NOTA TÉCNICA

Análise comparativa entre

O ANTEPROJETO DE LGPD PENAL E O PL 1515/2022

INSTITUTO DE REFERÊNCIA EM INTERNET E SOCIEDADE

LAPIN
LABORATÓRIO DE POLÍTICAS PÚBLICAS E INTERNET

AUTORIA
Cynthia Picolo Gonzaga de Azevedo
Eliz Marina Bariviera de Lima
Felipe Rocha da Silva
Gustavo Ramos Rodrigues
Luiza Corrêa de Magalhães Dutra
Paulo Renáda Silva Santarém
Victor Barbieri Rodrigues Vieira

REVISÃO[1]
Flora Sartorelli Venâncio de Souza
Renata Taise de Carvalho Feijó

PROJETO GRÁFICO, CAPA, DIAGRAMAÇÃO E FINALIZAÇÃO
Felipe Duarte

COMO CITAR EM ABNT
AZEVEDO, Cynthia Picolo Gonzaga de; LIMA, Eliz Marina Bariviera de; SILVA, Felipe Rocha da; RODRIGUES, Gustavo Ramos; DUTRA, Luiza Corrêa de Magalhães; SANTARÉM, Paulo Renáda Silva; VIEIRA, Victor Barbieri Rodrigues. **Nota técnica: análise comparativa entre o anteprojeto de LGPD penal e o PL 1515/2022**. Instituto de Referência em Internet e Sociedade (IRIS) e Laboratório de Políticas Públicas e Internet (LAPIN), novembro de 2022. Disponível em: <bit.ly/3U0OuU0> . Acesso em: dd mm aaaa.

1 Flora Sartorelli Venâncio de Souza e Renata Taise de Carvalho Feijó fazem parte da Coordenadoria do Núcleo de Constitucionalismo Digital do Departamento de Estudos e Projetos Legislativos do Instituto Brasileiro de Ciências Criminais

Apresentação

O IRIS – Instituto de Referência em Internet e Sociedade é um centro de pesquisa independente e interdisciplinar fundado em 2015 e dedicado a produzir e comunicar conhecimento científico sobre os temas de internet e sociedade, bem como a defender e fomentar políticas públicas que avancem os direitos humanos na área digital. Sua atuação busca qualificar e democratizar os debates sobre internet, sociedade e novas tecnologias ao trazer insumos científicos aos usuários da internet e aos diferentes setores que compõem a sociedade: governo, sociedade civil, setor privado, comunidade técnica e acadêmica.

O LAPIN – Laboratório de Políticas Públicas e Internet é um centro independente de pesquisa e ação voltado para os desafios sociais, éticos, e jurídicos que as tecnologias digitais trazem a uma sociedade global conectada. Desde 2016, o Laboratório desenvolve pesquisas científicas, notas técnicas, cursos, campanhas, e ações direcionadas a temas como privacidade, proteção de dados pessoais, liberdade de expressão e inovação. Trata-se de uma instituição sem fins lucrativos, apartidária, e com sede na capital federal. Sua atuação, contudo, transcende fronteiras locais, regionais, e nacionais. O LAPIN tem colaboradores em cidades de todas as regiões do Brasil e em diversos países do mundo.

Resumo Executivo

A Lei Geral de Proteção de Dados excetuou de seu escopo de aplicação as operações de tratamento de dados pessoais realizadas para fins exclusivos de segurança pública, defesa nacional, segurança de Estado e persecução penal. Essas exceções deverão ser normatizadas por legislação específica a ser subsequentemente aprovada pelo Congresso Nacional, norma que por vezes tem sido informalmente denominada “LGPD penal”. Duas propostas principais de texto legal têm capitaneado as discussões sobre o tema: um anteprojeto elaborado por uma comissão de juristas indicada pela Câmara dos Deputados e o Projeto de Lei nº 1515/2022, de autoria do deputado Coronel Armando (PL-SC).

O objetivo desta nota técnica foi analisar comparativamente as duas propostas acima elencadas, e apresentar apontamentos críticos sobre seus arranjos normativos, a fim de contribuir para a qualificação do debate legislativo sobre a matéria. A conclusão principal da análise foi de que o PL adota uma estrutura em linhas gerais similar à do APL, porém altera significativamente seu conteúdo de modo a suprimir diversas garantias dos titulares, bem como a ampliar excessivamente o poder discricionário do Estado. Por essa razão, recomenda-se o arquivamento do PL 1515/2022.

Entre os principais pontos de preocupação específicos, destacam-se:

- Debilitação do sistema de conceitos, princípios e fundamentos da proteção de dados, com a supressão de noções importantes, como “autodeterminação informativa”, “proporcionalidade”, “dados sigilosos” e “responsabilização e prestação de contas”;

- Ampliação indevida e excessiva do escopo regulado, incluindo atividades de defesa nacional, segurança de Estado e de inteligência, as quais são parametrizadas de forma insuficiente, podendo favorecer abusos;

- Supressão de todo o arcabouço de transparência e do controle sobre o tratamento dos dados pessoais na esfera penal, bem como daquele referente às tecnologias de monitoramento;

- Ampliação excessiva das bases legais para o tratamento de dados para os fins tutelados, bem como das hipóteses de compartilhamento entre autoridades e do acesso a dados mantidos por agentes privados, com a adição de incentivos para a precarização das infraestruturas tecnológicas;

- Enfraquecimento de direitos e proteções referentes a decisões automatizadas, como exigência de autorização prévia e de relatórios de impacto adequadamente procedimentalizados, em favor de disposições genéricas e de aplicabilidade limitada.

Introdução

A Lei Geral de Proteção de Dados Pessoais (Lei Federal nº 13.709/18 – "LGPD") adota modelo de regulação de aplicação ampla para diferentes setores, desde empresas privadas a autoridades públicas. A LGPD, no entanto, exclui do seu escopo o tratamento de dados pessoais para fins de segurança pública, persecução penal, defesa nacional e segurança do Estado (art. 4°, III, LGPD).

Contudo, a LGPD determinou que esta matéria deverá ser regulada por legislação específica e estabeleceu diretrizes para a sua elaboração: a lei futura 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 já previstos na LGPD (art. 4°, §1º, LGPD).

Buscando suprir essa lacuna legislativa, em novembro de 2020, uma comissão de juristas apresentou à Presidência da Câmara dos Deputados o Anteprojeto de Lei de Proteção de Dados Pessoais para Segurança Pública e Persecução Penal ("APL"), também conhecida como "LGPD Penal". A construção do texto contou com uma participação multissetorial e democrática, em um processo que durou cerca de um ano.

A Comissão de Juristas enfrentou o difícil desafio de criar um texto de lei capaz de endereçar os riscos relacionados à proteção de dados em âmbito de segurança pública e processo penal. Vale ressaltar que não é por acaso que o direito penal se pauta no princípio da "*ultima ratio*", ou seja, ele só poderá ser suscitado quando não houver nenhum outro ramo do direito para responder a determinada conduta desviante no campo social. O direito penal é o campo mais perigoso do direito, uma vez que pode determinar a medida mais grave prevista em nosso ordenamento: a privação de liberdade.

Assim, uma lei que regule o tratamento de dados para fins penais tem fundamentos e racionalidade bastante diferente de uma lei que vise regular o tratamento de dados para fins empresariais ou mesmo civis. Ao mesmo tempo em que ela deve traçar o caminho para atuações de prevenção e combate ao crime, ela também deve se preocupar com a limitação do poder punitivo estatal, evitando assim o fomento a um estado autoritário e/ou de vigilância.

Como a própria exposição de motivos do APL diz, o objetivo do texto foi o de proporcionar maior segurança jurídica para que os órgãos de investigação e repressão criminais pudessem exercer suas funções com maior eficiência e eficácia, sem perder de vista as garantias processuais penais e os direitos fundamentais dos titulares de dados envolvidos. Para tanto, buscou-se regular as atividades de tratamento de dados no âmbito penal de acordo com o seu grau de risco, delimitando a esfera de atuação das autoridades competentes e firmando o compromisso com a garantia aos princípios gerais de proteção e os direitos do titular.

Cerca de um ano e meio depois, em junho de 2022, o então deputado Coronel Armando (PL-SC) propôs o Projeto de Lei nº 1515/2022 ("PL") objetivando suprir a mesma lacuna legislativa do APL. O PL segue a mesma estrutura do APL, podendo se dizer que foi baseado amplamente no texto apresentado pela Comissão de Juristas. Até mesmo os seus objetivos

declarados (v. Justificativa) são bastante similares ao do APL[1]. Contudo, em termos de conteúdo, as propostas de normas são intrinsecamente diferentes entre si, como veremos no decorrer dessa Nota Técnica.

O objetivo dessa Nota Técnica é analisar o Projeto de Lei 1515/22, comparando-o com o APL e apresentando posicionamentos críticos quanto às suas disposições. Para tanto, analisaremos o PL sob os seguintes aspectos: (i) o escopo finalístico regulado; (ii) a fundamentação; (iii) as definições; (iv) a principiologia; (v) as bases legais de tratamento de dados pessoais; (vi) o acesso e compartilhamento de dados pessoais; (vii) o tratamento de dados pessoais sigilosos; (viii) o requisito transparência; (ix) os limites e o término do tratamento de dados; (x) os registros das atividades de tratamento; (xi) a segurança e sigilo dos dados; (xii) os direitos dos titulares; e (xiii) o controle sobre as tecnologias de monitoramento, decisões automatizadas e elaboração de relatórios de impacto.

Dois aspectos das propostas estão excluídos do escopo da presente análise: o mérito da mudança do Conselho Nacional de Justiça enquanto autoridade supervisora no anteprojeto para a Autoridade Nacional de Proteção de Dados no PL e a criação de um novo tipo penal de transmissão ilegal de dados pessoais. Quando da finalização desta nota, entendemos que ambos os temas demandam a ampliação da participação no debate e o amadurecimento técnico da reflexão multissetorial sobre os temas.

