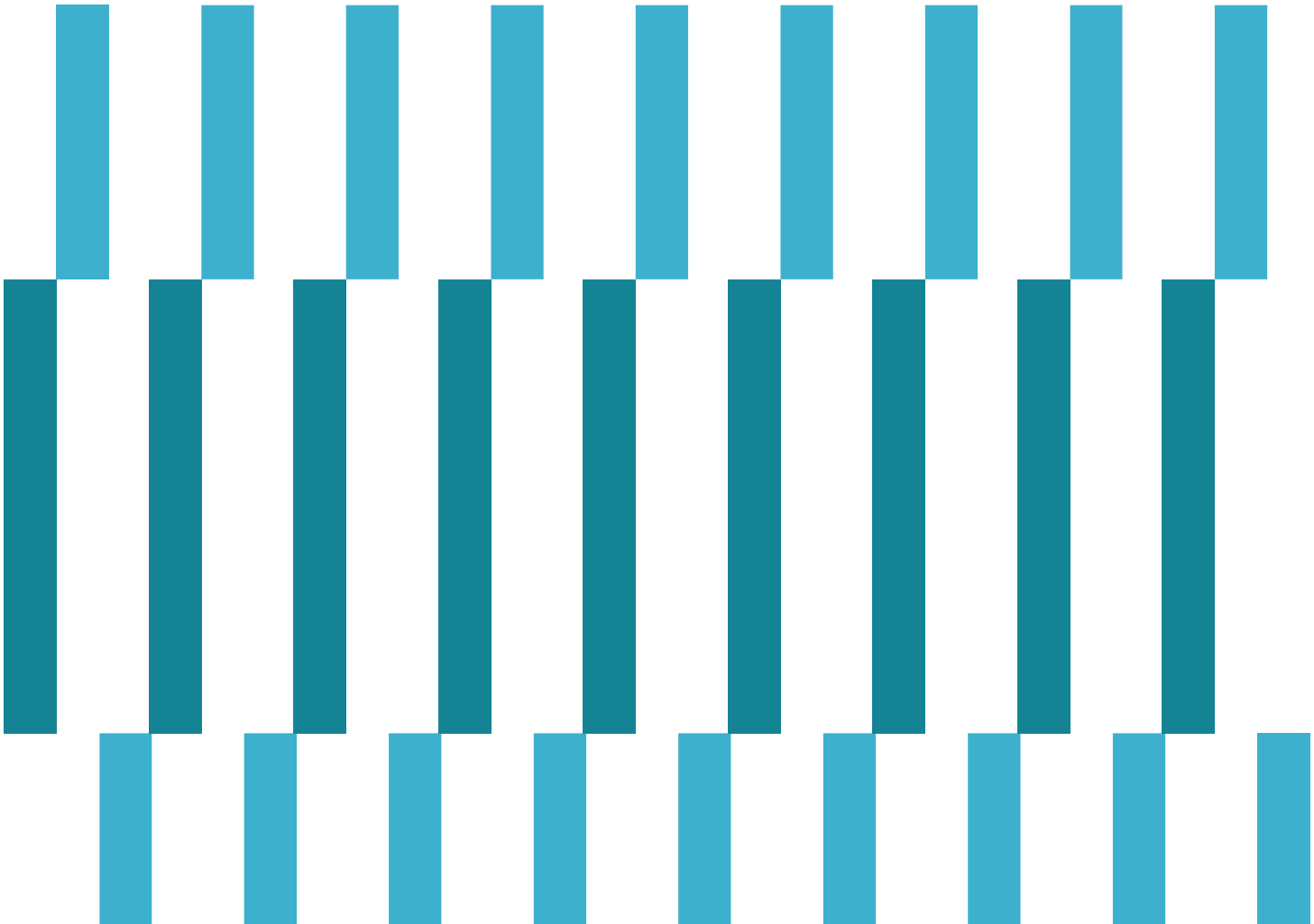
RED IBEROAMERICANA DE PROTECCION DE DATOS

Red Iberoamericana
Rede Ibero-Americana

Normas de Proteção de Dados dos Estados Ibero-americanos





Aprovadas a 26 de maio de 2026
em Cartagena das Índias, Colômbia.

Antecedentes

No âmbito do XV Encontro Ibero-americano de Proteção de Dados, a Rede Ibero-americana de Proteção de Dados (RIPD ou Rede) aprovou e apresentou oficialmente as denominadas «Normas de Proteção de Dados dos Estados Ibero-americanos», dando assim cumprimento a um objetivo há muito aguardado por todas as entidades que integram esta rede, bem como à decisão aprovada na XXV Cimeira Ibero-americana de Chefes de Estado e de Governo, que decorreu nos dias 28 e 29 de outubro de 2016, na Colômbia, de solicitar à Rede a elaboração de uma proposta de cooperação efetiva no domínio da proteção de dados pessoais e da privacidade.

O texto aprovado procurava dar resposta a um dos eixos da estratégia acordada pela RIPD em novembro de 2016, em Montevideu, exposta no documento «RIPD 2020», que consistia em «impulsionar e contribuir para o reforço e adaptação dos procedimentos regulatórios na região, mediante a elaboração de diretrizes que sirvam como referência para futuras regulamentações ou para a revisão das já existentes».

Neste sentido, as Normas Ibero-americanas forma um conjunto de diretrizes orientadoras, com o fim de contribuir para a elaboração de iniciativas regulatórias sobre a proteção de dados pessoais na região ibero-americana, mais concretamente no caso daqueles países que ainda não dispõem deste tipo de regulamentação, ou, se for o caso, de servir como referência para a modernização e atualização da legislação existente.

Entre os objetivos das Normas Ibero-americanas, podemos destacar os seguintes:

@ Estabelecer um conjunto de princípios e direitos comuns em matéria de proteção de dados pessoais que os Estados ibero-americanos possam adotar e desenvolver na sua legislação nacional, com o objetivo de dispor de um conjunto de regras homogéneas para a região.

@ Garantir o exercício efetivo e a tutela do direito à proteção de dados pessoais de qualquer pessoa singular nos Estados ibero-americanos, através do estabelecimento de regras comuns que assegurem o tratamento adequado dos seus dados pessoais.

@ Facilitar o fluxo de dados pessoais entre os Estados ibero-americanos e para além das suas fronteiras, com o objetivo de contribuir para o crescimento económico e social da região.

@ Promover a cooperação internacional entre as autoridades de controlo dos Estados ibero-americanos e outras autoridades de controlo não pertencentes à região, bem como com autoridades e organismos internacionais sobre esta matéria.

Como antecedentes diretos destas Normas, podem citar-se, por um lado, a adoção pela própria RIPD, em 2007, por ocasião do V Encontro Ibero-americano sobre Proteção de Dados, das «Diretrizes para a Harmonização da Proteção de Dados na Comunidade Ibero-americana», com a finalidade de estabelecer um «quadro harmonizado» de referência para as iniciativas regulatórias nacionais que surgissem na região em matéria de proteção de dados e, por outro lado, as normas aprovadas na

Conferência Internacional das Autoridades sobre Privacidade e Proteção de Dados, realizada em Madrid em 2009, conhecidas como as «Normas de Madrid», que constituíram, sem dúvida, um avanço na procura de soluções e disposições específicas «que pudessem ser aplicadas independentemente das diferenças que possam existir entre os diferentes modelos vigentes de proteção de dados e da privacidade».

Na elaboração das Normas Ibero-americanas, foram também tomados como referência outros relevantes instrumentos internacionais em matéria de proteção de dados pessoais, incluindo as Orientações relativas à proteção da privacidade e à circulação transfronteiriça de dados pessoais da Organização para a Cooperação e Desenvolvimento Económico; a Convenção n.º 108 do Conselho da Europa para a proteção das pessoas no que diz respeito ao tratamento automatizado de dados de caráter pessoal e o seu Protocolo; o Quadro de Privacidade do Fórum de Cooperação Económica Ásia-Pacífico; e o Regulamento do Parlamento Europeu e do Conselho sobre a proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, entre outros.

Com a aprovação destas Normas, a RIPD passou a dispor de uma ferramenta essencial, que lhe permite abordar com rigor o acompanhamento e o apoio aos futuros desenvolvimentos legislativos na Região, uma vez que as Normas Ibero-americanas se caracterizam por serem um modelo normativo que:

@ Responde às necessidades e exigências nacionais e internacionais decorrentes do direito à proteção dos dados pessoais, numa sociedade em que as tecnologias da informação e do conhecimento assumem uma importância cada vez maior em todas as atividades da vida quotidiana.

@ Incorpora as melhores práticas nacionais e internacionais nesta matéria.

@ Propõe uma série de normas flexíveis para facilitar a sua adoção pelos Estados ibero-americanos, sem infringir de nenhum modo o direito interno de cada estado, convertendo assim este documento numa realidade viva e viável para a região ibero-americana, em benefício do próprio titular.

@ Garante um nível adequado de proteção dos dados pessoais na região ibero-americana, com o objetivo de não obstaculizar a livre circulação de dados nos Estados Ibero-americanos e, consequentemente, promover as atividades comerciais na região e com outras regiões económicas

Os Estados ibero-americanos:

(1) Considerando que a proteção das pessoas singulares no que diz respeito ao tratamento dos seus dados pessoais constitui um direito fundamental reconhecido com o máximo estatuto na maioria das Constituições Políticas dos Estados ibero-americanos, sob a forma do direito à proteção dos dados pessoais ou *habeas data*, e que, em alguns casos, se encontra definido pela jurisprudência dos seus tribunais ou tribunais constitucionais;

(2) Constatando que o direito à proteção dos dados pessoais se encontra definida, em alguns países ibero-americanos, tanto a nível legislativo como jurisprudencial, como um direito de natureza diferente do direito à vida privada e familiar, à intimidade, à honra, ao bom nome e outros direitos semelhantes, que, no seu conjunto, garantem o livre desenvolvimento da personalidade da pessoa singular, consolidando-se consequentemente como um direito autónomo, com características e dinâmica próprias, que tem como finalidade salvaguardar o poder de disposição e controlo que toda a pessoa singular detém relativamente à informação que lhe diz respeito, fundamentalmente tendo em conta a utilização das tecnologias da informação e das comunicações, que assumem uma relevância cada vez maior em todas as atividades da vida quotidiana;

(3) Considerando que a salvaguarda do direito das pessoas singulares no que diz respeito ao tratamento dos seus dados pessoais é compatível com o objetivo de garantir e proteger outros direitos, os quais são reconhecidos como indivisíveis e interdependentes entre si, e que exigem uma proteção adequada para salvaguardar, na sua esfera mais ampla, as pessoas singulares contra intrusões ilegais ou arbitrárias, incluindo as decorrentes do tratamento dos dados pessoais.

