

PROJETO DE LEI Nº , DE 2022

(Do Sr. CORONEL ARMANDO)

Lei de Proteção de Dados Pessoais para fins exclusivos de segurança do Estado, de defesa nacional, de segurança pública, e de investigação e repressão de infrações penais.

O Congresso Nacional decreta:

CAPÍTULO I**DISPOSIÇÕES PRELIMINARES**

Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais realizado por autoridades competentes para fins exclusivos de segurança do Estado, de defesa nacional, de segurança pública e de atividades de investigação e repressão de infrações penais, previstas no inciso III do artigo 4º da Lei nº 13.709, de 14 de agosto de 2018, com os objetivos de:

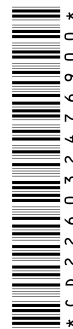
I - proteger os direitos fundamentais de segurança, liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural;

II - assegurar a eficiência da atuação dos órgãos incumbidos das atividades mencionadas no **caput** deste artigo; e

III - possibilitar o intercâmbio de dados pessoais entre autoridades competentes no exercício das atividades referidas no **caput** deste artigo.

§ 1º As normas gerais contidas nesta Lei são de interesse nacional e devem ser observadas pela União, Estados, Distrito Federal e Municípios.

§ 2º Esta lei aplica-se, ainda, às atividades de inteligência realizadas pelas autoridades competentes no cumprimento de suas



competências mencionadas no **caput** deste artigo, sem prejuízo de leis específicas que regulamentam tais atividades.

Art. 2º A disciplina da proteção de dados pessoais em atividades de segurança pública e de persecução penal tem como fundamentos:

I - a dignidade, os direitos humanos, o livre desenvolvimento da personalidade, e o exercício da cidadania pelas pessoas naturais;

II - o respeito à vida privada e à intimidade;

III - a liberdade de manifestação do pensamento, de expressão, de informação, de comunicação e de opinião;

IV - a presunção de inocência;

V - garantia do devido processo legal, da ampla defesa, do contraditório, da motivação e da reserva legal; e

VI - o dever estatal de eficiência nas atividades de segurança do Estado e de defesa nacional e de garantia do direito à segurança pública, por meio da instituição de mecanismos que otimizem a prevenção, investigação e repressão de infrações penais.

Art. 3º Para os fins desta Lei, considera-se:

I - autoridade competente: autoridade pública, órgão ou entidade do Poder Público responsável pelas atividades de segurança do Estado, de defesa nacional, e pela prevenção, detecção, investigação ou repressão de atos infracionais e infrações penais ou execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública, ou qualquer outro órgão ou entidade que, nos termos da lei, exerça autoridade ou execute políticas públicas para os referidos efeitos, total ou parcialmente;

II - atividade de segurança do Estado: toda e qualquer atividade que vise à preservação do território, das instituições, do povo e da soberania nacionais.



III - atividade de defesa nacional: é 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.

IV - atividade de segurança pública: toda e qualquer atividade exercida para a preservação da ordem pública, da incolumidade das pessoas e do patrimônio, e para prevenção de infrações penais, realizada por autoridades competentes previstas no artigo 144 da Constituição Federal;

V - atividade de investigação e repressão de infrações penais: toda e qualquer atividade exercida para a investigação, apuração, persecução e repressão de infrações penais e execução de penas, por autoridades competentes para a finalidade de persecução penal;

VI - dados cadastrais: são os dados apresentados pelo titular para realização ou manutenção do cadastro perante particular ou poder público, não sujeitos a sigilo constitucional ou legal.

§ 1º Os dados cadastrais a que se refere o inciso VI do caput deste artigo podem incluir informações referentes à 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.

§ 2º Aplicam-se a esta lei as definições estabelecidas no art. 5º da Lei nº 13.709, de 14 de agosto de 2018.

Art. 4º As atividades de tratamento e compartilhamento de dados pessoais em matéria de segurança do Estado, de defesa nacional, de segurança pública e de persecução penal deverão observar a boa-fé e os seguintes princípios:

I - licitude: embasamento do tratamento de dados pessoais em hipótese legal, nos termos do Capítulo II desta Lei;

II - finalidade: coletados para fins determinados, explícitas e legítimas, e não tratados de uma forma incompatível com essas finalidades, de modo a subsidiar a atuação dos órgãos incumbidos das atividades de



segurança pública, investigação e repressão de infrações penais, em conformidade com suas atribuições legais;

III - adequação: pertinência e relevância do tratamento com os objetivos pretendidos, de acordo com o contexto do tratamento;

IV - necessidade: limitação do tratamento ao necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;

V - segurança da informação: utilização de medidas físicas, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;

VI - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais

VII - supremacia do interesse público: prevalência do interesse público em conflito sobre um interesse particular;

VIII - qualidade dos dados: garantia de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;

IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;

X - auditabilidade: a tomada de medidas que viabilizem a verificação e a checagem do tratamento, bem como o controle do acesso à informação, sempre que tecnicamente possível.

Art. 5º No tratamento de dados pessoais, o responsável pelo tratamento deve, na medida do possível, fazer distinção clara entre as diferentes categorias de titulares dos dados, especialmente:

I - pessoas em relação às quais existem indícios de que cometeram uma infração penal;



II - pessoas em relação às quais existem indícios de que estão prestes a cometer uma infração penal;

III - pessoas processadas pela prática de infração penal;

IV - pessoas condenadas definitivamente pela prática de infração penal;

V - vítimas de uma infração penal ou pessoas em relação às quais certos fatos indicam que podem ser vítimas de uma infração penal;

VI - outras pessoas, tais como testemunhas, pessoas que possam fornecer informações, ou contatos ou associados das pessoas referidas nos incisos I a V; e

VII - pessoas em relação às quais existem indícios de que cometeram ou estão prestes a cometer ações que atentem contra a segurança do Estado.

Art. 6º No tratamento de dados, o responsável deve distinguir os dados pessoais baseados em fatos dos dados pessoais baseados em avaliações pessoais.

§ 1º Caso o responsável verifique que tratou dados pessoais inexatos ou que tratou dados pessoais de forma ilícita, os dados pessoais devem ser retificados ou apagados.

§ 2º É vedado o tratamento dos dados a que se refere o art. 1º desta lei por pessoa de direito privado, exceto em procedimentos sob tutela de pessoa jurídica de direito público, que serão objeto de informe específico à autoridade nacional e que deverão observar a limitação imposta no § 4º deste artigo.

