Adriana Rizzotto: Proteção de dados pessoais na persecução penal

O plenário do Supremo Tribunal Federal atualizou a proteção constitucional do direito à privacidade ao reconhecer a proteção de dados pessoais como categoria autônoma no rol de direitos fundamentais, com conteúdo normativo independente do direito ao sigilo das comunicações. Esse reconhecimento permite que se extraia do texto constitucional possibilidades interpretativas com impacto direto nos critérios de investigações criminais.

Em sessão realizada por videoconferência, dez ministros referendaram a medida cautelar deferida pela ministra Rosa Weber no julgamento conjunto de ações diretas de inconstitucionalidade [1] ajuizadas contra o inteiro teor da medida provisória [2] que dispõe sobre o compartilhamento de dados cadastrais de usuários por prestadores de serviço de telecomunicações com a Fundação Instituto Brasileiro de Geografia e Estatística (IBGE), durante a emergência sanitária decorrente da Covid-19. O ato normativo impugnado determina a disponibilização, ao IBGE, em meio eletrônico e caráter sigiloso, da relação de nomes, números de telefone e endereços de consumidores, com o objetivo de realizar censo virtual para a produção estatística oficial. Superada a situação emergencial, as informações compartilhadas seriam eliminadas das bases de dados do IBGE, no prazo de 30 dias.

No que tange à alegação de inconstitucionalidade material, prevaleceu o entendimento de que a ingerência estatal na esfera jurídica individual foi indevida, em razão de ser excessivamente ampla e deficitária de salvaguardas efetivas mínimas para a proteção do direito fundamental à proteção de dados pessoais. A relativização da proteção constitucional somente pode ser realizada em caráter excepcional e por legítimas intervenções de interesse público, condicionadas ao atendimento dos seguintes critérios: finalidade e amplitude específicas, acesso permitido na extensão mínima comprovadamente necessária ao atendimento do objetivo estabelecido, e adoção de procedimentos de segurança adequados para prevenção de danos, como vazamentos acidentais e utilização indevida.

Na seara processual penal, os novos parâmetros constitucionais estabelecidos pela Suprema Corte brasileira tornam definitivamente obsoleta a sua atual jurisprudência, fundamentada na compreensão de que dados em si, tais como registros telefônicos, não são objeto de proteção constitucional, que somente abrange as comunicações telefônicas realizadas [3]. A autoridade policial, na atuação de seu mister, pode obter informações armazenadas na memória de aparelho celular ligado à prática delitiva, independentemente de autorização judicial ou permissão do proprietário. Esse posicionamento tem sido sistematicamente confrontado pelo Superior Tribunal de Justiça, cuja jurisprudência consolidou-se em sentido diverso [4], em razão do advento de novas circunstâncias fáticas.

Com o avanço tecnológico, o aparelho celular deixou de ser apenas instrumento de conversação por voz à longa distância, com agenda de contatos e histórico de ligações. *Smartphones* multifuncionais são dotados de grande capacidade de armazenamento de dados pessoais, tais como fotos, áudios, vídeos e documentos, que, uma vez acessados, revelam dossiês completos sobre o comportamento do proprietário . A proteção constitucional visa a impedir devassas desarrazoadas, como as famigeradas *fishing expeditions*, meio de obtenção de prova arbitrário e incompatível com os postulados de uma sociedade democrática.

De acordo com pesquisa do IBGE [5], em 98,7% dos domicílios brasileiros em que há acesso à internet o celular é utilizado para esse fim. No âmbito normativo infraconstitucional, o artigo 7º, III, do Marco Civil da Internet [6] dispõe que o acesso à rede é essencial ao exercício da cidadania, e ao usuário é assegurada a inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial.

