PARECER SOBRE O ANTEPROJETO DE LEI DE PROTEÇÃO DE DADOS PARA SEGURANÇA PÚBLICA E PERSECUÇÃO PENAL APRESENTADO À CÂMARA DOS DEPUTADOS, EM NOVEMBRO DE 2020

Indicação nº 01/2021

Relatoras: Maíra Costa Fernandes, Daniella Meggiolaro e Fernanda Prates

Objeto: Análise do Anteprojeto de Lei de Proteção de Dados para Segurança Pública e Persecução Penal apresentado à Câmara dos Deputados, em novembro de 2020, por comissão de juristas liderada pelo então Ministro do Superior Tribunal de Justiça Nefi Cordeiro.

1. Introdução

O presente trabalho tem por objetivo analisar Anteprojeto de Lei de Proteção de Dados para Segurança Pública e Persecução Penal apresentado à Câmara dos Deputados em novembro de 2020, por comissão de juristas liderada pelo então Ministro do Superior Tribunal de Justiça Nefi Cordeiro.

Como se sabe, a Lei Geral de Proteção de Dados – LGPD (Lei no. 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, ressaltando em seu art. 4º, *caput*, inciso III, alíneas *a* e *d* c/c § 1º 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".

Por conta disso, o anteprojeto de lei em estudo busca complementar, com enfoque na área criminal, as determinações contidas na LGPD, para que contemple o tratamento de dados pessoais no âmbito das investigações criminais e de segurança pública (LGPD-Penal), a fim de proporcionar segurança jurídica para as investigações e procedimentos criminais[1]. Procura, portanto, disciplinar os princípios e as diretrizes centrais da proteção de dados nas investigações, além de impor deveres ao Estado para prevenção e repressão de ilícitos criminais sem violar os direitos tutelados na proteção de dados no exercício da segurança pública, bem como assegurar garantias processuais e prerrogativas fundamentais dos cidadãos brasileiros, tutelando tanto os direitos das pessoas investigadas quanto das pessoas indiretamente expostas ao fato apontado como criminoso.

A importância de uma lei que possa contemplar adequadamente o tema, preenchendo a enorme lacuna que mantém desprotegida a privacidade dos cidadãos submetidos aos órgãos de persecução penal, é patente e dispensaria grandes reflexões. A despeito disso, não é demais trazer à baila algumas situações de violação de direitos fundamentais que o avanço tecnológico infelizmente tem permitido ao Estado alcançar, gerando inaceitável devassa na vida de milhões de pessoas e uma ainda maior disparidade de armas entre a Acusação e a Defesa.

A utilização, sem autorização judicial, de fotografias e informações captadas das redes sociais e dos telefones celulares dos denominados "suspeitos" nas investigações policiais, com a obtenção de reconhecimentos invariavelmente falhos, é o maior demonstrativo da ilicitude do método e do quanto a invasão da intimidade e a utilização indevida de dados podem gerar prisões, acusações e condenações não somente ilegais, mas especialmente injustas. Isso sem mencionar o viés preconceituoso e racista que permeia os algoritmos utilizados nestes

[1]. O sistema europeu também possui uma dupla normativa, o Regulamento Europeu de Proteção de Dados e a Diretiva 680/20169 que trata de proteção de dados para fins de segurança pública e investigação criminal. (ITS Rio. Relatorio-Transferencia-de-dados-pessoais.pdf (itsrio.org))

procedimentos de investigação tão duvidosos, que levam diariamente à cadeia mais e mais pretos e pobres[2].

Apenas a título de exemplo – partindo do mais esdrúxulo – relembremos o caso do ator estadunidense e negro, Michael B. Jordan (que interpretou famosas produções hollywoodianas) e que, recentemente, 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[3]. Por sorte, Michael não mora no Brasil e a trapalhada da polícia cearense acabou não produzindo maiores consequências... O mesmo não pode ser dito em relação a Tiago Vianna Gomes, que chegou a ser 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[4]. Eventos como esses, infelizmente, não são isolados no cotidiano policial e, lamentavelmente, produzem diversas injustiças, como aponta a série "Fotos que Condenam"[5].

