

EXPOSIÇÃO DE MOTIVOS:

Anteprojeto de Lei de Proteção de Dados para segurança pública e persecução penal

O texto que ora se apresenta é um Anteprojeto de Lei de Proteção de Dados para segurança pública e investigação criminal, elaborado pela Comissão de Juristas instituída por Ato do Presidente da Câmara dos Deputados, de 26 de novembro de 2019. Esta breve exposição pretende demonstrar a necessidade, a estrutura e os principais conceitos da proposta legislativa para regular o tratamento de dados no âmbito da segurança pública e de atividades de persecução e repressão de infrações penais.

Desde logo, cabe destacar que foi opção do legislador não contemplar o tratamento de dados para segurança pública e investigação criminal no âmbito de aplicação da Lei Geral de Proteção de Dados (LGPD – Lei n. 13.709/2018), estabelecendo expressamente a necessidade de aprovação de lei específica para esse tema (art. 4, *caput*, inciso III, alíneas “a” e “d” c/c § 1º, da LGPD): “*O tratamento de dados pessoais previsto no inciso III [tratamento de dados realizado para fins de: segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais] 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*”. Trata-se de um mandamento legal para legislar sobre a matéria, a partir da constatação de que está sujeita a ponderações específicas sobre o uso de dados pessoais e que expressa reivindicação da sociedade e das autoridades competentes para regulação do tema, surgida no processo de debate da própria LGPD.

Nesse contexto, a elaboração de uma legislação específica fundamenta-se na necessidade prática de que os órgãos responsáveis por atividades de segurança pública e de investigação/repressão criminais detenham segurança jurídica para exercer suas funções com maior eficiência e eficácia – como pela participação em mecanismos de cooperação internacional –, porém sempre de forma compatível com as garantias processuais e os direitos fundamentais dos titulares de dados envolvidos. Trata-se, portanto, de projeto que oferece balizas e parâmetros para operações de tratamento de dados pessoais no âmbito de atividades de segurança pública e de persecução criminal, equilibrando tanto a proteção do titular contra mau uso e abusos como acesso de autoridades a todo potencial de ferramentas e plataformas modernas para segurança pública e investigações.

De fato, destaca-se que a grande lacuna legislativa existente hoje no ordenamento jurídico brasileiro nessa matéria se manifesta em duas problemáticas centrais.

O primeiro problema diz respeito à própria eficiência investigativa dos órgãos brasileiros, visto que a falta de adequação aos padrões internacionais de segurança quanto ao fluxo e ao tratamento de dados obsta a integração do Brasil com órgãos de inteligência e de investigação de caráter internacional (v.g., INTERPOL), obstando o próprio acesso a bancos de dados e a informações relevantes, e coloca o uso de aplicações tecnológicas em segurança pública e a adoção de técnicas modernas de investigação sob questionamento de sua validade jurídica.

Em segundo lugar, há um enorme déficit de proteção dos cidadãos, visto que não há regulação geral sobre a licitude, a transparência ou a segurança do tratamento de dados em matéria penal, tampouco direitos estabelecidos ou requisitos para utilização de novas tecnologias que possibilitam um grau de vigilância e monitoramento impensável há alguns anos. Apesar do crescimento vertiginoso de novas técnicas de vigilância e de investigação, a ausência de regulamentação sobre o tema gera uma assimetria de poder muito grande entre os atores envolvidos (Estado e cidadão). Nesse contexto, o titular dos dados é deixado sem garantias normativas mínimas e mecanismos institucionais aplicáveis para resguardar seus direitos de personalidade, suas liberdades individuais e até a observância do devido processo legal.

Reconhecida esta lacuna e elucidada a justificativa para a elaboração de uma nova lei para regular o tratamento de dados pessoais em matéria penal, passa-se então à apresentação da estrutura do anteprojeto de lei.

Primeiramente, importa destacar que se trata de uma Lei Geral de Proteção de Dados voltada para a investigação criminal e de segurança pública (LGPD-Penal). Ou seja, o intuito deste anteprojeto é disciplinar os princípios, as diretrizes e as linhas mestras da proteção de dados no referido âmbito. Busca-se, portanto, harmonizar, de um lado, os deveres do Estado na prevenção e na repressão de ilícitos criminais, protegendo a ordem pública; de outro, assegurar 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, esta “LGPD-Penal” pretende complementar o microsistema legislativo de tratamento de dados para fins de segurança pública e de investigação criminal hoje existente em leis esparsas e voltadas sobretudo à regulamentação de quebras de sigilo no contexto processual penal (v.g., disposições do Código de Processo Penal, da Lei das Interceptações Telefônicas e Telemáticas, da Lei Complementar n. 105, do Marco Civil da Internet, entre outras), modernizando-o à luz da nova realidade tecnológica e aprimorando-o com vistas a conferir maior segurança jurídica para todos os atores envolvidos.

O presente anteprojeto está estruturado em 12 capítulos, com 68 artigos. A sua estrutura e seu conteúdo estão inspirados, sobretudo, em duas legislações: uma nacional e outra internacional. Ademais, insta destacar que parte específica sobre tecnologias de vigilância e tratamento de elevado risco se inspira em leis dos Estados Unidos.

Das principais inspirações, a primeira é a própria Lei Geral de Proteção de Dados, que em seu artigo 4º, § 1º, determina que para fins da Lei vinculada a este anteprojeto devem ser “observados o devido processo legal, os princípios gerais de proteção e os direitos do titular previstos nesta Lei.”. Diante disso, constata-se devida previsão dos princípios que norteiam a atividade interpretativa e disciplinam o tratamento, uso, coleta de dados (art. 6º, LGPD), bem como a garantia dos direitos dos titulares dos dados às informações acerca do tratamento (arts. 17 a 22, LGPD). No anteprojeto, correspondem a esses artigos, respectivamente, o seu artigo 6º e os seus artigos 18 a 28.

A outra fonte importante para este anteprojeto consiste na Diretiva 680/2016, da União Europeia, que, em sentido convergente à experiência brasileira, regulou o tratamento de dados para fins de segurança pública e persecução penal separadamente de seu marco normativo aplicável ao tratamento de dados como um todo (Regulamento 679/2016, da União Europeia). Nessa dimensão, destacam-se pontos deste anteprojeto de

confluência com os da supracitada Diretiva, a saber: (i) os registros de atividade de tratamento; (ii) a segurança e o sigilo dos dados; e (iii) a transferência internacional de dados.

Noutro giro, aprofundando-se nas principais disposições legislativas introduzidas por este anteprojeto, busca-se uma breve análise dos seguintes eixos: (i) âmbito de aplicação da Lei; (ii) condições de aplicação; (iii) base principiológica; (iv) direitos e obrigações; (v) segurança da informação; (vi) tecnologias de monitoramento; (vii) transferência internacional de dados e; (viii) a autoridade de supervisão.

No que diz respeito ao âmbito de aplicação, destaca-se a necessidade de o tratamento ser realizado sempre, no papel de “controlador”, por uma autoridade competente (artigo 9º, I). Baseada em terminologia comum no campo a nível internacional, confere-se ao conceito de “autoridade competente” o seu sentido constitucional, ou seja, é a autoridade pública à qual está atribuída a responsabilidade para o exercício de atividades atinentes ao conteúdo deste anteprojeto, inclusive a execução de políticas públicas relacionadas à segurança pública.