Antes de passar para os tópicos específicos, é importante já fazer uma diferenciação entre os textos do APL e do PL. O APL apontou o Conselho Nacional de Justiça ("CNJ") como autoridade supervisora, uma vez que à época a Autoridade Nacional de Proteção de Dados ("ANPD") não contava, no entender da Comissão de Juristas, com a autonomia e independência necessária para aplicar, supervisionar e monitorar o tratamento de dados em âmbito penal. O PL, por sua vez, estabelece a própria ANPD como autoridade supervisora, o que ganha maior sentido após a transformação da autoridade em autarquia de natureza especial[2].

Do escopo regulado

Desde a formação da Comissão de Juristas, o APL se propôs a regular duas das quatro exceções endereçadas pela LGPD, quais sejam: o tratamento de dados pessoais para fins de **segurança pública e persecução penal** (art. 4º, inc. III, alíneas a e d, APL). Tal escolha está em consonância com diplomas internacionais de referência, como a Diretiva 680/16 do Parlamento Europeu, que regula o tema na União Europeia.

O PL, por outro lado, amplia o escopo de aplicação, ao enquadrar também os tratamentos realizados para fins de defesa nacional, segurança de Estado e atividades de inteligência (art. 1º, *caput* e § 2º, PL).

1 A Justificativa do PL traz a seguinte afirmação: "Busca-se, portanto, harmonizar, de um lado, os deveres do Estado no exercício das atividades de segurança do Estado, de defesa nacional, de segurança pública, e de investigação e repressão de infrações penais; e, de outro, a observância das garantias processuais e as prerrogativas fundamentais dos cidadãos brasileiros no que tange ao tratamento de dados pessoais para tais fins".

2 Em 26 de outubro de 2022, foi publicada a Lei Federal nº 14.460/22 que transformou oficialmente a ANPD em autarquia de natureza especial.

A restrição de escopo feita pelo APL tem uma razão de ser: as atividades de **segurança do Estado e de defesa nacional** são significativamente diferentes das atividades de segurança pública e persecução penal. Grosso modo, enquanto os conceitos de segurança do Estado e defesa nacional se relacionam com a proteção do Estado brasileiro contra ameaças internas e externas, os conceitos de segurança pública e persecução penal tratam da proteção – de forma preventiva e repressiva – a bem jurídicos tutelados pela legislação penal.

O escopo amplo estabelecido no PL é tecnicamente questionável, uma vez que tanto a atividade de segurança do Estado como a de defesa nacional possuem fundamentos, finalidades, regulações e ecossistemas institucionais incompatíveis com o desenho legal concebido no APL, e reproduzido parcialmente no PL. Assim, as inovações propostas para acomodar essas duas atividades não são capazes de oferecer níveis de controle proporcionais aos riscos, impactos sociais, econômicos e políticos gerados. Como veremos, no decorrer do texto do PL há várias incongruências quando o tema é segurança do Estado e defesa nacional.

Além disso, se por um lado a proposta amplia inadequadamente seu escopo no campo das exceções reguladas, por outro, ela o restringe de forma injustificada em outro aspecto: diferentemente do APL, o PL não se aplica às autoridades fiscais e aduaneiras, às unidades de inteligência financeira, às autoridades administrativas independentes, às autoridades de supervisão dos mercados financeiros e de valores mobiliários, obrigadas legalmente à comunicação de suspeita de prática de infração penal aos órgãos de segurança pública e de persecução penal. Ainda, o APL dispunha que a transmissão estaria sujeita ao princípio da necessidade, sem prejuízo de controle judicial legalmente exigido.

Essa supressão é criticável na medida em que os órgãos compelidos à comunicação de suspeita de infração penal são partes fundamentais do ecossistema de segurança pública e persecução penal. Como consequência, tais órgãos, devem ter sua atuação, referente a essas comunicações, regida pelos mesmos princípios e parâmetros aplicáveis aos demais órgãos incumbidos dessas atividades. Assim, a supressão carrega o risco de comprometer a eficácia da proteção dos dados pessoais nas esferas financeira e fiscal.

Vale lembrar que, nos últimos anos, o tema do compartilhamento de dados entre autoridades competentes de segurança pública e persecução penal e autoridades sem competência penal, mas com dever de comunicar suspeitas de infrações, pautou julgamentos polêmicos nos tribunais superiores. A imposição de regras específicas voltadas à proteção de dados em âmbito penal, com todos esses agentes em seu escopo, teria o potencial de definir posicionamento sobre essas discussões jurisprudenciais, criando maior segurança jurídica em investigações criminais.

Da fundamentação

No que diz respeito aos fundamentos do tratamento de dados pessoais para as exceções a serem disciplinadas na esfera penal, verifica-se que o PL retrocedeu na afirmação de diversos institutos constantes no APL.

Na fundamentação, destaca-se a supressão da autodeterminação informativa (art. 2º, II, APL), fundamento da proteção de dados pessoais e consagrado nas mais diversas legislações internacionais de proteção de dados pessoais, inclusive expressamente previsto na LGPD. Curiosamente, o fundamento da autodeterminação informativa está

na justificativa do PL como um dos objetivos perseguidos pela proposta. Entretanto, essa alegação não encontra ressonância no texto legislativo.

A autodeterminação informativa pode ser entendida como o direito do cidadão de controlar o que é feito com os seus próprios dados ou, quando o controle não for possível, ter informações em relação ao tratamento realizado. Nesse sentido, é preciso que os titulares disponham de mecanismos jurídicos-procedimentais eficientes para apreciar eventuais violações a direitos. A supressão desse fundamento não é mera formalidade. A bem da verdade, ela reflete um racional adotado pelo PL de ataque à garantia de transparência e aos direitos garantidos aos titulares de dados pessoais.

Esse fundamento já foi reconhecido tanto pelo plenário do Supremo Tribunal Federal, quando do julgamento da constitucionalidade da Medida Provisória nº 954/2020, quanto pelo Congresso Nacional, por ocasião da aprovação da Emenda Constitucional nº 115. A eliminação da referência expressa a essa liberdade é incompatível com o reconhecimento da autonomia do direito fundamental à proteção de dados pessoais frente a outros direitos, como, por exemplo, a inviolabilidade da intimidade e da vida privada. É, portanto, inconstitucional.

Similarmente, o PL eliminou a referência à confidencialidade e à integridade dos sistemas informáticos pessoais elencada no APL (art. 2º, VI, APL). Tal supressão é inconsistente com os ditames do próprio PL, posto que a segurança das informações é considerada como um princípio e um dever dos agentes de tratamento, e tanto a confidencialidade quanto a integridade são pilares fundamentais da Segurança da Informação.

Uma alteração mais adequada à harmonia interna da norma e ao estado da arte do conhecimento científico no campo da segurança informacional sobre a matéria seria a inclusão de outros princípios, como o da disponibilidade e da irretratabilidade, também considerados pilares da Segurança da Informação.

O PL também inovou em relação ao APL ao adicionar um dever de eficiência e da garantia do direito à segurança pública por meio de mecanismos que otimizem a prevenção e persecução penal (art. 2º, VI) entre os fundamentos. A alteração é parcialmente pertinente na medida em que a garantia do direito à segurança é constitucional e legalmente reconhecida como parte essencial do ecossistema normativo nacional relativo à segurança pública e à persecução penal.

Contudo, o fundamento da lei deve ser o de criar balizas para o correto funcionamento das atividades, sem que se comprometa os direitos assegurados. A eficiência por si só não pode ser considerada um fundamento, uma vez que uma lógica eficientista da segurança pública e da persecução penal pode levar à discricionariedades e intervenções injustificadas nas liberdades dos cidadãos. No mais, a inserção desse fundamento – concomitante ao notório enfraquecimento do rol de garantias do PL em comparação com o APL – pode gerar uma situação de desequilíbrio entre o poder punitivo estatal e a proteção das liberdades individuais.

Das definições

Em comparação ao APL, o PL altera definições importantes, como a de segurança pública, exclui as definições dos termos “análise de impacto regulatório”, “tecnologia de monitoramento” e “registros criminais”, e inclui definições para “atividade de segurança do estado”, “atividade de defesa nacional” e “dados cadastrais”.

O PL define atividade de segurança do Estado como "toda e qualquer atividade que vise à preservação do território, das instituições, do povo e da soberania nacionais" (art. 3º, II, PL) e a atividade de defesa nacional como "a atividade exercida, com ênfase na expressão militar, para a defesa do território, da soberania e dos interesses nacionais contra ameaças preponderantemente externas, potenciais ou manifestas"(art. 3º, III, PL).

A definição de segurança do Estado apresentada é demasiadamente abrangente e pode favorecer abusos, haja vista que permite o enquadramento de qualquer operação de tratamento que não seja classificável como de persecução penal, segurança pública ou defesa nacional. Note-se que aqui sequer há uma restrição sobre o tipo de atividade para que ela se configure enquanto tal, diferentemente do que ocorre com o conceito de atividade de segurança pública, por exemplo.

No contexto de uma fragilização de garantias e do controle sobre os agentes de tratamento, tal definição poderá ser facilmente instrumentalizada para práticas autoritárias.

O conceito de "atividade de segurança pública", por sua vez, foi alterado em relação ao APL para adicionar o patrimônio e a incolumidade física das pessoas como objetos de tutela. Uma vez que dentro do conceito de atividade de segurança pública já está, de forma ampla, a prevenção de infrações penais, essa adição perde sentido. Patrimônio e a integridade física são bem jurídicos tradicional tutelados pelo direito penal, entre diversos outros, e a sua proteção já estava garantida sem a menção expressa.

Ainda em relação a essa definição, o PL fez remissão ao art. 144 da Constituição Federal ("CF") que prevê as autoridades competentes para segurança pública e excluiu da definição atividades de inteligência institucional, policial e financeira (art. 5º, XXI, APL), estabelecendo, apenas, que "atividades de inteligência" estão dentro de seu escopo. Esse conceito, contudo, não é posteriormente definido, o que pode gerar situação de insegurança jurídica.