Bastante comuns também são os reconhecimentos realizados, sem qualquer critério, a partir de fotos das mídias sociais levadas aos autos da investigação, como o caso de Ângelo Gustavo, jovem negro, então com 22 anos, condenado por ter

---

[2]. STEIN, L. M., & ÁVILA, G. N. D. Avanços científicos em psicologia do testemunho aplicados ao reconhecimento pessoal e aos depoimentos forenses. Brasília: Secretaria de Assuntos Legislativos, Ministério da Justiça (Série Pensando Direito, No. 59). Disponível em: http://pensando.mj.gov.br/wp-content/uploads/2016/02/PoD_59_Lilian_web-1.pdf. Acesso em: 25 fev. 2022.

[3]. G1 GLOBO. **Foto de astro do cinema Michael B. Jordan aparece em lista de procurados pela polícia do Ceará**. Disponível 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: 25 fev. 2022.

[4]. G1 GLOBO. **'Fotos que condenam': homem ficou 10 meses preso injustamente e foi tido como criminoso 9 vezes por erro de reconhecimento**. Disponível 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: 25 fev. 2022.

[5]. Disponível 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: 3 mar 2022.

sido identificado através de uma foto em rede social e apontado como autor de um roubo também na cidade do Rio de Janeiro.[6]

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.[7] No entanto, a única forma de prevenir efetivamente que casos absurdos como esses ocorram se dá pela regulamentação da matéria, de modo que os atos investigatórios ocorram dentro de parâmetros mínimos de segurança, cientificamente válidos e sem o compartilhamento desregrado de dados, evitando-se, assim, espaço para arbitrariedade dos agentes públicos, tudo em consonância com a Agenda 2030 para o Desenvolvimento Sustentável da Organização das Nações Unidas – ONU, que tem como alguns de seus objetivos a eliminação de "práticas discriminatórias" (objetivo 10.3), bem como "promover e fazer cumprir leis e políticas não discriminatórias para o desenvolvimento sustentável" (objetivo 16.b).

Outro exemplo claro e muito comum de má utilização de dados e de invasão de privacidade pelos órgãos de persecução e repressão penal é a requisição indevida de geolocalização, em que um conjunto de pessoas não identificadas – e que tenham em comum transitado ao mesmo tempo em um determinado local – possa ter suas informações pessoais quebradas para fins de investigações criminais. Tal iniciativa certamente fomenta o envolvimento de um número incalculável de

---

6. INSTITUTO DE DEFESA DO DIREITO DE DEFESA. **IDDD questiona condenação baseada exclusivamente em reconhecimento fotográfico.** Disponível em: https://iddd.org.br/iddd-questiona-condenacao-baseada-exclusivamente-em-reconhecimento-fotografico/. Acesso em: 3 mar. 2022.

7. Tão somente a título de exemplo, citamos: BRASIL. Supremo Tribunal Federal. Recurso Ordinário em Habeas Corpus nº 206.846. Relator: Ministro Gilmar Mendes. **Diário Oficial da União**. Brasília, 30 set. 2021 e BRASIL. Superior Tribunal de Justiça. Habeas Corpus nº 598.886. Relator: Ministro Rogério Schietti Cruz – Sexta Turma. **Diário Oficial da União**. Brasília, 27 out. 2020.

pessoas figurando como potenciais investigados, em evidente abuso do poder de perquirir e punir do Estado.

Uma prática investigativa que também vem sendo bastante adotada, lamentavelmente com a anuência do Judiciário, é a quebra de sigilo de dados telemáticos, no âmbito de procedimentos penais, em relação a pessoas indeterminadas. Trata-se, por exemplo, da possibilidade de a polícia individualizar e identificar todas as pessoas que fizeram buscas no sistema Google por determinados termos, ou de individualizar e identificar todas as pessoas que estiveram em determinado local durante determinado horário. Não por acaso este *modus operandi*, que expande consideravelmente os horizontes de uma investigação penal a partir do uso da tecnologia, é o tema de repercussão geral nº 1.148 do Supremo Tribunal Federal, que deverá finalmente enfrentar um dos "maiores desafios contemporâneos à proteção da privacidade em conflito com os imperativos de segurança nacional e da eficiência do Estado, com a proliferação de sistemas de vigilância e mídias sociais, junto com a manipulação maciça de dados pessoais em redes computacionais por inúmeros agentes públicos e privados"[8]. Ora, ainda que efetivamente caiba à mais alta Corte do país debruçar-se sobre a matéria, é certo que ela merece regulamentação por instrumento adequado, que é a lei.