§ 3º A autoridade nacional emitirá opiniões técnicas ou recomendações referentes às exceções previstas no art. 1º desta lei e deverá solicitar aos responsáveis relatórios de impacto à proteção de dados pessoais.

§ 4º Em nenhum caso a totalidade dos dados pessoais de banco de dados de que trata o art. 1º desta lei poderá ser tratada por pessoa de direito privado, salvo por aquela que possua capital integralmente constituído pelo poder público.



CAPÍTULO II
DO TRATAMENTO DE DADOS PESSOAIS
SEÇÃO I
DO TRATAMENTO DE DADOS PESSOAIS EM ATIVIDADES DE
SEGURANÇA DO ESTADO E DE DEFESA NACIONAL

Art. 7º O tratamento de dados pessoais para atividades de segurança do Estado e de defesa nacional poderá ser realizado desde que haja previsão legal específica.

§ 1º A previsão legal de que trata o caput deste artigo se consubstanciará nas competências legais dos órgãos incumbidos das atividades mencionadas no **caput** deste artigo e nos diplomas legais exarados pelo Ministro de Estado Chefe do Gabinete de Segurança Institucional da Presidência da República, pelo Ministro de Estado da Defesa, pelo Diretor-Geral da Agência Brasileira de Inteligência e pelos Comandantes das Forças Armadas.

§ 2º O compartilhamento de dados pessoais para os fins de segurança do Estado e de defesa nacional poderá ser realizado entre os órgãos incumbidos dessas atividades, com o objetivo de proporcionar eficácia às ações daqueles órgãos, devendo ser observados, para tanto, os princípios descritos no art. 4º desta lei.

§ 3º As atividades a serem regulamentadas nos diplomas legais mencionados no §1º constituem-se, dentre 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. 8º Os órgãos incumbidos das atividades mencionadas no art. 7º deverão estar em condições de fornecer à Autoridade Nacional de Proteção de Dados, a qualquer tempo, informações sobre o tratamento de dados pessoais que realizam.

SEÇÃO II



DO TRATAMENTO DE DADOS PESSOAIS EM ATIVIDADES DE SEGURANÇA PÚBLICA

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;

II - para execução de políticas públicas, observados os princípios gerais de proteção, e os direitos dos titulares na forma desta lei; e

III - para a proteção da vida ou da incolumidade física do titular ou de terceiro, contra perigo concreto e iminente.

§ 1º As autoridades competentes poderão tratar os dados pessoais coletados no contexto da prevenção, investigação ou repressão de infrações penais específicas a fim de obter melhor compreensão das atividades criminais e de estabelecer ligações entre as diferentes infrações penais detectadas.

§ 2º O tratamento de dados pessoais sensíveis para atividades de segurança pública poderá ser realizado nas seguintes hipóteses:

I - cumprimento de obrigação legal;

II - execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;

III - proteção da vida ou da incolumidade física do titular, de terceiro ou da coletividade; e

IV - resguardar direitos relacionados aos titulares dos dados pessoais sensíveis.

Art. 10. Os dados anonimizados não serão considerados dados pessoais para os fins desta Lei, salvo quando o processo de anonimização ao qual foram submetidos for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido.



Art. 11. O acesso de autoridades competentes a dados pessoais e a bancos de dados controlados por órgãos e entidades da Administração Pública, para fins de segurança pública, inclusive de inteligência policial, observará as seguintes diretrizes:

I - os dados pessoais poderão ser compartilhados por órgãos e entidades federais, distritais, estaduais e municipais, observadas as restrições legais, os requisitos de segurança da informação e comunicações e o disposto na presente Lei;

II - o compartilhamento de dados sujeitos a sigilo implica a assunção, pelo receptor de dados, dos deveres de sigilo e auditabilidade impostos ao custodiante dos dados;

III - os mecanismos de compartilhamento, interoperabilidade e auditabilidade devem ser desenvolvidos de forma a atender às necessidades de negócio dos órgãos de segurança pública para facilitar a execução de políticas públicas orientadas por dados e o exercício de suas atribuições legais;

IV - os órgãos e entidades colaborarão para a redução dos custos de acesso a dados no âmbito da administração pública, inclusive, mediante o reaproveitamento de recursos de infraestrutura e de sistemas por múltiplos órgãos e entidades.

Art. 12. O acesso de autoridades competentes a dados pessoais e a bancos de dados controlados por pessoas jurídicas de direito privado se dará:

I - mediante previsão legal;

II - por cooperação voluntária por parte do particular, quando em conformidade com a Lei nº 13.709, de 2018;

III - por meio de contrato, acordo de cooperação ou instrumento congêneres.

Art. 13. O compartilhamento de dados pessoais controlados pelos órgãos incumbidos de atividades de segurança pública com pessoas jurídicas de direito privado se dará excepcionalmente, quando presentes



razões de interesse público devidamente motivadas em ato administrativo, devendo ser adotadas medidas para garantir um nível de proteção adequado.

SEÇÃO III

DO TRATAMENTO DE DADOS PESSOAIS EM ATIVIDADES DE INVESTIGAÇÃO E REPRESSÃO DE INFRAÇÕES PENAIS

Art. 14. É permitido o tratamento e o compartilhamento de dados pessoais e de dados pessoais sensíveis para finalidades de investigação e repressão de infrações penais, observada a legislação processual penal vigente no que couber.

Art. 15. O acesso de autoridades competentes, a dados pessoais e a bancos de dados controlados por órgãos e entidades da Administração Pública, para fins de investigação e repressão de infrações penais, observará as diretrizes definidas no artigo 11.

Art. 16. É permitido o tratamento e o compartilhamento de dados pessoais e de dados pessoais sensíveis para finalidades de inteligência de segurança pública (Decreto nº 3.695/2000), investigação e repressão de infrações penais, observada a legislação vigente no que couber.

Art. 17. O acesso de autoridades competentes, a dados pessoais e a bancos de dados controlados por órgãos e entidades da Administração Pública, inclusive dos órgãos integrantes do Subsistema e Inteligência de Segurança Pública (SISP) para fins de inteligência de segurança pública, investigação e repressão de infrações penais, observará as diretrizes definidas no artigo 12.

Art. 18. O acesso, tratamento e compartilhamento, no âmbito de atividades de investigação e repressão de infrações penais e de inteligência de segurança pública a dados pessoais e a bancos de dados controlados por pessoas jurídicas de direito privado dar-se-á por meio de:

I - requisição do delegado de polícia ou do membro do Ministério Público, com a respectiva indicação do seu fundamento legal;

II - por cooperação voluntária por parte do particular, quando em conformidade com a Lei nº 13.709, de 2018;



III - por meio de contrato, acordo de cooperação ou instrumento congênere; ou

IV - pelo canal técnico de inteligência de Estado.

