MINUTA: Anteprojeto de Lei de Proteção de Dados para segurança pública e investigação criminal

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 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 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 segurança pública e 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;

III - dado pessoal sigiloso: dado pessoal constitucionalmente protegido por sigilo, como aquele relativo a operações financeiras, registros e conteúdo de comunicações privadas, geolocalização, atividades e documentos físicos ou digitais em ambientes privados, fontes jornalísticas e segredo estatístico;

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;

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

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

VIII - encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD);

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

X - 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;

XI - 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;

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

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

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

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

XVI - 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;

XVII - 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 - autoridade nacional de proteção de dados: órgão da administração pública responsável por zelar, implementar e fiscalizar a proteção de dados em todo o território nacional;

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 policial e financeira, por autoridades competentes;

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;

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

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: 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 indícios suficientes de que estão prestes a cometer uma infração penal;
III – pessoas processadas pela prática de infração penal;
IV – pessoas condenadas definitivamente por uma 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.

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 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 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. 10º. É vedado o tratamento de dados pessoais para atividades de segurança pública e persecução penal 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, 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 específica, respeitados os princípios desta Lei e as obrigações regulatórias aplicáveis ao setor privado e ressalvadas as possibilidades de cooperação voluntária.

§ 1º. Toda e qualquer requisição administrativa ou judicial indicará o fundamento legal de competência expressa para o acesso e a motivação concreta para o pedido, incluindo sua adequação, necessidade e proporcionalidade, sendo vedados pedidos que sejam genéricos ou inespecíficos.

§2º. A pessoa jurídica de direito privado que não coletar ou já não possuir os dados pessoais solicitados deverá informar tal fato à autoridade solicitante, ficando desobrigada de fornecer tais dados.

§3º. É lícita a adoção de criptografia ponta-a-ponta ou outro recurso tecnológico que torne tecnicamente impossível a produção de dados requisitados pela autoridade competente, salvo nos casos em que sua implementação se destine principalmente a permitir ou facilitar a prática de ilícitos penais, ou para ocultar a identidade de seus autores.

§4º. É vedada a proibição genérica de notificação dos titulares de dados cujos dados pessoais forem fornecidos em razão de requisição administrativa ou judicial sigilosa, devendo a autoridade competente informar prazo mínimo para possibilidade de notificação.

Art. 12. A autoridade nacional 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 a autoridade nacional de proteção de dados.

Seção III

Do Tratamento de Dados Pessoais Sigilosos

Art. 14. O tratamento de dados pessoais sigilosos 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.

Seção IV

Do Tratamento de Registros Criminais

Art. 15. Nos autos de investigação e processo criminal, os dados pessoais de investigados, suspeitos, acusados e condenados sem trânsito em julgado da sentença condenatória terão os seus elementos identificadores protegidos.

§1º. É vedado o acesso automatizado e massificado a quaisquer documentos, como provas colhidas, peças processuais, laudos periciais e documentos análogos dos autos, salvo aos atos decisórios.

§2º. O Poder Judiciário, o Ministério Público e as Polícias deverão adotar as medidas de segurança para a proteção de dados das pessoas naturais envolvidas nos processos judiciais.

§3º. Regulamentação do Conselho Nacional de Justiça disporá sobre as medidas técnicas e administrativas para a implementação do disposto neste artigo.

Seção V
Dos Limites e do Término do Tratamento de Dados

Art. 16. 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. 17. 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;

II - fim do período de tratamento; ou

III - determinação da autoridade nacional, quando houver violação ao disposto nesta Lei.

Art. 18. 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. 19. 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 persecução penal.

Art. 20. 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

VII - 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 a autoridade nacional.

§ 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. 21. 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.

§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 autoridade nacional ou de iniciar ação judicial.

§3º. O controlador deve disponibilizar à autoridade nacional 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. 22. O direito à retificação de dados pessoais não alcançará informações baseadas em percepções pessoais colhidas por agentes de autoridades competentes e testemunhas.

Art. 23. 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, a critério do titular:

I - por meio eletrônico, seguro e idôneo para esse fim; ou

II - sob forma impressa.