(4) Lembrando que a Rede Ibero-americana de Proteção de Dados surgiu na sequência do acordo alcançado no Encontro Ibero-americano de Proteção de Dados, que teve lugar em La Antigua, na Guatemala, de 1 a 6 de junho de 2003, com a participação de representantes de 14 países ibero-americanos, iniciativa que contou, desde o seu início, com o apoio político refletido na Declaração Final da XIII Cimeira de Chefes de Estado e de Governo dos países ibero-americanos, que teve lugar em Santa Cruz de la Sierra, na Bolívia, nos dias 14 e 15 de novembro de 2003, e conscientes de que a proteção dos dados pessoais constitui um direito fundamental;

(5) Tendo em conta que, com motivo da Resolução adotada na XXV Cimeira Ibero-americana de Chefes de Estado e de Governo, que teve lugar em Cartagena das Índias, na Colômbia, nos dias 28 e 29 de outubro de 2016, foi reafirmado que a adoção, elaboração e promoção de diversos manuais, programas, iniciativas e projetos reforçariam a gestão e o impacto das ações de cooperação entre os países da Ibero-América;

(6) Partindo do princípio de que a Rede Ibero-americana de Proteção de Dados constitui um fórum permanente de intercâmbio de informação, aberto a todos os países membros da Comunidade Ibero-americana, que permite o envolvimento dos setores público, privado e social com o objetivo de promover os desenvolvimentos normativos necessários para garantir uma regulamentação avançada do direito à proteção dos dados pessoais num contexto democrático e global;

(7) Lembrando que, por ocasião da reunião ocorrida em Santa Cruz de la Sierra, na Bolívia, de 3 a 5 de maio de 2006, foi elaborado o documento intitulado «Orientações para a Harmonização da Proteção de Dados na Comunidade Ibero-americana», o qual estabelece um conjunto de disposições que têm como objetivo contribuir para a elaboração das iniciativas regulamentares em matéria de proteção de dados que surjam na Comunidade Ibero-americana, constituindo-se como uma referência para o desenvolvimento das normas;

(8) Tendo em conta que a União Europeia adotou, na altura, um novo quadro normativo nesta matéria, com o objetivo de modernizar as suas disposições e garantir maior solidez e coerência na proteção efetiva do direito fundamental à proteção de dados pessoais e de facilitar o desenvolvimento da economia digital, tanto no seu mercado interno como nas suas relações globais, quadro normativo que se posiciona como uma referência obrigatória e determinante para a elaboração das legislações nacionais de proteção de dados na Ibero-América;

(9) Reconhecendo a ausência de harmonização nos Estados ibero-americanos no que diz respeito ao reconhecimento, adoção, definição e desenvolvimento das figuras jurídicas, princípios, direitos e procedimentos que dão conteúdo ao direito à proteção dos dados pessoais nas suas legislações nacionais, o que, sem dúvida, dificulta atualmente a resposta aos novos desafios e dificuldades para a proteção deste direito, decorrentes da constante e vertiginosa evolução tecnológica e da globalização em diversos domínios;

(10) Conscientes da urgência, no contexto de uma inovação tecnológica constante, da adoção de instrumentos regulamentares que garantam, por um lado, a proteção das pessoas singulares no que diz respeito ao tratamento dos seus dados pessoais e, por outro, o livre fluxo de dados pessoais, que constituem atualmente a base para o desenvolvimento, o fortalecimento e o intercâmbio de bens e serviços numa economia global e digital, sobre a qual assentam as economias dos Estados ibero-americanos, mediante a inclusão de mecanismos eficazes de governação do tratamento, rastreabilidade e supervisão de sistemas automatizados e de inteligência artificial, orientados para garantir a proteção dos direitos e liberdades fundamentais.

Tendo também em consideração as «Orientações Específicas para o Cumprimento dos Princípios e Direitos que Regem a Proteção dos Dados Pessoais em Projetos de Inteligência Artificial» e as «Recomendações Gerais para o Tratamento de Dados em Inteligência Artificial», aprovadas pela Rede Ibero-americana de Proteção de Dados em 21 de junho de 2019, em Naucalpan de Juárez, no México.

(11) Considerando que, para garantir um elevado nível de proteção dos direitos e liberdades das pessoas singulares, entre outras questões, é necessário, por sua vez, um nível uniforme e elevado de proteção das pessoas singulares no que diz respeito aos seus dados pessoais, que responda às necessidades e exigências atuais num contexto global, com o objetivo de não criar barreiras à livre circulação de dados pessoais nos Estados ibero-americanos e, consequentemente, favorecer as atividades comerciais na região e com outras regiões económicas;

(12) Reconhecendo que, com o objetivo de alargar e reforçar o regime de proteção das pessoas singulares no que diz respeito ao tratamento dos seus dados pessoais, é imperativo estabelecer um equilíbrio entre os interesses de todos os intervenientes dos setores público, privado e social e dos titulares envolvidos, incluindo o estabelecimento de exceções por razões de interesse público que sejam razoáveis e compatíveis com os direitos e liberdades, com o fim de evitar quaisquer restrições ou limitações injustificadas ou desproporcionadas, que não estejam em conformidade com os objetivos perseguidos nas sociedades democráticas;

(13) Conscientes dos riscos potenciais que podem decorrer, no caso das pessoas singulares, do tratamento em grande escala dos seus dados pessoais por parte de organismos públicos e privados e, em particular, tendo em conta a especial vulnerabilidade das crianças e dos adolescentes, que exigem garantias adequadas e suficientes de proteção contra a utilização indevida ou arbitrária dos seus dados pessoais, preservando assim o seu interesse superior, o livre desenvolvimento da sua personalidade, a sua segurança e outros valores que são objeto de máxima proteção por parte dos Estados ibero-americanos, riscos que podem ver-se amplificados através de tratamentos automatizados, incluindo aqueles realizados por meio de sistemas de inteligência capazes de inferir, classificar, estabelecer perfis ou influenciar significativamente as pessoas.

(14) Reconhecendo que o desenvolvimento tecnológico facilita o tratamento de novas categorias de dados pessoais que apresentam riscos específicos, em particular a utilização inadequada dos mesmos, pelo que se reveste de grande importância alcançar um consenso mínimo relativamente às categorias de dados pessoais consideradas sensíveis ou especialmente protegidas, bem como às regras para o seu tratamento, tendo em conta que as consequências e interferências negativas que podem decorrer da utilização indevida deste tipo de dados pessoais podem gerar condições injustas ou discriminatórias para as pessoas singulares;

(15) Admitindo que nem todos os Estados ibero-americanos dispõem de legislação nesta matéria, situação que pode comprometer a proteção e o tratamento dos dados pessoais, tendo em conta a utilização acelerada das tecnologias da informação que facilitam e permitem a comunicação em massa de dados pessoais de forma imediata e quase ilimitada;

(16) Estabelecendo que as legislações em matéria de proteção de dados pessoais dos Estados ibero-americanos devem adotar as referências contidas nas presentes Normas, com o fim de dispor de um quadro regulamentar harmonizado que ofereça um nível de proteção às pessoas singulares no que diz respeito ao tratamento dos seus dados pessoais e, ao mesmo tempo, garanta o desenvolvimento comercial e económico da região;

(17) Salientando a necessidade de que, nos Estados ibero-americanos, o tratamento dos dados pessoais se leve a cabo seguindo as mesmas normas e regras homogéneas, oferecendo aos titulares as mesmas garantias de proteção, mediante o estabelecimento de um catálogo de princípios de cumprimento obrigatório que responda às atuais normas nacionais e internacionais sobre esta matéria, bem como aos requisitos necessários para o exercício e o respeito efetivos deste direito fundamental;

(18) Reconhecendo que, com o fim de garantir de forma efetiva o direito à proteção dos dados pessoais, é necessário adotar um quadro regulamentar que reconheça a qualquer pessoa singular, na sua qualidade de titular dos seus dados pessoais, a possibilidade de exercer, como regra geral de forma gratuita e, excecionalmente, com custos associados por razões naturais de reprodução, envio, certificação ou outras, os direitos de acesso, retificação, cancelamento, oposição e portabilidade, inclusive no contexto do tratamento dos dados pessoais efetuado por motores de busca ou motores de pesquisa na Internet; direitos que complementam as condições necessárias

para que os titulares exerçam plenamente o seu direito à autodeterminação informativa;

(19) Salientando a importância e o papel fundamental desempenhado pelos prestadores de serviços que levam a cabo o tratamento de dados pessoais em nome e por conta do responsável pelo tratamento, incluindo aqueles que prestam serviços de computação na nuvem e noutras áreas, o que leva os Estados ibero-americanos a adotar, num mundo globalizado, um regime que lhes permita regulamentar este tipo de serviços com o objetivo de estabelecer uma série de garantias para a proteção dos dados pessoais que, por força da sua missão, recolhem e tratam, sem isentar o responsável das suas obrigações e responsabilidades perante os titulares dos dados e as autoridades de controlo;

(20) Considerando que o desenvolvimento das novas tecnologias da informação e das comunicações, bem como os serviços desenvolvidos no contexto da economia digital, estão a contribuir para o crescimento contínuo dos fluxos transfronteiriços de dados pessoais no âmbito de uma sociedade global, é imprescindível estabelecer uma base mínima que facilite e permita aos responsáveis e aos subcontratantes, na sua qualidade de exportadores, a realização de transferências internacionais de dados pessoais, garantindo o pleno respeito pelos direitos dos titulares;

(21) Tendo em conta que, através da Internet, é possível aceder e recolher informação disponível em qualquer país, bem como proceder ao seu tratamento, nomeadamente recolher dados de milhões de pessoas sem estar fisicamente domiciliado nesse país, circunstância que não deve constituir um fator que impeça a proteção efetiva dos direitos e liberdades das pessoas no ciberespaço;

(22) Reconhecendo a importância da adoção de medidas preventivas que permitam ao responsável responder de forma proativa a possíveis problemas relacionados com o direito à proteção dos dados pessoais, como a adoção de regimes de autorregulação vinculativos ou de sistemas de certificação nesta matéria, a nomeação de um responsável pela proteção de dados pessoais, a elaboração de avaliações de impacto na proteção de dados pessoais e na privacidade por design e pela conceção, entre outras, o que se revela essencial no domínio das tecnologias da informação e das telecomunicações, e ainda a governação algorítmica, a rastreabilidade, a supervisão humana efetiva, a avaliação contínua de riscos, a documentação técnica e a auditoria periódica de sistemas automatizados e de inteligência artificial.

