O PROBLEMA DA QUEBRA COLETIVA DE SIGILO DE DADOS PESSOAIS CONTRA PESSOAS INDETERMINADAS

THE PROBLEM OF COLLECTIVE BREACH OF CONFIDENTIALITY OF PERSONAL DATA AGAINST UNDETERMINED PERSONS

Raquel Scalcon

Professora de Graduação e Pós-Graduação da FGV Direito SP. Realizou estágio pós-doutoral na Universidade Humboldt de Berlim/Alemanha. Doutora pela UFRGS. Integrante da Diretoria do IBCCRIM. Advogada.
Link Lattes: http://lattes.cnpq.br/6453281990607428
ORCID: https://orcid.org/0000-0001-9817-9229
raquelscalcon@gmail.com

André da Rocha Ferreira

Mestre em ciências criminais pela PUC-RS. Graduado pela UFRGS. Membro do Departamento de *amicus curiae* do IBCCRIM. Advogado.
Link Lattes: http://lattes.cnpq.br/6101770805111941
ORCID: https://orcid.org/0000-0002-8509-9366
andredarochaferreira@gmail.com

Resumo: Este artigo discute a constitucionalidade de quebras de sigilo de dados pessoais coletivas contra cidadãos indeterminados, questão cuja repercussão geral foi reconhecida pelo Supremo Tribunal Federal (Tema 1.148).

Palavras-chave: Provas digitais; Proteção de dados pessoais; Cidadãos indeterminados.

Abstract: This article discusses the constitutionality of breaches of confidentiality of collective personal data against undetermined citizens in Brazilian law.

Keywords: Digital evidence; Protection of personal data; Indeterminate citizens.

1. Introdução

Após a prática dos atos antidemocráticos do dia 8 de janeiro de 2023, uma das medidas cautelares solicitadas pela Advocacia Geral da União, nos autos do Inq. 4.879, foi que as operadoras de telefonia guardassem os registros de geolocalização de aparelhos telefônicos que estivessem no local dos fatos (Brasil, 2023). A medida remete a outra similar, quando o Ministério Público do Rio de Janeiro solicitou, no curso da investigação do covarde assassinato da vereadora Marielle Franco, que a empresa Google entregasse os números de IP de todos os que tivessem, no período do crime, realizado pesquisas de termos relacionados ao caso (Vieira; Scalcon; Ferreira, 2023).

Os casos demonstram uma nova tendência no Direito Penal, a saber, a tentativa de quebra de sigilo de dados pessoais em investigações criminais de forma coletiva contra pessoas indeterminadas, sem que haja, pois, a devida individualização de seus fundamentos (Vieira; Scalcon; Ferreira, 2023). A questão está em discussão no Supremo Tribunal Federal (STF) no RE 1.301.250 – Tema de Repercussão Geral 1.148 – "Limites para decretação judicial da quebra de sigilo de dados telemáticos, no âmbito de procedimentos penais, em relação a pessoas indeterminadas".

2. Novas tecnologias, dados pessoais e riscos de expansão do poder punitivo

O Direito Penal sempre teve como importante aliada, para sua insidiosa expansão, a tecnologia. O surgimento da prisão; a utilização do discurso médico na origem da criminologia; a identificação de suspeitos a partir das impressões digitais ou amostras de DNA; o uso de câmeras de vigilância e estatísticas para uma suposta prevenção de crimes; enfim, são inúmeros os exemplos em que o Direito Penal se valeu da tecnologia para expandir sua atuação e alterar suas dinâmicas de investigação, repressão e punição (Anitua, 2008; Ferreira, 2021).

Refratários a esse movimento de expansão, correntes da dogmática penal sempre pautaram o debate a respeito da implementação de novas tecnologias no Direto Penal a partir do risco a elas associado. De certa forma, o sistema punitivo é visto sempre por sua instabilidade, de modo que as mínimas mudanças podem trazer um cenário de desrespeito às garantias fundamentais que o limitam, resultando em um crescimento do autoritarismo estatal.

É justamente nesse ponto que se encontra a discussão a respeito da introdução de novos métodos investigativos oriundos da quebra de sigilo de dados pessoais. Com a massificação do uso da internet, principalmente com a popularização do *smartphone*, e, a partir disso, do tratamento de dados pessoais, uma imensa quantidade de informação passou a ficar acessíveis para as agências de segurança pública e para as investigações criminais.

É necessário, contudo, entender quais tipos de informações estão validamente à disposição das autoridades públicas — e à luz de quais critérios constitucionais e legais. Nesse sentido, salienta-se que o Marco Civil da Internet (MCI) regula a entrega de dois tipos de dados para fins de investigação criminal. O primeiro seriam os dados cadastrais (qualificação pessoal e endereço do usuário). Para esse tipo de dado pessoal, cuja revelação implica menor dano à privacidade em casos de investigação criminal, o MCI autoriza sua entrega a partir de mera requisição da autoridade administrativa competente para tanto (art. 10, § 3º) (Brasil, 2014).

