• • •

PARECER DO MINISTÉRIO PÚBLICO

Consultoria Jurídica da Procuradoria-Geral de Justiça

SEI 20.22.0001.0014628.2021-50

Origem: Conselho Nacional do Ministério Público

Ref.: Análise acerca da Proposição nº 1.00415/2021-60, que trata da proposta de resolução que busca instituir a política nacional de proteção de dados pessoais do Ministério Público brasileiro

EXMO. SR. PROCURADOR-GERAL DE JUSTIÇA,

I

Trata-se de processo administrativo instaurado a partir do Ofício Circular nº 03/2021/CNMP/GAB/SVC, subscrito pelo Presidente da Comissão de Preservação da Autonomia do Ministério Público, do Conselho Nacional do Ministério Público, no qual encaminha a este Ministério Público, para manifestação, a proposta de resolução apresentada pelo Grupo de Trabalho presidido pelo Conselheiro Marcelo Weitzel Rabello de Souza, que "Institui a Política Nacional de Proteção de Dados Pessoais e o Sistema Nacional de Proteção de Dados pessoais do Ministério Público Brasileiro e dá Outras Providências".

O oficiante reconhece sua prevenção à presente proposição, tendo em vista a conexão com a Proposição nº 1.00740/2020-42, relativa à proposta de recomendação que busca orientar o Ministério Público brasileiro a adotar medidas preparatórias e ações iniciais para adequação às disposições contidas na Lei Geral de Proteção de Dados.

O feito foi à Subprocuradoria-Geral de Justiça de Relações Institucionais e Defesa de Prerrogativas, que determinou a vinculação destes autos ao SEI nº 20.22.0001.0014631.2021-66, relativo à proposição acima indicada, determinando o encaminhamento dos autos à Chefia de Gabinete para ciência e sugestões.

No âmbito da Chefia Institucional, considerando a relevância da temática apresentada na proposição, foi determinada vista conjunta dos autos aos seguintes órgãos: (i) Corregedoria-Geral do Ministério Público; (ii) Subprocuradoria-Geral de Justiça de Administração; (iii) Subprocuradoria-Geral de Justiça de Planejamento e Políticas Institucionais; (iv) Consultoria Jurídica; (v) Coordenadoria de Segurança e Inteligência; (vi) Ouvidoria do Ministério Público; (vii) Coordenadoria de Comunicação Social (art. 171); (viii) Centro de Estudos e Aperfeiçoamento Funcional (art. 173); (ix)

Secretaria-Geral do Ministério Público; (x) Coordenadoria-Geral de Segurança Pública; (xi) Secretaria de Tecnologia da Informação e de Comunicação; (xii) Diretoria de Recursos Humanos (arts. 62, 111, 112 e 113); (xiii) Diretoria de Licitações e Contratos (arts. 68, 100, 115, 176 e 177); (xiv) Centro de Apoio Operacional das Promotorias de Justiça da Infância e da Juventude (arts. 8º, 12, V, e 85 a 91); (xv) Centro de Apoio Operacional das Promotorias de Justiça de Tutela Coletiva de Defesa da Cidadania; (xvi) Centro de Apoio Operacional das Promotorias de Justiça de Tutela Coletiva de Defesa do Consumidor e do Contribuinte (art. 57); (xvii) Centro de Apoio Operacional das Promotorias de Justiça Criminais (arts. 77, 92, 93 e 94); (xviii) Centro de Apoio Operacional das Promotorias de Justiça de Execução Penal (arts. 77, 92, 93 e 94); e (xix) Centro de Apoio Operacional das Promotoria de Justiça de Investigação Penal (arts. 77, 92, 93 e 94).

Manifestação da douta Subprocuradora-Geral de Justiça de Planejamento e Políticas Institucionais, no qual encaminha os autos à Assessoria de Planejamento Estratégico e Modernização Organizacional, indicando a existência de procedimento já instaurado no âmbito da Secretaria de Tecnologia da Informação e da Comunicação sobre o mesmo tema.

