dados armazenados são muito protegidos pelo direito – ainda que um pouco menos do que o fluxo telemático. Dados armazenados correspondem ao conteúdo das comunicações e da produção humana, pelo que sua aquisição pode ser muito custosa à privacidade e à intimidade. A quebra de sigilo somente pode ocorrer com autorização judicial, amparada em juízo de proporcionalidade – o custo da medida aos direitos fundamentais pode ser suportado apenas no interesse da apuração de ilícitos graves. Na falta de uma legislação específica, deve-se observar, por analogia, as normas quanto a busca e apreensão, interceptação telemática e quebra de sigilo de dados de registro. A quebra de sigilo de dados armazenados não pode ocorrer no interesse da apuração de ilícitos civis ou de delitos leves. A execução da ordem judicial pode ser feita pelos próprios policiais, mediante busca e apreensão de dados, ou mediante requisição a terceiros que sobre eles tenham controle – normalmente, provedores de aplicações de internet.

4. DADOS PESSOAIS, DADOS CADASTRAIS, REGISTROS DE CONEXÃO E DE ACESSO

Os dados pessoais, dados de conexão e de acesso são dados periféricos, os quais não representam o conteúdo da comunicação ou da produção intelectual do usuário.

O conceito de *dado pessoal* é, para fins do Marco Civil da Internet, bastante amplo. Na forma do art. 7º, VII, os dados pessoais são gênero, no qual os dados de registro de conexão e de acesso a aplicações de internet estão incluídos.

O Regulamento do Marco Civil da Internet define dado pessoal como o "dado relacionado à pessoa natural identificada ou identificável, inclusive números identificativos, dados locacionais ou identificadores eletrônicos, quando estes estiverem relacionados a uma pessoa" (art. 14, I, do Decreto 8.771/2016). A Lei Geral de Proteção de Dados (LGPD) usa definição semelhante – "informação relacionada a pessoa natural identificada ou identificável" (art. 5º, I, da Lei 13.709/2018).

Entre os dados pessoais, a lei dá tratamento especial aos *dados cadastrais*, definidos como os que "informem qualificação pessoal, filiação e endereço" (art. 10, § 3º, do Marco Civil da Internet).[29] Como se verá, esses recebem uma menor proteção do ordenamento jurídico.

Os *dados de registro* são de duas espécies: registro de conexão e registro de acesso a aplicações de internet. Os dados de registro também são dados pessoais – ao menos quando relacionados a pessoa natural.

Registro de conexão é "o conjunto de informações referentes à data e hora de início e término de uma conexão à internet, sua duração e o endereço IP utilizado pelo terminal para o envio e recebimento de pacotes de dados" (art. 5º, VI, do Marco Civil da Internet).[30]

Registro de acesso a aplicações de internet é "o conjunto de informações referentes à data e hora de uso de uma determinada aplicação de internet a partir de um determinado endereço IP" (art. 5º, VIII, do Marco Civil da Internet).[31]

---

29. O regulamento do Marco Civil da Internet define dados pessoais como "nome, prenome, estado civil e profissão do usuário" (art. 11, III, do Decreto 8.771/2016).

30. O registro de conexão pode ser requisitado juntamente com os dados cadastrais do usuário que contratou aquele acesso (art. 10, § 1º, do Marco Civil da Internet). Assim, por exemplo, pode-se descobrir que o acesso partiu de uma conta de internet banda larga instalada em uma casa. Nada obstante, é possível que o acesso tenha sido realizado por qualquer um dos moradores, ou mesmo por um terceiro que tenha usado a rede residencial.

31. A identificação do usuário nem sempre é imediata. Provedores de aplicações de internet podem não manter cadastro de seus usuários e, mesmo que o façam, a conta pode ter sido acessada por terceiro. Um passo adicional para identificação do usuário é a ligação dos dados de registro a um cliente de provedor de conexão. Com as informações IP e o momento de acesso, é possível pesquisar em *sites* "*whois*", como o "https://registro.br/cgi-bin/whois", e saber qual o provedor de conexão responsável por aquele endereço naquele momento. Em seguida, é possível obter do provedor de conexão os dados pessoais de quem contratou aquele acesso. Como descrito na nota anterior, isso não representa certeza de que determinada pessoa fez o acesso – a rede pode ter sido usada por terceiros.