Art. 19. O acesso de autoridades competentes para a investigação e repressão de infrações penais a dados pessoais controlados por pessoas jurídicas de direito privado que estejam sujeitos a sigilo legal ou constitucional será regulado pela legislação processual penal vigente, mediante autorização judicial, sem prejuízo do acesso aos dados cadastrais, nos termos do artigo anterior.

SEÇÃO IV

DAS DECISÕES AUTOMATIZADAS

Art. 20. É vedada a tomada de decisão realizada exclusivamente com base no tratamento automatizado, incluída a definição de perfis, que produzam efeitos adversos na esfera jurídica do titular dos dados ou que o afetem de forma significativa.

Art. 21. A tomada de decisões decorrentes de tratamento automatizado deve garantir o direito de solicitar a intervenção humana do responsável pelo tratamento.

§ 1º São vedadas as definições de perfis que conduzam à discriminação de titulares de dados, com base em dados pessoais sensíveis.

§ 2º Os sistemas responsáveis por decisões automatizadas a que se refere o artigo 21 devem ser auditáveis, não discriminatórios e passíveis de comprovação acerca de sua precisão e grau de acurácia.

§ 3º É vedada a adoção de qualquer medida coercitiva ou restritiva de direitos exclusivamente com base em decisão automatizada.

SEÇÃO V

DOS PRAZOS DE ARMAZENAMENTO DOS DADOS PESSOAIS

Art. 22. Os dados pessoais coletados em virtude das atividades escopo desta Lei deverão ser eliminados após o término de seu tratamento, autorizada a conservação para as seguintes finalidades:



I - cumprimento de obrigação legal ou regulatória pelo controlador;

II - transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos nesta Lei; ou

III - uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados.

Parágrafo Único. As autoridades competentes deverão estabelecer prazos para a eliminação dos dados pessoais mencionados no caput deste artigo, inclusive para realização de avaliações periódicas da necessidade de conservar tais dados.

CAPÍTULO III

DOS DIREITOS DO TITULAR

Art. 23. Toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade, nos termos desta Lei, sendo que qualquer restrição a estes direitos deverá ser proporcional e necessária para finalidades de atividades de segurança do Estado, de defesa nacional, de segurança pública e de persecução penal.

Art. 24. A autoridade competente deve manter procedimentos para evitar que, no curso de suas atividades, obtenha e trate dados pessoais irrelevantes ou excessivos à finalidade da operação de tratamento.

Art. 25. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, mediante requisição:

I - confirmação da existência de tratamento;

II - acesso aos dados; e

III - correção de dados incompletos, inexatos ou desatualizados.



§ 1º O titular dos dados pessoais tem o direito de peticionar em relação aos seus dados contra o controlador perante a Autoridade Nacional de Proteção de Dados ou em juízo, quando cabível habeas data.

§ 2º Os direitos previstos neste artigo serão exercidos mediante requerimento expresso do titular ou de representante legalmente constituído, a agente de tratamento.

§ 3º Em caso de impossibilidade de adoção imediata da providência de que trata o § 2º deste artigo, o controlador enviará ao titular resposta em que poderá:

I - comunicar que não é agente de tratamento dos dados e indicar, sempre que possível, o agente; ou

II - indicar as razões de fato ou de direito que impedem a adoção imediata da providência.

§ 4º O responsável deverá informar, de maneira imediata, aos agentes de tratamento com os quais tenha realizado uso compartilhado de dados a correção, a eliminação, a anonimização ou o bloqueio dos dados, para que repitam idêntico procedimento, exceto nos casos em que esta comunicação seja comprovadamente impossível ou implique esforço desproporcional.

Art. 26. A prestação de informações e a concessão e acesso a dados pode ser adiada, limitada ou recusada se e enquanto tal for necessário e proporcional para:

I - evitar prejuízo para investigações, inquéritos ou processos judiciais;

II - evitar prejuízo para a prevenção, detecção, investigação ou repressão de infrações penais ou para a execução de sanções penais;

III - evitar prejuízo às ações de inteligência;

IV - evitar prejuízo às atividades de defesa nacional;

V - proteger a segurança do Estado ou a defesa nacional; ou

VI - proteger os direitos e garantias de terceiros.



§1º Nos casos previstos, o responsável pelo tratamento deve informar ao titular dos dados, por escrito e sem demora injustificada, dos motivos da recusa ou da limitação do acesso, bem como indicar quando cessarão os motivos da recusa ou da limitação de acesso;

§2º A comunicação pode ser omitida apenas na medida em que a sua prestação possa prejudicar uma das finalidades enunciadas no caput, caso em que o titular deve ser informado da possibilidade de levar o questionamento à ANPD ou de iniciar ação judicial.

§3º O controlador deve disponibilizar à ANPD informação sobre os motivos de fato e de direito que fundamentam a decisão de recusa ou de limitação do direito de acesso, bem como da omissão de informação ao titular dos dados.

Art. 27. O direito à retificação de dados pessoais não alcançará informações baseadas em percepções pessoais colhidas por agentes de autoridades competentes e testemunhas.

Art. 28. O acesso às informações pessoais tratadas no âmbito de atividades de segurança do Estado, de defesa nacional e de segurança pública, pelos titulares, dar-se-á por meio de requerimento às autoridades competentes, que deverão providenciar resposta aos titulares no prazo de 20 (vinte) dias da entrada do requerimento.

§ 1º Os dados pessoais serão armazenados em formato que favoreça o exercício do direito de acesso.

§ 2º As informações e os dados poderão ser fornecidos por meio de documento eletrônico, desde que inteligível, seguro e idôneo.

§ 3º A ANPD poderá dispor de forma diferenciada acerca dos prazos previstos nos incisos I e II do caput deste artigo para os setores específicos.

Art. 29. O acesso, pelos titulares, às informações pessoais tratadas no âmbito de atividades de investigação e repressão de infrações penais se dará nos termos da legislação processual penal vigente.

CAPÍTULO IV



DA SEGURANÇA DOS DADOS PESSOAIS

Art.