(23) Reconhecendo a necessidade imperiosa de que cada Estado ibero-americano disponha de uma autoridade de controlo independente e imparcial nas suas competências, cujas decisões só possam ser objeto de recurso judicial, isenta de qualquer influência externa, com poderes de supervisão e investigação em matéria de proteção de dados pessoais e encarregada de zelar pelo cumprimento da legislação nacional sobre esta matéria, e dotada dos recursos humanos e materiais suficientes para garantir o exercício dos seus poderes e o desempenho efetivo das suas funções;

(24) Reconhecendo que os Estados ibero-americanos estão obrigados a adotar um regime que garanta aos titulares um conjunto de mecanismos e procedimentos para

apresentarem as suas reclamações perante a autoridade de controlo quando considerem que o seu direito à proteção dos dados pessoais foi violado, bem como para serem indemnizados caso tenham sofrido danos e prejuízos em consequência de uma violação desse direito;

(25) Salientando a importância de estabelecer uma base mínima para a cooperação internacional entre as autoridades de controlo latino-americanas e entre estas e as de países terceiros, com o objetivo de favorecer e facilitar a aplicação da legislação sobre esta matéria e a proteção efetiva dos titulares;

Acordaram em adotar as presentes Normas como máxima prioridade na Comunidade Ibero-americana, para que, com o carácter de diretrizes orientadoras, possam contribuir para a adoção de iniciativas regulamentares em matéria de proteção dos dados pessoais na região, nos países que ainda não dispõem de dita legislação, ou, no seu caso, que possam servir como referência para a modernização e atualização da legislação existente, promovendo a adoção de um quadro regulamentar harmonizado, que ofereça um nível adequado de proteção às pessoas singulares no que diz respeito ao tratamento dos seus dados pessoais e garantindo, por sua vez, o desenvolvimento comercial e económico da região.

Capítulo I
Disposições gerais

1. Objeto

1.1 As presentes Normas têm por objeto:

a. Estabelecer um conjunto de parâmetros normativos relativos ao direito à proteção de dados pessoais, que possam servir de orientação aos legisladores, aos responsáveis pela elaboração de políticas públicas e, em geral, aos responsáveis decisores dos Estados ibero-americanos para a conceção, desenvolvimento e modernização da legislação, regulamentos e, em geral, de qualquer regulamentação sobre esta matéria.

b. Contribuir para o fomento da interoperabilidade da regulamentação no domínio da proteção dos dados pessoais, com o fim de promover o desenvolvimento de quadros normativos que facilitem a cooperação entre as autoridades de proteção de dados pessoais e, em especial, o reforço da proteção dos direitos e liberdades fundamentais dos seus titulares na Ibero-América.

c. Promover o exercício efetivo e a tutela do direito à proteção dos dados pessoais de qualquer pessoa singular, nos Estados Ibero-americanos, através do desenvolvimento de diretrizes, critérios e parâmetros comuns que contribuam para o reforço deste direito, tanto a nível nacional como na região ibero-americana.

d. Estabelecer as bases comuns em matéria de transferência internacional de dados, para facilitar o fluxo de dados pessoais entre os Estados ibero-americanos e para além das suas fronteiras, com o objetivo de contribuir para o desenvolvimento social e o crescimento económico da região.

e. Impulsar o desenvolvimento de mecanismos para a cooperação internacional entre as autoridades de controlo dos Estados ibero-americanos, as autoridades de controlo não pertencentes à região e as autoridades e entidades internacionais neste âmbito de atuação.

f. Impulsar e promover o reconhecimento e a aplicação efetiva da autodeterminação informativa, como condição indispensável para o livre desenvolvimento da personalidade, com o objetivo de permitir que cada pessoa possa decidir livremente sobre a forma como se vê a si própria e como deseja apresentar-se aos outros, entre outros aspetos.

1.2. Perspetiva sobre direitos humanos e de género

a. A aplicação e interpretação da legislação relativa à proteção dos dados pessoais devem orientar-se de acordo com uma perspetiva transversal de género e de direitos humanos, procurando mitigar, na medida do possível, qualquer impacto negativo na esfera dos direitos das pessoas, em particular das que enfrentam situações de vulnerabilidade.

1.3. Inter-relação entre a regulamentação e o ecossistema digital

Com o objetivo de promover a existência de quadros regulamentares equilibrados e eficazes, procurar-se-á ter em conta os seguintes parâmetros:

a. A coerência normativa, evitando a duplicação entre regulamentações e a inconsistência conceptual, no que diz respeito a conteúdos transversais, em especial no referente às normas do ecossistema digital.

b. O impacto da regulamentação no que diz respeito à prevenção de uma carga administrativa desproporcionada e de eficácia limitada.

c. A promoção de mecanismos de governação digital e algorítmica que permitam garantir a rastreabilidade, a supervisão, a auditabilidade e o controlo dos tratamentos automatizados, dos sistemas de inteligência artificial e de outras tecnologias emergentes ou disruptivas.

2. Definições

2.1 As presentes Normas recomendam a definição e a determinação do alcance das seguintes definições:

a. Anonimização: procedimento através do qual se procede ao tratamento dos dados pessoais com o objetivo de impedir a identificação ou reidentificação do seu titular. Trata-se de um procedimento irreversível, devido à impossibilidade de reidentificar razoavelmente o titular dos dados pessoais.

b. Autoridade de proteção de dados pessoais: instituição pública do Estado, de carácter administrativo, dotada de plena autonomia e independência para exercer adequadamente as suas funções de supervisão do cumprimento da regulamentação e de garante do exercício efetivo dos direitos e liberdades fundamentais dos titulares.

c. Consentimento: manifestação da vontade, livre, específica, inequívoca e informada do titular, mediante o qual este aceita e autoriza o tratamento dos dados pessoais que lhe dizem respeito.

d. Dados Pessoais: qualquer informação relativa a uma pessoa singular identificada ou identificável, expressa de forma numérica, alfabética, gráfica, fotográfica, alfanumérica, acústica ou de qualquer outro tipo. Considera-se que uma pessoa é identificável quando a sua identidade pode ser determinada direta ou indiretamente, sempre e quanto dito procedimento não requeira prazos ou atividades desproporcionadas.

e. Dados biométricos: dados obtidos a partir de um tratamento técnico específico relativo às características físicas, fisiológicas ou comportamentais de uma pessoa singular, que permitam identificá-la ou verificar a sua identidade de forma única.

f. Dados genéticos: dados pessoais relativos às características genéticas, herdadas ou adquiridas, de uma pessoa física ou natural, que forneçam informação única sobre a fisiologia ou a saúde dessa pessoa, especificamente obtidos a partir da análise de uma amostra biológica dessa pessoa.

g. Dados de saúde: dados pessoais relativos à saúde física ou mental de uma pessoa singular, incluindo a informação sobre a prestação de serviços de cuidados de saúde, sempre que dita informação revele dados sobre o estado de saúde do seu titular.

h. Dados pessoais sensíveis ou categorias especiais de dados: aqueles que se referem à esfera íntima do seu titular, ou cuja utilização indevida possa dar origem a discriminação ou acarretar um risco grave para o mesmo. A título exemplificativo, consideram-se sensíveis os dados pessoais que possam revelar aspetos como a origem das pessoas, crenças ou convicções religiosas, filosóficas e morais, filiação sindical, opiniões políticas, dados relativos à saúde, dados biométricos, neurodados, informação neuronal da qual se possa inferir informação pessoal, sensível ou sobre estados emocionais, preferência ou orientação sexual, dados genéticos ou dados biométricos destinados a identificar de forma unívoca uma pessoa singular.

i. Elaboração de perfis: tratamento automatizado de dados pessoais para avaliar determinados aspetos pessoais de uma pessoa singular, nomeadamente para analisar ou prever aspetos relativos ao desempenho profissional, situação económica, saúde, preferências pessoais, interesses, fiabilidade, comportamento, localização ou deslocações dessa pessoa.

j. Encarregado: prestador de serviços, na qualidade de pessoa singular ou coletiva ou autoridade pública, alheio à organização do responsável pelo tratamento, que realiza o tratamento dos dados pessoais em nome e por conta deste.

k. Exportador: pessoa singular ou coletiva de carácter privado, autoridade pública, serviço, organismo ou prestador de serviços situado no território de um Estado, que efetue transferências internacionais de dados pessoais, em conformidade com o disposto nas presentes Normas.

l. Investigação científica: qualquer investigação que possa apoiar a inovação, o desenvolvimento tecnológico e a demonstração. Estas ações devem contribuir para o conhecimento científico existente ou aplicar o conhecimento existente de formas inovadoras, realizar-se com o objetivo de contribuir para o crescimento do conhecimento geral e para o bem-estar da sociedade e respeitar as normas éticas da área de investigação em questão. Isto não exclui que a investigação possa também ter um interesse comercial.

m. Limitação do tratamento: identificação dos dados pessoais a conservar, com o objetivo de limitar o seu subsequente tratamento, até que essa medida seja retirada ou deixe de produzir efeitos.

n. Neurodados: dados relacionados com o funcionamento, a atividade ou a estrutura do cérebro humano de uma pessoa física ou natural viva, que incluem informação única sobre a sua fisiologia, saúde ou estados mentais que permita a sua identificação ou torne identificável o seu titular.