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

Art. 24. As decisões tomadas com base no tratamento automatizado de dados pessoais que possam produzir efeitos adversos na esfera jurídica do titular dos dados ou que o afetem de forma significativa, incluídas as decisões destinadas a definir o seu perfil pessoal e o risco de envolvimento em infração penal ou de reincidência, deverão ser autorizadas por lei, que preveja garantias adequadas para os direitos e liberdades do titular, incluído o direito de obter a intervenção humana pelo controlador.

§1º. O processo legislativo será instruído de relatório público de impacto à proteção de dados pessoais, que demonstre as garantias para a proteção dos direitos e liberdades do titular requeridas no caput, que deverão ser adequadas à natureza dos dados tratados.

§2º. Em qualquer caso, é garantido ao titular obter a intervenção humana do responsável pelo tratamento.

§3º. O titular será notificado imediatamente da utilização de decisões automatizadas que tiverem influenciado ou fundamentado medida coercitiva ou restritiva de direitos.

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

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

Art. 25. 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 sensíveis, bem como aqueles referentes à situação sócio-econômica e os dados demográficos relacionados à residência ou os demais capazes de revelar informações sensíveis.

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

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

a) a precisão, incluindo a taxa de falsos positivos ou falsos negativos;

b) a reprodutibilidade e disponibilidade de documentação acerca do seu funcionamento.

Art. 26. O controlador deve assegurar o direito do titular de dados de realizar denúncias confidenciais a respeito de violações a esta Lei.

Art. 27. 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. 28. É obrigatória a elaboração de relatório de impacto à proteção de dados pessoais para tratamento de dados pessoais sensíveis, sigilosos, ou operações que apresentem elevado risco aos direitos, liberdades e garantias dos titulares de dados.

§1º A autoridade nacional poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, referente a suas operações de tratamento de dados.

§ 2º 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. 29. 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. 30. A autoridade nacional 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. Registos das atividades de tratamento

Art. 31. O controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem.

Art. 32. 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;

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

Art. 33. 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 serão mantidos por no mínimo 5 anos e poderão utilizados para efeitos de verificação da licitude do tratamento, controle administrativo, exercício do poder disciplinar, garantia da integridade e segurança dos dados pessoais, análise da autoridade nacional e instrução de processos penais, inclusive a pedido da defesa.

Seção III
Do Encarregado pelo Tratamento de Dados Pessoais

Art. 34. 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 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 A autoridade nacional 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

Seção I
Da Segurança e do Sigilo de Dados

Art. 35. 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. A autoridade nacional 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 art. 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:

a. controle de acesso ao equipamento: impedir o acesso de pessoas não autorizadas ao equipamento utilizado para o tratamento;
b. controle de suporte de dados: impedir que os suportes de dados sejam lidos, copiados, alterados ou retirados sem autorização;
c. controle da conservação: impedir a introdução não autorizada de dados pessoais, bem como qualquer inspeção, alteração ou apagamento não autorizados de dados pessoais conservados;
d. controle dos utilizadores: impedir que os sistemas de tratamento automatizado sejam utilizados por pessoas não autorizadas por meio de equipamento de comunicação de dados;
e. 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;
f. controle da comunicação: assegurar que possa ser verificado e determinado a organismos os dados pessoais foram ou podem ser transmitidos ou facultados utilizando equipamento de comunicação de dados;
g. 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;
h. 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;
i. recuperação: assegurar que os sistemas utilizados possam ser restaurados em caso de interrupção;
j. 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. 36. 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. 37. O controlador deverá comunicar à autoridade nacional 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 A autoridade nacional 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.

CAPÍTULO VI
ACESSO À INFORMAÇÃO E TRANSPARÊNCIA

Art. 38. 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, entre outras 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 no art.20 desta Lei.

§2º. A autoridade nacional 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. 39. 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 - a listagem das pessoas jurídicas de direito privado aos quais os dados foram requeridos;

IV - o número de pedidos deferidos e indeferidos judicialmente; e

V - o número de titulares afetados por tais solicitações.

CAPÍTULO VII
TECNOLOGIAS DE VIGILÂNCIA E TRATAMENTO DE DADOS DE ELEVADO RISCO

Art. 40. A utilização de tecnologias de vigilância 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 proteção de dados pessoais e vigilância.

§1º. O processo legislativo será instruído de relatório público de impacto à proteção de dados pessoais e vigilância 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 grupos protegidos;

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 §2º deste artigo.