30. Os agentes de tratamento devem adotar medidas de segurança, físicas, técnicas e administrativas, aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

§ 1º A ANPD poderá dispor sobre padrões técnicos mínimos para tornar aplicável o disposto no caput deste artigo, considerados a natureza das informações tratadas, as características específicas do tratamento e o estado atual da tecnologia, especialmente no caso de dados pessoais sensíveis, assim como os princípios previstos no caput do artigo 4º desta Lei.

§ 2º Os agentes de tratamento ou qualquer outra pessoa que intervenha em uma das fases do tratamento obriga-se a garantir a segurança da informação prevista nesta Lei em relação aos dados pessoais, mesmo após o seu término.

§ 3º No que se refere ao tratamento automatizado de dados, o controlador deve adotar as seguintes medidas:

I - impedir o acesso de pessoas não autorizadas ao equipamento utilizado para o tratamento;

II - impedir que as mídias de dados sejam lidos, copiados, alterados ou retirados sem autorização;

III - impedir a introdução não autorizada de dados pessoais, bem como qualquer inspeção, alteração ou apagamento não autorizados de dados pessoais armazenados;

IV - impedir que os sistemas de tratamento automatizado sejam utilizados por pessoas não autorizadas;



V - assegurar que as pessoas autorizadas a utilizar um sistema de tratamento automatizado só tenham acesso aos dados pessoais abrangidos pela sua autorização de acesso;

VI - assegurar que possam ser verificados os dados pessoais que foram ou que possam ser transmitidos ou disponibilizados por meio de equipamento de comunicação de dados;

VII - assegurar que possam ser verificados a posteriori quais os dados pessoais introduzidos nos sistemas de tratamento automatizado, quando e por quem;

VIII - impedir que, durante as transferências de dados pessoais ou o transporte de mídias de dados, os dados pessoais possam ser lidos, copiados, alterados ou suprimidos sem autorização;

IX - assegurar que os sistemas utilizados possam ser restaurados em caso de interrupção; e

X - assegurar que as funções do sistema operem corretamente, que os erros de funcionamento sejam assinalados e que os dados pessoais armazenados não possam ser corrompidos por mau funcionamento do sistema.

Art. 31. Os sistemas desenvolvidos, a partir da vigência desta Lei, para o tratamento de dados pessoais devem ser estruturados de forma a atender aos requisitos de segurança, aos padrões de boas práticas e de governança e aos princípios gerais previstos nesta Lei e às demais normas regulamentares.

§ 1º As medidas de que trata o caput deste artigo deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução.

§ 2º O responsável pelo tratamento deve implementar medidas técnicas e organizacionais adequadas para garantir a rastreabilidade e a auditabilidade dos sistemas de informação.

Art. 32. O controlador deverá comunicar à Autoridade Nacional de Proteção de Dados a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.



§ 1º A comunicação será feita em prazo a ser regulamentado pela ANPD e deverá mencionar, no mínimo:

- I - a descrição da natureza dos dados pessoais afetados;
- II - as informações sobre os titulares envolvidos;
- III - a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial;
- IV - os riscos relacionados ao incidente;
- V - os motivos da demora, no caso de a comunicação não ter sido imediata; e
- VI - as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.

§ 2º A Autoridade Nacional de Proteção de Dados verificará a gravidade do incidente e poderá, caso necessário para a salvaguarda dos direitos dos titulares, determinar ao controlador a adoção de providências, tais como:

- I - ampla divulgação do fato em meios de comunicação; e
- II - medidas para reverter ou mitigar os efeitos do incidente.

CAPÍTULO V

DOS AGENTES DE TRATAMENTO DE DADOS PESSOAIS

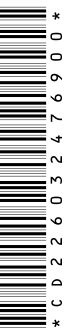
SEÇÃO I

DO CONTROLADOR E DO OPERADOR

Art. 33. É obrigatória a elaboração do relatório de impacto à proteção de dados pessoais, referente ao tratamento de dados pessoais sensíveis, sigilosos, ou em operações que apresentem elevado risco aos direitos, liberdades e garantias dos titulares de dados.

§ 1º O relatório mencionado no **caput** deste artigo deverá considerar, ao menos:

- I - descrição geral das operações de tratamento previstas;
- II - avaliação dos riscos para os direitos dos titulares de dados;



III - medidas previstas para fazer face a esses riscos; e

IV - medidas de segurança e mecanismos para assegurar a proteção dos dados pessoais.

§ 2º Outras informações podem ser solicitadas e determinadas pela ANPD para inclusão no relatório de impacto à proteção de dados pessoais.

§ 3º A ANPD poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, referente a outras hipóteses além daquelas mencionadas no caput deste artigo.

Art. 34. O operador deverá realizar o tratamento segundo as instruções fornecidas pelo controlador, que verificará a observância das próprias instruções e das normas sobre a matéria.

Art. 35. A Autoridade poderá dispor sobre aspectos referentes ao acesso aos dados e à segurança, e sobre o tempo de guarda dos registros, tendo em vista especialmente a necessidade e a transparência.

Art. 36. Os agentes de tratamento, no exercício de suas atribuições, devem cooperar com a autoridade nacional.

SEÇÃO II

DO REGISTRO DAS ATIVIDADES DE TRATAMENTO

Art. 37. O controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem.

Art. 38. O registro das operações de tratamento de que trata o art. 37 deverá conter:

I - o nome e o contato do encarregado;

II - a descrição das categorias de titulares de dados e das categorias de dados pessoais;

III - as finalidades das operações de tratamento;

IV - a indicação da base legal do tratamento;



V - a origem da coleta ou recebimento dos dados e as categorias de destinatários com quais os dados pessoais foram compartilhados;

VI - a utilização de técnicas e políticas de agrupamento de titulares em perfis, se for o caso;

VII - as categorias de transferências de dados pessoais para um país terceiro ou para uma organização internacional, se for caso disso;

VIII - os prazos de armazenamento das diferentes categorias de dados pessoais; e

IX - a descrição geral das medidas de segurança referidas no capítulo IV.

Parágrafo único. A ANPD poderá indicar outras informações a serem incluídas no registro das operações de tratamento.

SEÇÃO III

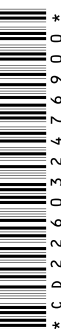
DO REGISTRO CRONOLÓGICO

Art. 37. O controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem.

Art. 39. Controladores e operadores devem conservar em sistemas de tratamento automatizado registros cronológicos das seguintes operações de tratamento: coleta; alteração; consulta; acesso; divulgação; transferências; interconexão, e apagamento.