ñ. Responsável: pessoa singular ou coletiva de direito privado, autoridade pública, serviço ou organismo que, sozinho ou em conjunto com outros, determina as finalidades, os meios, o âmbito e outras questões relacionadas com o tratamento dos dados pessoais.

o. Pseudonimização: processo através do qual os dados pessoais são alterados de forma a impossibilitar a sua atribuição ao seu titular, sem necessidade de informação adicional, desde que essa informação adicional se encontre separada e esteja sujeita a medidas de segurança destinadas a garantir que os dados pessoais não possam ser atribuídos a uma pessoa física ou natural identificada ou identificável.

p. Titular: pessoa física ou natural a quem dizem respeito ou correspondem os dados pessoais.

q. Terceiro: pessoa singular ou coletiva, autoridade, instituição, serviço ou organismo público, distinto do titular, do responsável pelo tratamento e do encarregado.

r. Tratamento: qualquer operação ou conjunto de operações efetuadas através de procedimentos físicos ou automatizados sobre dados pessoais, relacionadas, a título exemplificativo mas não limitativo, com a obtenção, acesso, registo, organização, estruturação, adaptação, indexação, modificação, extração, consulta, armazenamento, conservação, elaboração, transferência, divulgação, posse, aproveitamento e, em geral, qualquer utilização ou disposição de dados pessoais.

s. Violação da segurança dos dados pessoais: qualquer violação da segurança que cause a destruição, perda ou alteração acidental ou ilícita dos dados pessoais transmitidos, conservados ou tratados de outra forma, ou a sua comunicação ou acesso não autorizados.

3. Âmbito de aplicação subjetivo

3.1. As presentes Normas foram concebidas para constituir um quadro de referência destinado a abranger, como sujeitos regulados, as pessoas singulares ou físicas, as pessoas coletivas de direito privado, as autoridades e os organismos públicos que tratam dados pessoais no exercício das suas atividades e funções.

4. Âmbito de aplicação objetivo

4.1. As presentes Normas foram concebidas para constituir um quadro de referência destinado a ser aplicável ao tratamento de dados pessoais que se encontrem em suportes físicos, automatizados total ou parcialmente, ou em ambos os suportes, independentemente da forma ou modalidade da sua criação, do tipo de suporte, do processamento, do armazenamento e da organização.

4.2. As presentes Normas destinam-se a constituir um quadro de referência aplicável aos dados pessoais das pessoas singulares, na sua qualidade de titulares dos mesmos.

4.3. Estas Normas foram concebidas para servir de quadro de referência, considerando-se como exceções válidas os seguintes casos:

a) Quando os dados pessoais se destinem a atividades exclusivamente do âmbito da vida familiar ou doméstica de uma pessoa singular, ou seja, a utilização de dados pessoais num contexto de amizade, parentesco ou grupo pessoal próximo, não tendo como objetivo a sua divulgação ou utilização comercial.

b) Os dados pessoais submetidos a um processo efetivo de anonimização.

4.4. A legislação nacional dos Estados ibero-americanos poderá estabelecer exceções ou limitações ao cumprimento do quadro geral de proteção dos dados pessoais.

Para serem consideradas legítimas, estas exceções ou limitações devem estabelecer-se exclusivamente como medidas necessárias, numa sociedade democrática, para fazer face a ameaças contra a segurança do Estado, a segurança pública e a prevenção das mesmas, ou ainda, como medidas a adotar pelas autoridades competentes para fins de prevenção, investigação e julgamento de infrações penais, bem como para a execução de sanções.

Para o estabelecimento adequado das disposições destinadas a criar exceções, deverá seguir-se o esquema previsto no n.º 6 das presentes Normas.

5. Âmbito de aplicação territorial

5.1. As presentes Normas recomendam que a pertinente legislação nacional de cada Estado seja concebida de forma a ser aplicável ao tratamento dos dados pessoais efetuado:

a. Por um responsável ou encarregado pelo tratamento estabelecido no território dos Estados Ibero-americanos.

b. Por um responsável ou encarregado do tratamento não estabelecido no território dos Estados Ibero-americanos, quando as atividades de tratamento de dados estiverem relacionadas com a oferta de bens ou serviços destinados aos residentes em Estados Ibero-americanos, ou estiverem relacionadas com o controlo do seu comportamento, na medida em que este ocorra nos Estados Ibero-americanos.

c. Por um responsável ou encarregado que não esteja estabelecido num Estado ibero-americano, mas ao qual seja aplicável a legislação nacional desse Estado, em virtude da celebração de um contrato ou por aplicação do direito internacional público.

d. Por um responsável ou encarregado que não esteja estabelecido no território dos Estados ibero-americanos e que utilize ou recorra a meios, automatizados ou não, situados nesse território para o tratamento de dados pessoais, exceto no caso de os referidos meios serem utilizados exclusivamente para fins de trânsito.

5.2. Para os efeitos das presentes Normas, entende-se por estabelecimento o local da administração central ou principal do responsável ou encarregado, o qual deverá determinar-se com base em critérios objetivos e implicar o exercício efetivo e real de atividades de gestão que determinem as principais decisões quanto aos fins e meios do tratamento de dados pessoais que realiza, através de modalidades estáveis.

5.3. A presença e a utilização de meios técnicos e tecnologias para o tratamento de dados pessoais ou as atividades de tratamento não constituirão, em si mesmas, um estabelecimento principal e não serão consideradas como critérios determinantes para a definição do estabelecimento principal do responsável ou encarregado do tratamento de dados.

5.4. Quando o tratamento dos dados pessoais for realizado por um grupo empresarial, o estabelecimento principal da empresa que exerce o controlo deve considerar-se como sendo o estabelecimento principal do grupo empresarial, exceto quando as finalidades e os meios do tratamento forem efetivamente determinados por outra empresa do grupo.

6. Exceções gerais ao direito à proteção de dados pessoais

6.1. A legislação nacional dos Estados ibero-americanos aplicável nesta matéria poderá limitar o direito à proteção de dados nos termos do disposto no n.º 4.4.

6.2. As exceções e limitações serão reconhecidas expressamente numa lei, no sentido formal e material, com o objetivo de proporcionar aos titulares uma certeza suficiente quanto à natureza e ao âmbito da medida.

6.3. No caso de algum dos Estados ibero-americanos considerar necessário prever alguma exceção ou limitação ao direito à proteção dos dados pessoais,

Recomenda-se que a legislação, onde assim se estabeleça, indique, no mínimo, as disposições relativas:

a. Á finalidade do tratamento.

b. As categorias de dados pessoais em causa.

c. O alcance das limitações estabelecidas.

d. As garantias adequadas para evitar acessos ou transferências ilícitas ou desproporcionadas.

e. A identificação do responsável ou dos responsáveis.

f. Os prazos de conservação dos dados pessoais.

g. Os possíveis riscos para os direitos e liberdades dos seus titulares.

h. O direito dos titulares a serem informados sobre a limitação em questão, salvo nos casos em que tal resulte prejudicial ou incompatível com os fins da referida limitação.

6.4. Numa sociedade democrática, as leis devem ser necessárias, adequadas e proporcionais e respeitar os direitos e as liberdades fundamentais dos titulares.

7. Ponderação do direito à proteção dos dados pessoais

7.1. Os Estados ibero-americanos poderão estabelecer exceções, na sua Constituição, legislação ou decisões judiciais, ao cumprimento de determinados princípios ou direitos em matéria de proteção de dados pessoais, exclusivamente na medida em que tal seja necessário para a salvaguarda de outros direitos e liberdades fundamentais que assim o justifiquem, como poderá ser o caso da liberdade de expressão, de imprensa e de informação, entre outros.

As exceções devem aplicar-se de forma estrita, adotando medidas proporcionais aos objetivos pretendidos, devendo essa limitação estar sempre justificada e ser adequada e proporcional, como corresponde numa sociedade democrática.

7.2. Esta isenção deverá implicar uma avaliação com o objetivo de determinar a necessidade, a adequação e a proporcionalidade da restrição ou exceção, em conformidade com as regras e critérios estabelecidos pelos Estados ibero-americanos no seu marco jurídico interno.

8. Tratamento de dados pessoais de crianças e adolescentes, responsabilidade reforçada

8.1. No tratamento dos dados pessoais de crianças e adolescentes, os Estados ibero-americanos darão prioridade à proteção do interesse superior destes,

em conformidade com a Convenção sobre os Direitos da Criança e outros instrumentos internacionais que visem o seu bem-estar, o respeito pela sua autonomia progressiva e a sua proteção integral.

8.2. Os Estados ibéricos promoverão:

a. No âmbito da formação académica das crianças e adolescentes, a utilização responsável, adequada e segura das tecnologias da informação e comunicação e a prevenção dos eventuais riscos a que se enfrentam em ambientes digitais, no que diz respeito ao tratamento indevido dos seus dados pessoais, bem como o respeito pelos seus direitos e liberdades.

b. A conceção e implementação de políticas destinadas a garantir que a informação dirigida a menores seja apresentada numa linguagem clara, simples e acessível, de modo a facilitar a compreensão das implicações do tratamento dos seus dados pessoais.

8.3. O tratamento dos dados pessoais de crianças e adolescentes deve ser objeto de medidas especiais de responsabilidade reforçada. A natureza e a intensidade dessas medidas devem determinar-se com base numa abordagem orientada para o risco e tendo em consideração o seu interesse superior e a sua proteção integral.

Entre o tipo de medidas a considerar encontram-se as configurações de proteção de dados predefinidas, as limitações de acesso, as restrições de perfis e publicidade comportamental, a verificação efetiva da idade, quando for pertinente, os sistemas de recomendação ajustados para evitar conteúdos nocivos, as ferramentas para bloquear, silenciar e controlar grupos e a proibição de downloads e/ou capturas de ecrã de conteúdos sobre menores, entre outras.

9. Tratamento de neurodados

9.1. O tratamento de dados neuronais deverá ser objeto de medidas especiais de responsabilidade reforçada. A natureza e a intensidade dessas medidas deverão ser determinadas com base numa abordagem orientada para o risco.

No tratamento de dados neuronais deverá prestar-se especial atenção ao cumprimento dos princípios da minimização, exatidão, transparência, lealdade, segurança e responsabilidade proativa.

9.2. Consideram-se tratamentos de alto risco com dados neuronais aqueles que tenham por objeto:

a. Inferir indevidamente estados mentais ou convicções íntimas.

b. Alterar indevidamente a vontade, as decisões ou o comportamento das pessoas.

c. Efetuar vigilância em massa em contextos laborais, educativos ou governamentais, com fins de controlo ou supervisão.

d. Identificar ou autenticar pessoas através de padrões neuronais.

Os tratamentos descritos podem ser objeto de proibições na legislação dos Estados ibero-americanos.