Todos esses dados são protegidos pela privacidade (art. 5º, X, da CF), mas não são completamente sigilosos. Se, por um lado, a doutrina extrai "da Constituição Federal um verdadeiro direito fundamental à proteção de dados pessoais",[32] por outro, o compartilhamento deles é de grande interesse empresarial. Nos últimos anos, vários tratados e leis foram adotados para arbitrar essa tensão. No Brasil, o Marco Civil da Internet e a Lei Geral de Proteção de Dados Pessoais (LGPD) são os marcos legais.[33]

O Marco Civil da Internet veda o fornecimento de dados pessoais a terceiros, "salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei" (art. 7º, VII). A Lei Geral de Proteção de Dados Pessoais também tem um regramento sobre o compartilhamento de dados, elencando hipóteses além do consentimento (art. 7º). Essas normas vêm sendo objeto de estudo por doutrina especializada.

A este trabalho interessa especificamente o fornecimento de dados pessoais, dados cadastrais, registros de conexão e registros de acesso a aplicações de internet a autoridades públicas, de forma não espontânea – mediante requisição.

O provedor de conexão é obrigado a manter os registros de conexão pelo prazo de um ano.[34] O provedor de aplicações de internet "constituído na forma de pessoa jurídica e que exerça essa atividade de forma organizada, profissionalmente e com fins econômicos" é obrigado a manter os registros de acesso a aplicações de internet por seis meses.[35] Os provedores podem captar outros dados pessoais em algumas hipóteses, mas sua disponibilização deve "atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas" (art. 10 do Marco Civil da Internet).

Segundo a legislação, no art. 10, § 1º, a obrigação de compartilhar registros e dados pessoais ou "outras informações que possam contribuir para a

---

32. MENDES, Laura Schertel, *Privacidade, proteção de dados e defesa do consumidor*, São Paulo: Saraiva, 2014, p. 172.
33. Os dispositivos da LGPD mencionados neste trabalho entram em vigor em meados de agosto de 2020, conforme art. 65, II, com redação pela Lei 13.853/2019.
34. Art. 13 do Marco Civil da Internet. A autoridade policial e o Ministério Público podem requerer, cautelarmente, a prorrogação do prazo de guarda, na forma dos §§ 2º a 5º do art. 13.
35. Art. 15 do Marco Civil da Internet. Provedores de acesso que não se enquadram nos requisitos legais podem ser judicialmente compelidos a manter os registros (§ 1º). De forma semelhante aos registros de conexão, polícia e MP podem requerer a prorrogação do período de guarda (§§ 2º a 4º do art. 15).

identificação do usuário ou do terminal" só existe se houver ordem judicial (arts. 13, § 5º, e 15, § 3º, do Marco Civil da Internet). Há algumas exceções, entretanto.

Dados cadastrais podem ser compartilhados com "autoridades administrativas que detenham competência legal para a sua requisição" (art. 10, § 3º, do Marco Civil da Internet). O Regulamento esclarece que o compartilhamento só pode ser feito por requisição de autoridade administrativa que detiver competência legal expressa (art. 11 do Decreto 8.771/2016).

A legislação processual penal prevê a requisição de dados cadastrais de vítimas ou de suspeitos, mediante requisição de membro do MP ou de delegado de polícia, nas investigações de crimes graves contra a liberdade pessoal (art. 13-A do CPP) e de crimes praticados por organizações criminosas (art. 15 da Lei 12.850/2013).

Portanto, os dados cadastrais são aqueles menos protegidos pela legislação, admitindo quebra de sigilo sem ordem judicial, ainda que em hipóteses estritas.

O art. 22 do Marco Civil da Internet trata do pedido de ordem judicial para o fornecimento dos registros de conexão e de acesso a aplicações de internet. A lei fala que o pedido deve ter "propósito de formar conjunto probatório em processo judicial cível ou penal", deixando clara a possibilidade de requisição para causas não penais.

