Lei de ProteÃ§Ã£o de Dados para seguranÃ§a pÃºblica e persecuÃ§Ã£o penal

Às vésperas do segundo turno das eleições presidenciais, e com a próxima composição do Congresso já eleita, não faltam temas postergados para 2023. Dentre eles, um de grande urgência: a aprovação de uma dos no âmbito penal.

A atual Lei Geral de Proteção de Dados (LGPD, Lei 13.709/2018), deixou propositalmente de regular o tratamento de dados no âmbito da segurança pública e de atividades de persecução e repressão de infrações penais. Em seu artigo 4º, *caput*, III, "a" e "d", c/c §1º, ela expressa a necessidade de *"lei 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"*.

A regulamentação da proteção de dados pessoais no âmbito de investigação e persecução penal, por sua vez, também se revela urgente por ordem constitucional direta. Com a promulgação da Emenda Constitucional nº 115/2022, que acrescentou o inciso LXXIX ao artigo 5º da Constituição, o direito à proteção geral de dados foi alçado a nível de direito fundamental, *"a ser assegurado nos termos da lei"*.

Assim, em que pese a existência da LGPD, a proteção de dados individuais carece de previsão legal quanto às investigações criminais e ações penais, seara em que, sabidamente, os direitos e garantias fundamentais do indivíduo acusado ou investigado são mais relativizados.

Afinal, não faltam "reconhecimentos" — invariavelmente falhos (e com viés racial) — de pessoas alegadamente "suspeitas" realizados a partir da utilização, sem autorização judicial, de fotografias e informações captadas das redes sociais e dos telefones celulares dos investigados.

Apenas a título de exemplo, relembremos o caso do ator estadunidense e negro, Michael B. Jordan (intérprete de famosas produções hollywoodianas), que apareceu em uma das três imagens presentes no Termo de Reconhecimento Fotográfico da Polícia Civil do Ceará como um dos suspeitos da chacina que deixou cinco mortos em Fortaleza [1]. Por sorte, Michael não mora no Brasil e a trapalhada da polícia cearense não produziu maiores consequências…

O mesmo não pode ser dito em relação a Tiago Vianna Gomes, que foi preso duas vezes, após ter sido reconhecido erroneamente em nove oportunidades, por crimes distintos, em razão de uma fotografia sua que constava do álbum da Polícia Civil do Rio de Janeiro [2]. Eventos como esses, infelizmente, não são isolados no cotidiano policial e produzem injustiças, como aponta a série "Fotos que Condenam" [3].

Não se olvida que os Tribunais Superiores têm se voltado para tais casos e anulado diversas decisões que se baseiam em reconhecimentos que deixam de seguir requisitos básicos já previstos na legislação [4]. No entanto, a única forma de prevenir efetivamente que situações como essas ocorram se dá pela regulamentação da matéria, de modo que a prática de atos investigatórios ocorra dentro de parâmetros mínimos de segurança, cientificamente válidos e sem o compartilhamento desregrado de dados, evitando-se, assim, espaço para arbitrariedade de agentes públicos.

Outro exemplo comum de má utilização de dados e de invasão de privacidade pelos órgãos de persecução e repressão penal é a possibilidade de: 1) a polícia individualizar e identificar todas as pessoas que fizeram buscas no sistema Google por determinados termos, ou 2) individualizar e identificar todas as pessoas que estiveram em determinado local durante certo horário, mediante indevida requisição de geolocalização. Isso fomenta o envolvimento de um número incalculável de pessoas figurando como potenciais investigados, em evidente abuso do poder de perquirir e punir do Estado. Trata-se de debate urgente, objeto, inclusive, de discussão no STF (Repercussão Geral do tema 1148).

Fato é que, a pretexto de se apurar a autoria de crimes, não faltam devassas de toda ordem nos sigilos telefônicos, telemáticos, de dados, bancários, compartilhamentos de informações sigilosas, tudo em prol do sucesso das investigações.

Afinal, qual o limite dos poderes de vigilância, interferência e acesso do Estado aos dados pessoais dos cidadãos sem sua autorização e seu conhecimento?

O STF trouxe algumas respostas às indagações difíceis. No julgamento conjunto da Ação Direta de Inconstitucionalidade nº 6.649 e da Arguição de Descumprimento de Preceito Fundamental nº 695, sobre a validade do Decreto 10.046/2019, que dispõe sobre o compartilhamento de dados pessoais entre órgãos e entidades da Administração Pública, foram traçados alguns parâmetros para a interpretação conforme daquela norma.

No voto do ministro Gilmar Mendes venceu o entendimento de que o compartilhamento de dados pessoais por órgãos e entidades da Administração Pública deve pressupor: a) a eleição de propósitos legítimos, específicos e explícitos para o tratamento de dados (artigo 6º, inciso I, da Lei 13.709/2018); b) a compatibilidade do tratamento com as finalidades informadas (artigo 6º, II); c) a limitação do compartilhamento ao mínimo necessário para o atendimento da finalidade informada (artigo 6º, III); bem como o cumprimento integral dos requisitos, garantias e procedimentos estabelecidos na LGPD, no que for compatível com o setor público.

