Revista do Advogado

Nº 144 | NOV | 2019

AASP

Lei Geral de Proteção de Dados Pessoais

Proteção de dados pessoais e persecução criminal à luz da LGPD.

Jacqueline de Souza Abreu
Doutoranda em Direito na Universidade de São Paulo, Departamento de Filosofia e Teoria Geral do Direito. Mestra em Direito pela University of California, Berkeley (EUA) e pela Ludwig-Maximilians-Universität München (Alemanha). Advogada.

Sumário

A Lei Geral de Proteção de Dados (LGPD ou Lei nº 13.709/2018) entrará em vigor em agosto de 2020 sem força vinculante para operações de tratamento de dados pessoais para fins exclusivos de atividades de investigação e repressão de infrações penais. Este breve artigo apresenta um panorama do presente e do futuro da intersecção entre privacidade, proteção de dados e processo penal, em atenção à chegada da LGPD: como é o cenário hoje e como ele ficará com a entrada em vigor da LGPD até e se a promessa de uma "lei específica" se tornar realidade.

1 Como é hoje: privacidade e processo penal

A privacidade coloca diversos limites à persecução criminal. Alguns são de natureza fática: o quanto a polícia pode apurar de informações sobre quem alguém é, o que ele tem e o que ele fez depende da existência de algum tipo de registro sobre essas informações: se foram coletadas, se estão publicadas em meios abertos, se são conhecidas por ou estão na posse de alguém. Investigações não avançam

sem certa disponibilidade de elementos de informação que permitam a reconstrução histórica do fato investigado – e alguém não é punido, ou pelo menos não deve ser, sem que haja comprovação de que praticou ou concorreu para um tal fato criminoso.

Outros limites são mesmo de natureza jurídica: para utilizar meios de prova que afetam a privacidade, autoridades de investigação devem percorrer certos procedimentos – sobretudo e paradigmaticamente, convencer uma autoridade judicial de que há razões que demonstram por que há justa causa para uma quebra de sigilo e por que ela é necessária para a investigação. Basta pensar no exemplo clássico das interceptações telefônicas, que interferem no sigilo das comunicações e são reguladas pela Lei nº 9.296/1996: para que a autoridade policial possa ouvir as ligações de alguém, deve existir autorização judicial que ateste a existência de indícios de envolvimento do alvo em crime punível com reclusão e a impossibilidade de apuração por outros meios (art. 2º).

A proteção de dados ensejaria camada regulatória adicional da atuação policial.

Grande parte das controvérsias jurídicas sobre prerrogativas investigativas se dá nesse contexto e envolve, como pergunta inicial, o seguinte questionamento: a medida investigativa afeta mesmo um direito à privacidade? Nos termos da nossa Constituição, as perguntas giram principalmente em torno dos conceitos de "intimidade", "vida privada", "inviolabilidade" da "casa" (domicílio) e do "sigilo das comunicações" (art. 5º, incisos X, XI e XII). Em geral, concluir que um direito à privacidade é mesmo afetado significa impor, se não limites absolutos, pelo menos barreiras procedimentais à execução da medida. Quanto maior a intervenção, mais exigentes os requisitos.

Para autoridades de investigação, interessa restringir ao máximo as situações em que se entende que um "direito à privacidade" é afetado – o que significa menos obstáculos formais e materiais para a obtenção das informações e avanço de linhas investigativas. É por isso, portanto, que com frequência se vê autoridades policiais defendendo prerrogativas de acesso "direto" (sem autorização judicial) a dados por mera requisição sob o fundamento de que não são cobertos por "sigilo", por serem informações de "cadastro" ou de "registro" que não afetariam a privacidade (*vide*, por exemplo, a ADI nº 5.059). Variantes desse argumento aparecem em discussões atuais sobre compartilhamento de relatórios do Conselho de Controle de Atividades Financeiras com o Ministério Público (RE nº 1055941) ou sobre acesso de policiais a celulares encontrados em cenas de crimes (ARE nº 1042075) e em situações de flagrante (HC nº 168052), que estão no Supremo Tribunal Federal.

Quando se fala em medidas investigativas potencialmente mais invasivas que uma interceptação telefônica, por outro lado, autoridades de investigação por vezes também tentam responder a preocupações com a privacidade simplesmente propondo estender o âmbito de aplicação da Lei nº 9.296/1996 – para que outros obstáculos além dos tradicionais dessa lei não sejam adicionados. É o que se vê em discussões atuais do Projeto Anticrime (PL nº 882) sobre interceptações de sinais eletromagnéticos, ópticos ou acústicos (ambientais) – com a instalação de uma câmera com gravador em um ambiente privado – ou uso de *software* espião (*malware*) para invasão de dispositivos eletrônicos (e acesso a todos os dados armazenados e monitoramento de todas as atividades em tempo real, inclusive com capacidades de edição) (BORBA; NERY, 2015), por exemplo.