Não podemos deixar de lembrar também a atuação da famigerada Operação Lava Jato, cuja Força Tarefa obteve ilegalmente nada mais nada menos que 350 terabytes de dados de 38 mil pessoas[9], não poupando apenas os investigados e acusados de terem seus dados acessados e compartilhados indiscriminadamente,

[8]. Trecho do voto condutor da Ministra Rosa Weber, proferido em 6 de maio de 2021.
[9]. ESTADÃO. **'Curitiba tem 350 terabytes e 38 mil pessoas lá com seus dados depositados', diz Aras sobre pedido de acesso a banco da Lava Jato.** Disponível em: https://politica.estadao.com.br/blogs/fausto-macedo/curitiba-tem-350-terabytes-e-38-mil-pessoas-la-com-seus-dados-depositados-diz-aras-sobre-pedido-de-acesso-a-banco-da-lava-jato-assista-pgr-no-grupo-prerrogativas/.Acesso em: 3 mar. 2022.

mas também seus familiares, advogados, pessoas de seu relacionamento, terceiros envolvidos etc. Este número absolutamente vergonhoso e inexplicável de cidadãos que tiveram sua privacidade indevidamente invadida em nome de um suposto combate à corrupção jamais existiria se tivéssemos uma legislação que controlasse e punisse efetivamente tais práticas.

O cerne de todas essas questões é exatamente este: qual o limite dos poderes de vigilância, interferência e acesso do Estado aos dados pessoais dos cidadãos sem sua autorização e seu conhecimento? Neste sentido, o anteprojeto em estudo é, sem dúvida, a melhor resposta. Como bem salientado pelo Instituto de Tecnologia e Sociedade, "para que sejam respeitados os direitos fundamentais do indivíduo e, ao mesmo tempo, não seja inviabilizado o exercício do poder/dever estatal de prevenir, investigar e reprimir atos criminosos, é importante que exista uma lei que regule os tratamentos de dados pessoais para fins de segurança pública e persecução penal[10]".

Os casos citados são, como dissemos, apenas alguns exemplos do desproporcional e invisível poder que o Estado exerce sobre a intimidade dos brasileiros no campo da segurança pública e da persecução e repressão penal, sendo mais do que urgente a aprovação de uma lei que regule essas relações tão frequentes e abusivas.

Feitas essas considerações iniciais, passemos ao estudo do anteprojeto em si.

2. Limites e aspectos controvertidos

Apesar de trazer pontos positivos e avanços necessários, desde sua divulgação, o anteprojeto tem sido objeto de certas críticas e preocupações por parte de

[10]. ITS Rio. Relatorio-Transferencia-de-dados-pessoais.pdf (itsrio.org))

especialistas no tema[11]. Na presente seção compilaremos alguns desses pontos, indicando a necessidade de aprofundamento das discussões ao longo da tramitação do anteprojeto.

Um ponto bastante debatido diz respeito ao artigo 61, que define o Conselho Nacional de Justiça como autoridade competente para supervisão e monitoramento, apresentando a seguinte redação: *Art. 61. A estrutura necessária ao funcionamento da Unidade Especial de Proteção de Dados em Matéria Penal (UPDP) será provida pelo Conselho Nacional de Justiça mediante o remanejamento de servidores e serviços já existentes, nos termos da regulamentação, bem como de dotação orçamentária, se necessária, nos termos da legislação.*

Dois aspectos do referido artigo vêm sendo problematizados. O primeiro argumenta que esta nova atribuição prevista ao CNJ extrapola o âmbito daquelas previstas constitucionalmente, de acordo com a Emenda Constitucional nº 45 de 2004, bem como do art. 103-B, §4º da Constituição Federal, ambos os textos indicando o CNJ como órgão administrativo, e não jurisdicional. O segundo questiona a indicação do CNJ sem referência à Autoridade Nacional de Proteção de Dados (ANPD). Conforme salienta nota apresentada pelo ITS Rio,

(...) a não menção da ANPD ao longo do anteprojeto pode gerar dúvidas acerca de competências possivelmente concorrentes entre as duas autoridades e de como elas poderão atuar em conjunto. Isso se reforça ao se considerar o presente momento, em que a ANDP inicia seu processo de constituição e elaboração de diretrizes que