O segundo ponto diz respeito às condições de licitude e de legitimidade para o tratamento de dados no âmbito de investigação criminal e de garantia da segurança pública. Consoante depreende-se do art. 9º, I, II e III, do anteprojeto, além da evidente necessidade de conformidade com a base principiológica, as bases legais que autorizam o tratamento de dados são as seguintes: "I - quando necessário para o cumprimento de atribuição legal de autoridade competente, na persecução do interesse público, na forma de lei ou regulamento, observados princípios gerais de proteção, os direitos do titular e os requisitos do Capítulo VI desta Lei; II - para execução de políticas públicas previstas em lei, na forma de regulamento, observados os princípios gerais de proteção, os direitos do titular e os requisitos do Capítulo VI desta Lei; III - para a proteção da vida ou da incolumidade física do titular ou de terceiro, contra perigo concreto e iminente."

Destarte, percebe-se o requisito de licitude para o tratamento de dados pessoais em geral, conforme o art. 9º, I, diz respeito à necessidade para o cumprimento de atribuição legal de autoridade competente, na persecução do interesse público, na forma de lei ou regulamento, observados os princípios gerais de proteção e os direitos do titular da lei. É dizer: torna-se indispensável um comando legal para que o tratamento de dados ocorra, visto que a atribuição legal da autoridade é o primeiro aspecto a ser considerado como parâmetro de licitude. Ocorre que essa atribuição para o tratamento de dados precisa ser conferida por lei em sentido estrito, mas pode ser detalhada tanto em leis, como em regulamentos.

Já a legalidade estrita é exigida somente nas hipóteses cuja repercussão e o dano são mais sensíveis, quais sejam: (i) no tratamento de dado sensível, definido como “dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou dado biométrico”, tal como na LGPD; (ii) no tratamento de dado sigiloso, terminologia referente aos dados para os quais a Constituição ou leis infraconstitucionais resguardam o direito ao sigilo, alicerçado em maiores expectativas de privacidade do titular – como se vê em regulamentos e procedimentos para quebra de sigilo em leis esparsas; e (iii) na utilização de tecnologia de monitoramento e/ou tratamento de dado de elevado risco, nas quais a potencialidade de dano a direitos, garantias e liberdades de titulares é alta.

Esse recorte metodológico, que estabelece diferentes requisitos para o tratamento de dados, a depender dos tipos de dados tratados e da forma pelo qual se realiza, se justifica à luz dos diferentes riscos gerados à esfera de direitos do cidadão e está alinhado com uma moderna e atual concepção de proteção de dados pessoais.

Acerca dos princípios, com forte inspiração na LGPD, o anteprojeto consolida uma robusta base principiológica que deve conformar todas as etapas e as cadeias do tratamento de dados pessoais no âmbito da investigação. No ponto, o artigo 6º, do anteprojeto, elenca uma série de princípios, os quais, em síntese, vinculam o seguinte conteúdo: (I) licitude: embasamento do tratamento em hipótese legal; (II) finalidade: fins devem ser legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades; (III) adequação: pertinência do tratamento com suas finalidades; (IV) necessidade: o dados devem ser o mínimo suficiente para consecução dos objetivos do tratamento; (V) proporcionalidade: compatibilidade do tratamento com seus objetivos; (VI) livre acesso: garantia de facilidade e gratuidade aos titulares ao acesso às informações do tratamento de seus dados; (VII) qualidade dos dados: garantia aos titulares de dados de exatidão, clareza, relevância e atualização dos seus dados; (VIII) transparência: garantia aos titulares de informações claras, precisas e acessíveis sobre o tratamento e seu responsável; (IX) segurança: utilização de medidas técnicas e administrativas para a não violação de dados; (X) prevenção: adoção de medidas de prevenção de violações; (XI) não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos; e (XII) responsabilização e prestação de contas: demonstração de medidas que comprovem a observância e a eficácia das normas de proteção de dados.

Após a análise dos princípios estabelecidos no anteprojeto, vale salientar os direitos dos titulares e as obrigações dos agentes de tratamento, pontos de grande relevância na proposta legislativa. Quanto aos direitos dos titulares, o texto prevê, por um lado, os direitos clássicos de acesso aos dados e retificação, cuja base encontra-se até mesmo no remédio constitucional do *habeas data*, e por outro, direitos alinhados às tendências contemporâneas de regulação das decisões automatizadas, como o direito à proteção contra a discriminação e o direito à explicação de processos automatizados.

Sob a ótica das obrigações dos agentes de tratamento, destaca-se a necessidade de elaboração de relatórios de impacto à proteção de dados pessoais em casos de tratamento de dados pessoais sensíveis, sigilosos, ou operações que apresentem elevado risco aos direitos, liberdades e garantias dos titulares de dados. Além disso, é obrigatória a manutenção de registros das atividades de tratamento, detalhados no artigo 33 do anteprojeto.

Como destacado, a parte relativa à segurança e ao sigilo de dados teve forte influência da Diretiva 680/2016. Nesse contexto, no artigo 36, está prescrito um extenso rol de medidas que devem ser adotadas para fins de proteção de dados contra possíveis violações, à guisa de exemplo: controle de acesso ao equipamento, controle dos utilizadores e controle do acesso aos dados. Ademais, em um grande passo para a modernização desse tema no país, o artigo 37 traz os conceitos de *privacy by design* e *privacy by default* para o contexto da proteção de dados em matéria penal.

Paralelamente, um dos principais pilares do anteprojeto é a noção de acesso a informações e transparência. Como se sabe, qualquer operação que pretenda gerar confiança acerca de sua legitimidade e integridade, acompanhada de mecanismos de supervisão e controle institucional, passa pela garantia de publicidade aos tipos, escopo e

finalidades específicas de usos de dados. Nesse sentido, e em linha com o modelo internacional sobre a matéria, o anteprojeto inclui o dever de conferir transparência a modalidades de tratamento de dados realizadas por uma autoridade competente.

Outro eixo relevante do anteprojeto diz respeito ao conceito de tecnologia de monitoramento, compreendida como equipamento, programa de computador ou sistema informático que possa ser usado ou implementado para tratamento de dados pessoais captados ou analisados em vídeo, imagem, texto ou áudio, condicionada sempre a previsão legal específica, análise de impacto regulatório e a relatório de impacto à proteção de dados (art. 42). Os critérios para identificação de utilizações desse tipo de tecnologia que representem alto risco estão expressos no §1º desse dispositivo, que traz a natureza dos dados envolvidos, as finalidades específicas do tratamento ou mesmo a possibilidade de tratamento discriminatório como critérios mínimos para tal avaliação. Como antecipado, trata-se de abordagem regulatória que tem inspiração em legislações americanas modernas, sobretudo da cidade de Nova York e do estado de Washington.

O anteprojeto também endereçou a realidade do compartilhamento de dados entre autoridades públicas competentes para os fins da lei; entre estas e autoridades públicas cuja atribuição legal não versa sobre investigações e segurança pública; bem como entre autoridades competentes e pessoas jurídicas de direito privado. Em linha com os parâmetros fixados como requisitos para o tratamento, esses diferentes fluxos devem estar regrados por autorização legal ou judicial, resguardada a possibilidade de atuações conjuntas e colaborações, quando estas também forem lícitas. Dessa forma, endereçou-se a importante função do compartilhamento de dados em matéria penal, ao tempo em que se garantiu a proteção dos direitos e princípios previstos no anteprojeto.