Outra inovação trazida pelo PL diz respeito ao conceito de dados cadastrais, definido como dados apresentados pelo titular para realização ou manutenção de cadastro, restando excluídos do sigilo constitucional ou legal (art. 3º, VI, § 1º, PL). O rol exemplificativo apresentado no artigo para essas informações contempla "qualificação pessoal, **dados biométricos,** filiação, endereço, nome e endereço de assinante ou de usuário registrado ou autenticado para a conexão, identificação de usuário ou código de acesso que tenha sido atribuído no momento da conexão".

O conceito de dados cadastrais é inconsistente, posto que, enquanto dados cadastrais estão sujeitos ao mesmo nível de proteção legal que outros dados pessoais. Inclusive, o Supremo Tribunal Federal ("STF") estabeleceu o entendimento que dados cadastrais estão entre os dados constitucionalmente protegidos, aos julgar ações diretas de inconstitucionalidade que questionavam a validade da Medida Provisória nº 954/20, promulgada no contexto da pandemia da Covid-19.

Não cabe, no mais, desvincular esse tipo de dado de eventual sigilo, consistente em um requisito para a concretização de diversos dos parâmetros trazidos pela norma - segurança, prevenção, finalidade, necessidade, dentre outros. A decretação ou não de sigilo – legal ou constitucional – sobre determinado grupo de informações é uma escolha legislativa, não fazendo parte da definição intrínseca do grupo de dados. Cabe à legislação específica ou mesmo à jurisprudência determinar a incidência de sigilo nesse caso.

Ainda, quando o PL explicita que as definições da LGPD são aplicáveis a esta lei,

consequentemente outra incoerência emerge: posto que dados biométricos são dados pessoais sensíveis, nos termos da LGPD, estes gozariam de um grau de proteção ainda mais elevado que dados pessoais não sensíveis, considerando o potencial de gerar graves riscos e/ou danos aos titulares de dados, caso sejam utilizados de forma inapropriada (art. 3º, § 2º, PL). A inclusão de dados biométricos no conceito de dados cadastrais está em total desacordo com a construção jurisprudencial e doutrinária sobre o conceito. Está também em desacordo com outras leis que trouxeram tal definição, como, por exemplo, no art. 190-A, §2º, inc. II do ECA[3].

Além das alterações e adições, três conceitos presentes no APL foram suprimidos do PL : os de dado pessoal sigiloso (art. 5º, III, APL), tecnologia de monitoramento (art. 5º, XXIII, APL) e registros criminais (art. 5º, XXIV, APL). As supressões vieram acompanhadas da diminuição da importância dada a essas matérias pelo PL. As consequências das supressões desses três conceitos serão discutidas nas seções posteriores.

Por fim, importante, também, mencionar as alterações realizadas pelo PL sobre as categorias de titulares (art. 7º, APL). Considerando que a permissibilidade de intervenção em liberdades individuais pode variar a depender do contexto, o APL criou categorias de titulares, com variações a depender do envolvimento com eventual crime, podendo também ser vítimas ou testemunhas. É de se supor que quanto maior a suspeita que recai sobre alguém, maior a legitimidade de intervenção em sua esfera de direitos para fins de investigação e/ou promoção de estratégias preventivas.

Nessa matéria, a estrutura e conteúdo entre os textos do PL e do APL são bastante semelhantes. Contudo, o PL promoveu uma alteração relevante ao suprimir a expressão "suficientes" no tocante aos "indícios" (art. 5º, incisos I e II, PL). Isso faz, na prática, com que graus de intervenção sejam autorizados a um grupo indeterminado de pessoas, uma vez que apenas "indícios" pode indicar uma rede enorme de situações em um caso concreto. Atribuir a qualidade de suficientes aos indícios é uma forma de limitar ações sem justa causa.

Dos princípios

O PL alterou as disposições relativas aos princípios regentes do tratamento de dados pessoais, em comparação ao APL. As mudanças convergem para uma debilitação geral das regras de transparência e do controle, público e pelo titular, sobre o tratamento dos dados pessoais em âmbito penal.

Três princípios elementares da proteção de dados pessoais foram suprimidos: **(i)** *proporcionalidade,* que estabelece que o uso de tratamento de dados pessoais deverá ser compatível com as finalidades pretendidas, devendo sempre adotar métodos que sejam menos invasivos (art. 6º, V, APL); (ii) *livre acesso*, que garante aos titulares de dados a consulta facilitada e gratuita sobre a forma e duração do tratamento, bem como sobre a integralidade dos dados pessoais (art. 6º, VI, APL); e (iii) *transparência*, que preconiza aos titulares de dados o direito a informações claras, precisas e de fácil acesso sobre o

3 "§2° Para efeitos do disposto no inciso I do §1° deste artigo, consideram-se: (...) II – dados cadastrais: informações referentes a nome e endereço de assinante ou de usuário registrado ou autenticado para a conexão a quem endereço de IP, identificação de usuário ou código de acesso tenha sido atribuído no momento da conexão."

tratamento e os agentes, respeitados os segredos comercial e industrial (art. 6º, VIII, APL).

Os princípios do livre acesso e da transparência estão previstos na LGPD. A sua exclusão pode ser entendida como uma violação à determinação da LGPD de que a lei específica para fins penais deve se orientar nos princípios gerais de proteção de dados. Como veremos no decorrer desta Nota Técnica, o PL não só exclui a referência a esses princípios, como esvaziou importantes regras para a sua efetivação.

Já o princípio da proporcionalidade, assim como o princípio da legalidade, foi inicialmente previsto no APL. Para além dos já enunciados princípios gerais de proteção, são esses outros dois princípios os fundamentos para o tratamento legítimo de dados pessoais para fins penais. Ambos são princípios tradicionais do direito penal e, como tais, têm implicações no tratamento de dados pessoais para fins de segurança pública e persecução penal.

O princípio da proporcionalidade nada mais é do que a determinação de que os meios utilizados pelo Estado para o alcance de determinado fim devem ser proporcionais ao que se busca. Isso tem implicações tanto na esfera legislativa quanto na executiva, de aplicação das leis. Um exemplo é a exigência de que normas autorizativas estejam vinculadas a determinados bens jurídicos – nem toda medida é válida a todo tipo de crime, cabendo as mais intervencionistas aos crimes mais graves.

Assim, a exclusão do princípio da proporcionalidade do texto do PL é preocupante, uma vez que se perde uma baliza essencial de ponderação da validade do tratamento de dados pessoais perante os fins almejados pelas autoridades competentes, a partir da análise da intervenção nas liberdades individuais e direitos fundamentais dos titulares.

Outros dois princípios, constantes no APL, foram alterados de modo a restringir sua aplicação. O *princípio da finalidade* (art. 6º, II, APL; art. 4º, II, PL), que originalmente limitaria o tratamento de dados pessoais a finalidades específicas, legítimas, explícitas e informadas aos titulares, teve o requisito de especificidade suprimido e passou a ser vinculado com a atuação de órgãos competentes, em conformidade com suas atribuições legais.

Conjugadas, as duas alterações a este princípio podem tornar legítima a coleta de dados para usos excessivamente amplos. Uma vez que o tratamento não seria orientado por uma finalidade específica, órgãos poderiam coletar, analisar e compartilhar dados pessoais oferecendo justificativas tão abrangentes quanto alegar que é necessário para o exercício de suas funções.

O *princípio da qualidade dos dados* (art. 6º, VII, APL; art. 4º, VIII, PL), por sua vez, foi alterado para excluir a referência ao titular de dados enquanto sujeito deste direito, o que também reduz a capacidade do titular para exercer controle sobre seus dados.

Ainda, destaca-se a substituição do *princípio da responsabilização e prestação de contas* (art. 6º, XII, APL) pelo chamado *princípio da auditabilidade*, uma versão mais branda daquele (art. 4º, X, PL). Enquanto o princípio da responsabilização e da prestação de contas traduz-se na demonstração da adoção de medidas eficazes e aptas a comprovar o respeito das normas de proteção de dados pelo agente, a auditabilidade limita-se à tomada de medidas que possibilitem "a verificação e a checagem do tratamento, bem como o controle do acesso à informação, sempre que tecnicamente possível", havendo, assim, uma transferência com relação à demonstração de que o tratamento é realizado

por meio de medidas eficazes e com observância da lei para terceiros. Destaca-se que não há indicação do que será verificado e para qual finalidade, o que pode gerar enorme insegurança jurídica na aplicação desse princípio.

Em síntese, esse leque de mudanças implica na diminuição de controle sobre os agentes de tratamento de dados e na grave fragilização das garantias conferidas aos titulares de dados pelo arcabouço principiológico originalmente previstos no APL. Também representa um desrespeito à determinação da LGPD, de que nova lei para fins penais se paute nos princípios gerais de proteção.

Por fim, destaca-se a adição do princípio da supremacia do interesse público, entendido como "prevalência do interesse público em conflito com um interesse particular" (art. 4º, VII, PL).

O princípio da supremacia do interesse público, bastante importante na esfera do direito administrativo, não encontra guarida em âmbito penal. Como já mencionado nesta Nota Técnica, o norte do direito penal moderno é justamente encontrar equilíbrio entre a intervenção estatal – seja em medidas de segurança, seja em medidas de investigação e repressão – e os direitos individuais. Um não se sobrepõe ao outro. Um exemplo importante dessa lógica é a existência no direito penal do princípio do *in dubio pro reo*, que estabelece que a decisão deverá ser em favor do réu (indivíduo) em caso de dúvida.

No mais, essa inclusão interpretada em conjunto com uma fundamentação que excluiu a autodeterminação informativa e identificou tacitamente a tutela da proteção de dados pessoais somente com a intimidade e com a vida privada, pode levar a uma interpretação legal que reflita o senso comum de conceber a privacidade individual como oposta à segurança coletiva. Essa interpretação é incompatível com a compreensão científica atual do tema, bem como com o direito fundamental consagrado em nosso ordenamento.

Das bases legais de tratamento de dados pessoais

Inicialmente, vale lembrar, que bases legais são situações e critérios previstos em lei que, quando verificados no caso concreto, autorizam o tratamento de dados pessoais. O PL alterou profundamente a estrutura do APL no que tange às bases legais para o tratamento de dados pessoais.