De um lado ou de outro, como se vê, os contornos e o sentido como compreendemos o direito à privacidade são cruciais para o delineamento de mais ou menos limites para o emprego de medidas

investigativas e a avaliação de quais são pertinentes. A lógica ainda é traçar limites entre o que é público e aquilo que é privado. Sob esse paradigma, não há por que regular atividades sobre o que a polícia apura de informações públicas, por exemplo. "Privacidade não é afetada", dizem. Bem, neste ponto será preciso reconhecer que a privacidade já não anda desacompanhada: o direito da proteção de dados pessoais adiciona novas nuances e preocupações ao cenário.

2 Como fica: LGPD, proteção de dados pessoais e processo penal

O direito da proteção de dados pessoais é uma resposta jurídica para novas circunstâncias fáticas que moldam a privacidade. A crescente capacidade computacional alterou profundamente o modo como lidamos com informações – inclusive pessoais: entidades públicas e privadas coletam, transmitem, analisam, armazenam e agregam em escala **dados** que identificam ou podem identificar pessoas ou que constituem registros e vestígios sobre atividades e comunicações de pessoas (DONEDA, 2006; MENDES, 2014). Atividades que antes fazíamos em público e que permaneciam sem registros ou na obscuridade agora são rastreáveis por câmeras, *drones* e dispositivos celulares, por exemplo.

Essa era informacional, responsável por revoluções na economia e na Administração Pública (IGO, 2018), não está livre de riscos: desde o **vazamento** de uma informação pessoal confiada a uma entidade, caindo na mão de agentes maliciosos – como dados de acesso a uma conta bancária *on-line* ou a uma conta de *e-mail* profissional – até o uso ou a exploração completamente inesperada dessa mesma informação pessoal confiada para o uso específico pela mesma entidade ou por terceiro – ou o uso de dados pessoais (ou inferências extraídas de dados pessoais) – até mesmo equivocados – para tomada de decisões de forma discriminatória (SOLOVE, 2006).

Nesse cenário surge um novo ramo do Direito, voltado a garantir direitos a titulares de informações que resguardem certa medida razoável de controle e impor e fazer valer (com estruturas de supervisão) certos requisitos e parâmetros para operações de tratamento de dados pessoais, com o objetivo de evitar que operações abusivas ocorram e oferecer remédios para o caso de ocorrerem. Entre os princípios básicos que norteiam a matéria se destacam o **princípio da limitação da coleta**, segundo o qual dados devem ser obtidos de forma lícita, justa e transparente; o **princípio da finalidade legítima** (ou especificação do propósito), segundo o qual os objetivos de uso de dados coletados devem ser anunciados antes da coleta e vinculam as operações que podem ser feitas com tais dados, não podendo ser desvirtuados a não ser com consentimento do titular ou por dever legal; o **princípio da segurança**, segundo o qual dados pessoais devem ser protegidos contra riscos de perda ou acesso, destruição, uso ou modificação não autorizadas por meio de técnicas e boas práticas de segurança da informação; e o **princípio da prestação de contas**, segundo o qual detentores de dados devem estar sujeitos a mecanismos de responsabilização em caso de inobservância dos princípios e regras de proteção de dados pessoais.

A LGPD (ou Lei nº 13.709/2018) se insere nesse contexto e nasce com esses compromissos. Na área da persecução criminal, o direito da proteção de dados pessoais ensejaria uma camada regulatória adicional da atuação policial. Como o processo penal, suas regras e princípios serviriam para a canalização da conduta estatal que trata dados pessoais para fins de prevenção e repressão a condutas criminosas, de modo a também nessa área criar uma arquitetura de proteção contra coleta e uso de informações pessoais de forma indevida (DE HERT; GUTWIRTH, 2006). O poder de **controle** do indivíduo sobre o fluxo das informações nela perderia força frente ao interesse público na segurança, de modo que a noção de "consentimento" sobre o

tratamento de dados é praticamente anulada. No entanto, permaneceriam com toda a força os princípios da finalidade legítima, o princípio da segurança e o da prestação de contas, por exemplo.

A Lei de Acesso à Informação continuará uma importante aliada na obtenção de informações.

Como antecipei logo no início, a LGPD não se aplicará, entretanto, a operações de tratamento de dados pessoais para fins exclusivos de atividades de investigação e repressão de infrações penais (art. 4º, inciso III, alínea *d*). Isso significa que o regime atual de "desproteção" de dados nessa matéria tende a se perpetuar até que eventual legislação específica – uma promessa contida na lei (art. 4º, § 1º) – se torne realidade, prevendo

"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".