Quanto à transferência internacional de dados, em similitude com o previsto pela legislação europeia, em especial a Diretiva 680 e a legislação portuguesa, o anteprojeto prevê critérios para esse fluxo internacional de dados, que podem ser consolidados em três tipos: transferências com base numa decisão de adequação, transferências sujeitas a garantias adequadas e derrogações aplicáveis em situações específicas. Também aqui, a construção de uma arquitetura regulatória compatível com modelos internacionais amplia as capacidades de integração e parcerias a nível internacional do Brasil.

Impende destacar que a Comissão optou por criar um tipo penal relacionado à transmissão ilegal de dados, realizada para obter vantagem indevida ou causar prejuízos a outrem. A introdução de uma figura penal para a tutela dos ataques mais graves à proteção de dados pessoais pareceu-nos recomendável, tendo sido considerados os seguintes pontos: a) A tutela estendida aos ataques cometidos no âmbito do Anteprojeto (segurança pública e persecução penal) e da LGPD; b) Inclusão do dispositivo diretamente no Código Penal, em um novo capítulo destinado expressamente à tutela deste direito fundamental; c) Redação empregando os termos constantes nas definições da LGPD e do Anteprojeto para evitar remissão em bloco aos diplomas legais; d) Dosagem da gravidade a ser feita mediante causas de aumento da pena ou figuras qualificadas pela qualidade dos dados e/ou pelo agente infrator; e) Não introdução de figuras culposas; e f) Gradação de penas que levem em conta a possibilidade de medidas alternativas ao processo e à pena privativa de liberdade (transação penal, acordo de não persecução penal etc. Por fim, o tipo penal tem uma abrangência restrita, visto que só é aplicável caso o agente busque uma de duas finalidades específicas (prejudicar o titular dos dados ou terceiro ou obter vantagem indevida) e, naturalmente, estão excluídas do seu âmbito todas as hipóteses lícitas de tratamento de dados, como a atuação da imprensa, por exemplo.

Por fim, uma importante inovação trazida por esta Lei é a autoridade criada para sua aplicação, supervisão e monitoramento (*enforcement*): o Conselho Nacional de Justiça (CNJ). A escolha do CNJ como a autoridade responsável deu-se em razão da sua autonomia e da pluralidade de sua composição. Sabe-se que a autonomia e imparcialidade do órgão supervisor é fundamental para que um país esteja apto a pleitear uma decisão quanto à adequação de sua legislação de proteção de dados ao nível de proteção europeu, que permitiria às autoridades de investigação no país acessar e compartilhar uma maior quantidade de dados com autoridades e instituições europeias, como Europol, Interpol e Eurojust.

Dessa forma, a indicação do CNJ como órgão supervisor é importante na medida em que: (i) evita o dispêndio de novos gastos com a criação de um órgão específico; (ii) aproveita a *expertise* dos setores, dos Conselheiros e dos servidores do CNJ que já vêm expedindo atos normativos importantes sobre a proteção de dados no âmbito brasileiro (v.g. Recomendação CNJ n. 73, de 20/08/2020 e Portaria CNJ n. 63/2019); e (iii) permite a formulação de políticas públicas uniformes para todo território nacional, a partir de uma composição plural e independente com membros de instituições diversas à luz do art. 103-B, da Constituição Federal (v.g. Poder Judiciário estadual, federal e trabalhista, Ministério Público estadual e federal, Ordem dos Advogados do Brasil, Câmara dos Deputados e Senado Federal).

CAPÍTULO I

DISPOSIÇÕES PRELIMINARES

Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais realizado por autoridades competentes para atividades de segurança pública e de persecução penal, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

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

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 - a autodeterminação informativa;

III - o respeito à vida privada e à intimidade;

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

V - a presunção de inocência;

VI - confidencialidade e integridade dos sistemas informáticos pessoais; e

VII - garantia do devido processo legal, da ampla defesa, do contraditório, da motivação e da reserva legal.

Art. 3º Esta Lei aplica-se a qualquer operação de tratamento realizada por autoridades competentes em atividades de segurança pública e de persecução penal.

Art. 4º Esta Lei não se aplica ao tratamento de dados pessoais realizado para fins exclusivos de defesa nacional e segurança do Estado.

Art. 5º Para os fins desta Lei, considera-se:

I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;

II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou dado biométrico, quando vinculado à pessoa natural;

III - dado pessoal sigiloso: dado pessoal protegido por sigilo constitucional ou legal;

IV - dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;

V - banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico;

VI - titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;

VII - controlador: autoridade competente responsável pelas decisões referentes ao tratamento de dados pessoais;

VIII - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;

IX - encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e o Conselho Nacional de Justiça (CNJ);

X - agentes de tratamento: o controlador e o operador;

XI - tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, uso compartilhado, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;

XII - anonimização: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo;

XIII - consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;

XIV - bloqueio: suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados;

XV - eliminação: exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado;

XVI - transferência internacional de dados: transferência de dados pessoais para país estrangeiro ou organização internacional;

XVII - uso compartilhado de dados: divulgação por transmissão, comunicação, transferência, difusão ou qualquer forma de disponibilização, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicas no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados;

XVIII - relatório de impacto à proteção de dados pessoais: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco;

XIX - análise de impacto regulatório: 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;

XX - autoridade competente: autoridade pública, órgão ou entidade do Poder Público responsável 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;

XXI - atividade de segurança pública: toda e qualquer atividade exercida para a preservação da ordem pública e para prevenção e detecção de infrações penais, inclusive aquelas de inteligência institucional, policial e financeira, realizada por autoridades competentes para a finalidade de segurança pública;

XXII – atividade de persecução penal: toda e qualquer atividade exercida para a investigação, apuração, persecução e repressão de infrações penais e execução de penas,

por autoridades competentes, inclusive aquelas de inteligência policial, institucional e financeira realizada por autoridades competentes para a finalidade de persecução penal;

XXIII - tecnologia de monitoramento: equipamento, programa de computador ou sistema informático que possa ser usado ou implementado para tratamento de dados pessoais captados ou analisados, entre outros, em vídeo, imagem ou áudio;

XXIV - registros criminais: informações sobre investigações, indiciamentos, medidas cautelares, processos, condenações ou execução da pena.

Art. 6º As atividades de tratamento de dados pessoais 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: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;

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

IV - necessidade: limitação do tratamento ao mínimo 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 – proporcionalidade: compatibilidade do tratamento com os objetivos pretendidos, de acordo com o contexto do tratamento;

VI - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;

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

VIII - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;

IX - segurança da informação: utilização de medidas 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;

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

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

XII - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

Art. 7º No tratamento de dados pessoais, o responsável pelo tratamento deve, na medida do possível, fazer uma distinção clara entre as diferentes categorias de titulares dos dados, especialmente:

- I – pessoas em relação às quais existem indícios suficientes de que cometeram uma infração penal;
- II – pessoas em relação às quais existem indícios suficientes de que estão prestes a cometer uma infração penal;
- III – pessoas processadas pela prática de infração penal;
- IV – pessoas condenadas definitivamente pela prática de infração penal;
- V – vítimas de uma infração penal ou pessoas em relação às quais certos fatos indicam que podem ser vítimas de uma infração penal; e
- VI – outras pessoas, tais como testemunhas, pessoas que possam fornecer informações, ou contatos ou associados das pessoas referidas nos incisos I a V.