A decisão prevê a necessidade de o Poder Público conferir publicidade quando do uso de dados pessoais de particulares, bem como a instituição de mecanismos rigorosos de controle ao acesso destes dados, sob pena de responsabilização do Estado e do agente estatal em casos de abuso.

No Legislativo, o caminho para suprir o atual vácuo normativo e contemplar o tratamento de dados pessoais no âmbito criminal já teve início com a apresentação à Câmara dos Deputados, em novembro de 2020, do Anteprojeto de Lei de Proteção de Dados para Segurança Pública e Persecução Penal, realizado por comissão de juristas liderada pelo então ministro do STJ, Nefi Cordeiro.

O anteprojeto, caso se torne lei, marca um grande avanço normativo no sistema de justiça criminal brasileira, na medida em que o adequa aos ditames de investigação penal preconizados internacionalmente, buscando proteger direitos e garantias dos cidadãos frente ao poder de vigilância do Estado, bem como suprir, nos termos de sua exposição de motivos, *"um enorme déficit de proteção dos cidadãos, visto que não há regulamentação geral sobre a licitude, a transparência ou a segurança do tratamento de dados em matéria penal, tampouco direitos estabelecidos ou requisitos para utilização de novas tecnologias que possibilitam um grau de vigilância e monitoramento impensável há alguns anos"*.

O artigo 1º elenca o objetivo da lei: *"proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural"*.

Já o artigo 2º preceitua quais são os fundamentos da proteção de dados em matéria penal e de segurança pública, que são a dignidade, os direitos humanos, o livre desenvolvimento da personalidade, e o exercício da cidadania pelas pessoas naturais (inciso I); a autodeterminação informativa (inciso II); o respeito à vida privada e à intimidade (inciso III); a liberdade de manifestação do pensamento, de expressão, de informação, de comunicação e opinião (inciso IV); a presunção de inocência (inciso V); a confidencialidade e integridade dos sistemas informáticos pessoais (inciso VI); e a garantia do devido processo legal, da ampla defesa, do contraditório, da motivação e da reserva legal (inciso VII).

A proposta legislativa também busca definir conceitos necessários à sua aplicação, apontando, em seu artigo 5º, as distinções entre os tipos de dados que podem vir a ser utilizados na persecução penal ou na segurança pública, como os dados pessoais (referentes a pessoa natural identificada ou identificável), os dados pessoais sensíveis (referentes a origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, à saúde ou à vida sexual, dado genético ou dado biométrico, da pessoa natural), e os dados sigilosos (dado pessoal protegido por sigilo constitucional ou legal).

O artigo 7º impõe à pessoa responsável pelo tratamento de dados pessoais o dever de fazer a distinção clara sobre se o titular desses dados é 1) pessoa contra quem existem indícios suficientes de autoria de infração penal ou de que está prestes a cometer infração penal, 2) pessoa processada pela prática de infração penal, 3) pessoa condenada definitivamente pela prática e infração penal, 4) pessoa que é vítima de infração penal, ou 5) outras pessoas, como testemunhas, de modo a vedar a obtenção de dados de pessoas indiscriminadas, que não possuam relações com a investigação em curso ou que nada possam acrescentar a ela.

Além disso, talvez o ponto mais relevante do anteprojeto — foco central no que concerne à proteção de direitos e garantias dos cidadãos — é a definição dos requisitos para o tratamento de dados pessoais por uma autoridade pública, de modo a impedir um poder de acesso indiscriminado aos dados pessoais.

Nesse sentido, o artigo 9º exige o cumprimento de atribuição legal de autoridade competente, a execução de políticas públicas previstas em lei, ou a proteção da vida ou da incolumidade física do titular do dado ou de terceiro contra perigo concreto ou iminente. Já o artigo 11 preceitua que o acesso das autoridades a dados controlados por pessoas jurídicas de direito privado dependerá de previsão legal. E seu §2º estabelece que *"toda e qualquer requisição administrativa ou judicial indicará o fundamento legal de competência expressa para o acesso e a motivação concreta, incluindo sua adequação, necessidade e proporcionalidade, sendo vedados pedidos que sejam genéricos ou inespecíficos"*.

O tratamento de dados também é limitado pela imposição de marcos necessários ao seu término (artigo 16) e a obrigação do descarte dos dados ao final da análise (artigo 15).

O anteprojeto, em seu Capítulo III, também estabelece uma série de direitos aos titulares de dados, como diversas garantias à confirmação da existência de tratamento de dado, acesso aos dados, correção de dados incompletos ou inexatos, anonimização, bloqueio ou eliminação da dados desnecessários ou excessivos e informações das entidades com as quais os dados foram compartilhados.