Diante das novas premissas fáticas e jurídicas acima alinhavadas, a jurisprudência do STF já começou a ser revisitada pela 2ª Turma, com o início do julgamento de Habeas Corpus em que se discute a nulidade de processo penal no qual a autoridade policial teve acesso, sem autorização judicial, ao aparelho celular do paciente obtido em diligência de busca e apreensão, bem como às conversas travadas no aplicativo *WhatsApp*. O ministro relator votou pela concessão da ordem para anular as provas obtidas mediante acesso não autorizado, constatou a ilicitude por derivação das demais provas, declarou nulo o processo e determinou o trancamento da ação e a absolvição do paciente [7]. A matéria teve repercussão geral reconhecida [8] e será apreciada pelo plenário do STF no julgamento do Tema 977.

Noutro giro, destoa da orientação do STF a jurisprudência do STJ que afirma a desnecessidade de autorização judicial para acesso aos dados de identificação de horário, duração e geolocalização de chamadas de celulares, obtidos em registros de torres de telefonia, as denominadas Estação Rádio Base (ERB) [9]. O STJ sinaliza que esses dados podem ser obtidos diretamente, em razão de serem externos à comunicação telemática.

No paradigmático caso *Carpenter v. United States* [10], a Suprema Corte dos Estados Unidosdeliberou que acessar dados que registram o histórico de localizações físicas de celular sem mandado judicial viola a 4ª Emenda Constitucional. O telefone celular é praticamente uma extensão da anatomia humana e a sua localização, a mesma de seu proprietário. Outro ponto problemático é que os registros das torres de celular fornecem informações representativas da personalidade privada dos usuários de telefonia que utilizaram o serviço no local e tempo da prática delituosa, mas que não têm qualquer ligação com o crime investigado, assim como de outras pessoas relacionadas ao suspeito, que nada tem a ver com a ação delituosa. Intervenções estatais na legítima expectativa de privacidade dos afetados pela quebra de sigilo, portanto, devem ser submetidas à prévia decisão judicial, capaz de demonstrar a necessidade, adequação e proporcionalidade da pretensão dos órgãos de persecução penal.

A Lei do Tráfico de Pessoas [11] adotou posicionamento mais estrito do que o STJ ao prever clá usula de reserva de jurisdição temporária para a requisição, às empresas prestadoras de serviço de telecomunicações, de informações sobre aparelhos que utilizam antena de torres de celular que permitam a localização da vítima ou dos suspeitos de delito em curso, sendo dispensada a ordem do juiz apenas se não houver manifestação judicial no prazo de 12 horas.

Os contornos jurídicos do novo direito fundamental à proteção de dados pessoais tornam superada, outrossim, a distinção conceitual, firmada nos tribunais superiores, entre *dados* constitucionalmente protegidos, reveladores de aspectos da vida privada, e *dados cadastrais*, elementos identificadores objetivos que não permitem a criação de juízo de valor a partir de sua divulgação. Essa compreensão parte da premissa que dados cadastrais não revelam informações sensíveis e, portanto, não há motivo plausível para a cláusula de reserva de jurisdição [12].

A Lei Geral de Proteção de Dados (LGPD) [13] aborda a questão de forma diferenciada, ao determinar que dado pessoal sensível consiste naquele *"sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural"*.

O quadro fático em que se firmou a jurisprudência dos tribunais superiores ora comentada também mudou drasticamente, com a emergência de tecnologias que permitem a coleta, o cruzamento e a análise de grande variedade e volume de dados digitais, com extraordinária velocidade de processamento e finalidade de gerar conclusões significativas, reveladoras de tendências e padrões comportamentais, o denominado *Big Data*.

Dados pessoais aparentemente insignificantes são processados por algoritmos poderosos, que procedem o seu agrupamento, cruzamento, refino e posterior conversão em perfis psicológicos discriminatórios de identidade. Esses perfis são frequentemente monetizados e retornam ao titular, em efeito bumerangue, de forma personalizada e manipulada para moldar comportamento social e influenciar hábitos de consumo. Todo esse processo, que reduz drasticamente a autonomia da vontade e o livre arbítrio da pessoa humana, desenvolve-se à revelia do titular dos dados, que se encontra em situação de vulnerabilidade extrema, na esfera inviolável da sua vida privada.