Art. 8º No tratamento de dados, o responsável deve distinguir, na medida do possível, os dados pessoais baseados em fatos dos dados pessoais baseados em avaliações pessoais.

Parágrafo único. Caso o responsável verifique que tratou dados pessoais inexatos ou que tratou dados pessoais de forma ilícita, o destinatário deve ser informado tão logo seja possível e os dados pessoais devem ser retificados ou apagados.

CAPÍTULO II

DO TRATAMENTO DE DADOS PESSOAIS

Seção I

Dos Requisitos para o Tratamento de Dados Pessoais

Art. 9º O tratamento de dados pessoais para atividades de segurança pública e de persecução penal somente poderá ser realizado nas seguintes hipóteses:

- I - quando necessário para o cumprimento de atribuição legal de autoridade competente, na persecução do interesse público, na forma de lei ou regulamento, observados os princípios gerais de proteção, os direitos do titular e os requisitos do Capítulo VI desta Lei;
- II - para execução de políticas públicas previstas em lei, na forma de regulamento, observados os princípios gerais de proteção, os direitos do titular e os requisitos do Capítulo VI desta Lei;

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

Art. 10. É vedado o tratamento de dados pessoais para atividades de segurança pública e de persecução penal por pessoa de direito privado, exceto em procedimentos sob tutela de pessoa jurídica de direito público, que serão objeto de informe específico ao Conselho Nacional de Justiça, sem prejuízo de outras exigências legais.

Art. 11. O acesso de autoridades competentes a dados pessoais controlados por pessoas jurídicas de direito privado somente ocorrerá mediante previsão legal, respeitados os princípios desta Lei.

§1º É admitida a colaboração voluntária, quando em conformidade com a Lei nº 13.709/18.

§2º Toda e qualquer requisição administrativa ou judicial indicará o fundamento legal de competência expressa para o acesso e a motivação concreta, incluindo sua adequação, necessidade e proporcionalidade, sendo vedados pedidos que sejam genéricos ou inespecíficos.

§3º Ressalvadas as hipóteses de dever legal de coleta e de retenção, a pessoa jurídica de direito privado que não coletar ou não mais reter dados pessoais para a realização de sua atividade econômica ficará desobrigada de fornecer tais dados.

§4º É vedada a proibição desmotivada e genérica de notificação dos titulares de dados cujos dados pessoais forem fornecidos em razão de requisição administrativa ou judicial sigilosa, devendo a autoridade competente especificar quando será possível a notificação.

Art. 12. O Conselho Nacional de Justiça emitirá opiniões técnicas ou recomendações referentes às operações de tratamento e deverá solicitar às autoridades competentes responsáveis relatórios de impacto à proteção de dados pessoais.

Seção II

Do Tratamento de Dados Pessoais Sensíveis

Art. 13. O tratamento de dados pessoais sensíveis somente poderá ser realizado por autoridades competentes se estiver previsto em lei, observadas as salvaguardas desta Lei.

Parágrafo único. A autoridade competente responsável pelo tratamento de dados pessoais sensíveis elaborará relatório de impacto à proteção de dados pessoais e informará o Conselho Nacional de Justiça.

Seção III

Do Tratamento de Dados Pessoais Sigilosos

Art. 14. O tratamento de dados pessoais sigilosos por autoridades competentes somente poderá ser realizado se estiver previsto em lei e para atividades de persecução penal.

§1º O acesso a dados pessoais sigilosos por meio de ferramentas de investigação e medidas cautelares de obtenção de prova deve observar a legislação especial aplicável.

2º O acesso a dados pessoais sigilosos controlados por pessoas jurídicas de direito privado será específico a pessoas investigadas e dependerá de ordem judicial prévia baseada em indícios de envolvimento dos titulares de dados afetados em infração penal e na demonstração de necessidade dos dados à investigação, na forma da lei, sem prejuízo da comunicação de operações suspeitas, nos termos do art. 11 da Lei nº 9.613.

Seção IV

Dos Limites e do Término do Tratamento de Dados

Art. 15. 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, devendo descartá-los imediatamente.

Art. 16. O término do tratamento de dados pessoais ocorrerá nas seguintes hipóteses:

I - verificação de que os dados não são ou deixaram de ser necessários ou pertinentes ao alcance da finalidade específica almejada;

II - verificação de que a finalidade foi alcançada;

III - fim do período de tratamento; ou

IV - determinação do Conselho Nacional de Justiça, quando houver violação ao disposto nesta Lei.

Art. 17. Os dados pessoais serão eliminados após o término de seu tratamento, no âmbito e nos limites técnicos das atividades, autorizada a conservação para as seguintes finalidades:

I - cumprimento de obrigação legal ou regulatória pelo controlador; ou

II - estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais.

CAPÍTULO III

DOS DIREITOS DO TITULAR

Art. 18. 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,

limitada no tempo e necessária para finalidades de atividades de segurança pública e de persecução penal.

Art. 19. 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;

III - correção de dados incompletos, inexatos ou desatualizados;

IV - anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei; e

V - informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados.

§ 1º O titular dos dados pessoais tem o direito de peticionar em relação aos seus dados contra o controlador perante o Conselho Nacional de Justiça 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. 20. 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 - proteger a segurança do Estado ou a defesa nacional; ou

IV - proteger os direitos e garantias de terceiros.

§1º Nos casos previstos, o responsável pelo tratamento deve informar o 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 ao Conselho Nacional de Justiça ou de iniciar ação judicial.

§3º O controlador deve disponibilizar ao Conselho Nacional de Justiça 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. 21. O direito à retificação de dados pessoais não alcançará informações baseadas em percepções pessoais colhidas por agentes de autoridades competentes e testemunhas.

Art. 22. A confirmação de existência ou o acesso a dados pessoais serão providenciados, mediante requisição do titular:

I - em formato simplificado, imediatamente; ou

II - por meio de declaração clara e completa, que indique a origem dos dados, a inexistência de registro, os critérios utilizados e a finalidade do tratamento, observados os segredos comercial e industrial, fornecida no prazo de até 15 (quinze) dias, contado da data do requerimento do titular.

§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 O Conselho Nacional de Justiça poderá dispor de forma diferenciada acerca dos prazos previstos nos incisos I e II do caput deste artigo para os setores específicos.

Art. 23. As decisões tomadas com base no tratamento automatizado de dados pessoais, que afetem os interesses do titular, devem ser precedidas de autorização do Conselho Nacional de Justiça e de publicação de relatório de impacto, que comprove a adoção das garantias adequadas para os direitos e liberdades do titular, incluído o direito de solicitar a revisão da decisão por uma pessoa natural e observado o disposto no artigo 25.

§1º O relatório de impacto à proteção de dados pessoais deve ser publicado na página da autoridade competente e enviado ao Conselho Nacional de Justiça, demonstrando as garantias para a proteção dos direitos e liberdades do titular requeridas no caput, que deverão ser adequadas à natureza dos dados tratados.

§2º O Conselho Nacional de Justiça deverá examinar o relatório de impacto e decidir acerca da possibilidade da decisão automatizada com base no tratamento automatizado de dados, à luz das garantias para os direitos e liberdades do titular e dos riscos apresentados.

§3º O titular será notificado da utilização de decisões automatizadas.

§4º As decisões a que se refere o caput deste artigo não podem basear-se em dados sensíveis, com exceção de dados biométricos.