O pedido pode ser deduzido pela "parte interessada", dando a entender que não cabe a atuação de ofício do magistrado e, no âmbito criminal, a representação por Autoridade Policial – a parte na ação penal é o Ministério Público (art. 129, I, da CF).[36]

O parágrafo único do art. 22 do Marco Civil da Internet estabelece os requisitos do pedido de quebra de sigilo. O autor do requerimento tem o ônus de comprovar a presença de "fundados indícios da ocorrência do ilícito" (art. 22, parágrafo único, I). O ilícito pode ser criminal ou cível. No caso do ilícito cível, a disposição deve ser lida em conjunto com o art. 497, parágrafo único, do CPC, o qual considera que o ilícito pode ocorrer mesmo na ausência do dano ou de culpa ou dolo.[37]

---

36. É duvidoso que o legislador usou a expressão "parte interessada" de forma deliberada – há outras hipóteses, bem mais graves do que essa, em que essas iniciativas são admitidas em lei – por exemplo, na interceptação telefônica e telemática (art. 3º da Lei das Interceptações Telefônicas). Deixamos essa questão em aberto. A iniciativa probatória judicial e a postulação em juízo por Delegado de Polícia são temas controversos e impossíveis de aprofundar neste trabalho.

37. A requisição de dados pode ter por objetivo a instrução de ação na qual é pretendida tutela inibitória ou de remoção do ilícito. Ver MARINONI, Luiz Guilherme; ARENHART,

O requerente tem o ônus argumentativo de oferecer "justificativa motivada da utilidade dos registros solicitados para fins de investigação ou instrução probatória".

Por fim, deve especificar o "período ao qual se referem os registros". O período deve ser o mais estreito possível, considerando a probabilidade de demonstrar o ilícito em questão.

Note-se que o art. 22 do Marco Civil da Internet não fala em quebra de sigilo de dados pessoais – fala apenas em dados de registro. O art. 10, § 1º, resolve, em parte, essa situação, ao prever que, se requisitados judicialmente associados aos dados de registro, o provedor terá que fornecer "dados pessoais ou a outras informações que possam contribuir para a identificação do usuário ou do terminal".

O Marco Civil da Internet não prevê a requisição autônoma de dados pessoais. Isso demonstra apenas que o legislador preferiu não regulamentar essa questão de forma específica para a internet. A requisição judicial de dados a terceiros, especialmente agentes econômicos, no interesse de processos judiciais, é prática bem consolidada em nosso direito. Não resta dúvida de que dados pessoais podem ser requisitados judicialmente seguindo, no que couber, os parâmetros do art. 22 do Marco Civil.

A requisição deve ser direcionada àquele que dispõe dos dados. Os registros de conexão devem ser requisitados ao provedor de conexão e os registros de acesso a aplicações de internet ao respectivo provedor de aplicação. Demais dados pessoais devem ser requisitados, preferencialmente, ao controlador, pessoa a quem compete as decisões referentes ao tratamento dos dados, na definição do art. 5º, VI, da Lei Geral de Proteção de Dados Pessoais. Caso o controlador esteja inacessível, ou fora do país, temos por viável a requisição ao operador ou ao encarregado (art. 5º, VII e VIII, da LGPD). Em princípio, o procedimento de requisição não é contencioso.[38]

A lei impõe ao juiz o dever de "tomar as providências necessárias à garantia do sigilo das informações recebidas e à preservação da intimidade, da vida privada, da honra e da imagem do usuário" (art. 23 do Marco Civil da Internet). Os dados obtidos devem ser restritos às partes e aos interessados. Se necessário, o segredo de justiça deve ser imposto ao próprio requerimento.

Sérgio Cruz; MITIDIERO, Daniel. *Código de Processo Civil Comentado*. 4. ed. São Paulo: RT, 2018. p. 627.

38. Ver *infra*, capítulo 5.

A grande questão, no caso de dados pessoais, é que a legislação não obriga os provedores a coletá-los e armazená-los, levando à indagação: quais dados podem ser requisitados?