§2º. 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.

§3º. No processo legislativo, o relatório de impacto de proteção de dados pessoais e vigilância deverá ser submetido à consulta pública com ampla participação social.

§4º. 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.

Art. 41. A autoridade nacional 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. A autoridade nacional deverá publicar relatório anual acerca do uso de tecnologias de vigilância pelas autoridades competentes no território nacional.

§2º. Em caso de denúncia de uso de tecnologia de vigilância em descumprimento a esta Lei, a autoridade nacional 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. 42. Qualquer modalidade de uso compartilhado de dados pessoais entre autoridades competentes somente será possível nas hipóteses previstas em lei, desde que observados os propósitos legítimos e específicos para o tratamento e a preservação dos direitos do titular, assim como os fundamentos e os princípios previstos nesta Lei.

§ 1º. É vedado o compartilhamento direto e contínuo de bancos de dados estabelecidos no âmbito de atividades de segurança pública com autoridades competentes para fins de persecução penal, as quais somente terão acesso a dados dessa origem para investigação ou processo criminal específico, observadas as demais disposições deste artigo.

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

§ 3º. O uso compartilhado de dados pessoais sigilosos entre autoridades competentes, inclusive no âmbito de uma mesma autoridade competente, dependerá de autorização judicial específica e motivada que ateste a pertinência e cabimento do compartilhamento.

Art. 43. O uso compartilhado de dados pessoais entre uma autoridade competente e outro órgão ou entidade do Poder Público não competente para os fins desta Lei dependerá de autorização legal específica, sendo vedadas hipóteses em que o tratamento posterior seja incompatível com a finalidade original da coleta, em termos de expectativas legítimas de titulares de dados ou de 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 e devendo ser mantido o registro de acesso e de uso por período de no mínimo 5 anos.

Art. 44. 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. 45. 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. 46. Toda e qualquer operação de uso compartilhado de dados será informada ao público, nos termos e limites do Capítulo VI, e comunicada à autoridade nacional, que poderá determinar a sua imediata suspensão e posterior adequação, limitação e interrupção se configurada violação a dispositivo desta Lei.

Art. 47. Os registros a que se referem o artigo 42, §2º e o parágrafo único do artigo 43 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. 48. A autoridade nacional 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. 49. A autoridade nacional poderá estabelecer normas complementares para as atividades de que trata o art. 42.

CAPÍTULO IX
TRANSFERÊNCIA INTERNACIONAL DE DADOS E COOPERAÇÃO INTERNACIONAL

Seção I. Hipóteses

Art. 50. 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 art. 51 ou tiverem sido apresentadas garantias adequadas, nos termos do art. 52, ou forem aplicáveis as derrogações previstas no art. 53;

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 art. 54;

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 ulteriormente 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 numa decisão de adequação

Art. 51. A transferência de dados pessoais para um país estrangeiro ou para uma organização internacional pode ser efetuada com base numa decisão de adequação que determine que aquele país, território ou uma de suas unidades subnacionais, ou a organização internacional destinatária, asseguram um nível de proteção adequado.

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

§2º. A autoridade nacional 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 da autoridade nacional que revoguem, alterem ou suspendam a decisão de adequação não prejudicam as transferências de dados pessoais para outro país, território ou uma sua unidade subnacional, ou para uma organização internacional, quando efetuadas nos termos dos artigos 52 e 53.

Seção III. Transferências sujeitas a garantias adequadas

Art. 52. 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 a autoridade nacional sobre as categorias de transferências abrangidas pelo inciso II.

§ 2º. As transferências baseadas no inciso II serão documentadas, devendo o responsável pelo tratamento disponibilizar à autoridade nacional, a pedido desta, toda a documentação pertinente, incluindo informações sobre a data e a hora da transferência, a autoridade competente que as recebe, a justificação da transferência e os dados pessoais transferidos.

Seção IV. Derrogações aplicáveis em situações específicas

Art. 53. 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 um 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 à autoridade nacional, a pedido desta, incluindo informações sobre a data e a hora da transferência, a autoridade competente que as recebe, a justificação da transferência e os dados pessoais transferidos.