Nos anexos, foram juntados os seguintes documentos: (i) justificativa, exposição de motivos e minuta de resolução a ser apreciada; (ii) certidão de autuação do processo junto ao Conselho Nacional do Ministério Público; (iii) certidão de existência de processo conexo; (iv) certidão de distribuição; (v) informação de autuação da proposição, certidão de distribuição por prevenção e de redistribuição.

II

Inicialmente, considerando a abrangência do diploma normativo a ser editado pelo Conselho Nacional do Ministério Público, bem como sua especificidade operacional, ao estabelecer diretrizes de planejamento institucional e de gestão administrativa, sua análise pormenorizada está mais próxima da esfera de atribuições da Subprocuradoria-Geral de Justiça de Planejamento Institucional e da Secretaria-Geral do Ministério Público. Sem prejuízo dessa constatação, esta Consultoria Jurídica, no intuito de colaborar com a análise jurídica da proposta, realizará um breve cotejo da proposição com as normas e diretrizes emanadas da Lei Geral de Proteção de Dados (Lei nº 13.709/2018). Esta lei, como se sabe, buscou estabelecer cautelas e diretrizes de salvaguarda da segurança da informação e dos dados pessoais utilizados pelas estruturas estatais de poder, sendo oponível a todo o Poder Público, em todos os seus níveis de organização, aí incluído o Ministério Público brasileiro.

Acerca da Lei nº 13.709, de 14 de agosto de 2018, também denominada de Lei Geral de Proteção de Dados, já tivemos oportunidade de afirmar que esse diploma normativo inspirou-se no Regulamento Geral de Proteção de Dados (GDPR– *General Regulation for Data Protection*), norma europeia que está em vigor desde 25 de maio de 2018. Especificamente em relação à GDPR, o seu objetivo principal é o de compelir à

proteção de dados dos cidadãos europeus, obrigando todas as sociedades empresárias, de pequeno, médio e grande porte, a investirem em cibersegurança.

Nesse contexto, a promulgação da Lei nº 13.709/2018 representou inegável avanço, mas, além do seu longo período de *vacatio legis,* foram muitas as alterações legislativas que já sofreu. Inicialmente, foi editada a Medida Provisória nº 869, de 27 de dezembro de 2018, que reformulou densamente o seu texto original. Posteriormente, após a realização de diversas audiências públicas, acompanhadas de intensos debates a respeito das alterações, foi promulgada a Lei nº 13.853, de 08 de julho de 2019, que manteve alguns dos ajustes realizados, efetivou outros e recompôs o texto original em certos pontos.

O diploma normativo em comento não deixa margem a dúvidas quanto à incidência dos seus comandos no âmbito das estruturas estatais de poder, determinado a obrigatoriedade de sua observância em todos os níveis.

A aplicabilidade da Lei Geral de Proteção de Dados brasileira já vem sendo objeto de preocupação da Coordenação de Segurança e Inteligência desde a sua edição, quando encaminhou consulta à Chefia Institucional a respeito dos reflexos operados no âmbito institucional, especificamente em sede de tutela coletiva (vide Processo MPRJ nº 2018.00785367, com um longo histórico de tramitação, vide anexo).

O tratamento de dados pessoais, de modo geral, só é possível, nos termos do art. 7º: (a) com o consentimento livre e inequívoco da pessoa a que se referem os dados; (b) para o cumprimento de obrigação legal pelo responsável; (c) pela Administração Pública, no exercício de direitos ou deveres; (d) para estudos por órgãos de pesquisa; (e) para a proteção da vida e a tutela da saúde, nesse caso específico em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária, sinalizando a obrigação do sigilo de dados dessa natureza; (f) quando necessário para a execução de um contrato; (g) no exercício regular de direitos em processo judicial ou administrativo; e (h) se necessário, para atender aos interesses legítimos do responsável.

O diploma normativo de regência confere especial destaque aos direitos dos usuários, que podem ter acesso aos seus dados, podendo ainda solicitar aos controladores que lhes forneçam todas as informações que mantêm, incluindo o direito de retificação das informações, bem como sua atualização. Trata-se, aliás, de direitos de estatura constitucional.