A legislação exige o consentimento expresso do usuário e, ainda assim, limita a coleta e o tratamento dos dados em geral e incentiva a sua exclusão (art. 7º, VIII, IX e X, do Marco Civil da Internet; arts. 7º a 10, 15 e 16 da Lei Geral de Proteção de Dados Pessoais). Atenta a essas normas restritivas, a doutrina fala até mesmo em "princípio da minimização de dados".[39]

Pensamos que, ao menos em princípio, a ordem judicial não deve compelir o provedor a mudar sua política, expandindo a coleta e o armazenamento de dados. Há uma impossibilidade material de fornecer dados que não foram coletados ou que já foram excluídos. Mas também é, em princípio, indevido compelir o provedor a coletar ou a manter dados que ele normalmente não captaria. Por exemplo, não se pode intimar um serviço de mensagens instantâneas a criar um *backup* daquilo que foi dito, se é sua política eliminar as mensagens do servidor logo após a entrega.[40]

De outro lado, temos que quaisquer dados coletados e atualmente armazenados podem ser requisitados. Provedores costumam captar a posição geográfica, ou armazenar o histórico de pesquisas do usuário, dados esses que podem ser de grande interesse em uma investigação. O juiz pode determinar a entrega desses dados.

Uma categoria de dados que merece partilhar atenção diz respeito aos dados de localização. A legislação brasileira trata de forma expressa de sua requisição judicial, se "necessário à prevenção e à repressão de crimes relacionados ao tráfico de pessoas", para "localização da vítima ou de suspeitos do delito em curso" (art. 13-B do CPP).[41] Chega a permitir a requisição direta, por delegado ou membro do MP, caso o juiz demore a despachar o pedido (art. 13-B, § 4º, do CPP).

---

39. SOUZA, Carlos Affonso; LEMOS, Ronaldo; BOTTINO, Celina. *Marco Civil da Internet*. São Paulo: RT, 2017. p. 25.

40. A orientação da jurisprudência, para casos anteriores ao Marco Civil da Internet, é no sentido de que o provedor tem o dever de guardar os dados pessoais necessários à identificação do usuário pelo prazo prescricional de ações de reparação por danos causados a terceiros (REsp 1622483, Rel. Min. Paulo de Tarso Sanseverino, Terceira Turma, julgado em 15.5.2018; REsp 879.181, Rel. Min. Sidnei Beneti, Terceira Turma, julgado em 8.6.2010). Nossa compreensão é de que o Marco Civil inovou, regulando o ônus de coleta e de guarda de dados de registro, e superou a interpretação jurisprudencial.

41. A rigor, em caso de demora do juízo em apreciar o pedido, a lei permite a requisição direta das informações, art. 13-B, § 4º, do CPP.

Muito embora a lei mencione apenas crimes ligados ao tráfico de pessoas, é possível a quebra de sigilo de dados de localização, por ordem judicial, para apuração de quaisquer delitos graves. O interesse por dados de localização para investigações é enorme. Por meio deles, pode ser possível ligar o suspeito (ou, ao menos, seu telefone *smartphone*) à cena do crime.[42] Não temos maiores dúvidas de que é possível requisitar ao provedor que armazena dados de localização os dados de determinado usuário.

Polêmica é a possibilidade de requisitar os dados de localização em massa, usando a técnica de investigação conhecida nos Estados Unidos como *reverse location search* – busca por localização reversa. Tal busca consiste em requisitar ao provedor os dados de todos os usuários que estiveram logados em determinado local e hora. Normalmente, sabendo o momento e o local do crime, mas sem haver suspeitos, a investigação busca identificar todos aqueles que estavam na região para, por eliminação, chegar ao perpetrador.

O problema do *reverse location search* é que ele quebra o sigilo de dados de usuários indefinidos, alcançando terceiros inocentes. Os Estados Unidos registram casos polêmicos, como a quebra de sigilo por 33 horas, em área grande, para investigar roubo a residência.[43]

No Brasil, os primeiros casos que envolvem buscas reversas junto a provedores estão chegando ao Superior Tribunal de Justiça.[44] No entanto, há precedentes envolvendo medida semelhante, a partir de serviços de telefonia – requisição de informações de telefones que acessaram a antena de telefone celular (Estação de Rádio-Base – ERB) próxima ao local do crime em determinado momento. A jurisprudência do STJ formou-se pela validade da requisição.[45]