10. Tratamento de dados pessoais de carácter sensível ou de categorias especiais de dados

10.1. O responsável pelo tratamento não poderá tratar dados pessoais sensíveis nem categorias especiais de dados, salvo nos casos em que se verifique a ocorrência de alguma das seguintes exceções:

a. Quando o tratamento for indispensável por razões de interesse público, em cujo caso se deverá analisar a proporcionalidade em função do objetivo pretendido, respeitando, no essencial, o direito à proteção de dados e estabelecendo as medidas adequadas para a proteção dos interesses e direitos fundamentais do titular dos mesmos.

b. Quando o tratamento incidir sobre dados pessoais que o titular tenha tornado manifestamente públicos.

c. Quando o tratamento for necessário para a proteção de interesses vitais do titular ou de outra pessoa, caso o titular dos dados não esteja, física ou juridicamente, em condições de dar o seu consentimento.

d. Quando o tratamento for necessário para a formulação, o exercício ou a defesa de reclamações ou quando os tribunais intervenham no exercício da sua função judicial.

e. Quando o tratamento for necessário para fins de investigação científica ou histórica ou para fins estatísticos, devendo, nestes casos, analisar-se a proporcionalidade em função do objetivo pretendido, respeitando, no essencial, o direito à proteção de dados e estabelecendo as medidas adequadas para a proteção dos interesses e direitos fundamentais do titular dos dados.

f. Quando o tratamento for necessário por razões de interesse público, no âmbito da saúde pública, face a ameaças transfronteiriças graves para a saúde, com o fim de garantir os níveis adequados de qualidade e segurança dos cuidados de saúde e dos medicamentos ou dispositivos médicos, devendo adotar-se, para o efeito, as medidas adequadas para proteger os direitos e liberdades do titular dos dados.

g. Quando se trate de dados biométricos necessários para confirmar a identidade de um titular dos dados, sempre que os referidos dados biométricos, ou os meios necessários para a verificação, estejam sob o controlo exclusivo do titular de dados.

10.2. A legislação nacional dos Estados ibero-americanos aplicável nesta matéria poderá estabelecer exceções, garantias e condições adicionais para assegurar o tratamento adequado dos dados pessoais sensíveis, em conformidade com o seu marco jurídico interno.

Capítulo II
Princípios de proteção dos dados pessoais

11. Princípios aplicáveis ao tratamento dos dados pessoais

11.1. O tratamento dos dados pessoais deve respeitar os princípios da legitimidade ou licitude, lealdade, transparência, finalidade ou minimização, qualidade, responsabilidade proativa e comprovada, segurança e confidencialidade.

A leitura, interpretação, aplicação e implementação destes princípios devem fazer-se desde uma perspetiva de respeito pela dignidade humana, nomeadamente com o objetivo de garantir a autonomia pessoal e a integridade física e psíquica, bem como de evitar a instrumentalização das pessoas ou a sua discriminação.

Em qualquer caso, deve evitar-se a aplicação de limitações ou afetações desproporcionadas no que diz respeito à autonomia e à não instrumentalização das pessoas, especialmente no contexto de tratamentos de alto risco ou relacionados com inferências sobre dados sensíveis ou especialmente protegidos. As inferências, perfis, previsões ou dados derivados gerados a partir do tratamento de dados pessoais devem estar sujeitos a garantias adequadas de qualidade, pertinência, proporcionalidade e supervisão.

12. Princípio da legitimidade e da legalidade

12.1. Consideram-se causas habilitantes válidas para o tratamento de dados pessoais:

a. O consentimento do titular para uma ou várias finalidades específicas.

b. A necessidade do tratamento dos dados para o cumprimento de uma ordem judicial, decisão ou mandato fundamentado e motivado de uma autoridade pública competente.

c. A necessidade do tratamento dos dados para o exercício das competências próprias das autoridades públicas, ou ao abrigo de uma autorização legal.

d. A necessidade do tratamento dos dados para o reconhecimento ou defesa dos direitos do titular perante uma autoridade pública.

e. A necessidade do tratamento dos dados para a execução de um contrato ou pré-contrato em que o titular seja parte.

f. A necessidade do tratamento dos dados para o cumprimento de uma obrigação legal aplicável ao responsável pelo tratamento.

g. A necessidade do tratamento dos dados seja necessário para proteger interesses vitais do titular ou de outra pessoa singular.

h. A necessidade do tratamento dos dados por razões de interesse público estabelecidas ou previstas na lei.

i. A necessidade do tratamento dos dados para a satisfação de interesses legítimos do responsável pelo tratamento ou de um terceiro, em conformidade com a legislação aplicável em cada país, desde que se cumpram as seguintes condições:

1) A existência de um interesse legítimo e lícito relacionado com atividades reais, excluindo, por conseguinte, as situações hipotéticas.

2) Ter avaliado e determinado que não existem alternativas razoáveis, igualmente eficazes e menos intrusivas, para alcançar os objetivos pretendidos. Caso exista alguma alternativa razoável e com a mesma eficácia, o interesse legítimo não é admissível.

3) Ter realizado uma análise de ponderação para comprovar que os interesses individuais, juntamente com os direitos e liberdades fundamentais dos titulares, não prevalecem sobre esse interesse legítimo. Para este efeito, devem ser tidos em conta os interesses dos titulares, o impacto do tratamento e as suas expetativas razoáveis, bem como a existência de medidas de salvaguarda adicionais que possam limitar o impacto sobre o titular dos dados. Durante este exercício de ponderação, deverá ter-se especial cuidado se o titular for uma criança ou um adolescente.

As autoridades, instituições, entidades, organismos ou serviços públicos do Estado não poderão utilizar o interesse legítimo como fundamento para o tratamento de dados pessoais, no exercício das suas funções ou atribuições.

13. Condições para o consentimento

13.1. Sempre que for necessário obter o consentimento do titular, o responsável pelo tratamento deverá demonstrar, de forma inequívoca, que o titular prestou o seu consentimento, seja através de uma declaração ou de uma ação afirmativa clara.

13.2. Se o consentimento for prestado no contexto de uma declaração escrita que também aborde outros assuntos, o pedido de consentimento deverá ser apresentado de forma a distinguir-se de maneira clara desses outros assuntos, de modo compreensível e de fácil acesso, utilizando uma linguagem clara e simples. Qualquer consentimento obtido através de práticas contrárias à regulamentação aplicável será considerado nulo.

13.3. Sempre que for exigido o consentimento para o tratamento de dados pessoais, o titular poderá revogar dito consentimento em qualquer momento, para o que o responsável deverá estabelecer mecanismos simples, ágeis, eficazes e gratuitos.

14. Consentimento para o tratamento de dados pessoais de crianças e adolescentes

14.1. Na obtenção do consentimento de crianças e adolescentes, o responsável deverá obter a autorização do titular da autoridade parental ou da tutela, em conformidade com o disposto

nas regras de representação previstas no marco jurídico interno dos Estados ibero-americanos ou, se for o caso, solicitará diretamente a autorização do menor, no caso de o direito interno de cada Estado ibero-americano ter estabelecido uma idade mínima para que este possa concedê-la diretamente e sem qualquer representação por parte do titular da autoridade parental ou da tutela. O consentimento obtido de forma contrária à aqui estabelecida será considerado como sendo ilícito.

14.2. O responsável levará a cabo todos os esforços razoáveis para verificar se o consentimento foi concedido pelo titular da autoridade parental ou da tutela, ou diretamente pelo menor, tendo em conta a sua idade, em conformidade com o marco jurídico de cada Estado ibero-americano, e tendo em conta a tecnologia disponível.

14.3. O tratamento de dados para a elaboração de perfis com fins publicitários exigiria, no seu caso, um consentimento específico e distinto do consentimento para outros tratamentos.

15. Princípio da lealdade

15.1. O responsável pelo tratamento dos dados tratará os dados pessoais na sua posse, dando prioridade à proteção dos interesses do titular dos mesmos e abstendo-se de os tratar através de meios enganosos ou fraudulentos.

15.2. Para efeitos das presentes Normas, considerar-se-ão como desleais os tratamentos de dados pessoais que possam dar origem a uma discriminação injusta ou arbitrária contra os seus titulares.

16. Princípio de transparência

16.1. O responsável informará o titular sobre a existência dos dados e as principais características do tratamento a que serão submetidos, para que este possa tomar decisões informadas a este respeito.

16.2. O titular tem direito a conhecer, como mínimo, a seguinte informação:

a. A sua identidade e dados de contacto.

b. As categorias, classes ou tipos de dados objeto do tratamento.

c. A causa válida com base na qual o tratamento é realizado.

d. As finalidades do tratamento a que os seus dados pessoais serão submetidos.

e. Os dados de contacto do responsável pela proteção de dados, se for o caso.

f. O interesse legítimo perseguido, bem como a informação indispensável para garantir aos titulares dos dados que os seus direitos e liberdades fundamentais não serão prejudicados por este tratamento, baseado num interesse legítimo. Este caso aplica-se apenas se o interesse legítimo for a base jurídica do tratamento dos dados.

g. As transmissões, nacionais ou internacionais, de dados pessoais que pretenda levar a cabo, incluindo os destinatários e os fins da sua realização.

h. O prazo de conservação dos dados. Nos casos em que não seja possível indicar o prazo de conservação, indicar os critérios utilizados para o estabelecer.

i. A existência, forma e mecanismos ou procedimentos através dos quais o titular dos dados poderá exercer os direitos de acesso, retificação, cancelamento, supressão ou direito ao esquecimento, oposição, portabilidade, limitação do tratamento e de não ser objeto de decisões automatizadas.

j. A existência de decisões automatizadas que forneçam aos titulares dos dados informação útil sobre a lógica aplicada, a relevância do tratamento e as suas consequências, numa linguagem clara, simples e de fácil compreensão. Além disso, quando seja pertinente, os titulares dos dados devem ser informados sobre a criação de perfis, as fontes de dados de referência e as principais consequências desse tratamento. Quando forem utilizados sistemas de inteligência artificial, deverá ser fornecida informação relevante sobre o papel do sistema na tomada de decisões, o grau de automatização existente, as principais variáveis ou critérios utilizados e as limitações relevantes do sistema.

k. Se for o caso, a origem dos dados pessoais, quando o responsável pelo tratamento não os tenha obtido diretamente do seu titular.