[11] Ver p.ex: UK-Comentarios_LGPDPenal.pdf (itsrio.org); Nota Técnica sobre o Anteprojeto de Lei de Proteção de Dados para segurança pública e investigação criminal - Observatório - Por Data Privacy; https://www.dataprivacybr.org/wp-content/uploads/2020/12/NOTA-TÉCNICA-PROTEÇÃO-DE-DADOS-NO-CAMPO-PENAL-E-DE-SEGURANÇA-PÚBLICA-VF 31.11.2020.pdf; LGPD PENAL: LIVE DATA PRIVACY BRASIL - Observatório - Por Data Privacy (observatorioprivacidade.com.br)

irão nortear sua atuação de forma mais detalhada. Sem a condução estratégica da ANPD e CNJ, as múltiplas interpretações de esferas públicas tenderão a causar insegurança jurídica e muitas ações judiciais, que poderiam ser evitadas — em boa parte dos casos — por instruções e orientações prévias de delimitação, acordos de competência e atuação coordenada. Ressalta-se que o supramencionado art. 4º, inciso III, §3º, da LGPD estabelece que "A autoridade nacional emitirá opiniões técnicas ou recomendações referentes às exceções previstas no inciso III do caput deste artigo — dentre as quais: segurança pública e atividades de investigação e repressão de infrações penais — e deverá solicitar aos responsáveis relatórios de impacto à proteção de dados pessoais.". Ao mesmo tempo, a "LGPD Penal" atribui exclusivamente a atuação do CNJ em segurança pública e defesa nacional sem, contudo, modificar expressamente a redação da LGPD, gerando uma possível situação de insegurança jurídica a respeito da atuação da ANPD nas matérias[12]. Outro ponto se refere ao artigo 9°, II do Anteprojeto, que se apresenta da seguinte forma: *Art. 9º O tratamento de dados pessoais para atividades de segurança pública e de persecução penal somente poderá ser realizado nas seguintes hipóteses: II - para execução de políticas públicas previstas em lei, na forma de regulamento, observados os princípios gerais de proteção, os direitos do tido titular e os requisitos do Capítulo VI desta Lei.* Apesar de trazer importantes proteções, o inciso II do art.9º vem sendo objeto de discussões ao determinar que o tratamento de dados pessoais a ser utilizado na execução de políticas públicas previstas em lei, deva se dar na forma de *regulamento*, gerando conflito de normas entre a lei ordinária que disciplina a proteção de dados na esfera da segurança pública e da persecução penal que, segundo o anteprojeto, deverá ser submetida a regras estabelecidas por um ato regulamentar. Importante destacar ainda que um simples regulamento se origina de processo legislativo menos rígido.

Paralelamente, uma preocupação que decorre do referido anteprojeto diz respeito a possíveis confusões na utilização dos conceitos de segurança pública e

[12] UK-Comentarios_LGPDPenal.pdf (itsrio.org)

persecução, conforme se observa, por exemplo, no artigo 43: *No âmbito de atividades de segurança pública, é vedada a 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.* De fato, apesar de apresentar definição inicial, ao longo do texto os conceitos parecem enredar, deixando menos clara de que forma se dará a proteção de dados no âmbito desses dois diferentes contextos. Outro aspecto referido no artigo – e que certamente será objeto de discussões futuras – se refere aos problemas ligados à utilização da tecnologia de reconhecimento facial, ferramenta que já questionada (e, em alguns casos, banida) em inúmeros países, incluindo o Brasil.

Possível reflexo da limitada distinção no anteprojeto entre os conceitos de segurança pública e persecução penal, o artigo Art. 7º[13] se mostra particularmente problemático ao introduzir a possibilidade de uma eventual "antecipação do delito", ao indicar, em seus incisos II e V as seguintes figuras: *pessoas em relação às quais existem indícios suficientes de que* ***estão prestes a cometer uma infração penal***; *vítimas de uma infração penal ou pessoas em relação às quais certos fatos indicam* ***que podem ser vítimas de uma infração penal*** (grifos nossos). Aparentemente, os referidos incisos buscam incluir na proteção legislativa pessoas não investigadas que eventualmente se tornem objeto de atividades de inteligência. Assim, caso eventual atividade de inteligência identifique determinada pessoa e sobre ela se inicie coleta de dados e cruzamento de informações, esta pessoa