Outras contribuições relevantes são: 1) a imposição do dever do controlador registrar as atividades de tratamento de dados que estiver sob sua responsabilidade (artigos 32, 33 e 34); 2) a vedação, no âmbito de atividades de segurança pública, de utilização de tecnologias de vigilância diretamente acrescida de técnicas de identificação de pessoas indeterminadas em tempo real e de forma contínua quando não houver a conexão com a atividade de persecução penal individualizada e autorizada por lei e decisão judicial (artigo 43); 3) a previsão de que *"qualquer modalidade de uso compartilhado de dados pessoais entre autoridades competentes somente será possível com autorização legal, com autorização judicial ou no contexto de atuações conjuntas autorizadas legalmente, observados os propósitos legítimos e específicos para o tratamento, os direitos do titular, bem como os fundamentos, princípios e obrigações previstos nesta Lei"* (artigo 43); 4) a previsão de criação, no âmbito do Conselho Nacional de Justiça, de uma Unidade Especial de Proteção de Dados em Matéria Penal (UPDP), responsável por zelar, implementar e fiscalizar a presente Lei de Proteção de Dados para segurança pública e persecução penal; e 5) o estabelecimento de uma série de sanções pelo descumprimento das normas nele tratadas, incluindo, no artigo 66, a tipificação penal do crime de transmissão ilegal de dados pessoais, que seria apenada em um a quatro anos e multa.

O tratamento da matéria se inspira em estatutos jurídicos dos Estados Unidos, e constitui um dos pontos mais relevantes do anteprojeto.

Afinal, o avanço tecnológico tende a possibilitar a criação de um verdadeiro Leviatã digital, com poderes absolutos de vigilância — o que, certamente, requer cuidadoso regramento em leis específicas que visem a proteção da privacidade dos cidadãos. Para Estela Aranha e Paula Sion [5], o principal objetivo desse anteprojeto é assegurar que *"os direitos e garantias processuais que são válidos na vida off line também sejam válidos para a vida online e para o uso de recursos tecnológicos pelo Estado"*.

A análise do anteprojeto — com destaque para as normas citadas acima — demonstra que, caso seja aprovada no parlamento, a lei cumprirá importante papel na proteção de direitos e garantias fundamentais dos titulares de dados, ao passo que conferirá segurança jurídica a meios de investigação legítimos e adequados às inovações tecnológicas.

Por isso, inspirada em relevantes estatutos jurídicos do direito comparado — como a Diretiva 680/2016 da União Europeia e em leis dos Estados Unidos —, a chamada LGPD-Penal elevará o ordenamento jurídico brasileiro, nessa matéria, aos padrões internacionais.

Reconhecendo a importância do anteprojeto de Lei de Proteção de Dados para segurança pública e processo penal, o Instituto dos Advogados Brasileiros aprovou parecer elaborado pelas ora articulistas, destacando seus pontos positivos e realizando algumas contribuições críticas na visão da advocacia. Para o IAB, o anteprojeto cumpre a principal função de um estatuto jurídico nesse âmbito: restringir as possibilidades de arbítrio e do uso autoritário e ilegítimo das tecnologias de vigilância por parte de autoridades públicas.

Ao mesmo tempo, o anteprojeto possibilita e confere segurança jurídica ao uso de novas tecnologias para investigar e punir crimes, bem como para melhorar a segurança pública do país. Trata-se, portanto, de um documento que merece ser transformado em projeto de lei na próxima legislatura, com apoio da comunidade jurídica. Afinal, considerando-se o cenário atual de investigações no Brasil, sem a regulamentação que ora se propõe, ninguém está livre de uma devassa generalizada em suas vidas, nem mesmo o mais analógico dos cidadãos.

[1]. G1 GLOBO. Confira-se em: https://g1.globo.com/ce/ceara/noticia/2022/01/07/astro-do-cinema-michael-b-jordan-aparece-em-lista-de-procurados-pela-policia-do-ceara.ghtml. Acesso em: 26.10.22.

[2]. G1 GLOBO. Confira-se em: https://g1.globo.com/rj/rio-de-janeiro/noticia/2021/09/30/fotos-que-condenam-homem-ficou-10-meses-preso-injustamente-e-foi-tido-como-criminoso-9-vezes-por-erro-de-reconhecimento.ghtml. Acesso em: 26.10.22.

[3]. Confira-se em: https://g1.globo.com/rj/rio-de-janeiro/noticia/2021/09/28/fotos-que-condenam-veja-historias-de-presos-sem-provas-so-com-base-em-reconhecimento-em-imagens.ghtml. Acesso em:

26.10.22.

[4]. A título de exemplo: BRASIL. STF. ROHC nº 206.846. Relator ministro Gilmar Mendes. DOU. Brasília, 30/09/2021 e BRASIL. STJ. HC nº 598.886. Relator ministro Rogério Schietti Cruz — Sexta Turma. DOU. Brasília, 27/10/2020.

[5] Estadão. "A (falta de) proteção de dados pessoais no âmbito Penal". Estela Aranha e Paula Sion. 12/11/ 2020. Em: https://politica.estadao.com.br/blogs/fausto-macedo/a-falta-de-protecao-de-dados-pessoais-no-ambito-penal/