Art. 24. As decisões tomadas com base no tratamento automatizado de dados que ensejem um elevado risco para os direitos fundamentais do titular ou que possam acarretar medidas coercitivas ou restritivas de direitos deverão ser precedidas de autorização do Conselho Nacional de Justiça e autorizadas por lei, que estabeleça as garantias adequadas para os direitos e liberdades do titular, observado o disposto nos artigos 25 e 44.

§ 1º O processo legislativo será instruído de análise de impacto regulatório, que demonstre as garantias para a proteção dos direitos e liberdades do titular e a respectiva mitigação de riscos.

§ 2º O controlador elaborará relatório de impacto de proteção de dados pessoais à luz das circunstâncias concretas do tratamento em questão.

§ 3º O Conselho Nacional de Justiça deverá examinar o relatório de impacto e decidir acerca da possibilidade da decisão automatizada com base no tratamento automatizado de dados, às luz das garantias para os direitos e liberdades do titular frente aos riscos apresentados.

§ 4º O titular será notificado da utilização de decisões automatizadas.

§ 5º As decisões a que se refere o caput deste artigo não podem basear-se em dados sensíveis, com exceção de dados biométricos.

Art. 25. Os sistemas responsáveis por decisões automatizadas a que se referem os artigos 23 e 24 devem ser auditáveis, não discriminatórios e passíveis de comprovação acerca de sua precisão e grau de acurácia.

§ 1º A autoridade competente deverá disponibilizar informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada.

§ 2º O Conselho Nacional de Justiça poderá solicitar a realização de auditoria para verificação do disposto no caput, em especial, da precisão do algoritmo, da relevância dos fatores estatísticos ou da existência de vieses e aspectos discriminatórios no tratamento automatizado de dados pessoais.

§ 3º É garantido ao titular o direito de solicitar a revisão da decisão por uma pessoa natural.

§ 4º É vedada a adoção de qualquer medida coercitiva ou restritiva de direitos exclusivamente com base em decisão automatizada.

Art. 26. O relatório de impacto à proteção de dados que fundamentar decisões automatizadas nos termos desta lei verificará, entre outros, as medidas tomadas para a garantia da não-discriminação e transparência.

§ 1º Os parâmetros para verificação da natureza discriminatória contemplarão o peso de dados pessoais, incluindo aqueles referentes à situação socioeconômica e os dados demográficos relacionados à residência ou os demais, sejam potencialmente capazes de revelar informações sensíveis.

§ 2º Os sistemas responsáveis por decisões automatizadas conforme o caput devem ser auditáveis nos termos a serem determinados pelo Conselho Nacional de Justiça, que não serão restringidos pelo segredo industrial e comercial.

§ 3º Os parâmetros a serem considerados na auditoria prevista no § 2º contemplarão, entre outros:

I - a precisão, incluindo a taxa de falsos positivos ou falsos negativos;

II - a reprodutibilidade e disponibilidade de documentação acerca do seu funcionamento.

Art. 27. O controlador deve assegurar o direito do titular de dados de realizar denúncias confidenciais a respeito de violações a esta Lei.

Art. 28. A defesa dos interesses e dos direitos dos titulares de dados poderá ser exercida em juízo, individual ou coletivamente, na forma do disposto na legislação pertinente, acerca dos instrumentos de tutela individual e coletiva.

CAPÍTULO IV

DOS AGENTES DE TRATAMENTO DE DADOS PESSOAIS

Seção I

Do Controlador e do Operador

Art. 29. É obrigatória a elaboração de relatório de impacto à proteção de dados pessoais para tratamento de dados pessoais sensíveis, sigilosos, ou em operações que apresentem elevado risco aos direitos, liberdades e garantias dos titulares de dados.

§ 1º O Conselho Nacional de Justiça poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, referente a suas operações de tratamento de dados.

§ 2º A elaboração e apresentação de relatório de impacto à proteção de dados pessoais também poderá ser requisitada pelo Ministério Público e pela Defensoria Pública na defesa de direitos individuais ou coletivos, quando cabível no exercício de suas atribuições.

§ 3º Observado o disposto no caput deste artigo, o relatório deverá conter, no mínimo, a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados.

Art. 30. 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. 31. O Conselho Nacional de Justiça poderá dispor sobre padrões de interoperabilidade para fins de portabilidade, livre acesso aos dados e segurança, assim como sobre o tempo de guarda dos registros, tendo em vista especialmente a necessidade e a transparência.

Seção II

Registros das atividades de tratamento

Art. 32. O controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem.

Art. 33. O controlador deve manter registro de todas as categorias de atividades de tratamento sob a sua responsabilidade, o qual conterá:

I – o nome e os contatos de operadores, co-controladores e encarregados;

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 conservação das diferentes categorias de dados pessoais ou os procedimentos previstos para revisão periódica da necessidade de conservação;

IX – uma descrição geral das medidas técnicas e organizativas em matéria de segurança referidas no capítulo V; e

X – os pedidos apresentados pelos titulares dos dados e a respectiva tramitação, bem como as decisões do responsável pelo tratamento com a correspondente fundamentação.

Art. 34. Controladores e operadores devem conservar em sistemas de tratamento automatizado registos cronológicos das seguintes operações de tratamento: de coleta, alteração, consulta, acesso, divulgação, transferências, interconexão, apagamento.

§ 1º Os registos 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 registos cronológicos, cuja integridade e cuja reserva devem ser observadas pelos controladores e operadores, serão mantidos por no mínimo 5 anos e poderão ser utilizados para efeitos de verificação da licitude do tratamento, controle administrativo, exercício do poder disciplinar, garantia da integridade e segurança dos dados pessoais, análise pelo Conselho Nacional de Justiça e instrução de processos penais, inclusive a pedido da defesa.

Seção III

Do Encarregado pelo Tratamento de Dados Pessoais

Art. 35. 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 do Conselho Nacional de Justiça e adotar providências;

III - orientar os servidores e funcionários da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e

IV - executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.

§ 3º O Conselho Nacional de Justiça 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 V

DA SEGURANÇA E DO SIGILO DOS DADOS

Art. 36. Os agentes de tratamento devem adotar medidas de segurança, 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 O Conselho Nacional de Justiça 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 6º 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 As medidas de que trata o caput devem ser adotadas com as seguintes finalidades:

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

II - controle de suporte de dados: impedir que os suportes de dados sejam lidos, copiados, alterados ou retirados sem autorização;

III - controle da conservação: impedir a introdução não autorizada de dados pessoais, bem como qualquer inspeção, alteração ou apagamento não autorizados de dados pessoais conservados;

IV - controle dos utilizadores: impedir que os sistemas de tratamento automatizado sejam utilizados por pessoas não autorizadas por meio de equipamento de comunicação de dados;

V - controle do acesso aos dados: 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 - controle da comunicação: assegurar que possa ser verificado e determinado a organismos os dados pessoais que foram ou podem ser transmitidos ou facultados utilizando equipamento de comunicação de dados;

VII - controle da inserção: assegurar que possa ser verificado e determinado a posteriori quais os dados pessoais introduzidos nos sistemas de tratamento automatizado, quando e por quem;

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

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

X - assegurar que as funções do sistema funcionem, que os erros de funcionamento sejam assinalados (fiabilidade) e que os dados pessoais conservados não possam ser falseados por um mau funcionamento do sistema.

Art. 37. Os sistemas utilizados 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 deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução.

§ 2º Os dados pessoais serão tornados anônimos ou pseudonimizados o quanto antes, de acordo com a finalidade do processamento.