§ 1º Os registros cronológicos das operações de consulta e de divulgação devem permitir determinar o motivo, a data e a hora dessas operações, a identificação da pessoa que consultou ou divulgou dados pessoais e, sempre que possível, a identidade dos destinatários desses dados pessoais.

§ 2º Os registros cronológicos, cuja integridade deve ser observada pelos controladores e operadores, serão mantidos por no mínimo 6 (seis) meses e poderão ser utilizados para efeitos de verificação da licitude do tratamento, controle administrativo, garantia da integridade e da segurança dos



dados pessoais, e para instrução de processos penais, inclusive a pedido da defesa.

§ 3º A ANPD poderá:

- I - solicitar aos controladores e operadores a disponibilização dos registros cronológicos; e
- II - dispor sobre outros prazos de registro cronológico.

SEÇÃO IV

DO ENCARREGADO

Art. 40. O controlador deverá indicar encarregado pelo tratamento de dados pessoais.

§ 1º A identidade e as informações de contato do encarregado deverão ser divulgadas publicamente, de forma clara e objetiva, preferencialmente no sítio eletrônico do controlador.

§ 2º As atividades do encarregado consistem em:

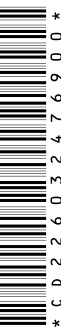
- I - aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;
- II - receber comunicações da Autoridade Nacional de Proteção de Dados e adotar providências; e
- III - orientar os servidores e funcionários da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais.

§ 3º A Autoridade Nacional de Proteção de Dados poderá estabelecer normas complementares sobre a definição e as atribuições do encarregado, inclusive hipóteses de dispensa da necessidade de sua indicação, conforme a natureza e o porte da entidade ou o volume de operações de tratamento de dados.

CAPÍTULO VI

TRANSFERÊNCIA INTERNACIONAL DE DADOS E COOPERAÇÃO INTERNACIONAL

SEÇÃO I



HIPÓTESES

Art. 41. Sem prejuízo de outras condições exigidas em Lei, as autoridades competentes poderão transferir dados pessoais para outro país ou para uma organização internacional, inclusive dados que se destinem a transferências ulteriores para outro país ou outra organização internacional, se:

I - a transferência for necessária para atividades de segurança do Estado, de defesa nacional, de segurança pública ou de persecução penal;

II - tiverem sido apresentadas garantias adequadas, nos termos do artigo 45, ou forem aplicáveis as derrogações previstas no artigo 46; e

III - os dados pessoais forem transferidos para agente no outro país ou na organização internacional com atribuições de segurança do Estado, de defesa nacional, de segurança pública ou de persecução penal, sem prejuízo do disposto no artigo 47.

§ 1º No caso de os dados pessoais terem sido transmitidos ou disponibilizados por país estrangeiro, é necessário ainda, para a transferência, que esse país tenha dado seu consentimento prévio, salvo se a transferência for necessária para prevenir ameaça imediata e grave à segurança pública do Brasil ou de país estrangeiro e o consentimento prévio não puder ser obtido em tempo hábil.

§ 2º Sendo aplicada a exceção prevista na parte final do §1º, a autoridade responsável por dar o consentimento deve ser informada em até 48 horas.

§ 3º Quando do envio de dados pessoais a outro país ou organização internacional, deverá ser ressaltado expressamente que a transferência ulterior desses dados para um terceiro país ou organização internacional só será permitida mediante consentimento da autoridade competente nacional responsável pela transferência inicial.

§ 4º O consentimento previsto no § 3º deverá levar em conta todos os fatores pertinentes, nomeadamente a gravidade da infração penal, a finalidade para que os dados pessoais foram inicialmente transferidos



e o nível de proteção no país ou na organização internacional para os quais se pretende que os dados pessoais sejam ulteriormente transferidos.

Art. 42. As transferências serão sempre documentadas, devendo o responsável pelo tratamento manter registro das informações sobre a data e hora da transferência, a autoridade competente que as recebe e a natureza dos dados pessoais transferidos.

SEÇÃO II

TRANSFERÊNCIAS SUJEITAS A GARANTIAS ADEQUADAS

Art. 43. Os dados pessoais podem ser transferidos para um país estrangeiro ou para uma organização internacional se:

I - tiverem sido apresentadas garantias adequadas no que diz respeito à proteção de dados pessoais, mediante documento formal subscrito pela autoridade destinatária competente; ou

II - o responsável pelo tratamento tiver avaliado todas as circunstâncias inerentes à transferência de dados pessoais e concluído que existem garantias adequadas no que diz respeito à proteção desses dados.

§ 1º Sem prejuízo da possibilidade de avaliações adicionais, presume-se a existência de garantias adequadas quando:

I - o destinatário se tratar de Estado Parte da Convenção do Conselho da Europa, de 1981 (CETS 108) e de seus protocolos; ou

II - a transferência se der no âmbito de organização internacional criada com a finalidade de cooperação nas atividades previstas no artigo 1º, integrada pelo Brasil como país-membro ou participante, e que tenha, em seus tratados constitutivos ou normativos internos, previsões de mecanismos adequados de proteção de dados.

SEÇÃO III

DERROGAÇÕES APLICÁVEIS EM SITUAÇÕES ESPECÍFICAS



Art. 44. A análise da existência de garantias adequadas nos termos do artigo anterior poderá ser dispensada, sem prejuízo das demais exigências legais, quando a transferência de dados pessoais para país estrangeiro ou para uma organização internacional for necessária:

I - para proteger os interesses vitais do titular dos dados ou de outra pessoa;

II - para salvaguardar os legítimos interesses do titular dos dados;

III - para prevenir ameaça imediata e grave contra a segurança pública no Brasil ou em país estrangeiro;

IV - para exercer direitos de defesa do Estado no âmbito de processo judicial ou administrativo punitivo; ou

V - para a cooperação jurídica internacional, de acordo com regras e instrumentos de direito internacional aplicáveis.

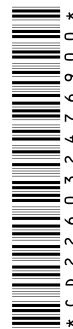
§ 1º Ainda que se verifiquem os fundamentos previstos no inciso IV, os dados pessoais não serão transferidos se a autoridade competente para proceder à transferência considerar que os direitos, liberdades e garantias fundamentais do titular dos dados em causa prevalecem sobre as finalidades que motivariam a transferência por interesse público.

§ 2º As transferências de dados efetuadas com base neste artigo serão limitadas aos dados estritamente necessários para a finalidade almejada.