16.3. A informação proporcionada ao titular dos dados deverá ser suficiente e facilmente acessível, redigida e estruturada numa linguagem clara, simples e de fácil compreensão para os titulares a quem se destina, especialmente no caso de crianças e adolescentes.

16.4. Todo o responsável deverá dispor de políticas transparentes relativas aos tratamentos de dados pessoais que realizar.

17. Princípio da finalidade

17.1. Qualquer tratamento de dados pessoais deverá limitar-se ao cumprimento de finalidades determinadas, explícitas e legítimas.

17.2. O responsável pelo tratamento não poderá tratar os dados pessoais na sua posse para finalidades diferentes daquelas que motivaram o seu tratamento original, salvo nos casos em que se verifique alguma das causas que autorizem um novo tratamento de dados, em conformidade com o princípio da legitimidade.

O tratamento de dados para fins distintos daqueles que motivaram o tratamento será viável sempre e quando se avalie e verifique, previamente, que esses fins são compatíveis com aqueles que motivaram inicialmente o tratamento dos dados. Para avaliar a compatibilidade, deverão considerar-se os seguintes fatores:

a. A ligação entre a finalidade inicial e a nova.

b. A natureza dos dados, em particular quando se trata de dados sensíveis.

c. O contexto em que os dados foram obtidos.

d. A existência de garantias técnicas e organizacionais em benefício dos titulares dos dados.

e. As expetativas razoáveis dos titulares dos dados.

f. A existência de medidas adequadas de governação, rastreabilidade e proteção de direitos, particularmente nos casos em que se pretenda a reutilização de dados para o treino, ajuste, validação ou melhoria de sistemas automatizados ou de inteligência artificial.

Esta disposição não se aplica ao tratamento de dados baseados no consentimento.

17.3. O tratamento posterior de dados pessoais para fins de arquivo, de investigação científica e histórica ou para fins estatísticos, quando em prol do interesse público, não será considerado incompatível com as finalidades iniciais.

17.4. No caso do tratamento dos dados de menores para uma nova finalidade, a proteção dos direitos da criança deve ser considerada com a mesma importância que quando os dados foram obtidos pela primeira vez.

18. Princípio da finalidade

18.1. O responsável pelo tratamento tratará apenas os dados pessoais que sejam adequados, pertinentes e limitados ao mínimo necessário para os fins que justificam o seu tratamento. A utilização de tecnologias automatizadas ou de sistemas de inteligência artificial não justificará, por si só, a recolha massiva, indiscriminada ou desproporcionada de dados pessoais.

19. Princípio da qualidade

19.1. O responsável pelo tratamento adotará as medidas necessárias para manter os dados pessoais na sua posse exatos, completos, pertinentes e atualizados, de modo a não alterar a sua veracidade, fiabilidade e adequação às finalidades que motivaram o seu tratamento. A qualidade dos dados pessoais deverá ser avaliada tendo em conta a natureza, o contexto, as finalidades e os possíveis efeitos do tratamento sobre os direitos e liberdades das pessoas.

Nos tratamentos automatizados, incluindo os realizados através de sistemas de inteligência artificial, o responsável pelo tratamento deverá adotar todas as medidas razoáveis para garantir a qualidade, a pertinência, a representatividade, a integridade e a atualização dos dados utilizados ao longo do ciclo de vida do sistema, incluindo os dados de treino, validação, teste, ajuste, introdução, supervisão e funcionamento.

Além disso, o responsável pelo tratamento deverá implementar mecanismos de governação e supervisão destinados a prevenir ou mitigar enviesamentos indevidos, inferências imprecisas, discriminação arbitrária, associações erradas, degradação da qualidade dos dados ou resultados manifestamente falsos, imprecisos, desproporcionados ou enganosos, ou decorrentes de dados incompletos, desatualizados, não representativos ou fora de contexto.

Quando o tratamento envolver a criação de perfis, sistemas preditivos ou inteligência artificial, o responsável pelo tratamento dos dados deverá avaliar periodicamente a fiabilidade, a pertinência, a exatidão, a proporcionalidade e a qualidade das inferências, classificações, recomendações, previsões ou resultados gerados pelo sistema, especialmente quando possam produzir efeitos jurídicos ou impactos significativos sobre as pessoas.

19.2. Quando os dados pessoais deixarem de ser necessários para a concretização dos fins que motivaram o seu tratamento, o responsável pelo tratamento deverá suprimir ou eliminar esses dados dos seus arquivos, registos, bases de dados, processos ou sistemas de informação ou, se for o caso, submetê-los a um procedimento de anonimização. No tratamento automatizado, incluindo o realizado através de sistemas de inteligência artificial, o responsável deverá adotar medidas razoáveis para evitar a reutilização incompatível, a persistência indevida ou a conservação desproporcionada de dados pessoais e das inferências deles decorrentes.

19.3. Na supressão dos dados pessoais, o responsável pelo seu tratamento deverá implementar métodos e técnicas orientados para a sua eliminação definitiva e segura.

19.4. Os dados pessoais serão conservados apenas durante o período necessário para o cumprimento dos fins que justificam o seu tratamento ou relacionados com os requisitos legais aplicáveis ao responsável pelo tratamento.

No entanto, a legislação nacional dos Estados Ibero-americanos aplicável nesta matéria poderá estabelecer exceções relativamente ao prazo de conservação dos dados pessoais, no pleno respeito pelos direitos e garantias do titular.

20. Princípio da responsabilidade proativa e comprovada

20.1. O responsável pelo tratamento dos dados implementará medidas técnicas e organizativas proporcionais ao risco assumido, para comprovar o cumprimento da legislação em matéria de proteção de dados pessoais.

Para a determinação do risco, deverá ter-se em conta a natureza, o âmbito, o contexto e as finalidades do tratamento, bem como a probabilidade de quaisquer violações dos direitos e liberdades fundamentais dos titulares dos dados, e a sua gravidade.

As certificações, as normas corporativas vinculativas, os códigos de conduta ou esquemas análogos poderão servir para demonstrar o cumprimento destes princípios, sempre e quando os referidos mecanismos possuam os seguintes atributos: sejam reconhecidos por uma autoridade de proteção de dados pessoais, que esse reconhecimento se baseie numa supervisão independente e acreditada, e que sejam mecanismos transparentes e publicamente verificáveis.

20.2. O acima exposto aplicar-se-á quando os dados pessoais forem tratados por um encarregado do tratamento em nome e por conta do responsável pelo tratamento, bem como no momento da realização de transferências de dados pessoais.

20.3. Entre os mecanismos que o responsável pelo tratamento poderá adotar para cumprir o princípio da responsabilidade encontram-se, a título exemplificativo e não exaustivo, os seguintes:

a. Destinar recursos à implementação de programas e políticas de proteção de dados pessoais.

b. Implementar sistemas de gestão de riscos associados ao tratamento de dados pessoais.

c. Elaborar políticas e programas de proteção de dados pessoais obrigatórios e exigíveis no seio da organização do responsável.

d. Implementar um programa de formação e atualização do pessoal sobre as obrigações em matéria de proteção de dados pessoais.

e. Revisar periodicamente as políticas e os programas de segurança dos dados pessoais para determinar quais as alterações requeridas a implementar, se for o caso.

f. Estabelecer um sistema de supervisão e vigilância interna e/ou externa, incluindo auditorias, para verificar o cumprimento das políticas de proteção de dados pessoais.

g. Estabelecer procedimentos para receber e responder a dúvidas e reclamações dos titulares dos dados.

h. Manter mecanismos razoáveis de governação, rastreabilidade, documentação, registo de decisões relevantes, supervisão, controlo e gestão de riscos, incluindo, quando pertinente, mecanismos de supervisão humana eficazes e de revisão periódica dos impactos.

20.4. O responsável revisará e avaliará de forma contínua os mecanismos que, para esse efeito, adotar voluntariamente para cumprir o princípio da responsabilidade, com o objetivo de avaliar o seu nível de eficácia no que diz respeito ao cumprimento da legislação nacional aplicável.

21. Princípio da segurança

21.1. O responsável pelo tratamento dos dados e o encarregado do tratamento estabelecerão e manterão, independentemente do tipo de tratamento efetuado, as medidas de carácter administrativo, físico e técnico pertinentes para garantir um nível de segurança adequado aos riscos a que estejam expostos, incluindo os elementos para garantir a confidencialidade, integridade, resiliência e disponibilidade permanentes dos sistemas e serviços de tratamento, a pseudonimização e encriptação dos dados, bem como a possibilidade de restabelecer rapidamente a disponibilidade e o acesso aos dados pessoais, na eventualidade da ocorrência de um incidente físico ou técnico.

21.2. Para a determinação das medidas referidas no número anterior, o responsável terá em consideração os seguintes fatores:

a. O risco para os direitos e liberdades dos titulares dos dados, em particular devido ao valor potencial, tanto quantitativo como qualitativo, que os dados pessoais tratados possam ter para um terceiro não autorizado a possuí-los.

b. O estado da técnica.

c. Os custos de aplicação.

d. A natureza dos dados pessoais tratados, especialmente no caso de dados pessoais sensíveis.

e. O âmbito, o contexto e as finalidades do tratamento dos dados.

f. As transferências internacionais de dados pessoais que se realizem ou se pretenda realizar.

g. O número de titulares.

h. As possíveis consequências que uma violação da segurança poderia acarretar para os titulares dos dados.

i. As violações da segurança ocorridas anteriormente no tratamento de dados pessoais.

21.3. O responsável e o encarregado do tratamento dos dados levarão a cabo, de forma periódica, uma série de ações que garantam o estabelecimento, a implementação, o funcionamento, a monitorização, a revisão, a manutenção e a melhoria contínua das medidas de segurança aplicáveis ao tratamento dos dados pessoais.

O responsável e o encarregado do tratamento dos dados implementarão as medidas pertinentes destinadas a assegurar que todas as pessoas que intervenham, sob a sua autoridade, no tratamento de dados, sejam obrigadas a cumprir as instruções e os compromissos destinados a garantir a segurança dos dados ao longo de toda a cadeia de tratamento.

No caso do tratamento de dados automatizado, incluindo o realizado através de sistemas de inteligência artificial, estas medidas devem incluir, quando for pertinente, controlos sobre a integridade dos dados, controlo de versões, monitorização do funcionamento, proteção contra a manipulação do sistema e mitigação de comportamentos imprevistos.