---

42. O sistema não é imune a falhas e a limitações técnicas. A maior parte das aplicações de internet se contenta com a localização aproximada e sem grau alto de confiabilidade. Se a acusação for fundada nos dados de localização, a acurácia da informação deve ser devidamente investigada.
43. Disponível em: https://www.mprnews.org/story/2019/02/07/google-location-police-search-warrants. Acesso em: 27 jul. 2019.
44. No RMS 61.419 (2019/0212818-0), a liminar foi denegada pelo Min. João Otávio de Noronha, no exercício da Presidência, em 31.7.2019. No RMS n. 59.716/RS, Ministro Sebastião Reis Junior; e na TP n. 292/SP, Ministro Antonio Saldanha Palheiro, os relatores suspenderam a quebra de sigilo.
45. HC 247.331, Rel. Min. Maria Thereza de Assis Moura, Sexta Turma, julgado em 21.8.2014; AgRg no REsp 1.760.815, Rel. Min. Laurita Vaz, Sexta Turma, julgado em 23.10.2018. Os precedentes citados foram formados a partir de contestação das defesas – as companhias telefônicas não tinham por hábito resistir à requisição judicial.

A busca por localização reversa apresenta custo ao direito à intimidade de um número indefinido de usuários. Entretanto, o custo individual à intimidade é modesto, visto que o que se obtém é a localização momentânea do aparelho. Informações adicionais, como a rota do sujeito, dependem de aprofundamento das apurações.

Pensamos que a medida deve ser usada com moderação e apenas se indispensável à apuração de delitos graves. De outro lado, deve-se ter em conta o número de usuários que serão potencialmente atingidos e o custo à privacidade que a identificação com aquele local específico pode representar.

Além disso, deve-se ter o máximo cuidado com os dados de terceiros. Por atingir pessoas não envolvidas no ilícito, o juiz deve redobrar o zelo pelo sigilo dos dados requisitados (art. 23 do Marco Civil da Internet). Na medida do possível, os dados de terceiros não implicados devem ser descartados.[46]

Os dados pessoais, aí compreendidos dados cadastrais e registros de conexão e de acesso a aplicações de internet, têm proteção modesta. São informações periféricas, não correspondem ao conteúdo da comunicação ou da produção intelectual do usuário, pelo que a quebra de sigilo é menos custosa à privacidade e à intimidade. Em algumas hipóteses, dados cadastrais podem ser obtidos por autoridades administrativas, prescindindo de autorização judicial. A requisição dos dados pessoais e de registro submete-se ao art. 22 do Marco Civil da Internet, exigindo, pelo requerente, a comprovação de ilícito – cível ou criminal – e a relevância para o processo. Os dados são requisitados ao controlador, operador ou encarregado.

5. Requisição a terceiros

Há questões comuns à requisição de dados a terceiros, em todas as suas hipóteses, que merecem análise em conjunto. Como visto, a quebra de sigilo de fluxo telemático, de dados armazenados e de dados pessoais, cadastrais e de registro pode ser executada mediante requisição a terceiros.

O terceiro será alguém que tenha acesso ao fluxo de dados, que tenha o controle dos dados armazenados, ou que seja controlador, operador ou encarregado

---

Já os provedores de aplicações na internet adotam por procedimento contestar as ordens judiciais, alegando o dever de proteger a privacidade de seus clientes.

46. Não se pode deixar de considerar, entretanto, que o implicado pode ter interesse sobre o conjunto das informações obtidas. Assim, pode querer saber o número de usuários que estavam no local e, caso opte por uma defesa agressiva, maiores detalhes sobre suas identidades. Esse conflito precisa ser bem avaliado pelo magistrado.

dos dados pessoais. No mais das vezes, a requisição será dirigida a um provedor de conexão ou de aplicação de internet.

O procedimento de requisição em si não é detalhado na Lei de Interceptações Telefônicas, no Marco Civil da Internet, ou em outra lei específica. O procedimento mais próximo é o da requisição de exibição de coisa ou documento a terceiro, previsto nos arts. 380, II, e 401 a 404 do CPC. De acordo com essas disposições, o juiz pode ordenar a exibição de coisa ou documento, sob pena de medidas coercitivas.

A legislação fala em citação do terceiro, com prazo de quinze dias para a resposta (art. 401). Na prática, a requisição costuma ser enviada por ofício ou mandado, sem que se observe uma citação formal. Se houver urgência ou for recomendável pela economia processual, o juiz pode requisitar os dados sem ouvir previamente o controlador.