SEÇÃO IV

TRANSFERÊNCIAS DE DADOS PESSOAIS PARA DESTINATÁRIOS ESTABELECIDOS EM OUTROS PAÍSES

Art. 45. Sem prejuízo de outras disposições estabelecidas em acordo internacional tal como definido no parágrafo único deste artigo, a autoridade pública com poderes de prevenção, investigação, detecção ou repressão de infrações penais ou de execução de sanções penais, incluindo a prevenção de ameaças à segurança pública, poderá transferir dados pessoais diretamente a destinatários estabelecidos em outros países, desde



que respeitadas as disposições da presente lei, estejam preenchidas as seguintes condições cumulativas:

I - a transferência ser estritamente necessária a uma função desempenhada pela autoridade competente que efetua a transferência e prevista por lei, tendo em vista as finalidades indicadas no artigo 1º;

II - a autoridade competente que efetuar a transferência considerar que os direitos, liberdades e garantias fundamentais do titular dos dados a serem transferidos não prevalecem sobre as finalidades que exigem a transferência no caso em apreço;

III - a autoridade competente que efetua a transferência considerar que a transferência para uma autoridade competente para os fins do artigo 1º, no outro país, revela-se ineficaz ou inadequada, especificamente por não ser possível efetuá-la em tempo hábil;

IV - a autoridade competente para os efeitos referidos no artigo 1º no outro país, seja informada sem demora injustificada, a menos que tal comunicação se revele ineficaz ou inadequada; e

V - a autoridade competente que efetua a transferência informar o destinatário da finalidade ou das finalidades específicas para as quais deve tratar os dados pessoais, desde que o tratamento seja necessário.

Parágrafo Único. Para os fins previstos no **caput**, por acordo internacional entende-se um acordo internacional bilateral ou multilateral em vigor entre o Brasil e o outro país no campo da cooperação jurídica ou policial internacional.

SEÇÃO V

COOPERAÇÃO INTERNACIONAL NO DOMÍNIO DA PROTEÇÃO DE DADOS PESSOAIS

Art. 46. Em relação a países estrangeiros e a organizações internacionais, as autoridades competentes nacionais adotarão as medidas necessárias destinadas a:



I - estabelecer procedimentos internacionais de cooperação que visem facilitar a aplicação efetiva da legislação em matéria de proteção de dados pessoais;

II - prestar assistência mútua em matéria de aplicação da legislação de proteção de dados pessoais, nomeadamente através da notificação, da transmissão de reclamações, da assistência na investigação e do intercâmbio de informações, sob reserva das garantias adequadas para a proteção dos dados pessoais e dos outros direitos e liberdades fundamentais;

III - associar as partes interessadas aos debates e às atividades que visem promover a cooperação internacional no âmbito da aplicação da legislação relativa à proteção de dados pessoais; e

IV - promover o intercâmbio e a documentação da legislação e das práticas em matéria de proteção de dados pessoais, inclusive sobre conflitos jurisdicionais com outros países.

CAPÍTULO VII

DA AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS E DO CONSELHO NACIONAL DE PROTEÇÃO DE DADOS PESSOAIS E DA PRIVACIDADE

SEÇÃO I

DA AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

Art. 47. A Autoridade Nacional de Proteção de Dados (ANPD), criada pela Lei nº 13.709, de 14 de agosto de 2018, será responsável por zelar, implementar e fiscalizar a presente lei em todo o território nacional, de forma cumulativa às suas atribuições estabelecidas na Lei nº 13.709, de 14 de agosto de 2018.

Art. 48. À ANPD ficam acrescidas às suas competências descritas na Lei nº 13.709, de 14 de agosto de 2018:

I - zelar pela proteção dos dados pessoais na segurança do Estado, na defesa nacional, na segurança pública e na persecução penal, nos termos da legislação;



II - fiscalizar e aplicar sanções em caso de tratamento de dados realizado em descumprimento à legislação, mediante processo administrativo que assegure o contraditório, a ampla defesa e o direito de recurso;

III - apreciar petições de titular contra o controlador no prazo estabelecido em regulamentação;

IV - promover na população o conhecimento das normas e das políticas públicas sobre proteção de dados pessoais na segurança do Estado, na defesa nacional, na segurança pública e persecução penal;

V - promover e elaborar estudos sobre as práticas nacionais e internacionais de proteção de dados pessoais na segurança do Estado, na defesa nacional, na segurança pública e persecução penal;

VI - promover ações de cooperação com autoridades de proteção de dados pessoais de outros países, de natureza internacional ou transnacional;

VII - solicitar, a qualquer momento, às autoridades competentes submetidas a esta lei informe específico sobre o âmbito, a natureza dos dados e os demais detalhes do tratamento realizado, com a possibilidade de emitir parecer técnico complementar para garantir o cumprimento desta Lei;

VIII - editar regulamentos e procedimentos sobre proteção de dados pessoais e privacidade na segurança do Estado, na defesa nacional, na segurança pública e persecução penal;

IX - solicitar relatórios de impacto à proteção de dados pessoais para os casos em que o tratamento representar alto risco aos direitos previstos nesta Lei;

X - ouvir os agentes de tratamento e a sociedade em matérias de interesse relevante e prestar contas sobre suas atividades e planejamento;

XI - realizar auditorias, ou determinar sua realização, no âmbito da atividade de fiscalização sobre o tratamento de dados pessoais efetuado pelas autoridades competentes;



XII - comunicar às autoridades competentes as infrações penais das quais tiver conhecimento;

XIII - comunicar aos órgãos de controle interno o descumprimento do disposto nesta Lei pelas autoridades competentes; e

XIV - implementar mecanismos simplificados, inclusive por meio eletrônico, para o registro de reclamações sobre o tratamento de dados pessoais em desconformidade com esta Lei.

Art. 49. O funcionamento e a organização da Autoridade permanecem os mesmo estabelecidos na Lei nº 13.709, de 14 de agosto de 2018.

SEÇÃO II

DO CONSELHO NACIONAL DE PROTEÇÃO DE DADOS PESSOAIS E DA PRIVACIDADE

Art. 50. Compete ao Conselho Nacional de Proteção de Dados Pessoais e da Privacidade, em acréscimo às suas competências estabelecidas na Lei nº 13.709, de 14 de agosto de 2018:

I - promover e elaborar estudos sobre as práticas nacionais e internacionais de proteção de dados pessoais na segurança do Estado, na defesa nacional, na segurança pública, investigação e persecução penal;

II - propor à Autoridade Nacional de Proteção de Dados a edição de regulamentos e procedimentos sobre proteção de dados pessoais e privacidade na segurança do Estado, na defesa nacional, na segurança pública e persecução penal; e

III - ouvir os agentes de tratamento e a sociedade em matérias de interesse relevante e prestar contas sobre suas atividades e planejamento;

Art. 51. O funcionamento e a organização do Conselho permanecem os mesmo estabelecidos na Lei nº 13.709, de 14 de agosto de 2018.