A portabilidade de dados foi tratada no art. 18, inciso V, da Lei e reiterada no inciso I do § 4º do art. 11. O inciso II do § 4º corrobora a autodeterminação informativa, realçando direitos do titular para a proteção dos seus dados sensíveis. A portabilidade de dados, nos termos do inciso V e do § 6º do art. 18, está vinculada à posterior regulamentação, a cargo da autoridade nacional, o que demonstra que o poder regulamentar infralegal exige atento acompanhamento.

Como inovação específica, introduziu na ordem jurídica nacional regras básicas para a transferência internacional de dados, reconhecendo a possibilidade de

transferência lícita (a) para "país ou organização internacionais com grau de proteção adequado", a ser declarado por autoridade competente; (b) mediante consentimento específico, livre e informado do titular dos dados; e (c) quando o responsável oferecer garantias ao titular do cumprimento dos direitos, princípios e regime de proteção da lei brasileira na jurisdição de destino. Cabe destacar que essas hipóteses são direcionadas às sociedades empresárias que transferem dados ao exterior (arts. 33-36).

No tocante à aplicação da lei por entidades públicas, especificamente quanto ao uso de banco de dados pelo Ministério Público em investigações de cunho não penal, o Capítulo IV detalha as normas e responsabilidades dos órgãos e setores públicos frente à proteção dos dados pessoais que utilizam, dispondo que o tratamento de dados pessoais pelas pessoas jurídicas de direito público referidas no parágrafo único do art. 1º da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação) deverá ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público (arts. 23-32).

Note-se que o art. 4º da Lei nº 13.709 exclui do seu alcance o tratamento de dados pessoais para as finalidades ali referidas, entre as quais estão aquelas direcionadas à segurança pública, à defesa nacional, à segurança do Estado e às atividades de investigação e repressão de infrações penais, o que será regido por legislação específica. A *contrario sensu*, é possível afirmar que esse diploma normativo incidirá sobre as demais instâncias de responsabilização de caráter não penal, naquilo que diga respeito ao tratamento da informação. Entende-se por tratamento, nos termos do art. 5º, X, "*toda operação realizada com dados pessoais, como os que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração*". Esse tratamento recebeu uma sistemática específica, como se disse, em se tratando do Poder Público (Capítulo IV), devendo ser realizado para o atendimento de uma finalidade pública, o que deve ser feito de forma transparente, observadas as regras de segurança e de sigilo de dados (Capítulo VII, Seção I).

Ao contrário de uma restrição pontual no âmbito das investigações não penais a cargo do Ministério Público, o marco legal inaugurado com a promulgação da Lei nº 13.709/2018 confere à tutela coletiva a atribuição de "*promover a defesa dos interesses e direitos difusos, coletivos e individuais homogêneos dos titulares de dados pessoais*". Vide, por exemplo a atuação desta Instituição, em sede de tutela coletiva, em face do sítio "decolar. com", pela prática de *geo-blocking*, quando há o bloqueio da oferta com base na origem geográfica do consumidor e de *geo-pricing*, a precificação diferenciada da oferta também com base na localização. A demanda foi ajuizada pela 5ª Promotoria de Justiça de Tutela Coletiva de Defesa do Consumidor e do Contribuinte da Capital (Inquérito Civil nº 347/5ª PJDC/2016, ACP nº 0008914-24.2018.8.19.0000).

Quanto à proposta de resolução apresentada, seus pressupostos conduzem a dois instrumentos institucionais de fomento à cultura de proteção de dados pessoais

no âmbito do Ministério Público brasileiro, um de ordem finalístico-educacional, por instituir a "*Política Nacional de Promoção da Proteção de Dados Pessoais*", outro de ordem instrumental, pois cria instrumentos para operacionalizar o "*Sistema Nacional de Proteção de Dados Pessoais*", de modo a dar concretude aos ditames da Lei n. 13.709/2018.