A Lei traz, ainda, a possibilidade de entrega dos chamados metadados, os dados sobre dados. Ou seja, são informações que descrevem e circunscrevem outra informação, geralmente o conteúdo de algo em si. Para exemplificar, os dados de catálogo em um livro da biblioteca (metadados) são as informações que permitem acessar ao conteúdo do livro em si (dado). Assim, para fins de investigação criminal, o MCI subdivide os metadados em duas categorias, determinando sua guarda por determinado período: (i) os registros de conexão devem ser armazenados pelas operadoras de internet por um ano; (ii) os registros de acesso, pelas provedoras de aplicações, por seis meses.[1]

Registros de conexão são os registros que ficam sob a guarda das empresas de telecomunicação, que permitem o acesso à internet e estão relacionados com o número de IP e momento em que uma determinada conexão de internet se iniciou. Registros de acesso a aplicações de internet são os metadados referentes à utilização de serviços *on-line* (Google, redes sociais, demais aplicativos).

No caso do RE 1.301.250 — Tema de Repercussão Geral 1148/STF —, há um pedido de acesso ao conteúdo das informações geradas pela internet, o que, aparentemente, não encontraria guarida nas autorizações do MCI (não seriam registros de conexão nem registros de acesso). Com relação à investigação dos atos antidemocráticos, há de se indagar se registros de localização poderiam ser enquadrados na expressão legal "conjunto de informações referentes à data e hora de uso de uma determinada aplicação de internet" (registro de acesso – art. 5º, inc. IV, MCI), o que, em caso positivo, conferiria embasamento legal ao pedido. O ponto, contudo, não é isento de controvérsia.

Dessa forma, o que se constata da leitura do MCI é que ele permite a entrega, para as autoridades de segurança, apenas de metadados e, mais ainda, apenas de alguns metadados (art. 5º, inc. VI a VIII, MCI). Retomando-se o exemplo do livro na biblioteca, haveria possibilidade de acesso aos registros do catálogo, mas não ao conteúdo do livro em si. Tal decisão do legislador se deu, com razão, para limitar o perigoso acesso de autoridade a uma enorme quantidade de informações e de dados pessoais.

Em resumo, o art. 10, §3º, do MCI, autoriza a entrega de dados cadastrais com requisição da autoridade administrativa, enquanto os artigos 13 e 15 do MCI determinam a guarda de metadados pelo período de um ano nos casos de registros de conexão e de seis meses no caso de registros de acesso (art. 5º, inc. VI e VIII, MCI), cujo acesso está protegido por reserva de jurisdição (art. 22 e 23. MCI). Contudo, além da adequada interpretação desses dispositivos legais, é necessário compreender os limites de uma decisão que autoriza a entrega dos dados no âmbito de uma investigação criminal.

3. Quebras de sigilo coletivas indeterminadas em investigações criminais são constitucionais?

Retomando os casos enunciados quando da abertura do texto, observa-se que ambos buscam identificar, a partir da quebra de sigilo de dados pessoais, a responsabilidade pessoal por um delito. Da mesma forma, ambos compartilham o risco de uma expansão do poder das agências de investigação criminal ainda não definitivamente avaliada, em sua constitucionalidade e legalidade, pelos Tribunais brasileiros. Trata-se da possibilidade de se investigar uma coletividade de pessoas, a partir da quebra do sigilo de dados pessoais, sem a necessidade de uma individualização específica dos fundamentos da quebra para cada um dos atingidos, o que denominados de "quebra coletiva indeterminada". Em tais casos, sequer se poderia antecipar quem e quantos seriam atingidos pela quebra em si (Vieira; Scalcon; Ferreira, 2023).

Daí se indagar: é constitucionalmente válido que o Estado obtenha tamanho espectro de dados pessoais para fins persecutórios? Quais seriam os limites que uma eventual decisão judicial de quebra de sigilo de dados pessoais deveria respeitar? Historicamente, o direito à privacidade e ao sigilo das comunicações (art. 5, inc. XII, da CF) foi utilizado pela jurisprudência como um limitador desse tipo de medida. Na interpretação jurisprudencial ainda dominante, a proteção constitucional não se referiria, todavia, ao conteúdo das informações, mas ao seu fluxo, o que não seria o mesmo.