Se o terceiro apresentar os dados, sem oferecer resistência, não deve ser condenado nos ônus da sucumbência. Trata-se de procedimento de jurisdição voluntária, visto que a ordem judicial de requisição é necessária, por força de lei. O juiz atua como garantidor da privacidade do titular dos dados. O terceiro, em princípio, não tem interesse direto na questão.[47]

Ainda assim, o terceiro tem legitimidade para se opor à ordem. Muito embora não seja o titular dos dados, é o responsável por lei – e muitas vezes também por contrato – pela segurança dos dados contra acessos não autorizados. Se entender que a requisição não está conforme o direito, pode contestar a ordem. Sobrevindo contestação pelo controlador, o juiz deve lhe dar imediata atenção, suspendendo, se for o caso, o cumprimento da ordem.

As hipóteses de negativa de entrega estão nos arts. 402 e 404 do CPC.

A principal hipótese de recusa é a inexistência de acesso ou fluxo ou de controle sobre a informação (correspondente ao art. 402 do CPC). Enquadram-se, nessa hipótese, os casos em que o requerido nega ser o responsável por aquele serviço, nega que o dado foi captado, ou afirma que não mais está armazenado.[48]

A jurisprudência vem enfrentando casos em que o responsável pelos dados está no exterior, mas mantém filial no Brasil. Em face da requisição, a filial

47. REsp 1.068.904, Rel. Min. Massami Uyeda, Terceira Turma, julgado em 7.12.2010.

48. Como comentamos nos capítulos referentes a cada uma das hipóteses de quebra de sigilo de dados, defendemos que o terceiro não é, ao menos em regra, obrigado a mudar sua política para atender à requisição judicial. Se não faz a captação ou armazenamento de determinado dado, não deve ser obrigado a fazê-lo, ainda que para o futuro.

brasileira afirma não ter a posse dos dados (art. 402 do CPC). A matriz, por sua vez, costuma alegar que, de acordo com o direito do país de seu domicílio, está impedida de entregar as informações, salvo mediante ordem das autoridades locais (art. 404, IV, do CPC). Com isso, as autoridades brasileiras só poderiam ter acesso mediante pedido de assistência judiciária internacional.

O Superior Tribunal de Justiça vem rechaçando essa linha de defesa e afirmando a autoridade dos tribunais brasileiros para requisitar dados diretamente à filial aqui localizada.[49]

Esse é um tema com muitas facetas, impossível de ser esgotado neste trabalho. Na forma do Marco Civil da Internet, o direito brasileiro é aplicável a todas as operações que tenham conexão com território nacional (art. 11). Em princípio, a legislação brasileira afirma que a atuação empresarial no país sujeita o estrangeiro a nossa legislação e aos nossos tribunais (art. 1.137 do Código Civil).

A Convenção de Budapeste sobre Crimes Cibernéticos (*Budapeste Convention on Cybercrime*) não impõe restrições à requisição de informações a provedores de serviços estrangeiros, muito embora estabeleça aos países signatários a obrigação de exigir diretamente apenas os dados cadastrais a provedores estrangeiros que oferecem serviços em seu território. Nesse sentido, o artigo 18, 1, *b*, afirma que o direito interno dos países signatários dará aos seus agentes poder de ordenar a "um fornecedor de serviços que preste serviços no território da Parte, que comunique os dados na sua posse ou sob o seu controle, relativos aos assinantes e respeitantes a esses serviços". Para as demais hipóteses, a Convenção deixa a critério de cada país estabelecer limites ao seu próprio poder de requisição. Até pela dificuldade em submeter agentes que não atuam em seu país ao direito interno, a territorialidade pode surgir como um limite ao poder de requisição. Considerando essa realidade, a Convenção estabelece aos signatários o compromisso de prestar assistência internacional "na medida mais ampla possível" – artigo 23.[50]

A concessão a ser feita aos provedores estrangeiros é quanto à inconveniência de submeter a ordens contraditórias sobre o mesmo fato. Assim, é

---

49. Inq 784, Rel. Min. Laurita Vaz, Corte Especial, DJe 28.8.2013; RMS 53.213, Rel. Min. Ribeiro Dantas, Quinta Turma, julgado em 7.5.2019; RMS 53.757, Quinta Turma, Rel. Min. Joel Ilan Paciornik, DJe de 5.11.2018.