Enquanto a Política Nacional de Promoção da Proteção de Dados Pessoais tem por objetivo introduzir a cultura da proteção de dados pessoais sob bases principiológicas, como os da proporcionalidade e da razoabilidade, da vedação da proteção insuficiente, da boa-fé, da adequação, da necessidade e finalidade, da segurança e prevenção, da responsabilização e prestação de contas, do livre acesso e não discriminação (Cap. II, arts. 2º - 19), o Sistema Nacional de Proteção inclui, entre as funções institucionais do Ministério Público, a proteção integral dos dados pessoais, por meio de estruturas orgânicas voltadas a dar suporte ao agir institucional, em prol da proteção de dados pessoais (Cap. III, arts. 20-62).

A proposta de resolução disciplina a temática em 178 artigos, distribuídos em cinco capítulos. O art. 1º, do Capítulo I, traz as disposições gerais, traçando os objetivos do ato normativo em sentido *lato*.

O Capítulo II, dividido em cinco seções, disciplina a Política Nacional de Proteção de Dados Pessoais (arts. 2º a 19), estabelecendo: fundamentos (seção I); princípios (seção II); conceitos (seção III); direitos dos titulares de dados pessoais (seção IV); e prerrogativas do Ministério Público (seção V).

Especificamente quanto aos direitos do titular de dados, a regra é que a pessoa natural tem assegurada a titularidade de seus dados pessoais e o seu uso deve receber tratamento transparente. A exceção somente se aplica se a operação de tratamento dos dados pessoais ocasionar prejuízo às atividades do Ministério Público em prol da defesa da ordem jurídica, do regime democrático e dos interesses sociais e individuais indisponíveis, difusos e coletivos, bem como às atividades preventivas, persecutórias e de produção de conhecimento e à salvaguarda dos objetivos da Instituição (§ 3º, art. 9º e art. 16).

O Capítulo III estabelece o Sistema de Proteção de Dados Pessoais, em nível nacional e local (CNMP e demais ramos do Ministério Público), de modo a instrumentalizar a Instituição para o tratamento, o uso, a colheita, o compartilhamento e o armazenamento dos dados pessoais nas atividades administrativas e, principalmente, das atividades-fim.

A estrutura do Sistema Nacional (SINPRODAP) deverá ser composta pelos seguintes órgãos: (i) a Unidade Especial de Proteção de Dados Pessoais (UEPDAP), vinculada à Comissão de Preservação da Autonomia do Ministério Público, órgão colegiado que exercerá a função de Autoridade Nacional de Proteção de Dados Pessoais (arts. 25-29); (ii) a Secretaria Executiva de Proteção de Dados Pessoais (SEPRODAP), órgão executivo e regulador do Sistema Nacional (arts. 30-32); (iii) o Comitê Nacional de Encarregados de Proteção de Dados Pessoais do Ministério Público (CONEDAP), órgão

consultivo, deliberativo e propositivo, que tem a função de promover a padronização das ações dos ramos e das unidades do Ministério Público quanto à Política Nacional de Proteção de Dados Pessoais, sendo integrado pelos encarregados do Conselho Nacional do Ministério Público de cada ramo ou unidade do Ministério Público brasileiro (art. 33).

A estrutura local do Sistema de Proteção deverá ser formada pelo: (i) *controlador e cocontrolador* (o CNMP e cada ramo e unidade do Ministério Público) (arts. 36-39); (ii) *operador* (pessoa natural ou jurídica, de direito público ou privado, que, sem pertencer aos quadros do Ministério Público, com independência jurídica e econômica, realiza, por sua conta e responsabilidade, o tratamento de dados pessoais a mando do controlador) e *cooperador* (nas hipóteses que a lei autoriza, é contratado para realizar o tratamento concomitante de dados pessoais) (arts. 40-43); (iii) *encarregado* (pessoa indicada pelo controlador para atuar como canal de comunicação e interação entre o controlador, os titulares dos dados pessoais e a Autoridade Nacional (arts. 44-48); (iv) *Comitê Estratégico de Proteção de Dados Pessoais-CEPDAP* (órgão colegiado de natureza permanente, subordinado à Chefia da Instituição), que deverá ser instituído, no prazo de até 90 (noventa) dias a contar da entrada em vigor da resolução (arts. 49-55).