De maneira simplificada, esse entendimento consideraria haver proteção constitucional sobre o caminho da comunicação, mas não sobre a informação armazenada em si, o que se convencionou chamar de "dado armazenado". Essa compreensão, contudo, em nada acompanha as mudanças tecnológicas nem a maneira como se dão as comunicações hoje. Ademais, ela daria margem, por exemplo, a decisões que não consideram o conteúdo de mensagens de *e-mails* (dado armazenado) como algo protegido constitucionalmente (Brasil, 2020a).

É perceptível que mesmo o direito fundamental à privacidade não dá conta de tutelar a maneira pela qual os dados pessoais são tratados por novas tecnologias — tampouco controla os incontáveis riscos advindos dessa prática. Não por acaso, a última década foi marcada pelo desenvolvimento e pelo fortalecimento da disciplina de proteção de dados. No Brasil, ela é constitucionalmente representada pelo direito fundamental à proteção de dados pessoais (art. 5º, inc. LXXIX, CF), pelo reconhecimento do direito à autodeterminação informativa pelo Plenário do STF (Brasil, 2020b) e pela legislação infraconstitucional, principalmente o já citado MCI e a Lei Geral de Proteção de Dados (LGPD).

Nosso país ainda não conta com uma legislação específica para o tratamento de dados em âmbito criminal, mas a LGPD determina sua realização, bem como que os princípios que a regem sejam replicados na futura legislação.[2] Todavia o desenvolvimento da disciplina de proteção de dados, acima relatado, não deixa dúvidas: os limites das decisões de quebra de sigilo de dados pessoais devem passar por uma análise dos princípios e das regras que fundamentam a disciplina da proteção de dados, a privacidade,

o sigilo das comunicações, além, é claro, daqueles afeitos ao Direito Penal, sendo necessária uma profunda ressignificação da jurisprudência sobre o tema pró-cidadão.

Essa mudança jurisprudencial passa pelo abandono da arcaica concepção de "dado armazenado", para a adoção completa do conceito de "dado pessoal" no Direito Penal.[3] A partir da adoção desse conceito, o espectro de proteção se alargará, passando a estar "pareado" com os riscos relacionados ao tratamento de tais dados. Esse movimento jurisprudencial já pode ser vislumbrado em algumas decisões do STF, sendo inclusive evocada uma "mutação constitucional" (Brasil, 2020c) no tema, o que tende a ser confirmado — ou, ao menos, debatido — no julgamento de duas importantes ações que tramitam na Suprema Corte. A primeira é o Recurso Extraordinário com Agravo 1.042.075, que debate a legalidade do acesso a dados pessoais de celular apreendido sem decisão judicial (Tema 977/STF); a segunda, a ADIn 5.063, que tem por objeto a constitucionalidade dos artigos 15, 17 e 21 da Lei de Organizações Criminosas, os quais permitiriam, no curso de investigações, que a autoridade investigante obtivesse dados cadastrais sem necessária autorização judicial. Ademais, o próprio RE 1.301.250, Tema 1.148/STF, ainda sem previsão de pauta, irá necessariamente abordar essa importante questão.

Mas qual a repercussão desse panorama para os pedidos coletivos de quebra de sigilo de dados pessoais contra cidadãos indeterminados? Veja-se que o argumento central para a medida cautelar probatória, nos dois casos citados ao início deste artigo, é de que, em sendo desconhecida a autoria delitiva, não seria possível a individualização seja do pedido, seja da quebra em si.

De fato, a identificação da autoria através de um dado pessoal pode ser, sim, uma técnica investigativa muito eficiente, na medida que se vale de "um rastro" deixado quando do cometimento do delito (geolocalização e número de IP, nos casos analisados). Isso, contudo, é um argumento pragmático do qual não deriva, logicamente, sua constitucionalidade. A prática, se expandida para além dos casos concretos, poderia se assemelhar à chamada "*fishing expedition*" (procura especulativa) relacionada à obtenção de provas contra alguém sem que haja uma razão prévia para, a partir daí, justificar uma acusação (Silva; Melo e Silva; Da Rosa, 2019, p. 41).

4. Considerações finais

De forma provisória, conclui-se que, considerando a reserva de lei necessária a qualquer intervenção em direitos fundamentais, o ordenamento jurídico brasileiro atual, pelas razões acima trazidas, não possuiria regras legais que amparem decisões judiciais que venham a determinar, para fins de persecução penal, uma quebra de dados pessoais coletiva contra pessoas indeterminadas.