CAPÍTULO VIII

SANÇÕES



Art. 52. As infrações às normas previstas nesta Lei ficam sujeitas, conforme o caso, às seguintes sanções, aplicadas de forma isolada ou cumulativa:

I - advertência, com indicação de prazo para adoção de medidas corretivas;

II - bloqueio dos dados pessoais a que se refere a infração até a sua regularização, quando cabível;

III - suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 2 (dois) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador, quando cabível;

§ 1º O agente público que facilitar ou der causa à infração das normas desta Lei responderá administrativamente, conforme a lei disciplinar aplicável, incluindo, conforme o caso, a Lei de Improbidade Administrativa.

§ 2º Se o mesmo fato constituir simultaneamente crime e infração administrativa contra a mesma pessoa natural, o procedimento administrativo será suspenso quando iniciada medida de investigação de infração penal, retomando-se caso não sobrevenha sentença declarando a inexistência material do fato ou sua prática em legítima defesa, estado de necessidade, exercício regular de um direito ou cumprimento de um dever.

§ 3º A responsabilização administrativa não afastará a civil e a penal.

Art. 53. A fixação da sanção aplicável será feita de maneira fundamentada e considerará:

I - a gravidade da lesão; e

II - a culpabilidade do agente;

§ 1º São circunstâncias que agravam a sanção:

I - a reiteração de infrações;

II - a motivação político-partidária, preconceituosa ou de qualquer forma direcionada a grupos ou instituições determinadas; e



III - A condição de funcionário público no exercício da função.

§ 2º São circunstâncias que atenuam a sanção:

I - a comunicação espontânea da infração à ANPD e aos titulares dos dados;

II - o emprego espontâneo dos meios disponíveis para mitigação do dano;

III - a reparação espontânea dos danos;

IV - a adoção de política eficaz de proteção de dados;

§ 3º Quando a lesão for de menor magnitude e presentes as atenuantes do § 2º, a Autoridade Nacional de Proteção de Dados poderá, em decisão motivada e fundamentada, deixar de aplicar a sanção, ausentes as agravantes do § 1º.

CAPÍTULO IX

DISPOSIÇÕES FINAIS E TRANSITÓRIAS

Art. 54. A Lei nº 12.850, de 2 de agosto de 2013 passa a vigorar com as seguintes alterações:

Artigo 10 -A

§ 1º

II - dados cadastrais: são os dados apresentados pelo titular para realização ou manutenção do cadastro perante particular ou poder público, abrangendo aquelas informações referentes à 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, bem como demais dados não sujeitos a sigilo constitucional ou legal.

Artigo 15. O delegado de polícia e o Ministério Público terão acesso, independentemente de autorização judicial, apenas aos dados cadastrais do investigado mantidos pela Justiça Eleitoral, empresas telefônicas, instituições financeiras, provedores de internet e administradoras de cartão de crédito.



Art. 55. A Lei nº 12.965, de 23 de abril de 2014, passa a vigorar com as seguintes alterações:

“Art. 5º

VI - registro de conexão: o conjunto de informações referentes à data e hora de início e término de uma conexão à internet, sua duração e o endereço IP e porta lógica de acesso utilizados pelo terminal para o envio e recebimento de pacotes de dados;

.....

IX - dados cadastrais: são os dados apresentados pelo titular para realização ou manutenção do cadastro perante particular ou poder público, abrangendo aquelas informações referentes à 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, bem como demais dados não sujeitos a sigilo constitucional ou legal.” (NR)

“Artigo 10

.....

§ 3º O disposto no **caput** não impede o acesso aos dados cadastrais, na forma da lei, pelas autoridades administrativas que detenham competência legal para a sua requisição.” (NR)

Art. 56. A Lei nº 9.613, de 3 de março de 1998, passa a vigorar com as seguinte alteração:

“Art. 17-B. A autoridade policial e o Ministério Público terão acesso, exclusivamente, aos dados cadastrais do investigado, na forma da lei, mantidos pela Justiça Eleitoral, pelas empresas telefônicas, pelas instituições financeiras, pelos provedores de internet e pelas administradoras de cartão de crédito.” (NR)

Art. 57. A Lei nº 12.037, de 1º de outubro de 2009, passa a vigorar com as seguintes alterações:

“Art. 7º-C



.....

§ 2º O Banco Nacional Multibiométrico e de Impressões Digitais tem como objetivo armazenar dados de registros biométricos, de impressões digitais e, quando possível, de íris, face e voz, para subsidiar investigações criminais federais, estaduais ou distritais, bem como apoiar a identificação ou verificação de identidade do cidadão.

.....

§ 6º No caso de bancos de dados de identificação de natureza civil, administrativa ou eleitoral, a integração ou o compartilhamento dos registros do Banco Nacional Multibiométrico e de Impressões Digitais incluirá impressões digitais, biometria facial, voz, íris, entre outras, e às informações necessárias para identificação do seu titular.

§ 7º A integração ou a interoperação dos dados de registros multibiométricos constantes de outros bancos de dados com o Banco Nacional Multibiométrico e de Impressões Digitais ocorrerá por meio de acordo ou convênio com a unidade gestora e não dependerá de ressarcimento ao detentor dos dados.

.....

§ 11. A mera verificação biométrica da autenticidade de documento de identificação pessoal, com uso do BNM, é permitida a agentes públicos para fins de segurança pública e de identificação do cidadão (NM).”
(NR)

Art. 58. O compartilhamento de dados, entre unidades da Administração Pública Federal, com a finalidade de subsidiar atividades de segurança pública e investigação criminal, é obrigatório, respeitará o disposto nesta Lei e independerá de ressarcimento ou de qualquer tipo de remuneração ao detentor originário do banco de dados.

Parágrafo Único. O disposto no **caput** respeitará o sigilo legal ou constitucional de dados, regulados pela legislação processual penal vigente, e será, nesses casos de sigilo, operado mediante autorização judicial.



Art. 59. Esta lei entrará em vigor 180 dias a contar da data de sua publicação.