Para garantir a estrutura orgânica do sistema de proteção, o art. 34 fixa o *prazo de 90 dias*, a partir da publicação da resolução, para que os ramos do Ministério Público constituam uma estrutura administrativa interna para o atendimento das diretrizes determinadas na resolução, para o uso e o tratamento de dados pessoais, que será compreendida, no mínimo, pelo encarregado (pessoa indicada pelo controlador e operador para atuar como canal de comunicação) e pelo Comitê Estratégico de Proteção de Dados Pessoais-CEPDAP.

O art. 35 prevê a elaboração de um Plano Diretor que deverá conter regras de boas práticas e de governança, que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais, conforme previsto na presente Resolução. O processo de elaboração e revisão do Plano Diretor de Proteção de Dados Pessoais será coordenado pelo Comitê Estratégico (art. 50).

Os arts. 56 a 62 estabelecem os deveres e atribuições dos órgãos do Ministério Público para a defesa da ordem jurídica, na dimensão coletiva do direito à proteção aos dados pessoais, o que inclui a criação de promotorias ou procuradorias especializadas, grupos especiais de atuação, admitida a incorporação às estruturas orgânicas já existentes das atribuições que assegurem a efetiva tutela da privacidade e a proteção dos dados pessoais. Também foi objeto de previsão o desenvolvimento de ações de capacitação de membros e servidores, para qualificar a atuação finalística na tutela do direito fundamental à privacidade, no tocante à proteção dos dados pessoais, inclusive nos cursos de ingresso e vitaliciamente de membros e servidores.

O capítulo IV veicula as diretrizes para a proteção dos dados pessoais pelo Ministério Público, que deverão ser protegidos e tratados, quer na atuação administrativa, quer na finalística, vinculando o tratamento de dados diretamente à Lei Geral de Proteção de Dados (art. 64).

São diretrizes a serem observadas: a divulgação no sítio eletrônico do encarregado e as hipóteses em que o tratamento de dados pessoais será realizado; a Lei Geral de Proteção de Dados se aplica somente para o tratamento de dados pessoais que digam respeito à atividade administrativa do Ministério Público (art. 66); a proteção das pessoas naturais, no que diz respeito ao tratamento dos seus dados pessoais, é um direito fundamental (art. 67); todos os contratos, convênios e atos formais equivalentes, a serem celebrados, deverão trazer definidas as responsabilidades, de forma transparente e detalhada, dos controladores, dos operadores e, quando possível, de eventuais terceiros envolvidos (art. 68).

Os princípios do tratamento de dados pessoais são explicitados nos arts. 69 a 71, com especial deferência à regra que estabelece que princípios da proteção de dados pessoais não se aplicam às informações anônimas (art. 70).

As exceções que autorizam o tratamento de dados pessoais pelo Ministério Público, na sua atividade fim, estão elencadas nos arts. 72 a 75, o que inclui dados relativos a DNA, voz, imagem facial, reconhecimento automatizado, inclusive facial, expressão corporal, inclusive trejeitos e modo de andar, impressões digitais e outros dados biométricos ou de comportamento, quando imprescindíveis à segurança da sociedade ou institucional do Ministério Público, principalmente visando ao não comprometimento das atividades de produção de conhecimento, bem como de investigação ou fiscalização, relacionadas com a prevenção ou repressão de infrações.

O art. 76 disciplina a forma como o titular pode requerer o acesso ao tratamento de seus dados pessoais, trabalhado pelo Ministério Público, que deverá ser protocolizado e recepcionado pelo controlador ou operador, o qual, de imediato, o encaminhará ao encarregado para análise e providências cabíveis. As exceções ao fornecimento das informações ao titular dos dados estão elencadas nos arts. 77-79, que estabelecem as hipóteses em que o Ministério Público pode adiar, limitar ou recusar o seu acesso aos dados.

Os arts. 80 a 82 definem a metodologia de mapeamento e inventário dos bancos de dados pessoais, que estejam sob o controle do Ministério Público, incluindo aqueles que tenham sido compartilhados, independentemente do modo como se realizou a sua coleta.