No APL há previsão de bases legais únicas para atividades de segurança pública e persecução penal. Já o PL subdividiu as hipóteses de incidência de bases legais em três grupos: (i) segurança do Estado e defesa nacional; (ii) segurança pública; e (iii) investigação criminal. Neste último caso, como veremos, não há bases legais enquanto hipóteses restritivas, mas tão somente uma autorização ampla de tratamento de dados pessoais e dados pessoais sensíveis para essa finalidade.

Segurança do Estado e defesa nacional

No que tange às hipóteses de tratamento de dados pessoais para fins de **segurança de Estado e defesa nacional**[4], a única condição apresentada é a existência de previsão legal específica (art. 7º, *caput,* PL), que "se consubstanciará nas competências legais" dos órgãos competentes e em normativas exaradas das autoridades máximas do Gabinete de Segurança Institucional ("GSI"), do Ministério da Defesa, da Agência Brasileira de Inteligência ("ABIN") e/ou das Forças Armadas (art. 7º, § 1º, PL).

Não fica claro, entretanto, qual o conteúdo do requisito de legalidade. Ao que parece, não estamos diante de uma legalidade estrita parlamentar, na qual o tratamento deve ser regulado por lei em sentido estrito. Diante da importância e sensibilidade da matéria, é importante haver um grau de controle externo a eventuais regulamentos das autoridades elencadas. Vale lembrar, ainda, que a competência para legislar em matéria penal, de competência da polícia federal, defesa territorial e mesmo proteção de dados é exclusiva da União (art. 22, CF).

A forma como o PL está redigido representa flagrante violação da hierarquia de normas e consequente usurpação das competências do Congresso Nacional. Ainda que o rol fosse taxativo, a enorme variedade de operações de tratamento citadas, muitas delas envolvendo riscos gravíssimos aos direitos fundamentais dos titulares, já seria suficiente para justificar a existência de contornos legais mais estritos para disciplinar cada uma delas.

Segurança pública

No âmbito da **segurança pública**, duas das três bases legais foram alteradas no PL .

O APL prevê a possibilidade de tratamento de dados pessoais para **(i)** cumprimento de atribuição legal de autoridade competente; **(ii)** na persecução do interesse público, na forma de lei ou regulamento, observados os princípios gerais de proteção, os direitos dos titulares e os parâmetros de acesso e transparência; e **(iii)** para a proteção da vida ou da incolumidade física do titular ou de terceiro, contra perigo concreto e iminente (art. 9º, APL). A terceira hipótese foi mantida pelo PL.

Já em relação à primeira, o termo "persecução do interesse público" foi substituído por "garantia do interesse público" e foram suprimidas as referências à existência de lei ou regulamento e ao respeito às garantias de transparência e acesso[5]. Essas alterações permitem que as autoridades competentes se pautem em justificativas excessivamente amplas para o tratamento dos dados e contribuem para a debilitação geral do princípio de

4 No PL, exemplos de atividades a serem regulamentadas "constituem-se, entre outras, naquelas referentes à inteligência de Estado; à garantia da lei e da ordem (GLO); às de emergência e de ajuda humanitária; às missões de paz: à segurança de grandes eventos; aos exercícios ou operações militares; e aos casos de emprego real das Forças Armadas, na forma da lei" (art. 7º, § 3º, PL).

5 PL, art. 9º O tratamento de dados pessoais para atividades de segurança pública poderá ser realizado nas seguintes hipóteses: I - quando necessário para o cumprimento de atribuição legal de autoridade competente, **na garantia do interesse público**, observados os princípios gerais de proteção e os direitos dos titulares na forma desta lei (nosso grifo).

transparência. O texto do PL representa, portanto, um risco para o controle social sobre as práticas das autoridades.

Em relação à segunda hipótese, o PL suprimiu a condicionante de previsão legal ("em forma de regulamento") da política pública[6]. Essa alteração está em desacordo com o próprio texto da LGPD que estabelece, para base legal similar, o respaldo das políticas públicas em instrumento formal que, conforme a ANPD, deve, em regra, prever metas, objetivos, prazos e meios executórios. Essa supressão viola o princípio da legalidade e, em particular, o da reserva legal. Com isso, permite tratamento expansivo de dados pessoais, em desrespeito aos princípio gerais de proteção.

Com relação aos dados pessoais sensíveis, também houve mudanças substanciais. O APL (art. 13, *caput* e parágrafo único) condicionava explicitamente essas operações à legalidade estrita, observadas as salvaguardas presentes na lei, sendo necessária a elaboração de Relatório de Impacto à Proteção de Dados Pessoais ("RIPD") e comunicação do documento à autoridade supervisora. Essas condicionantes não estão presentes no texto do PL, que, de forma geral, não endereça o risco derivado do tratamento de dados sensíveis de maneira suficiente.

No PL, por outro lado, quatro hipóteses foram apresentadas para tratamento de dados pessoais sensíveis para atividades de segurança pública: **(i)** cumprimento de dever legal; **(ii)** execução de políticas públicas, previstas em leis ou regulamentos pela administração pública; **(iii)** proteção da vida ou da incolumidade física, e **(iv)** defesa de direitos dos titulares (art. 9º, § 2º, PL).

A primeira hipótese é excessivamente ampla, o que pode levar a uma banalização do tratamento de dados pessoais sensíveis, uma vez que "dever" não se confunde com "obrigação". Assim, as autoridades competentes podem invocá-la com o simples argumento de que estão cumprindo a sua função. A segunda e a terceira hipóteses se assemelham às bases legais elencadas pelo APL. A quarta e última hipótese parece restrita ao atendimento dos direitos dos titulares.

Persecução penal

No âmbito do tratamento para fins de persecução penal, as mudanças realizadas carregam riscos ainda maiores. O PL estabeleceu uma autorização genérica para o tratamento de dados pessoais e de dados pessoais sensíveis, colocando como única condicionante a observância da legislação processual penal aplicável (art. 14, *caput,* PL). Trata-se de uma prerrogativa absolutamente ampla e da qual se poderia abusar facilmente, uma vez que o tratamento de dados pessoais significa qualquer operação realizada com estes dados.

No mais, a opinião unânime é de que a legislação penal e processual vigente não traz disposições suficientes para regular o tratamento de dados pessoais da matéria. O que temos são leis esparsas que regulam aspectos específicos da privacidade, como o direito ao sigilo.

Ainda, cumpre destacar que a legislação processual penal brasileira está notoriamente desatualizada, inclusive com relação às novas tecnologias, razão pela qual o Congresso Nacional discute há uma década a realização de uma reforma no Código de Processo Penal.

6 PL, art. 9º (...): II- para execução de políticas públicas, observados os princípios gerais de proteção, e os direitos dos titulares na forma desta lei.

Nesse sentido, a mera delegação da deliberação legal sobre o tema para a norma processual penal não pode ser considerada uma solução adequada aos dilemas normativos suscitados pela informatização da sociedade.

Do acesso e compartilhamento de dados pessoais

O APL propõe uma regulamentação ao compartilhamento e ao acesso a dados pessoais que parte de uma lógica de garantia ao devido processo legal, à privacidade e proteção de dados. Para tanto, cria uma seção própria para disciplinar a matéria. O PL, em sentido oposto, diluiu o regramento sobre compartilhamento no decorrer de seu texto.

Em comparação ao texto do APL, o PL fragiliza os limites ao acesso e ao compartilhamento de dados pessoais e dados pessoais sensíveis, ao mitigar o princípio constitucional da legalidade e reserva legal - base da atuação da Administração Pública e do direito penal e processual penal -, privilegiando uma genérica e pretensa eficiência na atuação dos órgãos públicos em detrimento dos direitos fundamentais à privacidade e à proteção de dados dos cidadãos.

Tal mitigação é evidenciada pela inclusão da eficiência e do intercâmbio de dados pessoais como objetivos do PL, em mesmo grau hierárquico da proteção dos direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural (art. 1°, I, II e III, PL). Além disso, há flexibilização de várias regras para o acesso a banco de dados, definindo que, para tanto, não seria necessário haver autorização legal ou judicial prévia, ou mesmo formalização dos pedidos de acesso e tratativas de compartilhamento.

A distinção entre o PL e o APL fica clara quando analisadas as regras para **(i)** o compartilhamento de dados entre autoridades competentes; **(ii)** o compartilhamento entre autoridades competentes e órgão ou entidade pública não competente; e **(iii)** o compartilhamento de dados entre as autoridades competentes e entes privados. Abaixo, trataremos das modificações propostas no PL, seguindo essa estrutura.

Compartilhamento entre autoridades competentes

Em linhas gerais, no que se refere ao compartilhamento de dados pessoais entre as autoridades competentes, o APL prevê importantes balizas, enquanto o PL prevê um regime de compartilhamento irrestrito.

O APL determina que o uso compartilhado de dados pessoais só será possível mediante autorização legal, autorização judicial ou no contexto de "atuações conjuntas legalmente autorizadas" (art. 45, APL). Além disso, o APL estabeleceu a vedação ao compartilhamento direto e contínuo de bancos de dados entre autoridades competentes para fins de persecução penal, sendo autorizado o compartilhamento apenas para investigações ou processos criminais específicos, ou seja, já existentes (art. 45, §1º, APL). Por fim, o APL acrescenta, ainda, a obrigatoriedade de que as requisições de acesso a dados, entre autoridades competentes, ocorram de forma devidamente motivada (art. 45, §2º, APL).

Por outro lado, no que concerne ao tratamento de dados pessoais no âmbito da **segurança do Estado e da defesa nacional**, o PL prevê prerrogativa geral de compartilhamento de dados pessoais entre as autoridades competentes incumbidas dessas atividades "com o objetivo de proporcionar eficácia às ações daqueles órgãos", submetendo tal compartilhamento unicamente ao respeito dos princípios estabelecidos no PL (art. 7º, § 2º, PL). O caráter genérico dessa redação traduz-se numa autorização ampla para o compartilhamento de dados pessoais entre os órgãos.

Já para o tratamento de dados pessoais em **atividades de segurança pública e investigação e repressão de infrações penais**, o PL suprimiu as garantias presentes no APL. Especificamente no âmbito da persecução penal, há previsão autorizativa ampla de compartilhamento de dados pessoais (art. 14, PL).