13 Art. 7. No tratamento de dados pessoais, o responsável pelo tratamento deve, na medida do possível, fazer uma distinção clara entre as diferentes categorias de titulares dos dados, especialmente: I – pessoas em relação às quais existem indícios suficientes de que cometeram uma infração penal; II – pessoas em relação às quais existem indícios suficientes de que estão prestes a cometer uma infração penal; III – pessoas processadas pela prática de infração penal; IV – pessoas condenadas definitivamente pela prática de infração penal; V – vítimas de uma infração penal ou pessoas em relação às quais certos fatos indicam que podem ser vítimas de uma infração penal; e VI – outras pessoas, tais como testemunhas, pessoas que possam fornecer informações, ou contatos ou associados das pessoas referidas nos incisos I a V.

também teria seus direitos garantidos, ainda que não haja em relação a ela qualquer investigação formal. Louvável a ampliação de direitos trazida pelo anteprojeto a pessoas não suspeitas. Entretanto, há que se registrar a preocupação com a inclusão dos termos "***prestes a cometer uma infração penal"*** e ***"podem ser vítimas de uma infração penal"***, dando ensejo a possíveis incursões do poder punitivo estatal no campo das antecipações e previsões, violando assim as garantias mais basilares de nosso ordenamento. Nesse sentido, e levando em consideração a possível *ratio legis* do referido artigo, sugere-se a alteração do texto aqui mencionado para que não pairem dúvidas em relação ao escopo e objetivos do artigo 7º. Assim, seria possível, por exemplo, a substituição da atual redação do inciso II por um texto equivalente a "pessoas objeto de atividades de inteligência", para que a devida proteção seja dada ao indivíduo, sem que com isso haja extrapolação do poder punitivo. Caso, ao longo dos debates, seja identificada a impossibilidade de reformulação dos incisos, sugerimos então sua supressão, tendo em vista sua clara incompatibilidade com direitos e garantias previstos em nosso ordenamento.

Assim, recomenda-se a seguinte redação para o artigo 7º do Anteprojeto:

> Art. 7º. No tratamento de dados pessoais, o responsável pelo tratamento deve distinguir, claramente, e qualificar, ainda que previamente, as diferentes categorias de titulares dos dados para fins de proteção de seus direitos individuais, especialmente:
>
> I – pessoas em relação às quais existem indícios fidedignos ou suficientes de que cometeram uma infração penal;
>
> II – pessoas sujeitas a quaisquer atividades de inteligência investigativa ou probatória que apure manifestação e preparação para a prática de crime;
>
> III – pessoas processadas pela prática de infração penal;

IV – pessoas condenadas definitivamente pela prática de infração penal;

V – vítimas de uma infração penal ou pessoas em relação às quais fatos concretos coletados por atividade investigativa (oculta ou não) ou probatória indicam que serão vítimas de uma infração penal; e

VI – outras pessoas, tais como testemunhas, pessoas que possam fornecer informações, ou contatos ou associados, por fato concreto coletado em investigação preliminar (oculta ou não) e processual, das pessoas referidas nos incisos I a V.

§ 1º - Atividade de inteligência deve ser compreendida como qualquer ato de investigação, preliminar ou processual, oculto ou não, de natureza criminal ou de quaisquer outros caráteres, realizado por órgãos públicos ou privados.

§ 2º - A desobediência, dolosa ou culposa, às regras estabelecidas no caput tornará absolutamente nulos todos os atos investigativos e atos de prova praticados e, consequentemente, imprestáveis todas informações coletadas, sendo, obrigatoriamente, desentranhados dos procedimentos e processos correlatos.

§ 3º - as pessoas que manipularem os dados pessoais em descumprimento das determinações legais estarão sujeitas às responsabilizações pertinentes.

Ainda, o artigo 8º, parágrafo único, do Anteprojeto, determina o descarte de dados pessoais tratados de forma "*inexata*" ou "*ilícita*", bem como demanda que o destinatário desses dados seja informado pelo responsável sobre essas circunstâncias. Nesse sentido, a par do que já determina o Anteprojeto sobre a matéria, entendemos ser relevante que se faça discussão específica sobre a eventual cominação de sanções, administrativas e/ou penais, ao "*uso inexato de dados*" e ao "*trato de dados pessoais de forma ilícita*".