§ 3º O responsável pelo tratamento deve implementar medidas técnicas e organizacionais adequadas para garantir que, por padrão, apenas os dados pessoais necessários para cada finalidade específica do tratamento sejam processados.

Art. 38. O controlador deverá comunicar ao Conselho Nacional de Justiça e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.

§ 1º A comunicação será feita no prazo de 72 (setenta e duas) horas 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 O Conselho Nacional de Justiça 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.

§ 3º No juízo de gravidade do incidente, será avaliada eventual comprovação de que foram adotadas medidas técnicas adequadas que tornem os dados pessoais afetados ininteligíveis, no âmbito e nos limites técnicos de seus serviços, para terceiros não autorizados a acessá-los.

Art. 39. O tratamento de registros criminais deverá atender aos princípios e fundamentos desta lei, em especial a presunção da inocência e a finalidade de integração social do condenado.

§ 1º O Poder Judiciário, o Ministério Público, as Polícias e todos os demais agentes de tratamento que tenham acesso a autos sigilosos deverão adotar as medidas de segurança para garantia do sigilo decretado judicialmente em todas as fases e instâncias processuais.

§ 2º Nos autos de investigação e nos processos relativos a atos infracionais, os elementos identificadores das crianças ou adolescentes envolvidos serão protegidos em todas as fases e instâncias processuais, independentemente da decretação de sigilo do processo.

§ 3º Nos autos de investigação e processo penal que tiverem por objeto crimes contra a dignidade sexual, os elementos identificadores dos ofendidos serão protegidos em todas as fases e instâncias processuais, independentemente da decretação de sigilo do processo.

CAPÍTULO VI

ACESSO À INFORMAÇÃO E TRANSPARÊNCIA

Art. 40. As autoridades competentes informarão as hipóteses em que, no exercício de suas competências, realizam o tratamento de dados pessoais, fornecendo informações claras e atualizadas sobre a base legal, a finalidade, os objetivos específicos, os procedimentos e as práticas utilizadas para a execução dessas atividades.

§ 1º As informações a que se refere este artigo serão pormenorizadas em lei ou regulamento, conforme a base legal, observadas as normas do Capítulo II;

§ 2º O acesso facilitado às informações sobre o tratamento de dados se dará em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos, de forma clara, adequada e

ostensiva, devendo incluir informações previstas em regulamentação para o atendimento do princípio do livre acesso, sobre:

- I - finalidade específica do tratamento;
- II - forma, escopo e duração do tratamento;
- III - políticas de retenção, descarte e acesso;
- IV - identificação do controlador;
- V - informações de contato do controlador;
- VI - informações acerca do uso compartilhado de dados pelo controlador e a finalidade;
- VII - responsabilidades dos agentes que realizarão o tratamento; e
- VIII - direitos do titular, com menção explícita aos direitos contidos nesta Lei.

§ 3º O Conselho Nacional de Justiça poderá dispor sobre as formas de publicidade das operações de tratamento, especialmente tendo em vista a garantia da segurança pública e atividades de repressão, investigação e persecução de infrações penais e execução da pena.

Art. 41. A autoridade máxima de cada autoridade competente publicará anualmente em seu sítio na internet relatórios estatísticos de requisição de dados pessoais sigilosos para atividades de persecução penal, contendo:

- I - o número de pedidos realizados;
- II - a natureza dos dados solicitados;
- III - as categorias de pessoas jurídicas de direito privado aos quais os dados foram requeridos;
- IV - quando o dado for protegido por reserva de jurisdição, o número de pedidos deferidos e o número de pedidos indeferidos judicialmente à luz dos pedidos totais realizados; e
- V - o número de titulares afetados por tais solicitações.

CAPÍTULO VII

TECNOLOGIAS DE MONITORAMENTO E TRATAMENTO DE DADOS DE ELEVADO RISCO

Art. 42. A utilização de tecnologias de monitoramento ou o tratamento de dados pessoais que representem elevado risco para direitos, liberdades e garantias dos titulares dos dados

por autoridades competentes dependerá de previsão legal específica, que estabeleça garantias aos direitos dos titulares e seja precedida de relatório de impacto de vigilância.

§ 1º Para fins de avaliação do risco, deve-se considerar, pelo menos:

I - a natureza dos dados pessoais envolvidos;

II - as finalidades específicas do tratamento;

III - a quantidade de agentes de tratamento de dados envolvidos;

IV - a quantidade de titulares de dados potencialmente atingidos;

V - se é utilizado algum tipo de nova tecnologia;

VI - a possibilidade de tratamento discriminatório; e

VII - as expectativas legítimas do titular de dados.

§ 2º O processo legislativo será instruído de análise de impacto regulatório que contenha:

I - uma descrição do escopo do tratamento e das capacidades da tecnologia de vigilância;

II - quaisquer testes ou relatórios relativos aos efeitos do tratamento e da tecnologia de vigilância na saúde e na segurança de pessoas;

III - quaisquer impactos potencialmente díspares do tratamento de dados e da tecnologia de vigilância ou de sua política de uso em quaisquer populações específicas;

IV - as medidas previstas para fazer frente aos riscos mencionados nos incisos anteriores;

V - as garantias, as medidas de segurança e os mecanismos para assegurar a proteção dos dados pessoais e demonstrar a conformidade do tratamento com a presente lei; e

VI - a política de uso e as garantias dos direitos dos titulares, conforme o disposto no § 3º deste artigo.

§ 3º A lei deve estabelecer política de uso que garanta os direitos dos titulares de dados e contenha:

I - regras, processos e diretrizes emitidas pela autoridade competente que regulem o tratamento de dados, incluindo o acesso e o uso interno de tal tecnologia de vigilância;

II - salvaguardas ou medidas de segurança destinadas a proteger as informações coletadas por tal tecnologia de vigilância contra o acesso não autorizado, incluindo, mas não se limitando à existência de criptografia e mecanismos de controle de acesso;

III - políticas e práticas relacionadas à retenção, acesso e uso dos dados tratados;

IV - políticas e procedimentos relativos ao acesso ou uso dos dados tratados por meio de tal tecnologia de vigilância por membros do público;

V - as hipóteses de uso compartilhado, se admitido;

VI - se algum treinamento é exigido pela autoridade competente para um indivíduo realizar o tratamento, usar tal tecnologia de vigilância ou acessar informações tratadas;

VII - uma descrição da auditoria interna e mecanismos de supervisão dentro da autoridade competente para garantir a conformidade com a política de uso que rege o uso de tal tecnologia de vigilância.

VIII - diretrizes sobre realização, atualização e revisão do relatório de impacto de proteção de dados pessoais.

§ 4º No processo legislativo, a análise de impacto regulatório deverá ser submetida à consulta pública com ampla participação social.

§ 5º Quando admitida por lei, a utilização de tecnologias de monitoramento ou o tratamento de dados pessoais de alto risco por autoridade competente será objeto de relatório de impacto de proteção de dados pessoais, que abrangerá os mesmos quesitos do artigo 42, §2º e §3º.

Art. 43. No âmbito de atividades de segurança pública, é vedada a utilização de tecnologias de vigilância diretamente acrescida de técnicas de identificação de pessoas indeterminadas em tempo real e de forma contínua quando não houver a conexão com a atividade de persecução penal individualizada e autorizada por lei e decisão judicial.