Ainda assim, esse recorte material não pode ser compreendido como carta branca – e neste ponto é importante afastar ao menos duas compreensões equivocadas. Em primeiro lugar, o recorte não significa que autoridades encarregadas de investigação e repressão a infrações penais não devem se preocupar com proteção de dados pessoais. Há diversas razões para isso. **Primeiro**, porque a exclusão do âmbito de aplicação está vinculada ao tipo de tratamento – operações com fins **exclusivos** de investigação e repressão de infrações penais, podendo haver instâncias em que a Polícia Civil ou o Ministério Público se engajam em operações de tratamentos de dados pessoais para fins de apurações administrativas internas ou mesmo para pagamento de pessoal. **Segundo**, porque seria paradoxal e incoerente aceitar que a atuação dessas autoridades pudesse atropelar princípios básicos de proteção de dados, podendo se esperar que se espelhem tanto quanto possível nos direitos e princípios da LGPD, conforme já sugere o próprio texto do art. 4º, § 1º. **Terceiro**, porque a LGPD impõe à Autoridade Nacional de Proteção de Dados o dever de solicitar "aos responsáveis relatórios de impacto à proteção de dados pessoais" e lhe dá a prerrogativa de emitir opiniões técnicas e recomendações (art. 4º, § 3º), de modo que deverão estar preparados a elaborá-los e a acolhê-las.

Em segundo lugar, o recorte não significa que não há direitos ou remédios jurídicos contra operações de tratamento de dados pessoais para fins de segurança que sejam abusivas.

Há, mas infelizmente de forma limitada ao que é mais grosseiramente abusivo: por exemplo, independentemente da LGPD, qualquer banco de dados de entidades governamentais ou de caráter público está sujeito a prerrogativas de acesso e retificação por força da própria Constituição Federal, no ponto em que resguarda o *habeas data* (art. 5º, inciso LXXII). Há aqui, portanto, espaço para inovar estrategicamente na utilização dessa ação mandamental, com o objetivo de fazer valer tais direitos de informação frente a operações de tratamento de dados pessoais por órgãos de segurança.

Também a Lei de Acesso à Informação (Lei nº 12.527/2011) continuará uma importante aliada na obtenção de informações – de uma perspectiva otimista, é possível esperar que a cultura da proteção de dados pessoais repercuta também na compreensão que é dada sobre os limites hoje impostos ao acesso a informações. Igualmente, se alguém for preso erroneamente porque um *software* de reconhecimento facial atribui uma identidade equivocada, esta pessoa ainda poderá buscar eventual ação de indenização por danos causados pelo Estado. De todo modo, certamente o recorte significa que continuará mais difícil trazer operações abusivas de tratamento à luz (pois, muitas

vezes, ocorrem sem que saibamos) e que ainda se dependerá da superação de ônus argumentativo e de uma boa disputa no Judiciário para obter reparação por danos.

3 Como poderia ser: o que esperar da intersecção entre processo penal e proteção de dados

A persecução criminal moderna, para se manter legítima e funcional, necessita de compatibilidade com princípios de proteção de dados pessoais (WOLTER, 2018). A contrapartida essencial para o interesse em integração de bancos de dados de órgãos públicos, compartilhamento de informações entre autoridades nacionais e internacionais, para viabilização e facilitação da persecução criminal, e nas promessas do *big data* para policiamento é o compromisso com procedimentos e salvaguardas que respeitem direitos e mitiguem riscos a titulares de informações pessoais. É simbólico que a aprovação do Regulamento Geral de Proteção de Dados Pessoais (GDPR) da União Europeia tenha vindo acompanhada de uma nova Diretiva 2016/680

"relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, detecção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados".

O Brasil deve superar o atraso nesse debate. Como primeiro passo, para superar a aversão, o avanço na direção de uma legislação específica – que equilibre as preocupações de proteção de dados pessoais com as necessidades de autoridades de persecução criminal – passa pelo convencimento de que essa legislação será benéfica não só para os titulares de dados, mas para as próprias autoridades de investigação: com balizas claras, há menos questionamentos, maior segurança, cooperação, eficiência e confiança no respeito a direitos. ■

Bibliografia

BORBA, Julia; NERY, Natuza. PF quer instalar vírus em telefone grampeado para copiar informações, *Folha de S.Paulo*, 27 abr. 2015. Disponível em: https://www1.folha.uol.com.br/poder/2015/04/1621459-pf-quer-instalar-virus-em-telefone-grampeado-para-copiar-informacoes.shtml.

DE HERT, Paul; GUTWIRTH, Serge. Privacy, Data Protection and Law Enforcement: Opacity of the Individual and Transparency of the Power. *In*: CLAES; DUFF; GUTWIRTH (Ed.). *Privacy and the criminal law*. Oxford: Intersentia, 2006. p. 61-104.

DONEDA, Danilo. *Da Privacidade à Proteção de Dados Pessoais*. Rio de Janeiro: Renovar, 2006.

IGO, Sarah. *The Known Citizen*: A History of Privacy in Modern America. Cambridge, MA: HUP, 2018.

MENDES, Laura Schertel. *Privacidade, proteção de dados e defesa do consumidor*: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014.

SOLOVE, Daniel. A Taxonomy of Privacy. *University of Pennsylvania Law Review*, v. 154, p. 477-560, 2006.

WOLTER, Jürgen. *O inviolável e o intocável no direito processual penal*: reflexões sobre dignidade humana, proibições de prova, proteção de dados (e separação informacional de poderes) diante da persecução penal. São Paulo: Marcial Pons, 2018. p. 159-209.