Na persecução penal, a mineração de dados constitui ferramenta de grande relevância na investigação de crimes de alta complexidade, praticados por organizações criminosas. A segurança pública também é otimizada por estruturas de *Big Data* como o *Detecta*, sistema de monitoramento inteligente implantado pelo Governo do Estado de São Paulo, que integra múltiplos bancos de dados com câmeras de vídeo

monitoramento e outras soluções de inteligência artificial para acompanhar situações suspeitas, prevenir e elucidar crimes. Nesse cenário *orwelliano*, em que o perigo de vigilância indiscriminada e desenvolvimento de algoritmos com viés discriminatório constitui possibilidade concreta, a amplitude do poder requisitório do Ministério Público e da autoridade policial não está livre de críticas e deve ser calibrada pelo direito fundamental à proteção de dados pessoais.

O poder requisitório dos órgãos de persecução penal tem fundamento na teoria dos poderes implícitos, bem como em normas específicas autorizadoras de acesso direto, como as contidas em leis de enfrentamento à lavagem de dinheiro [14], ao crime organizado [15] e ao tráfico de pessoas [16]. Apesar de a LGPD não ser aplicável ao tratamento de dados pessoais realizado para fins exclusivos de segurança pública, investigação e repressão de infrações penais, o dever genérico de sigilo na fase inquisitorial constitui tutela insuficiente do novo direito fundamental em jogo, que reclama a adoção de *standards* abrangentes de proteção, mediante a efetivação da garantia do devido processo legal no trato de dados pessoais sensíveis.

As profundas transformações tecnológicas da sociedade da informação tornaram necessária a reconfiguração jurídica do direito à privacidade, com a ampliação do sentido e alcance da proteção conferida aos dados pessoais, promovida pelo STF à categoria de direito fundamental autônomo, que atua como importante escudo protetor da dignidade da pessoa humana na era digital, inclusive no âmbito da persecução penal.

[1] ADIs 6.389, 6.390, 6.393, 6.388 e 6.387.

[2] MP nº 954/2020.

[3] HC 91.867/ PA, 2a Turma, Rel. Min Gilmar Mendes, DJe 20/09/2012.

[4] HC 51.531/RO, 6ª Turma, Rel. ministro Nefi Cordeiro, DJe 09/05/2016 e RHC 67.379/RN, 5ª Turma, Rel. ministro Ribeiro Dantas, DJe 09/11/2016.

[5] https://biblioteca.ibge.gov.br/visualizacao/livros/liv101631_informativo.pdf

[6] Lei nº 12.965/2014.

[7] HC 168.052/SP 2ª Turma Rel. Min Gilmar Mendes, em julgamento, Informativo 944.

[8] ARE 1.042.075, Rel. Min Dias Toffoli, em julgamento.

[9] HC 247.331/RS, 6a Turma, Rel. ministro Maria Thereza de Assis Moura, DJe 03/09/2014; AgRg no REsp 1760815/ PR, 6a Turma, Min Laurita Vaz, DJe 13/11/2018.

[10] 585 U. S. (2018).

[11] Artigo 13-B do CPP, incluído pela Lei nº 13.344/2016.

[12] Resp 1.561.191/SP, 2a Turma, Rel. Min Herman Benjamin, DJe 26/11/2018; RHC 82868/MS, 5a Turma, Rel. Min Felix Fischer, DJe 01/08/2017.

[13] Artigo 5, II, da Lei nº 13.709/2018.

[14] Artigo 17-B da Lei nº 9.613/1998, incluído pela Lei nº 12.683/2012.

[15] Artigo 15 da Lei nº 12.850/2013.

[16] Artigo 13-A do CPP, incluído pela Lei nº 13.344/2016.

Date Created
08/06/2020