Art. 44. O Conselho Nacional de Justiça emitirá opiniões técnicas ou recomendações referentes à utilização de tecnologias de vigilância ou o tratamento de dados pessoais que representem elevado risco para direitos, liberdades e garantias dos titulares dos dados.

§ 1º O Conselho Nacional de Justiça deverá publicar relatório anual acerca do uso de tecnologias de monitoramento pelas autoridades competentes no território nacional.

§ 2º Em caso de denúncia de uso de tecnologia de monitoramento em descumprimento a esta Lei, o Conselho Nacional de Justiça realizará auditoria para verificação da base legal, da publicação de relatório de impacto e da implementação das medidas e garantias para preservação do direito dos titulares, sem prejuízo de outros mecanismos de controle e supervisão administrativo e judicial.

CAPÍTULO VIII

COMPARTILHAMENTO DE DADOS

Art. 45. Qualquer modalidade de uso compartilhado de dados pessoais entre autoridades competentes somente será possível com autorização legal, com autorização judicial ou no contexto de atuações conjuntas autorizadas legalmente, observados os

propósitos legítimos e específicos para o tratamento, os direitos do titular, bem como os fundamentos, princípios e obrigações previstos nesta Lei.

§ 1º Ressalvadas as hipóteses legais, é vedado o compartilhamento direto e contínuo de bancos de dados que contenham dados pessoais estabelecidos no âmbito de atividades de segurança pública com órgãos responsáveis pela persecução penal, exceto:

I - nos casos em que os dados forem acessíveis publicamente, observadas as disposições desta Lei;

II - para investigação ou processo criminal específico.

§ 2º Requisições de acesso a dados entre autoridades competentes para uso compartilhado ocorrerão de forma devidamente motivada quanto ao contexto específico do pedido, à base legal, finalidade, necessidade e proporcionalidade, devendo o registro de acesso e de uso por agentes de autoridades competentes ser mantido por período de no mínimo 5 anos.

Art. 46. O uso compartilhado de dados pessoais entre uma autoridade competente e um órgão ou entidade da administração pública não competente para os fins desta lei dependerá da demonstração de que o tratamento é compatível com a finalidade original da coleta, observadas as expectativas legítimas de titulares de dados e os objetivos de políticas públicas que ensejaram a coleta original.

Parágrafo único. Nas situações compatíveis, o acesso de agentes de autoridades competentes dependerá de requisição e autorização administrativa devidamente motivada quanto ao contexto específico do pedido, à base legal, à finalidade, necessidade e proporcionalidade, resguardada a reserva de jurisdição para dados pessoais sigilosos, quando exigida por lei ou pela Constituição, e devendo ser mantido o registro de acesso e de uso por período de no mínimo 5 anos.

Art. 47. É vedado a autoridades competentes praticar quaisquer das modalidades de uso compartilhado de dados pessoais com pessoas jurídicas de direito privado, exceto:

I - em casos de execução descentralizada de atividade pública, autorizada em lei, e que exija a transferência, exclusivamente para esse fim específico e determinado, observadas as demais disposições desta Lei;

II - nos casos em que os dados forem acessíveis publicamente, observadas as demais disposições desta Lei e da Lei nº 13.709/18;

III - por aquela que possua capital integralmente constituído pelo poder público e esteja na qualidade de operadora de tratamento de dados.

Art. 48. É vedado a pessoas jurídicas de direito privado praticar modalidades de uso compartilhado de dados com autoridades competentes, exceto nas hipóteses específicas previstas em lei ou mediante cooperação voluntária, desde que observadas as demais disposições dos Capítulos I e II desta Lei e da Lei nº 13.709/18.

Art. 49. Toda e qualquer parceria institucional para uso compartilhado de dados será informada ao público, nos termos e limites do Capítulo VI, e comunicada ao Conselho Nacional de Justiça, que poderá determinar a sua imediata suspensão e posterior adequação, limitação e interrupção se configurada violação a dispositivo desta Lei.

Art. 50. Os registros a que se referem o artigo 45, §2º e o parágrafo único do artigo 46 incluirão a identificação funcional do agente, o endereço IP, a data e o horário do acesso e poderão ser objeto de análise no âmbito de processos administrativos e judiciais, inclusive por titulares de dados pessoais.

Art. 51. O Conselho Nacional de Justiça poderá requisitar, a qualquer momento, às autoridades competentes, informe específico sobre o âmbito e a natureza dos dados e demais detalhes do tratamento realizado e poderá emitir parecer técnico para garantir o cumprimento desta Lei.

Art. 52. O Conselho Nacional de Justiça poderá estabelecer normas complementares para as atividades de que trata o artigo 45.

CAPÍTULO IX

TRANSFERÊNCIA INTERNACIONAL DE DADOS E COOPERAÇÃO INTERNACIONAL

Seção I **Hipóteses**

Art. 53. Sem prejuízo de outras condições exigidas em lei, as autoridades competentes só podem 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 pública ou persecução penal;

II - tiver sido adotada uma decisão de adequação, nos termos do disposto no artigo 54 ou tiverem sido apresentadas garantias adequadas, nos termos do artigo 55, ou forem aplicáveis as interrogações previstas no artigo 56;

III - os dados pessoais forem transferidos para agente responsável no outro país ou na organização internacional competente para fins de atividades de segurança pública ou persecução penal, sem prejuízo do disposto no artigo 57;

IV - no caso de os dados pessoais terem sido transmitidos ou disponibilizados por país estrangeiro, esse país tiver dado o seu consentimento prévio à transferência, sem prejuízo do disposto no inciso II;

V - no caso de uma transferência ulterior para outro país ou para uma organização internacional, a autoridade competente que realizou a transferência inicial ou outra autoridade competente do mesmo país autorizar a transferência ulterior, após análise de 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 os dados pessoais forem posteriormente transferidos; e

VI - a transferência não comprometer o nível de proteção das pessoas assegurado pela presente lei.

§ 1º As transferências sem o consentimento prévio a que alude o inciso IV apenas são permitidas se forem necessárias para prevenir uma ameaça imediata e grave à segurança pública do Brasil ou de um país estrangeiro e o consentimento prévio não puder ser obtido em tempo hábil.

§ 2º No caso previsto no §1º, a autoridade responsável por dar o consentimento deve ser informada em até 48 horas.

Seção II

Transferências com base em decisão de adequação

Art. 54. A transferência de dados pessoais para um país estrangeiro ou para uma organização internacional pode ser efetuada com base em decisão de adequação que determine que aquele país, território ou uma de suas unidades subnacionais, ou a organização internacional destinatária, asseguram nível de proteção adequado.

§ 1º A transferência de dados pessoais com base em decisão de adequação deve observar o artigo 34 da Lei nº 13.709/2018 e dispensa autorização específica, sem prejuízo dos demais requisitos legais.

§ 2º O Conselho Nacional de Justiça poderá estabelecer procedimento simplificado para a tomada de decisão sobre o nível de adequação de um país, quando este for um Estado Parte da Convenção do Conselho da Europa, de 1981 (CETS 108) e de seus protocolos.

§ 3º Os atos do Conselho Nacional de Justiça que revoguem, alterem ou suspendam a decisão de adequação não prejudicam as transferências de dados pessoais para outro país, território ou uma unidade subnacional, ou para organização internacional, quando efetuadas nos termos dos artigos 55 e 56.