Quanto às quebras de sigilo de dados pessoais contra um pessoa individualizada ou contra um grupo de pessoas claramente pré-delimitado, alguns critérios mínimos devem ser adotados: (i) a adequação da jurisprudência criminal do País de modo a respeitar o direito fundamental à proteção de dados, iniciando-se pelo abandono do termo "dado armazenado" e pela adoção do conceito de "dado pessoal", fazendo com que os princípios inerentes à matéria sejam incorporados em qualquer procedimento criminal que envolva dados pessoais; (ii) o dado ou metadado em si que o Estado pretende obter com a quebra deve estar entre aqueles cuja utilização, para fins de persecução penal, está legalmente autorizada; (iii) a decisão deve garantir o respeito aos princípios da proteção de dados, notadamente os trazidos pela LGPD, inclusive devendo haver adequação das agências de segurança para tanto; e, (iv) além de outros princípios de Direito Penal, deve haver atenção para a existência de *fumus delicti comissi* (e *periculum in mora*) por parte de cada titular do dado pessoal, com justificação da efetividade da medida para o caso concreto.

Notas

[1] A própria Lei define o que são registros de conexão e de acessos a aplicações em seu art. 5º: "VI - registro de conexão: 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; VII - aplicações de internet: o conjunto de funcionalidades que podem ser acessadas por meio de um terminal conectado à internet; e, VIII - registros de acesso a aplicações de internet: o conjunto de informações referentes à data e hora de uso de uma determinada aplicação de internet a partir de um determinado endereço IP".

[2] LGPD, Art. 4º - "Esta Lei não se aplica ao tratamento de dados pessoais: [...] III - realizado para fins exclusivos de: a) segurança pública; b) defesa nacional; c) segurança do Estado; ou d) atividades de investigação e repressão de infrações penais [...] § 1º O tratamento de dados pessoais previsto no inciso III será regido por legislação específica, que deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular previstos nesta Lei." (Brasil, 2018).

[3] A definição de dado pessoal no MCI é dada pelo seu Decreto Regulamentador (8.771): "art. 14. Para os fins do disposto neste Decreto, considera-se: I - dado pessoal - dado relacionado à pessoa natural identificada ou identificável, inclusive números identificativos, dados locacionais ou identificadores eletrônicos, quando estes estiverem relacionados a uma pessoa". Também a LGPD, posterior e com maior hierarquia, traz o conceito de "dano pessoal" em seu artigo 5º, inc. I: "dado pessoal: informação relacionada a pessoa natural identificada ou identificável".

Referências

ANITUA, Gabriel Ignácio. *Histórias do pensamento criminológico.* Rio de Janeiro: Revan, 2008.

BRASIL. *Lei 12.965, de 23 de abril de 2014*. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília: Presidência da República, 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 10 ago. 2023.

BRASIL. *Lei 13.709, de 14 de agosto de 2018*. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília: Presidência da República, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 10 ago. 2023.

BRASIL. Superior Tribunal de Justiça. AgRg no RMS 63041, 5ª Turma, Rel. Min. Ribeiro Dantas. Brasília, DF, 17 de novembro de 2020a. Disponível em: https://scon.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=202000479211&dt_publicacao=23/11/2020. Acesso em: 10 ago. 2023.

BRASIL. Supremo Tribunal Federal. ADI 6387; 6388; 6389; 6390; 6393, Plenário, Rel. Min. Rosa Weber. Brasília, DF, 6 e 7 de maio de 2020b.

BRASIL. Supremo Tribunal Federal. *HC* 168052, 2ª Turma, Rel. Min. Gilmar Mendes. Brasília, DF, 20 de outubro de 2020c. Disponível em: https://portal.stf.jus.br/processos/detalhe.asp?incidente=5635177. Acesso em: 10 ago. 2023.

BRASIL. Supremo Tribunal Federal. Inq. 4.879, Rel. Min. Alexandre de Moraes. Brasília, DF, 8 de janeiro de 2023. Disponível em: https://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/DECISA771OAfastagovernadoreoutrasmedidas2.pdf. Acesso em: 10 ago. 2023.

DA ROSA, Silva, Viviani Ghizoni da; MELO E SILVA, Philipe Benoni; DA ROSA, Alexandre Morais. *Fishing expedition e encontro fortuito na busca e na apreensão*: um dilema oculto no processo penal. Florianópolis: Emais, 2019.

FERREIRA, André da Rocha. Tratamento de dados pessoais em investigações criminais: o direito fundamental à autodeterminação informativa como limite constitucional. *Revista Brasileira de Ciências Criminais*, v. 29, n. 185, p. 115-159, nov. 2021.

VIEIRA, Renato Stanziola; SCALCON, Raquel; FERREIRA, André da Rocha. Quebras de sigilo coletivas indeterminadas. *O Estado de São Paulo*, 26 de julho de 2023. Disponível em: https://www.estadao.com.br/opiniao/espaco-aberto/quebras-de-sigilo-coletivas-indeterminadas/. Acesso em: 10 ago. 2023.

Autores convidados