50. Está em elaboração o Segundo Protocolo Adicional à Convenção. De acordo com as primeiras minutas, pretende-se estabelecer medidas mais simplificadas de Cooperação e a possibilidade de submeter os provedores de serviço diretamente à jurisdição do Estado requerente, ao menos quanto às informações cadastrais de seus usuários.

aflitiva a situação de um empresário proibido de entregar dados pelo direito de um país e, simultaneamente, obrigado a fazê-lo pelo direito de outro – conflito de jurisdições. A solução para esse problema parece passar por mecanismos de reconhecimento recíproco de ordens judiciais e de simplificação da assistência judiciária internacional.

Ao não atender à requisição judicial, o terceiro submete-se às sanções legais, inclusive à aplicação de multa diária.[51]

Portanto, a requisição ao terceiro é, em princípio, um procedimento não contencioso, mas o terceiro tem interesse em resistir à determinação, aplicando-se os arts. 402 e 404 do CPC. Os mecanismos para obter dados de provedores estrangeiros não são suficientemente eficientes, pelo que é relevante que os países adotem mecanismos de reconhecimento recíproco de ordens judiciais e simplifiquem a assistência judiciária internacional.

CONCLUSÃO

Há três grandes regimes de quebra de sigilo de dados digitais, conferindo maior ou menor proteção à privacidade e à intimidade do usuário. A maior proteção é reservada ao fluxo de dados. Em seguida, com um grau de proteção um tanto menor, estão os dados armazenados. Por último, com uma proteção modesta, os dados pessoais – entre estes, os cadastrais são ainda mais vulneráveis

O fluxo de dados é o estado mais protegido dos dados digitais. A interceptação dos dados telemáticos ocorre em tempo real e adquire todo o conteúdo comunicado, pelo que é muito custosa à privacidade e só pode ser adotada mediante autorização judicial, com o objetivo de apurar crimes graves. A interceptação pode ser executada diretamente, pelas próprias autoridades, ou envolver requisição a terceiros – normalmente, provedores de acesso ou de aplicações de internet.

Os dados armazenados são protegidos pelo direito, ainda que um pouco menos do que o fluxo telemático. Dados armazenados correspondem ao conteúdo das comunicações e da produção humana; no entanto, sua aquisição pode ser muito custosa à privacidade e à intimidade. A quebra de sigilo de dados armazenados somente pode ocorrer com autorização judicial, amparada em juízo

51. REsp 1.560.976, Rel. Min. Luis Felipe Salomão, Quarta Turma, julgado em 30.5.2019; AgRg no RMS 60.005, Rel. Min. Felix Fischer, Quinta Turma, julgado em 7.5.2019; RMS 53.213/RS, Rel. Min. Ribeiro Dantas, Quinta Turma, julgado em 7.5.2019; RMS 53.757, Rel. Min. Joel Ilan Paciornik, Quinta Turma, julgado em 18.10.2018.

de proporcionalidade. Na falta de uma legislação específica, deve-se observar, por analogia, as normas quanto a busca e apreensão, a interceptação telemática e a quebra de sigilo de dados de registro. A quebra de sigilo de dados armazenados não pode ocorrer no interesse da apuração de ilícitos civis ou de delitos leves. A ordem judicial pode ser executada pelos próprios policiais, mediante busca e apreensão de dados, ou mediante requisição a terceiros que sobre eles tenham controle – normalmente, provedores de aplicações de internet.

Os dados pessoais, tais como dados cadastrais e registros de conexão e de acesso a aplicações de internet, têm proteção modesta. Eles são informações periféricas, que não correspondem ao conteúdo da comunicação ou da produção intelectual do usuário, sendo a quebra de sigilo menos custosa à privacidade e à intimidade. Em algumas hipóteses, dados cadastrais podem ser obtidos por autoridades administrativas, prescindindo de autorização judicial. A requisição dos dados pessoais e de registro submete-se ao art. 22 do Marco Civil da Internet, exigindo, pelo requerente, a comprovação do ilícito – cível ou criminal – e da relevância para o processo. Os dados são requisitados ao controlador, operador ou encarregado.

A requisição de dados a terceiro é, em princípio, um procedimento não contencioso, mas o terceiro tem interesse em resistir à determinação, aplicando-se os arts. 402 e 404 do CPC. Os mecanismos para obter dados de provedores estrangeiros não são suficientemente eficientes, pelo que é relevante que os países adotem mecanismos de reconhecimento recíproco de ordens judiciais e simplifiquem a assistência judiciária internacional.