22. Notificação de violações da segurança dos dados pessoais

22.1. Quando o responsável pelo tratamento dos dados tiver conhecimento de uma violação da segurança dos mesmos, ocorrida em qualquer fase do seu tratamento, deverá notificar a autoridade de proteção de dados pessoais desse acontecimento, sem demora, salvo se, após avaliação, se determinar que a suposta violação não representa um risco para os direitos e liberdades dos titulares dos dados.

A notificação a apresentar à autoridade de proteção de dados pessoais pelo responsável pelo tratamento deve incluir, pelo menos, os seguintes elementos:

a. A natureza da violação da segurança dos dados pessoais.

b. As possíveis consequências da violação da segurança dos dados pessoais.

c. As medidas adotadas ou propostas pelo próprio responsável para remediar a referida violação.

d. As medidas destinadas a mitigar os possíveis efeitos negativos, se for o caso.

O encarregado do tratamento deverá notificar sem demora o responsável sobre as violações de segurança de que tenha conhecimento.

22.2. Os titulares dos dados deverão ser informados sobre as violações da segurança dos dados pessoais que impliquem um risco elevado para os seus direitos e liberdades. O responsável deverá notificá-los sem qualquer demora injustificada.

22.3. A notificação que o responsável pelo tratamento dos dados enviar aos seus titulares afetados deverá estar redigida numa linguagem clara e simples.

22.4. A notificação a enviar pelo responsável ao titular dos dados deverá conter, no mínimo, a seguinte informação:

a. A natureza do incidente.

b. Os dados pessoais comprometidos.

c. As medidas corretivas tomadas com carácter imediato.

d. As recomendações ao titular dos dados sobre as medidas que este possa adotar para proteger os seus interesses.

e. Os meios à disposição do titular dos dados para obter mais informação sobre esta matéria.

22.5. O responsável deverá documentar todas as violações de segurança dos dados pessoais ocorridas em qualquer fase do tratamento, identificando, a título exemplificativo mas não exaustivo, a data em que ocorreram, o motivo da violação, os factos com ela relacionados e os seus efeitos, e as medidas corretivas implementadas de forma imediata e definitiva, informação que ficará à disposição da autoridade de controlo.

22.6. A legislação nacional dos Estados Ibero-americanos aplicável nesta matéria estabelecerá os efeitos das notificações de violações de segurança que o responsável efetuar à autoridade de controlo, no que se refere aos procedimentos, forma e condições da sua intervenção, com o objetivo de salvaguardar os interesses, direitos e liberdades dos titulares afetados.

23. Princípio da confidencialidade

23.1. O responsável pelo tratamento dos dados estabelecerá os controlos ou mecanismos pertinentes para que todos aqueles que intervenham em qualquer fase do tratamento dos dados pessoais mantenham e respeitem a sua confidencialidade, obrigação que subsistirá mesmo após a terminação das suas relações com o titular.

O acima exposto não impede que as comunicações e transferências de dados pessoais sejam realizadas em conformidade com o disposto na legislação vigente.

Capítulo III
Direitos do titular

24. Direitos

24.1. Em qualquer momento, o titular dos dados ou o seu representante poderão solicitar ao responsável pelo seu tratamento o acesso, a retificação, a supressão e o direito ao esquecimento, a oposição, o direito a não ser objeto de decisões exclusivamente ou essencialmente automatizadas, a portabilidade dos dados pessoais e a limitação do tratamento dos dados que lhe dizem respeito.

24.2. O exercício de qualquer dos direitos referidos no número anterior não constitui um requisito prévio, nem impede o exercício de outros direitos.

25. Direito de acesso

25.1. O titular tem o direito de solicitar o acesso aos seus dados pessoais que estejam na posse do responsável pelo seu tratamento, bem como de conhecer qualquer informação relacionada com as condições gerais e específicas do seu tratamento.

26. Direito de retificação

26.1. O titular tem o direito de obter do responsável pelo tratamento a retificação ou correção dos seus dados pessoais, sempre que estes se revelem inexatos, incompletos ou desatualizados.

27. Direito à supressão e direito ao esquecimento

27.1. O titular tem o direito de solicitar ao responsável a supressão dos seus dados pessoais, para que estes sejam eliminados sem demora, nos seguintes casos:

a. Quando os dados não forem necessários para os fins para os quais foram recolhidos.

b. Se o titular revogar o seu consentimento, caso o tratamento se tenha baseado no mesmo.

c. Quando o titular tenha manifestado a sua oposição ao seu tratamento, nos termos do n.º 28.1, alínea a), e não prevaleçam outros motivos legítimos, ou quando o interessado manifestar a sua oposição nos termos da alínea b) do referido n.º.

d. Quando os dados tenham sido tratados de forma ilícita.

No caso de que os dados pessoais tenham sido tornados públicos, especialmente em ambientes digitais, e o responsável pelo seu tratamento seja obrigado a suprimir os dados nos termos de qualquer uma das situações descritas, o responsável deverá informar os outros responsáveis pelo tratamento que estejam a tratar os dados abrangidos do pedido de supressão de qualquer ligação a esses dados ou a qualquer cópia ou réplica dos mesmos. O exercício deste direito poderá ser validamente limitado quando o tratamento for indispensável para o exercício da liberdade de expressão e de informação, o cumprimento de uma obrigação legal, por motivos de interesse público, para fins de investigação científica, histórica ou estatística e para a formulação, exercício e defesa de reclamações.

28. Direito de oposição

28.1. O direito de oposição só poderá ser exercido quando o tratamento tiver ocorrido no âmbito do cumprimento de uma ação baseada no interesse público, decorrente do exercício de funções, atribuições ou poderes públicos ou para a satisfação de interesses legítimos.

O titular dos dados poderá exercer o seu direito de oposição:

a. Por motivos relacionados com a sua situação particular, incluindo a elaboração de perfis. O responsável pelo tratamento dos dados deverá cessar o seu tratamento, a menos que comprove a existência de motivos legítimos imperiosos que prevaleçam sobre os direitos e liberdades fundamentais do titular dos dados, ou para a formulação, exercício ou defesa de reclamações.

b. O tratamento dos seus dados pessoais tenha por objeto a realização de ações de marketing direto, incluindo a elaboração de perfis, na medida em que esteja relacionado com essa atividade.

28.2 No que se refere ao ponto anterior, quando o titular dos dados se opuser ao seu tratamento para fins de marketing direto, os seus dados pessoais deixarão de ser tratados para esses fins.

28.3. Quando o tratamento dos dados pessoais tiver sido realizado com base nos interesses legítimos do responsável pelo seu tratamento, no contexto do desenvolvimento e da exploração de um sistema de inteligência artificial, em cujo caso o direito de oposição será incondicional para o titular dos dados.

O responsável pelo tratamento dos dados deverá adotar as medidas razoáveis de governação, rastreabilidade e controlo destinadas a facilitar o exercício efetivo deste direito, tendo em conta a natureza do tratamento e os casos em que a supressão, a dissociação ou a cessação total da

utilização dos dados pessoais ou das inferências deles decorrentes não for técnica ou materialmente viável.

29. Direito a não ser objeto de decisões individuais automatizadas

29.1. O titular tem direito a não ser objeto de decisões que lhe produzam efeitos jurídicos ou que o afetem de forma significativa, quando estas se baseiem exclusiva ou essencialmente em tratamentos automatizados, incluindo os realizados através de sistemas de inteligência artificial destinados a avaliar, classificar, recomendar, traçar perfis, analisar ou prever aspetos pessoais do titular dos dados.

Os menores de idade não devem ser objeto de decisões que produzam efeitos jurídicos ou significativos baseadas exclusivamente no tratamento automatizado dos dados, salvo quando existam garantias reforçadas.

29.2. O disposto no número anterior não será aplicável quando o tratamento automatizado dos dados pessoais for necessário para a celebração ou execução de um contrato entre o titular e o responsável pelo seu tratamento, se for autorizado pela legislação nacional dos Estados Ibero-americanos ou se se basear no consentimento comprovável do titular dos dados.

29.3. No entanto, quando tal for necessário para a relação contratual ou se o titular tiver manifestado o seu consentimento, este terá direito a obter uma intervenção humana qualificada, significativa e efetiva, o que implica a capacidade real de compreender os fundamentos principais do sistema, avaliar criticamente os seus resultados e afastar-se deles de forma fundamentada, receber uma explicação significativa e clara sobre a lógica aplicada, de modo a poder conhecer os principais critérios e fatores determinantes em torno da decisão tomada e a importância e as principais consequências desse tratamento para o titular dos dados, bem como a expressar o seu ponto de vista e contestar a decisão.

29.4. O responsável pelo tratamento dos dados não poderá proceder ao tratamento automatizado de dados pessoais que tenham como efeito a discriminação dos seus titulares com base na sua origem, crenças ou convicções religiosas, filosóficas e morais, filiação sindical, opiniões políticas, dados relativos à saúde, à vida, neurodados, preferência ou orientação sexual, bem como dados genéticos ou biométricos.

30. Direito de oposição

30.1. Quando os dados pessoais forem tratados por via eletrónica ou por meios automatizados, o seu titular terá direito a obter uma cópia dos dados pessoais que tenha fornecido ao responsável pelo tratamento ou que sejam objeto de tratamento, num formato eletrónico estruturado, de uso comum e de leitura mecânica (formato interoperável), que lhe permita continuar a utilizá-los e transferi-los para outro responsável pelo tratamento, caso o solicite.

Este direito só poderá ser exercido quando:

a. Se trate exclusivamente de um tratamento automatizado.

b. O tratamento se baseie no consentimento ou num contrato.

30.2. O titular poderá solicitar que os seus dados pessoais sejam transferidos diretamente de um responsável para outro, sempre que tal seja tecnicamente possível.

30.3. O direito à portabilidade dos dados pessoais não afetará negativamente os direitos e liberdades de terceiros.

30.4. Sem prejuízo de outros direitos do titular, o direito à portabilidade dos dados pessoais não será aplicável quando se trate de informação inferida, derivada, criada, gerada ou obtida a partir da análise ou do tratamento efetuado pelo responsável com base nos dados pessoais fornecidos pelo titular, como é o caso dos dados pessoais que tenham sido submetidos a um processo de personalização, recomendação, categorização ou criação de perfis.