Finalmente, destacamos o artigo 29 do anteprojeto[14], que prevê a possibilidade de apresentação de relatório de impacto ao Ministério Público bem como à Defensoria Pública, excluindo, neste caso, a advocacia. Tendo em vista se tratar de função essencial à justiça conforme o disposto no art. 133 do texto constitucional, sugerimos a inclusão da advocacia – por meio do Conselho Federal da OAB – no presente artigo, quando cabível a atuação no exercício de suas atribuições.

Mesmo apresentando alguns pontos problemáticos, há que se reconhecer que, de modo geral, as inovações trazidas pelo anteprojeto são, sem dúvida, positivas e necessárias. Além disso, por se tratar ainda de anteprojeto com uma longa tramitação e inúmeras discussões futuras, espera-se que eventuais limitações sejam dirimidas ao longo deste processo.

3. Os avanços normativos contidos no anteprojeto

O anteprojeto de Lei de Proteção de Dados para segurança pública e persecução penal introduz importantes inovações e, caso se torne lei, representará um marco no sistema de justiça criminal. Segundo sua exposição de motivos, a proposta busca superar duas problemáticas centrais. A primeira delas é adequar os padrões e mecanismos de investigação penal das polícias brasileiras àqueles preconizados em âmbito internacional.

14 Art. 29. É obrigatória a elaboração de relatório de impacto à proteção de dados pessoais para tratamento de dados pessoais sensíveis, sigilosos, ou em operações que apresentem elevado risco aos direitos, liberdades e garantias dos titulares de dados. § 1º O Conselho Nacional de Justiça poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, referente a suas operações de tratamento de dados. § 2º A elaboração e apresentação de relatório de impacto à proteção de dados pessoais também poderá ser requisitada pelo Ministério Público e pela Defensoria Pública na defesa de direitos individuais ou coletivos, quando cabível no exercício de suas atribuições.

A segunda, proteger direitos e garantias dos cidadãos frente ao poder de vigilância do Estado, suprindo "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".

Esses objetivos também se alinham à agenda 2030 da Organização das Nações Unidas, cuja meta 16.10 consiste em "assegurar o acesso público à informação e proteger as liberdades fundamentais, em conformidade com a legislação nacional e os acordos internacionais".

Com efeito, essas são preocupações legítimas e urgentes do legislador – especialmente no que toca à proteção de direitos e garantias de cidadãos, como o direito à privacidade, eis que a tendência do poder de vigilância e repressão do Estado é sempre aumentar o controle sobre a esfera de autonomia do indivíduo. Por isso, às inovações tecnológicas e de possibilidades de esquadrinhamento, pelo Estado, da vida das pessoas, devem corresponder estatutos jurídicos que protejam os direitos fundamentais.

E o anteprojeto de Lei de Proteção de Dados para a segurança pública e persecução penal se presta, satisfatoriamente, a essa finalidade.

Essa tendência é observada logo no artigo 1º do anteprojeto, segundo o qual a lei tem como objetivos "proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural". No mesmo sentido, 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 atende à importante atribuição de definir com clareza os conceitos necessários à sua aplicação. Por exemplo, o artigo 5º aponta as distinções, dentre outras categorias, sobre os diferentes tipos de dados que podem vir a ser utilizados na persecução penal ou na segurança pública:

- Dado pessoal (informação relacionada a pessoa natural identificada ou identificável);
- Dado pessoal sensível (dado pessoal 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 dado biométrico, quando vinculado à pessoa natural); e
- Dado sigiloso (dado pessoal protegido por sigilo constitucional ou legal).

Da mesma forma, o artigo 7º impõe que a pessoa responsável pelo tratamento de dados pessoais faça distinção clara sobre se o titular desses dados é (i) pessoa contra quem existem indícios suficientes de autoria de infração penal ou de que está prestes a cometer infração penal, (ii) pessoa processada pela prática de infração penal, (iii) pessoa condenada definitivamente pela prática e infração

penal, (iv) pessoa que é vítima de infração penal, ou (v) outras pessoas, como testemunhas.

Essa distinção é relevante, pois pode controlar a obtenção de dados de pessoas indiscriminadas, que não possuam relações com a investigação em curso ou que nada possam acrescentar a ela.

Outro ponto relevante do anteprojeto – e particularmente importante para a proteção de direitos e garantias dos cidadãos – é a definição dos requisitos para o tratamento de dados pessoais por uma autoridade pública. 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".