Uma das razões para as restrições ao compartilhamento estabelecidas no APL é o respeito ao princípio da finalidade. Órgãos de segurança pública tratam dados para finalidades diferentes de órgãos de persecução penal e, por isso, o compartilhamento irrestrito de dados pessoais entre eles violaria esse importante princípio geral de proteção. O PL, ao suprimir essas restrições e violar o princípio da finalidade, fomenta a existência a um estado de vigilância, no qual as autoridades competentes poderão ter acesso a amplíssimo grupo de informações dos cidadãos, mesmo sem autorização legal ou prova de motivo para tanto.

Compartilhamento entre autoridade competente e entidade da Administração Pública não competente

O PL deixa também de trazer regras suficientes para o compartilhamento de dados entre uma autoridade competente e órgão ou entidade da Administração Pública não competente. Vale lembrar que o APL determinou que, no contexto desse tipo de compartilhamento, é necessária a comprovação da convergência de finalidade com aquela da coleta original (art. 46, APL). Nesse caso, o compartilhamento dependeria ainda de requisição e autorização administrativa devidamente motivada (art. 46, § único, APL).

Diferentemente, o PL prevê diretrizes gerais para esse tipo de compartilhamento, no âmbito das atividades de segurança pública e persecução penal, quais sejam: **(i)** previsão expressa autorizando o compartilhamento de dados pessoais entre órgãos e entidades federais, distritais, estaduais e municipais, desde que observadas as restrições legais, os requisitos de segurança da informação e comunicações; (**ii)** assunção pelo recebedor de dados dos deveres de sigilo e auditabilidade; **(iii)** conformidade dos mecanismos de compartilhamento, interoperabilidade e audibilidade ao que foi chamado pelo PL de "*necessidades de negócio dos órgãos de segurança pública";* e **(iv)** colaboração para redução dos custos, inclusive, mediante o reaproveitamento de recursos de infraestrutura e de sistemas por múltiplos órgãos e entidades (arts. 11 e 15, PL).

O PL estabelece, ainda, que as diretrizes do tipo de compartilhamento com pessoas de direito privado também se aplicam a essa hipótese de compartilhamento (art. 17, PL; v. tópico abaixo).

As diretrizes estabelecidas no PL para esse tipo de compartilhamento podem ser objeto de diversas críticas. Em primeiro lugar, cabem aqui as observações feitas no tópico anterior sobre violação do princípio da finalidade e fomento de um estado de vigilância, uma vez que as autoridades competentes poderão ter acesso a uma gama infinita de informações

de outras entidades (podendo, inclusive, compartilhá-las entre si) sem necessária análise prévia de legalidade, proporcionalidade e necessidade.

Em segundo lugar, não fica claro o que seriam "necessidades de negócio" dos órgãos de segurança pública e, por isso, causa preocupação. As autoridades competentes, por não serem entidades de direito privado, não seriam pautadas por "negócios", mas sim por suas funções constitucionalmente estabelecidas no contexto de um estado democrático.

Por fim, tampouco cabe ao PL definir que o compartilhamento deve se pautar por redução de custos. Tal determinação pode levar à sobreposição de uma lógica eficientista, com resultados lesivos a direitos fundamentais. O reaproveitamento de recursos e estrutura eleva não só os riscos técnicos relacionados à segurança da informação, como também aumenta riscos de desvio de finalidade. Como já dito reiteradamente nessa Nota Técnica, o tratamento de dados pessoais deve se pautar em diretrizes de proteção a direitos e regulação de risco, devendo os mecanismos de compartilhamento seguir o mais alto padrão técnico e administrativo no tocante à proteção de dados pessoais.

No mais, sobre a segunda diretriz, ver crítica quanto à substituição do princípio de responsabilização e prestação de contas pelo da auditabilidade no item "Dos Princípios".

Compartilhamento entre autoridades competentes e pessoas jurídicas de direito privado

O texto do APL veda, como regra geral, o compartilhamento de dados pessoais pelas autoridades competentes com pessoas jurídicas de direito privado (art. 47, *caput,* APL), mas abre algumas exceções devidamente reguladas[7].

O PL, por sua vez, não prevê limitações ao compartilhamento de dados pessoais entre autoridades competentes e pessoas jurídicas de direito privado para as atividades de segurança do Estado e de defesa nacional.

Para as atividades de segurança pública, o PL adota um regime geral de autorização ao acesso de autoridades competentes a dados pessoais e a bancos de dados privados (art. 12, PL), prevendo a possibilidade de compartilhamento mediante previsão legal, cooperação voluntária, celebração de contrato, acordo de cooperação ou instrumento congênere para o acesso aos dados pessoais (art. 12, III, PL). Determina apenas que estejam presentes "razões de interesse público devidamente motivadas em ato administrativo", com adoção de medidas de proteção (art. 13, PL).

Para fins de investigação e repressão de infrações penais, o PL mantém o regime geral de autorização ao compartilhamento ainda mais amplo. Em comparação com as hipóteses de compartilhamento previstas em âmbito de segurança pública, o PL substitui a modalidade de previsão legal por requisição do delegado de polícia ou Ministério Público, mantém a possibilidade de celebração de contrato (ou outro instrumento equivalente) e cooperação voluntária, e inclui a possibilidade de "canal técnico de inteligência de Estado" (art. 18, PL).

7 São elas: i) nos casos de execução descentralizada de atividade pública, autorizada em lei, e que exija a transferência, exclusivamente para esse fim específico e determinado; ii) nos casos em que os dados forem acessíveis publicamente, observadas as demais disposições desta Lei e da LGPD; e iii) nos casos das pessoas jurídicas de direito privado que possuam capital integralmente constituído pelo poder público, desde e que esteja na qualidade de operadora de tratamento de dados (art. 47, I, II e III, APL).

O PL delega à legislação processual penal a função de regular o acesso a dados sujeitos a sigilo legal ou constitucional, "sem prejuízo do acesso aos dados cadastrais" (art. 19, PL).

Da forma como está redigido, o PL instrumentaliza agentes privados para serem uma espécie de continuação dos órgãos de segurança pública e persecução penal. Com esse delineamento, o PL afronta o Marco Civil da Internet (MCI) e todo o arcabouço protecionista da proteção de dados pessoais e da privacidade construído, sem estipulação de limites mínimos como, por exemplo, necessidade de demonstração de um inquérito policial ou de um processo judicial em curso, e até mesmo de autorização judicial (art. 18, I, PL).

Ainda, ao negar necessidade de previsão legal e permitir o compartilhamento mediante instrumentos amplos, relegando às partes envolvidas a decisão de como o compartilhamento será feito (sem controle prévio ou posterior), há violação clara ao princípio da reserva legal, ao princípio da presunção de inocência, ao princípio da finalidade, proporcionalidade e necessidade, apenas para citar alguns. Com isso, cria-se o risco de compartilhamento irrestrito de dados dos cidadãos, ainda que não estejam sendo investigados por prática delituosa.

De modo geral, a redação do PL sobre compartilhamento de dados carrega riscos relacionados ao exercício das atribuições de zelar pelos dados pessoais, uma vez que órgãos com capacidades econômicas e infraestruturas tão díspares dificilmente conseguirão assegurar a segurança, a prevenção de incidentes de segurança e os demais deveres associados a um cenário de amplo compartilhamento de dados. No mais, qualquer norma que busque regular a proteção de dados pessoais em âmbito penal deve prever expressamente as hipóteses em que o acesso e compartilhamento poderá ocorrer, de forma a trazer segurança jurídica e reduzir espaços para arbitrariedades na atuação do Estado.

Do tratamento de dados pessoais sigilosos

O conceito de dado pessoal sigiloso apresentado no APL diz respeito a "dado pessoal protegido pelo sigilo constitucional ou legal" (art. 5º, III, APL).

O conceito remete, por um lado, às regras de proteção de dados pessoais, articulado por normas como o Marco Civil da Internet, a Lei de Acesso à Informação, a Lei do Cadastro Positivo e a própria LGPD. Por outro lado, vincula-se à dogmática processual penal, calcada na noção de tutela do sigilo dos dados e das comunicações e conformada a partir dos regramentos constitucionais e infraconstitucionais sobre hipóteses de quebra legítima de sigilo.

O APL condiciona o tratamento dessa categoria de informações aos termos previstos em lei e limita o âmbito de atuação, só podendo ser utilizado para fins de persecução penal (art. 14, *caput,* APL). Além disso, enfatiza a observância da legislação especial aplicável quando desse acesso via ferramentas de investigação e medidas cautelares de obtenção de prova (art. 14, § 1º, APL).

Ainda, eventual acesso a essa categoria de informações sob tutela de entes privados dependeria de autorização judicial, sendo requerida a demonstração da necessidade da medida e de indícios quanto ao envolvimento dos titulares afetados pela medida em infração penal específica, sem prejuízo da comunicação de operações suspeitas (art. 14, § 2º, APL).

O PL suprimiu tanto o conceito de dado pessoal sigiloso quanto as garantias estabelecidas no APL. Com isso, o projeto, caso aprovado, pode gerar grave insegurança jurídica, posto que elimina uma ferramenta normativa fundamental à construção de uma interpretação sistêmica dos dois paradigmas legais representados pela legislação de proteção de dados e pela legislação processual penal.

Além disso, vale destacar que a decretação de sigilo pelo legislador penal em determinadas situações foi uma forma encontrada de proteger informações consideradas especialmente críticas para o indivíduo, em consideração à sua privacidade. Ao possibilitar o tratamento dessas informações de forma ampla, o PL acaba por desvirtuar esses fundamentos.

Das decisões automatizadas

Diferente de outros termos bem definidos na LGPD, não há em seu texto uma definição clara de sistemas de decisão automatizada. Apesar da nebulosidade quanto ao tema, esses sistemas são tratados, em linhas gerais, como os processamentos de dados feitos a partir de inteligências artificiais, aptas a correlacionar informações disponibilizadas em bancos de dados para a tomada de decisões.