Seção V – Transferências de dados pessoais para destinatários estabelecidos em outros países

Art. 54. Em derrogação do disposto do inciso III do art. 50 e sem prejuízo de um acordo internacional tal como definido no §1º deste artigo, uma 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 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.

§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. 55. 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
AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

Art. 56. A Autoridade Nacional de Proteção de Dados será responsável por implementar a presente lei, nos termos do art. 55- J da Lei 13.709 de 2018, destacando recursos especializados para essa atribuição.

Parágrafo único. Quando houver infração a esta Lei em decorrência do tratamento de dados pessoais, a autoridade nacional poderá enviar informe com medidas cabíveis para fazer cessar a violação.

CAPÍTULO XI
SANÇÕES

Art. 57. 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;

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

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;

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;

§ 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 o 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. 58. 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 à autoridade 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 poderá, em decisão motivada e fundamentada, deixar de aplicar a sanção, ausentes as agravantes do § 1º.

Art. 59. O descumprimento desmotivado de ordem judicial de quebra de sigilo por pessoas jurídicas de direito privado controladoras de dados poderá ser considerado ato atentatório à dignidade da Justiça, nos termos do artigo 77, § 2o, do Código de Processo Civil, sem prejuízo do crime de desobediência, caso a determinação possua previsão legal.

§ 1º. O cálculo da multa deve se dar de maneira fundamentada, observando as balizas do art. 58, e considerará:

I - Eventual cumprimento parcial da ordem;

II - Capacidade do controlador do dados; e

III - Onerosidade ao controlador dos dados.

§ 2º. Nos termos do artigo 11,§3º, a incapacidade técnica decorrente do emprego de mecanismo de proteção de dados, a exemplo da criptografia ponta-a-ponta, torna impossível o cumprimento da ordem judicial, não dispensando o destinatário da ordem da obrigação quanto aos dados disponíveis.

§ 3º. Em casos de questionamento razoável sobre a validade da ordem à luz da legislação regente em matéria de proteção de dados pessoais que for levado a juízo ou à autoridade nacional, o controlador de dados não será punido por atraso no cumprimento.

CAPÍTULO XII
DISPOSIÇÕES FINAIS E TRANSITÓRIAS

Art. 60. O órgão previsto no artigo 14 da Lei n. 9.613, de 3 de março de 1998, é autoridade competente e submete-se ao disposto nesta Lei.

§1º. Os dados pessoais tratados pelas pessoas obrigadas referidas no artigo 9o, *caput* e parágrafo único, da Lei 9.613, de 3 de março de 1998, devem se limitar ao mínimo necessário para o cumprimento do disposto no artigo 11 do mesmo diploma legal, submetendo-se ao disposto na presente Lei.

§2º. Os dados referidos no *caput* não podem ser tratados pelas autoridades competentes de forma incompatível com as finalidades previstas na Lei 9.613, de 3 de março de 1998, e as normas da presente Lei.

§3º. É vedado o tratamento dos dados referidos no *caput* deste artigo para quaisquer outros fins, como os fins comerciais.

Art. 61. As autoridades fiscais e aduaneiras, as unidades de investigação de inteligência financeira, as autoridades administrativas independentes, ou as autoridades dos mercados financeiros, responsáveis pela regulamentação e supervisão dos mercados 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 à transmissão aos dados estritamente necessários para o atendimento da finalidade legal específica, sem prejuízo de prévia autorização judicial quando exigida em lei.

Art. 62. O Decreto-Lei n. 2.848, de 7 de dezembro de 1940 (Código Penal), passa a vigorar com as seguintes alterações:

"**Invasão de dispositivo informático**

Art. 154-A. Acessar indevidamente ou invadir dispositivo informático alheio, conectado ou não à rede de computadores, ou nele instalar vulnerabilidade: (NR)

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

Petrechos para invasão

§ 1º Produzir, oferecer ou difundir dispositivo, programa de computador, técnica ou vulnerabilidade com o intuito de permitir a prática da conduta definida no *caput*: (NR)

Pena – detenção, de 6 (seis) meses a 2 (anos), e multa. (NR)

§ 2º A pena será de reclusão, de 2 (dois) a 5 (cinco) anos, se o fato não constitui crime mais grave, se resultar:

I - na obtenção, modificação ou eliminação de: (NR)

a) dados de comunicações eletrônicas privadas; (NR)

b) segredos profissionais, comerciais ou industriais; (NR)

c) informações sigilosas, assim definidas em lei ou decisão judicial; (NR)

d) dados pessoais sensíveis. (NR)

II - na modificação, alteração ou interrupção do funcionamento de sistema informático ou no impedimento de seu restabelecimento: (NR)

§ 3º Aumenta-se a pena de um a dois terços se: (NR)

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

II – o sistema informático pertencer à Administração Pública, nacional ou estrangeira, ou a organização internacional; (NR)

II – o crime for praticado com o fim de obtenção de vantagem indevida; (NR)

IV - resultar em prejuízo econômico a outrem; (NR)

V - o agente obtiver o controle remoto não autorizado do dispositivo; (NR)

VI - o agente obtiver informações classificadas como reservadas, secretas ou ultrassecretas, conforme a lei; (NR)

VII - houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos; (NR)

III - houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos. (NR)

§4º Considera-se dispositivo informático todo equipamento tecnológico com capacidade computacional, fixo ou móvel. (NR)

Ação Penal

Art. 154-B. Nos crimes definidos no art. 154-A, somente se procede mediante representação, salvo se o crime é cometido contra a administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviços públicos. (NR)

Parágrafo único. Se o crime é cometido contra organização internacional ou entidades estatais ou representações diplomáticas de país estrangeiro, somente se procede mediante requisição do Ministro da Justiça. (NR)

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: (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 – praticado por funcionário público em razão do exercício de suas funções; (NR)

III – praticado com o fim de obtenção de vantagem indevida; (NR)

IV – a conduta causar dano ao titular dos dados ou a terceiros a ele relacionados. (NR)

.....

Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública

Art. 266 - Interromper ou perturbar serviço telegráfico, radiotelegráfico ou telefônico, impedir ou dificultar-lhe o restabelecimento:

Pena - detenção, de um a três anos, e multa.

Parágrafo único. Aplicam-se as penas em dobro se o crime é cometido por ocasião de calamidade pública. (NR)

.....

Inserção de dados falsos em sistema informático (NR)

Art. 313-A. Inserir ou facilitar a inserção de dados falsos, alterar ou excluir indevidamente dados corretos no sistema informático ou em bancos de dados da Administração Pública com o fim de obter vantagem indevida para si ou para outrem ou para causar dano: (NR)

Pena – reclusão, de 3 (três) a 8 (oito) anos, e multa. (NR)

Modificação ou alteração não autorizada de sistema informático (NR)

Art. 313-B. Modificar ou alterar o funcionamento de sistema informático sem autorização ou solicitação de autoridade competente: (NR)

Pena – detenção, de 3 (três) meses a 2 (dois) anos, e multa.

Parágrafo único. As penas são aumentadas de um terço até a metade se da modificação ou alteração resulta prejuízo para a Administração Pública ou para o administrado. (NR)

.....

Desobediência

Art. 330……..

Pena - reclusão, de 1 (um) a 3 (três) anos, e multa.” (NR)

Art. 63. O artigo 1º, parágrafo único, da Lei 8.137, de 27 de dezembro de 1990, passa a vigorar com a seguinte redação:

“Art. 1º.....

.....

Parágrafo único. A falta de atendimento da exigência da autoridade, no prazo de 10 (dez) dias, que poderá ser convertido em horas em razão da maior ou menor complexidade da matéria ou da dificuldade quanto ao atendimento da exigência, sujeitará o autor à pena de reclusão, de 1 (um) a 3 (anos), e multa.” (NR)

Art. 64. O disposto no artigo 69 da Lei n. 9.605, de 12 de fevereiro de 1998, passa a vigorar com a seguinte redação:

“Art. 69.....

Pena – reclusão, de um a três anos, e multa” (NR)

Art. 65. A adequação do tratamento de dados às normas previstas nesta lei deverá ser implementada pelos agentes de tratamento até a sua entrada em vigor.

§ 1º. O não atendimento ao disposto no *caput* dentro prazo de dois anos implicará na ilicitude do tratamento e os dados deverão serem eliminados.

§2 º. A autoridade nacional 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, a amplitude do compartilhamento de bancos de dados.

Art. 67. Esta lei entrará em vigor 18 (dezoito) meses após a data de sua publicação.