Essas normas são importantes para impedir um poder de acesso indiscriminado a dados, exigindo, nesses casos, a expressa previsão legal e a fundamentação idônea das requisições, administrativas ou judiciais, para tanto.

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 prevê uma série de direitos aos titulares de dados. Previstos no Capítulo III do projeto (artigos 18 a 28), esses direitos incluem 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.

Nos termos da exposição de motivos, "quanto aos direitos dos titulares, o texto prevê, por um lado, os direitos clássicos de acesso aos dados e retificação, cuja base encontra-se até mesmo no remédio constitucional do *habeas data*, e por outro, direitos alinhados às tendências contemporâneas de regulação das decisões automatizadas, como o direito à proteção contra a discriminação e o direito à explicação de processos automatizados".

Para tanto, o anteprojeto impõe a obrigação do controlador registrar as atividades de tratamento de dados que estiver sob sua responsabilidade (artigos 32, 33 e 34).

Outro ponto importante do anteprojeto é o tratamento dispensado às tecnologias de monitoramento de dados de elevado risco para direitos, liberdades e garantias dos titulares dos dados por autoridades, aspecto tratado entre os artigos 42 e 44 do projeto.

Por exemplo, o artigo 43 preceitua que no âmbito de atividades de segurança pública, é vedada a 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.

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.

O anteprojeto também oferece vasto arcabouço regulatório sobre o compartilhamento de dados. Por exemplo, o artigo 45 estabelece 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".

Por fim, para fiscalizar o cumprimento da lei, o anteprojeto determina a criação, no âmbito do CNJ, de uma Unidade Especial de Proteção de Dados em Matéria Penal (UPDP), que será responsável por zelar, implementar e fiscalizar a presente Lei de Proteção de Dados para segurança pública e persecução penal.

Além disso, o anteprojeto prevê uma série de sanções pelo descumprimento das normas nele tratadas, chegando a propor, em seu artigo 66, a tipificação penal do crime de transmissão ilegal de dados pessoais, que seria apenada em um a quatro anos e multa.

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.

4. Conclusões

O anteprojeto de Lei de Proteção de Dados para segurança pública e processo penal, adequando-se à Agenda 2030 da ONU, 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 projeto de lei analisado 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 projeto urgente e necessário ao Brasil, cujo tratamento no anteprojeto em questão merece a aprovação da comunidade jurídica.

Conquanto se tenha apontado acima alguns pontos sobre os quais o Legislativo poderia empreender melhor reflexão, isso não afasta os méritos e os avanços do anteprojeto, com as seguintes ressalvas:

- Necessidade de maior debate sobre a pertinência e a constitucionalidade de se atribuir ao Conselho Nacional de Justiça a autoridade para supervisionar e monitorar a aplicação da LGPD-Penal, conforme artigo 61 do Anteprojeto;

- Necessidade de se conferir maior clareza, ao longo da Anteprojeto, aos conceitos de "segurança pública" e de "persecução penal" para evitar confusões ou interpretações equivocadas, a exemplo do que ocorre no artigo 43 do Anteprojeto;

- Recomendação para que se modifique a redação do artigo 7º do Anteprojeto, conforme item 2 supra;

- Necessidade de emenda ao artigo 29 do Anteprojeto para incluir a advocacia – por meio do Conselho Federal da Ordem dos Advogados do Brasil –, ao lado do Ministério Público e da Defensoria Pública, dentre as instituições às quais poderão ser apresentados os relatórios de impacto;

- Recomenda-se, por fim, posterior discussão sobre a eventual cominação, no artigo 8º, parágrafo único, de sanções, penais e/ou administrativas, pelo uso inexato de dados e pelo tratamento da dados pessoais de forma ilícita.

Diante de todo o exposto, submetemos à apreciação dos ilustres membros da Comissão de Direito Penal o Presente Parecer, favorável à aprovação do anteprojeto de Lei de Proteção de Dados para a persecução penal e segurança pública, com as ressalvas apontadas e sem prejuízo de recomendar que haja maior reflexão sobre os pontos tratados no item 2 supra.

Se aprovado pela Comissão, recomendamos que seja submetido aos demais integrantes do IAB, em sessão Plenária do Instituto dos Advogados Brasileiros, para votação.

Rio de Janeiro, 10 de março de 2022.

DANIELLA MEGGIOLARO

FERNANDA PRATES

MAÍRA FERNANDES