JUSTIFICAÇÃO

O texto que ora se apresenta é um Anteprojeto com o objetivo de orientar a aplicação da Lei de Proteção de Dados Pessoais para fins exclusivos de segurança do Estado, de defesa nacional, de segurança pública, e de investigação e repressão de infrações penais. A presente exposição demonstra a necessidade, a estrutura e os principais conceitos da proposta legislativa para regular o tratamento de dados pessoais no âmbito das atividades dantes mencionadas.

A Lei Geral de Proteção de Dados Pessoais – LGPD (Lei n. 13.709, de 2018) dispõe sobre o tratamento de dados pessoais das pessoas naturais, definindo as hipóteses em que tais dados podem ser legitimamente utilizados por terceiros e estabelecendo mecanismos para proteger os titulares dos dados contra usos inadequados. A Lei é aplicável ao tratamento de dados realizado por pessoas naturais ou por pessoas jurídicas de direito público ou privado, e tem, conforme definido em seu art 1º, o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Entretanto, ressalta-se que a mencionada Lei criou um regime jurídico especial para determinadas operações envolvendo o tratamento de dados pessoais, e excepcionalizou de seu escopo o tratamento de dados pessoais, dentre outras, para quatro finalidades relacionadas diretamente com a atuação estatal, sendo tais a de segurança do Estado, a de defesa nacional, a de segurança pública, e a de investigação e repressão de infrações penais, conforme disposto nas alíneas do inciso III do artigo 4º, onde se lê que:

“Art. 4º Esta Lei não se aplica ao tratamento de dados pessoais:

.....



III - realizado para fins exclusivos de:

- a) segurança pública;
- b) defesa nacional;
- c) segurança do Estado; ou
- d) atividades de investigação e repressão de infrações penais;”

Nesse sentido, mesmo excepcionalizando a aplicação da Lei para operações de tratamento de dados pessoais para as finalidades supramencionadas, a mesma Lei estabeleceu expressamente, no § 1º do Art. 4º, a necessidade de aprovação de lei específica para esse tema, conforme se vê:

§ 1º O tratamento de dados pessoais previsto no inciso III será regido por legislação específica, que deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular previstos nesta Lei.

Desse modo, reconhecida a lacuna e justificada a necessidade da elaboração de uma nova lei para regular o tratamento de dados pessoais em matérias afetas à segurança do Estado, à defesa nacional, à segurança pública, e à investigação e repressão de infrações penais, passa-se então à apresentação da estrutura do anteprojeto de lei.

Primeiramente, importa destacar que se trata de uma regulamentação acerca da aplicação do regime de proteção de dados pessoais voltada para as quatro atividades listadas nas alíneas do inciso III do art. 4º da LGPD, ou seja, o intuito deste anteprojeto é disciplinar os princípios e as diretrizes para que as operações de tratamento de dados pessoais no mencionado âmbito ocorram com respeito aos direitos fundamentais de liberdade e privacidade e à autodeterminação informativa.

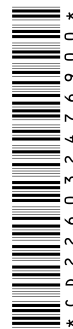


Busca-se, portanto, harmonizar, de um lado, os deveres do Estado no exercício das atividades de segurança do Estado, de defesa nacional, de segurança pública, e de investigação e repressão de infrações penais; e, de outro, a observância das garantias processuais e as prerrogativas fundamentais dos cidadãos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

Nesse sentido, tendo em vista a pretensão de introduzir normas gerais, este projeto pretende complementar o sistema legislativo de tratamento de dados pessoais, com ênfase nos fins de segurança do Estado, de defesa nacional, de segurança pública, e de investigação e repressão de infrações penais, abordando de forma abrangente as responsabilidades dos órgãos incumbidos dessas atividades, sem fragmentar sua interpretação ou endereçá-la a instrumentos posteriores.

Isto posto, passa-se a apresentar a estrutura do proposto instrumento. Para atender ao propósito a que se destina, o presente projeto está estruturado em 9 capítulos, com 59 artigos, onde são abordados conceitos, princípios, direitos dos titulares de dados e responsabilidades dos agentes de tratamento no desempenho de atividades específicas de segurança do Estado, de defesa nacional, de segurança pública, e de investigação e repressão de infrações penais.

Com o presente projeto de lei, espera-se obter os seguintes benefícios: (i) maior segurança jurídica, ao tratar as finalidades estabelecidas no inciso III do art. 4º da LGPD de forma conjunta, no mesmo instrumento, o que evitará a necessidade de instrumentos correlatos posteriores, que naturalmente trariam abordagens redundantes; (ii) atribuição proporcional, razoável e factível das devidas responsabilidades aos órgãos encarregados das atividades mencionadas no inciso III do art. 4º, quanto ao tratamento de dados pessoais, sem contudo lhes obstaculizar no exercício de suas atividades finalísticas; (iii) não impede o necessário e, por vezes, imprescindível fluxo de dados pessoais entre órgãos responsáveis pelas atividades elencadas no referido inciso III, permitindo o desempenho desses órgãos no cumprimento de suas atividades finalísticas; (iv) mantém o foco no tratamento de dados pessoais pelos mencionados órgãos, e não nas tecnologias por eles utilizadas



no cumprimento de suas atribuições, uma vez que tecnologias podem evoluir, o que levaria à necessidade de frequentes alterações no texto legal; e (v) preenche relevante vácuo normativo ao cumprir a determinação da LGPD sobre lei específica quanto às mencionadas atividades do inciso III do art. 4º.

Por fim, o presente projeto apresentará à sociedade os necessários cânones quanto à proteção de dados pessoais a serem adotados pelos órgãos responsáveis pelas atividades de segurança do Estado, de defesa nacional, de segurança pública, e de investigação e repressão de infrações penais, e o dever desses agentes quanto ao inalienável respeito ao direito fundamental dos titulares de dados pessoais na proteção desses dados, em todas as operações de tratamento sob a responsabilidade dos citados entes estatais.

A aprovação do presente instrumento, com a necessária participação da sociedade e consideradas, ainda, as opiniões técnicas ou as recomendações advindas da Autoridade Nacional de Proteção de Dados - ANPD, conforme previsão legal, completará o ciclo normativo superior da proteção de dados, e reforçará a indispensável segurança jurídica no ecossistema da proteção de dados pessoais e da privacidade no Brasil.

Diante dessas razões, tomamos a presente iniciativa, esperando contar com o apoio de nossos ilustres pares para a aprovação deste Projeto de Lei.

Sala das Sessões, em de de 2022.

Deputado CORONEL ARMANDO