É necessário redobrar a atenção às possíveis violações de direitos fundamentais decorrentes deste modelo de tratamento de dados, já que são várias as experiências, nacionais e internacionais, que comprovam a fragilidade e a alta taxa de erros, vieses algorítmicos discriminatórios e consequentes injustiças perpetradas por sistemas de decisões automatizadas. Em âmbito penal, a situação ganha maior gravidade, uma vez que esses erros e vieses podem eventualmente levar à privação de liberdade de alguém. No mais, estamos falando de um campo em que tramitam informações de alto potencial discriminatório.

Uma das causas mais evidentes para esses problemas é a opacidade do funcionamento dos sistemas baseados em algoritmos, que operam sob parâmetros pouco conhecidos e de difícil acesso. Diante disso, sua implementação, especialmente para os fins do escopo do PL em análise, deve ser meticulosamente avaliada.

Enquanto o APL preocupa-se em regulamentar de maneira rígida a forma de aplicação, explicação e avaliação do impacto do funcionamento de decisões automatizadas, o PL suprime ou altera boa parte desse conteúdo.

O APL regra o tratamento automatizado de forma detalhada, contemplando as diversas etapas: **anterior, durante** e **após o tratamento**. Além disso, separa em artigos distintos a consequência do tratamento ao titular, prevendo regras próprias para cada possibilidade. Também, o APL dispõe sobre o tratamento que afete o direito dos titulares e discorre sobre o que poderá ensejar risco elevado para os direitos fundamentais do titular ou que possa acarretar medidas coercitivas ou restritivas de direitos (art. 23 e 24, APL). Com isso, o APL propõe-se a regrar uma efetiva gestão de riscos no tocante a esse tratamento.

Apesar da escolha estrutural do texto do PL em reservar uma seção exclusiva para abordar o tema, há apenas dois artigos bastante genéricos disciplinando a matéria. Neles ficam vedadas decisões tomadas exclusivamente com base no tratamento automatizado, além de haver previsão de, quando houver decisão automatizada, haverá garantia ao titular de dados do direito de solicitação de intervenção humana do responsável pelo tratamento automatizado (arts. 20 e 21, PL).

Assim, percebe-se que, comparativamente, o APL se refere a decisões que "afete o direito dos titulares" e "que enseje um elevado risco para os direitos fundamentais do titular ou que possam acarretar medidas coercitivas ou restritivas de direitos", enquanto a vedação do PL é referente apenas a tratamentos exclusivamente automatizados que produzam "efeitos adversos na esfera jurídica do titular de dos dados ou que o afetem de forma significativa" (art. 20, PL). Podemos inferir que a adição do qualificador "exclusivamente" pode tornar o dispositivo materialmente ineficaz, já que a existência de intervenção humana em qualquer etapa da decisão poderia fundamentar que a vedação não seria aplicada ao caso concreto.

Somado a isso, com a exclusão de parte considerável do texto do APL que trata da elaboração de RIPDs, abordado a seguir, fica mais difícil determinar quais circunstâncias justificariam a vedação, tendo em vista que a nova redação não traz parâmetros concretos para avaliação do risco da atividade.

Apesar de haver previsões semelhantes à realização do tratamento automatizado em sistemas auditáveis, não discriminatórios e passíveis de comprovação acerca de sua precisão e grau de acurácia, o APL vai além ao prever também o papel da autoridade competente em fornecer informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada. O APL também prevê a discricionaridade da autoridade para solicitar a realização de auditorias para verificação do procedimento e do cumprimento de regras quanto à acurácia e à não discriminação, o que implicaria em menos erros procedimentais.

Se o APL tem a preocupação em tornar público os RIPDs com informações sobre os mecanismos para proteção dos direitos e das liberdades dos titulares, submetendo à autoridade competente para exame e decisão acerca da possibilidade de efetivação do tratamento automatizado, o mesmo não ocorre com o PL, que excluiu tal previsão. Por consequência, o novo texto suprimiu também o direito do titular em receber notificações sobre decisões automatizadas e excluiu qualquer previsão a respeito da exclusão de dados sensíveis para este tratamento (art. 23, APL).

Ainda que no PL a exclusão da tomada de decisão realizada exclusivamente com base no tratamento automatizado pareça ser revestida de preocupação com o titular e com a garantia aos seus direitos, a supressão de todos os demais procedimentos previstos pelo APL deixa uma lacuna significativa a respeito do tratamento efetivado por esses sistemas e do risco ou não que o uso dessa tecnologia representa para os titulares.

Outro ponto que chama atenção, é que o PL acrescenta, com o artigo 21, a possibilidade de solicitar a intervenção humana do responsável pelo tratamento, não esclarecendo, porém, se isso constitui um efetivo direito de revisão, como previsto de forma expressa no art. 25, §3°, do APL.

Ademais, são previstas de forma genérica a vedação geral da constituição de perfis e de tecnologias que conduzam à discriminação, com base em dados pessoais sensíveis (art. 21, §1°, PL), e transporta para essa sessão a previsão de auditoria acerca da não discriminação e acurácia (art. 21, §2°, PL); porém, com a já referida exclusão do procedimento, o dispositivo acaba por ficar esvaziado.

Das tecnologias de monitoramento

Tecnologias de monitoramento e tratamento de dados pessoais de elevado risco têm sido implementadas no mundo todo. Como resposta, há uma tendência legislativa mundial de limitar, ou mesmo proibir, o uso desse tipo de tecnologia. Países dividem-se entre a implementação dessa inovação com medidas de mitigação de riscos, imposição de estratégias intermediárias (como moratórias) e o completo banimento dessas tecnologias. Dada sua importância, o uso de tecnologias de monitoramento recebeu um capítulo específico no APL. Porém, o PL suprimiu as previsões quase em sua totalidade.

A utilização de tecnologias de monitoramento pode facilmente ser vendida sob o discurso de inovação e aprimoramento tecnológico no campo da segurança pública e persecução penal. No entanto, a implementação desse tipo de tecnologia já demonstrou seu potencial de violação aos direitos fundamentais, individuais e coletivos.

Isso porque, sua implementação, tradicionalmente, materializa-se na forma de instrumentos para tratamento de dados pessoais captados ou analisados em vídeo, imagem, texto ou áudio, como câmeras de segurança combinadas com tecnologias de reconhecimento facial instaladas em espaços públicos. Com isso, cria-se um cenário de permanente vigilância, em que a busca de uma suposta segurança acaba por violar direitos como privacidade e intimidade, presunção de inocência e outros, havendo um desequilíbrio entre os benefícios trazidos por essas tecnológicas e os riscos oferecidos aos direitos fundamentais dos cidadãos.

Em análise direta, o APL estabelece que as tecnologias de monitoramento sejam condicionadas à **(i)** previsão legal específica; **(ii)** análise do impacto regulatório; **(iii)** RIPD, visando a observância dos princípios acima mencionados (art. 42, APL). Além disso, define critérios para a avaliação dos riscos do tratamento, como definição da: **(i)** natureza dos dados envolvidos; **(ii)** finalidades específicas do tratamento; **(iii)** possibilidade de discriminação como critério mínimo para avaliação (art. 42, §1º, APL).

Outro ponto importante é a previsão da criação de uma norma específica para regulamentar o uso da tecnologia de vigilância, que estabeleça garantias aos direitos dos titulares e que deverá ser precedido da avaliação de análise de impacto regulatório[8] (art. 42, §2º APL).

Ademais, o APL veda a utilização de tecnologia de vigilância diretamente acrescida de técnica de identificação de pessoas indeterminadas e de forma contínua quando não houver conexão com a atividade de persecução penal individualizada e autorizada por lei e combinada com decisão judicial. Determina, ainda, que o CNJ, enquanto autoridade supervisora, emitirá opiniões e pareceres técnicos referente à utilização das referidas tecnologias, ante a potencialidade de violação de direitos.

O PL, no entanto, suprimiu todo o regramento do APL voltado para tecnologias de monitoramento. A única exceção (ainda que parcial) é a possibilidade geral da autoridade supervisora (no caso, a ANPD) de opinar tecnicamente e solicitar RIPDs às autoridades competentes (art. 6º, §3º, PL; art. 44, §1º).

8 Pela definição do APL, análise de impacto regulatório seria a "documentação para instruir o processo legislativo acerca da autorização para a utilização de tecnologias de vigilância e o tratamento de dados pessoais por autoridades competentes que implique elevado risco aos direitos, liberdades e garantias dos titulares dos dados" (art. 5º, inc. XIX, APL).

Com isso, o PL cria uma permissão irrestrita para o tratamento de dados pessoais por meio de tecnologias de monitoramento, prática entendida como de alto risco aos direitos fundamentais e liberdades individuais dos titulares de dados. Assim, vai na contramão da tendência global de regular esses riscos, ignorando todo o conhecimento já produzido sobre os potenciais efeitos deletérios produzidos através do uso desregulado dessas tecnologias.

Dos direitos dos titulares

Em comparação com o APL e a própria LGPD, o PL enfraquece os direitos dos titulares dos dados pessoais (arts. 25, 28 e 29, PL). Isso porque suprimiu os direitos de anonimização, bloqueio ou eliminação de dados e o direito de requerimento sobre informações a respeito do compartilhamento de dados pessoais.

Em primeiro lugar, o PL exclui o direito de requisitar a anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com as disposições da Lei (art. 25, PL). Além disso, exclui a possibilidade de o titular ter conhecimento sobre as entidades públicas e privadas com as quais o controlador realizou o compartilhamento dos dados, deixando-o, portanto, às cegas no que diz respeito ao compartilhamento de seus dados, dos procedimentos executados com suas informações e dos dados em posse do controlador (art. 25, PL; art. 19, APL).

A supressão do direito de exclusão representa um grande retrocesso, já que enfraquece o controle pelo próprio titular de eventual tratamento desnecessário. Com isso, há um controle a menos para evitar que agentes de tratamento de dados mantenham desnecessariamente a posse de quantidade significativa de dados pessoais, o que cria riscos de segurança e desvio de finalidade. Essa previsão representa também uma violação ao princípio da minimização de dados consolidado na LGPD, que direciona a atuação do controlador no sentido de minimizar a coleta dos dados pessoais dos titulares, tratando somente aqueles estritamente necessários à finalidade pretendida.