Os arts. 83 a 91 avançam na especificidade dos dados pessoais, distinguindo do dado pessoal sensível (art. 83-84) aqueles relativos aos dados pessoais de crianças e adolescentes (art. 85-91). O tratamento dos dados sensíveis, para instruir investigação de natureza cível ou criminal, deve observar o reforço de proteção e os cuidados específicos. Nas atividades administrativas, esse tratamento somente

poderá ser realizado mediante consentimento expresso e específico do titular ou de seu representante legal, salvo as exceções previstas (§ 1º, art. 84).

O tratamento de dados pessoais de crianças e adolescentes é submetido à proteção especial. No âmbito administrativo, somente podem ser tratados com o consentimento específico e com permissão dada por pelo menos um dos pais ou pelo responsável legal, salvo as exceções previstas (§§ 1º e 2º, art. 86).

O tratamento dos dados pessoais na esfera da tutela dos interesses sociais e individuais indisponíveis, das infrações penais, da segurança e da inteligência está previsto na seção X, do Capítulo III, nos arts. 92 a 96. Na esfera penal, a proposição estabelece que o tratamento dos dados pessoais precisa passar pela categorização dos seus titulares (art. 92). Na defesa dos interesses sociais e individuais indisponíveis, de prevenção, investigação, detecção ou repressão de infrações penais, bem como de proteção dos ativos institucionais e de produção do conhecimento, é exigido que os agentes de tratamento e os titulares de dados pessoais cumpram o que lhes é solicitado e requisitado, não sendo o caso de se invocar o consentimento. Salvo nas hipóteses de expressa previsão constitucional de reserva de jurisdição, o tratamento de dados pessoais pelo Ministério Público não dependerá de prévia autorização judicial (art. 95).

A proposição possibilita o tratamento automatizado de dados pessoais, quando decisões possam produzir efeitos adversos na esfera jurídica do titular, de modo a evitar práticas abusivas, erros, tratamentos discriminatórios, manipulação etc. (art. 97).

O limite territorial, aplicado na proposição para tratamentos de dados pessoais, abrange todo território nacional, principalmente no compartilhamento e na transferência, exportação e importação, com outras instituições internacionais e, ainda, na hipótese de incidentes de tratamento de dados pessoais que extrapolem o território nacional (art. 98).

Os arts. 99 a 108, além de distinguirem, definem as medidas de compartilhamento e transferência dos dados pessoais. Segundo a resolução: (i) compartilhamento é a troca de informações e dados, inclusive pessoais, entre os órgãos do CNMP e os órgãos dos ramos e das unidades do Ministério Público brasileiro; e (ii) transferência significa a troca realizada com órgãos e entidades distintas. Para tal fim, normatiza a transferência entre instituições públicas parceiras e de controle (art. 104), os casos de atuação conjunta (art. 105), a transferência público-privada (art. 106) e a transferência internacional (arts. 107-108).

A proposição, em seu art. 109, hierarquiza a base legal do tratamento de dados pelo Ministério Público, principiando pelas leis, em um segundo momento, o consentimento, finalizando no legítimo interesse.

Os dados pessoais sensíveis dos membros, servidores, estagiários e prestadores de serviços, no âmbito do Ministério Público brasileiro, deverão ser tratados de acordo com as exceções previstas no art. 11, II, da LGPD (art. 110).

Os comunicados (art. 111), o armazenamento dos registros pessoais (art. 112) o monitoramento e a prevenção da perda de dados (art. 113), o modelo de reclamação

(art. 114), os contratos administrativos e a terceirização dos serviços (art. 115), as técnicas de boas práticas e governança de dados pessoais (arts. 116-117), ciclo de vida do tratamento de dados pessoais (art. 118-119) e o término do tratamento dos dados (arts. 120-124) estão disciplinados de modo objetivo e sistêmico na proposição.