Seção III

Transferências sujeitas a garantias adequadas

Art. 55. Na falta de decisão de adequação, 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 um instrumento juridicamente vinculativo; 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 O responsável pelo tratamento informará o Conselho Nacional de Justiça sobre as categorias de transferências abrangidas pelo inciso II.

§ 2º As transferências baseadas no inciso II serão documentadas, devendo o responsável pelo tratamento disponibilizar ao Conselho Nacional de Justiça, a pedido deste, toda a documentação pertinente, incluindo informações sobre a data e a hora da transferência, a autoridade competente que as recebe, a justificativa da transferência e os dados pessoais transferidos.

Seção IV **Derrogações aplicáveis em situações específicas**

Art. 56. Na falta de uma decisão de adequação ou de garantias adequadas nos termos dos artigos anteriores, a transferência ou as categorias de transferências de dados pessoais para país estrangeiro ou para uma organização internacional só podem ser efetuadas se forem necessárias:

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 uma ameaça imediata e grave contra a segurança pública no Brasil ou em país estrangeiro;

IV - em casos específicos, para exercer direitos de defesa no âmbito de processo judicial ou administrativo punitivo, sem prejuízo das demais exigências legais; ou

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

§ 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.

§ 3º O responsável pelo tratamento documentará a informação pertinente referente às transferências realizadas com base no *caput*, devendo disponibilizar a documentação ao Conselho Nacional de Justiça, a pedido deste, incluindo informações sobre a data e a hora da transferência, a autoridade competente que as recebe, a justificativa da transferência e os dados pessoais transferidos.

Seção V

Transferências de dados pessoais para destinatários estabelecidos em outros países

Art. 57. Em derrogação do disposto do inciso III do artigo 53 e sem prejuízo de um acordo internacional tal como definido no §1º deste artigo, 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, pode, em casos específicos, 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 efetuar-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.

§ 1º 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 internacional ou da cooperação policial.

§ 2º A autoridade competente que efetuar a transferência deve informar a autoridade de controle sobre as transferências realizadas na forma deste artigo.

§ 3º As transferências efetuadas nos termos do presente artigo devem ser documentadas pelo responsável pelo tratamento.

Seção VI

Cooperação internacional no domínio da proteção de dados pessoais

Art. 58. Em relação a países estrangeiros e a organizações internacionais, os agentes responsáveis pelo tratamento 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;

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 X

UNIDADE ESPECIAL DE PROTEÇÃO DE DADOS EM MATÉRIA PENAL

Art. 59. O Conselho Nacional de Justiça (CNJ), por meio da sua Unidade Especial de Proteção de Dados em Matéria Penal (UPDP), será responsável por zelar, implementar e fiscalizar a presente lei em todo o território nacional.

Art. 60. A diretoria da Unidade Especial de Proteção de Dados em Matéria Penal (UPDP) será composta por 1 (um) Diretor, 3 (três) coordenações especializadas para a aplicação da lei e assessoria técnica.

§ 1º É assegurada autonomia técnica e decisória à Unidade Especial de Proteção de Dados em Matéria Penal (UPDP).

§ 2º O Diretor será escolhido pelo Conselho Nacional de Justiça dentre brasileiros que tenham reputação ilibada, nível superior de educação e notório saber no campo da proteção de dados ou segurança pública e persecução penal.

§ 3º O mandato do Diretor será de 4 anos e este não poderá perder o cargo, salvo em virtude de renúncia, condenação judicial transitada em julgado ou pena de demissão decorrente de processo administrativo disciplinar.

§ 4º A natureza jurídica da Unidade Especial de Proteção de Dados em Matéria Penal (UPDP) é transitória e deverá ser avaliada após 2 (dois) anos de sua instituição.

Art. 61. A estrutura necessária ao funcionamento da Unidade Especial de Proteção de Dados em Matéria Penal (UPDP) será provida pelo Conselho Nacional de Justiça mediante o remanejamento de servidores e serviços já existentes, nos termos da regulamentação, bem como de dotação orçamentária, se necessária, nos termos da legislação.

Parágrafo único. Ato do Conselho Nacional de Justiça disporá sobre a estrutura e o funcionamento da Unidade Especial de Proteção de Dados em Matéria Penal (UPDP).

Art. 62. Compete à Unidade Especial de Proteção de Dados em Matéria Penal (UPDP):

I - zelar pela proteção dos dados pessoais na segurança pública e 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 pública e persecução penal;

V - promover e elaborar estudos sobre as práticas nacionais e internacionais de proteção de dados pessoais 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 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;

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

XV - elaborar relatórios de gestão anuais acerca de suas atividades.

CAPÍTULO XI

SANÇÕES

Art. 63. 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 - publicização da infração após devidamente apurada e confirmada a sua ocorrência;

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

IV - eliminação dos dados pessoais a que se refere a infração, quando cabível;

V - suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador, quando cabível;

VI - suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, 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.

Art. 64. A fixação da sanção aplicável será feita de maneira fundamentada e considerará:

I - A gravidade da lesão;

II - A culpabilidade do agente;

III - A capacidade econômica do infrator.

§ 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;

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

§ 2º São circunstâncias que atenuam a sanção:

I - A comunicação espontânea da infração ao Conselho Nacional de Justiça 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, o Conselho Nacional de Justiça poderá, em decisão motivada e fundamentada, deixar de aplicar a sanção, ausentes as agravantes do § 1º.

CAPÍTULO XII

DISPOSIÇÕES FINAIS E TRANSITÓRIAS

Art. 65. As autoridades fiscais e aduaneiras, as unidades de inteligência financeira, as autoridades administrativas independentes, as autoridades de supervisão dos mercados financeiros e de valores mobiliários, obrigadas legalmente à comunicação de suspeita de prática de infração penal às autoridades definidas no artigo 1º, submetem-se ao disposto nesta Lei, restringindo-se a transmissão aos dados necessários para o atendimento da finalidade legal específica, sem prejuízo de prévia autorização judicial quando exigida em lei.

Art. 66. O Decreto-Lei n. 2.848, de 7 de dezembro de 1940 (Código Penal), passa a vigorar com as seguintes alterações:

Capítulo V - Dos crimes contra a proteção de dados pessoais (NR)

Transmissão ilegal de dados pessoais (NR)

Art. 154-C. Transmitir, distribuir, usar de forma compartilhada, transferir, comunicar, difundir dados pessoais ou interconectar bancos de dados pessoais sem autorização legal para obter vantagem indevida ou prejudicar o titular dos dados ou a terceiro a ele relacionados: (NR)

Pena - reclusão, de 1 (um) a 4 (quatro), anos e multa. (NR)

Parágrafo único. Aumenta-se a pena de um a dois terços se: (NR)

I - os dados pessoais forem sensíveis ou sigilosos; (NR)

II - o crime for praticado por funcionário público em razão do exercício de suas funções. (NR)

Art. 67. A adequação do tratamento de dados às normas previstas nesta lei deverá ser implementada pelos agentes de tratamento até a sua entrada em vigor, sob pena de ilicitude do tratamento.

Parágrafo único. O Conselho Nacional de Justiça deverá supervisionar o cumprimento do disposto neste artigo, emitindo orientações e estabelecendo normas sobre a adequação progressiva de bancos de dados constituídos até a entrada em vigor desta lei, considerando a complexidade das operações de tratamento, a natureza dos dados e a amplitude do compartilhamento de bancos de dados.

Art. 68. Esta lei entrará em vigor 365 dias após a data de sua publicação.