A exclusão do direito de acesso à informação sobre compartilhamento também é bastante preocupante, uma vez que intrinsecamente relacionada com o princípio da transparência e do livre acesso, e com o fundamento da autodeterminação informativa. Não por acaso, como já visto no decorrer da Nota Técnica, esses princípios e fundamentos foram suprimidos.

Vale lembrar que a LGPD determina que essa nova lei observe os direitos do titular. Com a exclusão de dois importantes direitos, há violação clara dessa determinação.

O PL, ao tratar do direito de acesso às informações sobre o tratamento de dados pessoais, prevê que o acesso deverá ser feito através de requerimento à autoridade competente, que deverá providenciar respostas aos titulares no prazo de 20 dias da entrada do requerimento (art. 28, PL). Em comparação ao APL, o prazo foi expandido de 15 para 20 dias (art. 22, III, APL). Além disso, o PL retira a possibilidade de confirmação de existência ou acesso imediato às informações, prejudicando um rápido, diligente e completo procedimento (art. 28, PL).

O PL exclui, ainda, o acesso aos parâmetros da declaração mais detalhada de confirmação de existência de dados, como o dever de informar a origem, inexistência de registro, critérios e finalidades do tratamento - direito antes previsto no APL (art. 22, inc. II, PL).

Foram excluídos também o direito de realizar denúncias confidenciais sobre violação à lei e a possibilidade do exercício de defesa dos interesses e dos direitos dos titulares por via judicial individual ou coletiva acerca dos instrumentos de tutela individual e coletiva (arts. 27 e 28, APL). Esse contexto, além de obstar o exercício do direito do titular, o coloca em situação de maior vulnerabilidade em caso de vazamento ou compartilhamento indevido de dados.

Por fim, o PL determina que o direito de acesso pelos titulares se dará nos termos da legislação processual vigente (art. 29, PL), transferindo sua responsabilidade de regulação para as normas como o Código de Processo Penal ("CPP"). Essa determinação é problemática por dois motivos: (i) cabe ao próprio PL, a partir da determinação da LGPD ao tratar da necessidade de legislação específica, disciplinar a matéria - a regulação sobre o atendimento a direitos dos titulares é tema típico de legislação sobre proteção de dados; (ii) a legislação processual vigente, e em particular o CPP, não conta hoje com regras nesse sentido – haveria, portanto, a criação de uma lacuna relevante.

Diante das alterações trazidas pelo PL, o titular dos dados pessoais ficará mais vulnerável, já que perde a salvaguarda legal de pleitear alguns direitos relativos à posse e ao compartilhamento de seus dados pelo controlador, ainda que em latente violação à lei.

Vale ressaltar que por se tratar de tratamento de dados para fins de segurança pública e persecução penal, é legítimo pensar em limitações aos direitos dos titulares, uma vez que a sua efetivação, em alguns casos, pode comprometer uma medida governamental preventiva ou uma investigação ou processo criminal. Contudo, já havia no APL previsão expressa de que a prestação de informações e acesso a elas pode ser recusada para evitar prejuízos nesses campos (art. 20, APL). Essa previsão foi mantida pelo PL (art. 26, PL). Ou seja, uma vez que essa previsão já está presente, as novas limitações de direitos não podem se justificar na ideia de manter a eficiência da atividade preventiva ou repressiva penal.

Da ausência de transparência

O APL dedicava um capítulo inteiro ao tema da transparência e do acesso à informação. Tendo em vista a histórica falta de transparência sobre as atividades realizadas no âmbito da segurança pública e persecução penal, a redação do APL significou importante avanço.

No APL, entre as obrigações atribuídas às autoridades, estavam o dever de prestar informações claras e atualizadas sobre base legal, finalidade, objetivos específicos, procedimentos e práticas associadas ao tratamento realizado (art. 40, *caput,* APL), informações essas que seriam pormenorizadas em lei ou regulamento (art. 40, § 1º, APL).

Ainda, o acesso a tais informações deveria ser ofertado de forma facilitada, preferencialmente, em seus sítios eletrônicos, de maneira clara, adequada e ostensiva sobre finalidade do tratamento, forma, escopo, duração, políticas aplicáveis, identificação e contato do controlador, uso compartilhado, responsabilidades dos agentes e direitos dos titulares (art. 40, § 2º, APL).

Adicionalmente, previa-se a publicação anual de relatórios de requisição de dados pessoais sigilosos pelas autoridades máximas de cada autoridade competente, os quais

deveriam informar o número de pedidos realizados e de titulares afetados, a natureza dos dados solicitados, as categorias de atores privados destinatários dos requerimentos e, quando da proteção do dado por reserva de jurisdição, os números de pedidos deferidos e indeferidos à luz do total de solicitações (art. 41, APL). Essa iniciativa seria similar ao que ocorre atualmente com o Sistema Nacional de Controle de Interceptações, mantido pelo Conselho Nacional de Justiça ("CNJ"), que agrega e exibe dados enviados pelos tribunais sobre as interceptações realizadas para fins de controle público e transparência. Uma vez que os dados sobre requisição de dados sigilosos seriam divulgados em formato agregado, não há risco identificável a algum bem ou interesse legalmente protegido.

O PL suprimiu essas obrigações integralmente, em mais um ataque à efetivação dos princípios da transparência e do livre acesso. A prestação de informações sobre o tratamento realizado é um pressuposto da construção moderna do direito à proteção de dados, constituindo condição inafastável para o exercício do controle social sobre potenciais usos abusivos e discriminatórios.

A divulgação pública desses dados é essencial não somente para que as autoridades competentes possam exercer seu poder de fiscalização, mas para que outros setores da sociedade, como, por exemplo, pesquisadores e jornalistas, possam avaliar a observância dos requisitos legais e a verificar a eficácia das políticas atuais, no contexto dos objetivos da lei, podendo propor mudanças ao longo do tempo. Além disso, é extremamente importante para os titulares, os quais devem ter o direito à informação, até mesmo para pautar o seu comportamento.

A supressão desse tópico no PL relaciona-se com outras alterações legislativas, em comparação com o APL: supressão dos princípios de transparência e livre acesso, supressão do fundamento da autodeterminação informativa, desidratação do rol de direitos dos titulares e supressão de diversas regras relacionados no decorrer do texto legislativo.

Dos limites e do término do tratamento de dados pessoais

O APL estabelece um dever de descarte imediato de dados pessoais irrelevantes ou excessivos em relação à sua finalidade pela autoridade competente que obtivesse tais informações (art. 15, *caput*, APL). Essa previsão foi suprimida no PL, o que pode prejudicar a minimização da coleta, ferindo o princípio da necessidade e levando a um armazenamento excessivo e desproporcional de dados (art. 24, *caput)*.

Ainda, o APL parametrizava o término do tratamento, estabelecendo quatro hipóteses para sua ocorrência imediata: (i) verificação de ausência de necessidade ou finalidade; (ii) verificação de cumprimento da finalidade; (iii) fim do período de tratamento; ou (iv) determinação do CNJ, enquanto autoridade supervisora (art. 16, APL). Tais disposições foram integralmente suprimidas, representando um prejuízo aos direitos dos titulares e a retirada de um incentivo para a observância dos requisitos de finalidade, necessidade, segurança e prevenção.

As hipóteses autorizativas da conservação dos dados após o período de tratamento também foram modificadas. Enquanto o APL previa autorização para tratamento de dados pessoais para fins de estudo por órgão de pesquisa, garantida, sempre que possível, a

anonimização (art. 17, II, APL), o PL suprimiu essa possibilidade, reduzindo a transparência e prejudicando a realização de pesquisas científicas necessárias ao aprimoramento das políticas públicas de segurança pública (art. 22, APL). Além disso, adicionou uma autorização ampla para manutenção para fins de transferência a terceiros e uso exclusivo do controlador quando anonimizados (art. 22, II e III, PL). Nesses casos, as autoridades competentes deverão definir prazos para a eliminação (art. 22, § único, PL).

Na prática, as alterações realizadas podem levar ao armazenamento dos dados pessoais por tempo indeterminado, em clara violação ao princípio da necessidade. Nesse sentido, chama particular atenção a inclusão da hipótese de armazenamento para fins de transferência a terceiros. Além de possibilitar o tratamento de dados por período de tempo desproporcional, incentiva eventual desvio de finalidade quando do compartilhamento e dificulta o controle sobre o ciclo de vida dos dados. No mais, a transferência não pode ser enquadrada como um fim em si mesmo, mas como uma operação de tratamento destinada a satisfazer uma finalidade legítima, explícita e determinada.

Dos registros das atividades de tratamento de dados pessoais

O PL suprimiu uma série de requisitos previstos no APL para o cumprimento das obrigações de registro das atividades de tratamento. Foram retirados do texto apresentado o dever de registrar os contatos dos agentes de tratamento (art. 33, I, APL; art. 38, I, PL); os procedimentos previstos para revisão periódica da necessidade de conservação dos dados (art. 33, VIII, APL; art. 38, VIII, PL); as qualificações sobre as medidas de segurança utilizadas (art. 33, IX, APL; art. 38, IX, PL); e os pedidos dos titulares, sua tramitação, as decisões do responsável a respeito dos pedidos e a fundamentação das referidas decisões (art. 33, X, APL). Ademais, foi adicionada a possibilidade de inclusão de outras informações a serem registradas, conforme determinação da ANPD (art. 38, parágrafo único, PL)

Essa debilitação das informações a serem registradas é prejudicial à fiscalização do cumprimento dos fins da lei pelos agentes de tratamento. No mais, para o próprio agente de tratamento também é importante manter registros completos, uma vez que são essenciais para a construção e manutenção de um programa de governança de dados adequado, visando garantir a transparência, o acesso aos dados, a segurança, entre outros princípios legais.