Também são abordadas na proposição as "técnicas de sistema de informação", com a utilização de instrumentos como: segurança da informação (arts. 125-130); proteção por concepção de padrão (*design* e *default*) (arts. 131-136); sítios eletrônicos e sistemas informatizados (arts. 137-139); aferição dos riscos (arts. 140-141); relatório de impacto à proteção de dados pessoais-RIPD (arts. 142-149); comunicações e respostas a incidentes de segurança (arts. 150-157). Todos esses instrumentos estão disciplinados de forma pormenorizada e com especificidades direcionadas a cada agente que controla e trata dos dados pessoais no âmbito interno do Ministério Público.

Acerca das técnicas de sistema de informação, observamos, unicamente, um erro material no § 3º do art. 142. Em tal dispositivo, é referida a "*Seção VI do Capítulo VII*". Nota-se que o referido capítulo VII não integra o corpo da proposição. Nesse sentido, a remissão que melhor se coaduna ao referido dispositivo é a seguinte:

"§ 3º A aferição dos riscos de qualquer tratamento decorre do resultado da realização do inventário de dados pessoais, conforme previsto na Seção VII do Capítulo IV *da presente Resolução."*

Por fim, o Capítulo V apresenta as disposições transitórias e finais da proposição, com ênfase nos seguintes aspectos: (i) a indicação de que diretrizes complementares para a adequação progressiva de bancos de dados pessoais a serem constituídos deverão ser editadas (art.158); as Ouvidorias de cada ramo do Ministério Público poderão funcionar como órgãos de apoio e canal auxiliar para a adequação da resolução ao cotidiano institucional (art. 160); o estabelecimento do prazo de 1 ano, a contar da publicação da resolução, para que cada ramo do Ministério Público crie a estrutura administrativa e se ajuste a todos os dispositivos da resolução (parágrafo único do art. 160 e art. 161); a exclusividade das atribuições ao encarregado (§ 1º do art. 45) não se aplica no primeiro ano de vigência da resolução (art. 162); a elaboração de cronograma para adaptar o plano diretor e as rotinas na estrutura administrativa da Instituição (art. 163); a obrigação de que a tutela coletiva do direito à proteção de dados pessoais seja implementada imediatamente, devendo ser comunicado à Unidade Especial de Proteção de Dados da Autoridade Nacional, no prazo de 30 dias, quais órgãos de execução possuem atribuição para a tutela coletiva do direito fundamental à proteção de dados pessoais (art. 164); a elaboração de relatório em conformidade com a resolução, por cada unidade do Ministério Público, no prazo de 120 dias, a contar da publicação da proposição (art. 166); a resolução se aplica às Escolas de Governo, aos Centros de Estudos, Aperfeiçoamento e Capacitação, ou equivalentes, dos ramos e das unidades do Ministério Público (art. 173); no prazo

de 1 ano, a contar da entrada em vigor da resolução, o armazenamento em nuvem dos bancos de dados pessoais deverá ser contratado e realizado em servidores que estejam localizados em território nacional (art. 176).

III

Considerando o exposto, esta Consultoria Jurídica esclarece que maiores subsídios a respeito da abrangência e da adequação deste Ministério Público às disposições constantes no ato normativo a ser editado pelo Conselho Nacional do Ministério Público, podem ser colhidos a partir da manifestação dos demais órgãos já relacionados pela douta Chefia de Gabinete.

Quanto ao teor da minuta de resolução, constante no index. 0600406, esta Consultoria Jurídica não opõe qualquer óbice aos seus termos, pois visa apenas a observância das cautelas necessárias à salvaguarda da segurança da informação e ao fluxo de dados utilizados, tal qual disciplinados pela Lei nº 13.709/2018. A única ressalva que se opõe é aquela já referida no corpo da presente análise, em que se verificou um erro material constante do § 3º do art. 142. Nesse caso específico, sugere-se a correção para que conste do dispositivo o seguinte: "*art. 142 (...) 3º A aferição dos riscos de qualquer tratamento decorre do resultado da realização do inventário de dados pessoais, conforme previsto na* Seção VII do Capítulo IV *da presente Resolução.*"

Rio de Janeiro, 21 de abril de 2021.

EMERSON GARCIA

Consultor Jurídico