Da segurança e do sigilo dos dados pessoais

O APL elencou uma série de objetivos a serem alcançados pelas medidas de segurança impostas tomadas pelos controladores, como controle de acesso aos equipamentos, de suporte e acesso a dados, da conservação, da comunicação, etc. (art. 36, §2º, APL). Nesse sentido, seguindo lógica similar, o PL lista algumas medidas que deverão ser seguidas pelo controlador a fim de evitar possíveis violações aos direitos dos titulares de dados processados de forma (não exclusivamente) automatizada e determina o registro em sistemas de tratamento automatizado das informações relativas às operações que realizam o tratamento (arts. 30 e 39, PL).

Como é possível notar, na redação dada aos dispositivos referentes à matéria no PL (art. 30, § 3º, PL), esses objetivos passaram a ser concebidos como medidas em si mesmas e sua aplicabilidade foi restringida ao tratamento automatizado de dados.

Ambas as mudanças são problemáticas. Ao tratar objetivos de segurança como medidas, o PL pode inviabilizar sua concretização, dado que mesmo a tomada de todas as medidas possíveis pelo agente não torna o sistema invulnerável a ataques. Nesse sentido, é preciso compreender que as medidas visam aumentar os custos de um ataque, reduzir os danos derivados e a probabilidade de concretização do ataque, sendo impossível eliminar completamente os riscos.

Quanto à restrição ao tratamento automatizado, ela é incompatível com o direito fundamental à proteção de dados pessoais, posto que essa proteção não se limita aos dados pessoais tratados de forma automatizada, mas se estende a todo e qualquer dado pessoal. E isso não se dá por acaso: todo e qualquer tratamento de dados pessoais apresenta riscos que precisam ser mitigados por medidas técnicas e administrativas.

Também foi removido o dever de adequação dos sistemas desenvolvidos previamente à vigência da lei aos requisitos de segurança, aos padrões de boas práticas e de governança e aos princípios gerais previstos na norma e demais regulamentos (art. 37, APL). Essa alteração remover qualquer eficácia material de tais requisitos, uma vez que praticamente todas as infraestruturas existentes e utilizadas pelas instituições atualmente estarão isentas de sua aplicabilidade. Ainda, foi suprimido o dever de anonimizar ou pseudonimizar os dados o quanto antes, o que contrapõe o princípio da necessidade (art. 37, § 2º, APL).

A obrigação de implementação de medidas para garantir a realização dos princípios da necessidade e da finalidade, prevista originalmente no APL deu lugar no PL a um dever de adotar medidas para garantir a "rastreabilidade e a auditabilidade dos sistemas" (art. 37, § 3º, APL; art. 31, §2º, PL). Essa alteração pode provocar insegurança jurídica substancial, haja vista que "rastreabilidade" não é um conceito definido no texto legal e tampouco no campo da segurança da informação e políticas de internet.

Quando da ocorrência de incidentes de segurança, foi suprimido o dever de notificação aos titulares dos dados (art. 38, *caput,* APL) e o prazo para notificação à autoridade supervisora, antes de 72 horas (38, § 1º, APL), foi submetido à determinação pela autoridade (art. 32, § 1º, PL). Tais alterações são lesivas aos titulares, que poderão ser prejudicados pelo desconhecimento de um vazamento de seus dados ou de outro incidente que os afete.

No âmbito do juízo de gravidade dos incidentes de segurança, foram excluídos os critérios de segurança e prevenção (APL, art. 38, § 3º), uma alteração inexplicável, haja vista que a introdução desse critério opera precisamente como um incentivo para que os agentes de tratamento ajam proativamente na prevenção e mitigação dos riscos.

Também foram suprimidas a referência à presunção de inocência e finalidade de integração social do condenado entre os objetivos do tratamento dos registros criminais (art. 39, *caput*, APL), bem como o dever de adoção de medidas de segurança para garantia do sigilo processual pelos agentes que tenham acesso a autos sigilosos (art. 39, § 1º, APL).

Por fim, foi suprimida a proteção de elementos identificadores em investigações ou processos relativos a atos infracionais. Com isso, o PL suprimiu a única menção de aplicabilidade do APL à justiça juvenil. A supressão está em desconformidade com o Estatuto da Criança e do Adolescentes e normativas internacionais (como as Regras de Beijing e a Convenção Internacional sobre os Direitos da Criança), que estabelecem que o direito à privacidade dos menores de idade deve ser particularmente respeitado no âmbito

da justiça juvenil[9]. Em contexto similar, também foi suprimida a proteção de elementos identificadores em caso de crimes contra a dignidade sexual, independentemente de sigilo judicialmente comandado (art. 39, §§ 2º e 3º, APL,).

Da transferência internacional de dados e cooperação internacional

Um dos pontos mais aguardados durante as discussões do APL era o de uma regulamentação sobre transferência internacional de dados e cooperação internacional. Isso porque as autoridades brasileiras há anos sofrem com entraves no campo internacional, principalmente a partir de países europeus, por não ter uma regulamentação efetiva de tratamento de dados pessoais nesse campo. Por isso, o APL buscou construir uma regulação compatível com modelos internacionais, de modo a ampliar parcerias e promover maior integração com diferentes países para o combate ao crime transfronteiriço.

Em linhas gerais, o APL o prevê três tipos de critérios para a transferência internacional: **(i)** transferências com base numa decisão de adequação, **(ii)** transferências sujeitas a garantias adequadas e **(iii)** derrogações aplicáveis em situações específicas (capítulo IX, APL).

O PL suprimiu a hipótese de transferência com fundamento em decisões de adequação do ambiente regulatório de proteção de dados pessoais dos países aos quais estão vinculadas as autoridades destinatárias. Alternativamente, o PL limita as hipóteses de compartilhamento a países estrangeiros ou organizações internacionais que apresentarem garantias adequadas através de documentação formal subscrita pelo destinatário competente.

Essa previsão não apenas desconsidera as hipóteses de transferência internacional de dados pessoais previstas na LGPD (art. 33, I, LGPD), como também representa um método mais oneroso e lento de realização de transferências internacionais a destinatários que já são reconhecidamente adequados aos padrões de privacidade e proteção de dados.

Ainda, observa-se que, ao longo de todo o Capítulo VI do PL, foram suprimidas menções a obrigações de documentação e transparência nas atividades de compartilhamento internacional de dados e cooperação internacional para fins de persecução criminal. Como nas demais instâncias de supressão de obrigações dessa natureza ao longo do PL, a deficiência dos mecanismos de transparência em atividades de tratamento de dados pessoais representa riscos à fiscalização dessas atividades, bem como para a concretização dos direitos de titulares de dados pessoais. No caso de transferências internacionais de dados, contudo, esses riscos se amplificam em decorrência da realização do tratamento em país estrangeiro.

9 As Regras de Beijing determinam que o direito à privacidade dos jovens precisará ser respeitado, em todas as fases processuais, para evitar danos causados por publicização indevida de informações ou pela potencial estigmatização decorrente. Por isso, determinam que informações que possam identificar o adolescente não sejam tornadas públicas e reconhecem a necessidade de proteção dos jovens contra a publicação de informações sobre o caso deles em mídias de grande circulação. Estabelecem também que eventuais antecedentes infracionais de um jovem devem ser considerados confidenciais e incomunicáveis a terceiros, não podendo ser disponibilizados e usados quando ele atingir a maioridade.

Ao alterar essas disposições, o PL cria o risco de o Brasil continuar não sendo considerado um país com regulação adequado, apto a receber dados pessoais oriundos de outros países.

Conclusão

O Projeto de Lei nº 1515/2022 foi apresentado à Câmara dos Deputados para regular o tratamento de dados para segurança do Estado, defesa nacional, segurança pública e atividades de investigação e repressão de infrações penais viola os direitos fundamentais à proteção de dados e à privacidade. Como analisado, o texto do PL utiliza-se de estrutura semelhante ao APL elaborado pela Comissão de Juristas, mas desmobiliza as garantias aos titulares de dados e as restrições a uma atuação discricionária por parte do Estado.

As supressões a garantias referem-se principalmente aos direitos dos titulares, aos princípios norteadores da disciplina da proteção de dados pessoais no Brasil e às limitações à atuação das autoridades de controle. O tratamento de dados no contexto do PL, incluindo dados pessoais sensíveis, conecta-se aos mais caros direitos fundamentais, devendo suas limitações serem explícitas de modo a evitar abusos.

Destaca-se, também, a supressão do arcabouço protetivo dos direitos dos titulares frente às tecnologias de monitoramento. Estando a construção dos projetos direcionados ao âmbito criminal, é evidente que as regras sobre atividades de monitoramento precisam ser adequadas também às garantias penais e processuais penais, como do contraditório, da ampla defesa, da garantia do devido processo legal, da reserva legal, da presunção de inocência e da intervenção mínima.

O princípio da legalidade, um dos princípios basilares do direito penal e processual penal, limita o poder punitivo do Estado, salvaguardando as liberdades e os direitos fundamentais do indivíduo, orientando a política legislativa criminal e subsumindo a aplicação da Lei às exigências de um Estado democrático de direito e garantista, sem abrir brechas para uma interpretação extensiva ou analógica in *malla partem*. Uma das funções deste princípio é a de que o conhecimento da lei pelos indivíduos (ou ao menos a clareza do texto) possa garantir que estes não serão submetidos a abusos e a arbitrariedades do Estado, mas sim à aplicação da regra penal como está prevista.

A expansão do escopo do PL, a extensiva supressão de garantias referentes à transparência no uso de dados pessoais pelo poder estatal, bem como a previsão de ampliamento do uso de tecnologias de monitoramento e de tomada automatizada de decisões no âmbito da persecução criminal, ainda, representam um esforço ativo para o enfraquecimento de garantias legais como o livre acesso aos dados e a autodeterminação informativa da população.

Nesse sentido, a análise comparativa apresentada sugere que a eventual aprovação do texto proposto ocasionaria danos imensuráveis aos direitos fundamentais das pessoas brasileiras, comprometendo a harmonia entre a dogmática processual penal e a dogmática de proteção de dados e ocasionando enorme insegurança jurídica. Assim sendo, recomendamos o arquivamento do PL 1515/2022.

LAPIN

LABORATÓRIO DE POLÍTICAS
PÚBLICAS E INTERNET