31. Direito à limitação do tratamento de dados pessoais

31.1. O titular terá direito à limitação do tratamento de dados pessoais nos seguintes casos:

a. Quando o titular exerça o seu direito de retificação, durante o prazo que permita ao responsável pelo tratamento dos dados dar cumprimento a esse direito.

b. Quando o titular se opuser ao tratamento dos seus dados, durante o tempo necessário para que o responsável possa verificar a existência de interesses legítimos ineludíveis que prevaleçam sobre os do titular.

c. Quando o titular solicitar que os dados não sejam suprimidos, em caso de tratamento ilícitos dos seus dados, para poder exercer ou defender os seus direitos.

Quando o titular assim o solicitar para a formulação, exercício ou defesa de reclamações, no caso de dados que tenham cumprido as suas finalidades.

31.2. Os titulares serão informados do cesse da limitação do tratamento, em todos os casos, antes do levantamento dessa medida.

32. Exercício dos direitos de proteção de dados pessoais

32.1. O responsável pelo tratamento estabelecerá meios e procedimentos simples, ágeis, acessíveis e gratuitos que permitam ao titular dos dados exercer os seus direitos de acesso, retificação, cancelamento, oposição e portabilidade.

32.2. A legislação nacional dos Estados Ibero-americanos aplicável nesta matéria estabelecerá os requisitos, prazos, termos e condições em que os titulares poderão exercer os seus direitos de acesso, retificação, cancelamento, oposição e portabilidade, bem como os motivos de improcedência do exercício dos mesmos, incluindo, a título exemplificativo, mas não limitativo, os seguintes:

a. Quando o tratamento for necessário para o cumprimento de um objetivo importante de interesse público.

b. Quando o tratamento for necessário para o exercício das funções próprias das autoridades públicas.

c. Quando o responsável pelo tratamento dos dados demonstrar possuir motivos legítimos para que o tratamento dos dados prevaleça sobre os interesses, os direitos e as liberdades do seu titular.

d. Quando o tratamento dos dados for necessário para o cumprimento de uma disposição legal.

e. Quando os dados pessoais forem necessários para a manutenção ou cumprimento de uma relação jurídica ou contratual.

32.3. A legislação nacional dos Estados Ibero-americanos aplicável nesta matéria poderá reconhecer que as pessoas singulares vinculadas a pessoas falecidas ou por estas designadas exerçam os direitos a que se refere a presente norma relativamente aos dados pessoais das pessoas falecidas que lhes digam respeito.

32.4. A legislação nacional dos Estados ibero-americanos aplicável nesta matéria reconhecerá o direito do titular a manifestar a sua discordância ou a contestar as respostas dadas pelo responsável pelo tratamento dos dados a um pedido de exercício dos direitos referidos no presente número ou perante a ausência de resposta deste, junto da autoridade de controlo e, se for caso disso, das instâncias judiciais, em conformidade com o marco jurídico interno de cada Estado ibero-americano.

32.5. A existência de mecanismos alternativos de resolução de litígios será possível, desde que seja garantida a sua revisão judicial e se trate de uma alternativa voluntária e imparcial, que não exclua a via judicial. A autoridade de proteção dos dados pessoais deverá supervisionar o cumprimento destas condições, com o fim de reconhecer a validade das ações desenvolvidas através destes mecanismos.

Capítulo IV
Encarregado do tratamento

33. Âmbito de atuação do encarregado do tratamento

33.1. O encarregado do tratamento dos dados realizará as atividades de tratamento de dados pessoais sem deter qualquer poder de decisão sobre o âmbito e o conteúdo do mesmo, limitando as suas ações aos termos estabelecidos pelo responsável pelo tratamento.

34. Formalização da prestação de serviços do encarregado

34.1. A prestação de serviços entre o responsável pelo tratamento e o encarregado será formalizada mediante a celebração de um contrato ou de qualquer outro instrumento jurídico previsto pelos Estados ibero-americanos na legislação nacional aplicável a esta matéria.

34.2. O contrato ou instrumento jurídico estabelecerá, no mínimo, o objeto, o âmbito, o conteúdo, a duração, a natureza e a finalidade do tratamento dos dados, o tipo de dados pessoais, as categorias de titulares, bem como as obrigações e responsabilidades do responsável e do encarregado do tratamento dos dados.

34.3. O contrato ou instrumento jurídico deverá estabelecer, como mínimo, as seguintes cláusulas gerais relacionadas com os serviços prestados pelo encarregado do tratamento:

a. Levar a cabo o tratamento dos dados pessoais de acordo com as instruções do responsável pelo tratamento.

b. Abster-se de tratar os dados pessoais para fins diferentes dos indicados pelo responsável pelo tratamento.

c. Implementar as medidas de segurança em conformidade com os instrumentos jurídicos aplicáveis.

d. Informar o responsável pelo tratamento em caso de violação dos dados pessoais de cujo tratamento estiver encarregue, de acordo com as suas instruções.

e. Manter a confidencialidade dos dados pessoais tratados.

f. Eliminar, devolver ou comunicar a um novo responsável pelo tratamento designado pelo responsável os dados pessoais que constituem objeto de tratamento, uma vez cessada a relação jurídica com o responsável ou por instruções deste, salvo nos casos em que uma disposição legal exija a conservação dos dados pessoais, ou se o responsável autorizar a comunicação dos mesmos a outro responsável pelo seu tratamento.

g. Abster-se de transferir os dados pessoais, salvo se o responsável pelo tratamento assim o determinar, ou se a comunicação dos dados decorrer de uma subcontratação, ou por mandato expresso da autoridade de controlo.

h. Permitir que o responsável pelo tratamento e a autoridade de controlo realizem inspeções e verificações nas instalações e dependências do subcontratado.

i. Elaborar, atualizar e conservar a documentação necessária que lhe permita comprovar o cumprimento das suas obrigações.

j. Colaborar com o responsável do tratamento em tudo o que se refira ao cumprimento da legislação nacional do Estado ibero-americano aplicável nesta matéria.

k. Quando o serviço envolver sistemas automatizados, inteligência artificial ou outras tecnologias emergentes, fornecer ao responsável informação suficiente sobre o funcionamento geral do sistema, as suas limitações relevantes, medidas de segurança, rastreabilidade, qualidade dos dados, supervisão e gestão de riscos, na medida necessária para que o responsável possa cumprir as suas obrigações.

34.4. Quando o encarregado do tratamento não cumprir as instruções do responsável e decidir por si próprio sobre o âmbito, o conteúdo, os meios e outras questões relativas ao tratamento de dados pessoais, assumirá a qualidade de responsável, em conformidade com a legislação nacional do Estado ibero-americano aplicável nesta matéria.

35. Subcontratação de serviços

35.1. O encarregado do tratamento dos dados poderá, por sua vez, subcontratar serviços que impliquem o tratamento de dados pessoais, sempre e quando exista uma autorização prévia por escrito, específica ou geral, do responsável, ou que tal esteja expressamente estipulado no contrato ou instrumento jurídico celebrado entre este último e o encarregado.

35.2. O subcontratado assumirá a qualidade de responsável pelo tratamento nos termos previstos na legislação nacional do Estado ibero-americano aplicável nesta matéria.

35.3. O responsável pelo tratamento formalizará a prestação de serviços do subcontratado mediante um contrato ou de qualquer outro instrumento jurídico que determine a legislação nacional do Estado ibero-americano aplicável a esta matéria.

35.4. Quando o encarregado não cumprir as suas obrigações e responsabilidades relativamente ao tratamento de dados pessoais que leva a cabo, de acordo com as instruções do responsável pelo tratamento, assumirá a qualidade de responsável pelo tratamento, nos termos da legislação nacional do Estado ibero-americano aplicável nesta matéria.

Capítulo V
Transferências internacionais de dados pessoais

36. Regras gerais para as transferências internacionais de dados pessoais

As únicas transferências internacionais de dados pessoais recomendadas como válidas serão aquelas realizadas pelos responsáveis e pelos encarregados do tratamento dos dados, em conformidade com as regras da presente secção.

O responsável pelo tratamento e o encarregado poderão efetuar transferências internacionais de dados pessoais em qualquer uma das seguintes situações:

a. Um país terceiro, parte do seu território, setor ou atividade, ou ainda uma organização internacional, que tenha sido reconhecido como possuindo um nível adequado de proteção de dados pessoais pelo país a partir do qual os mesmos serão exportados.

   Para levar a cabo a avaliação adequada do nível de proteção, as autoridades responsáveis pela proteção de dados pessoais devem avaliar, pelo menos, os seguintes aspetos:

   1) O Estado de Direito, nomeadamente o respeito pelos direitos fundamentais e pelas liberdades individuais, a legislação pertinente em matéria de proteção de dados pessoais, tanto a nível geral como setorial, a legislação relativa à segurança nacional, à segurança pública e ao âmbito penal, bem como a legislação relativa ao acesso, por parte das autoridades do Estado, aos dados pessoais, com o objetivo de verificar o nível de equivalência entre ambos os países nas matérias descritas.

   2) A existência e o funcionamento efetivo de uma ou mais autoridades de proteção de dados pessoais, devendo verificar-se se essa autoridade ou autoridades correspondem à estrutura e às características previstas no n.º 42 das presentes Normas.

   3) A existência de direitos individuais que possam ser efetivamente exercidos pelos seus titulares perante as autoridades de proteção de dados e os tribunais competentes.

   4) Os compromissos internacionais assumidos pelo país terceiro ou pela organização internacional, com o fim de verificar o alcance dos seus compromissos em matéria de dados pessoais.

Concluída a avaliação, poderá ser tomada uma decisão sobre a possibilidade de reconhecer, ou não, um país terceiro ou uma organização internacional como possuindo um nível adequado de proteção. No próprio documento em que for adotada a decisão favorável ao reconhecimento, deverá ser estabelecido o mecanismo de revisão periódica, para verificar a manutenção das condições ao longo do tempo. Dita revisão deverá realizar-se, como mínimo, de 5 em 5 anos.

b. Nos casos em que o país terceiro ou a organização internacional de destino de uma transferência internacional de dados pessoais não disponha do reconhecimento de nível adequado por parte do país a partir do qual os dados serão exportados, o responsável pelo tratamento ou o encarregado poderão oferecer as garantias adequadas através dos seguintes instrumentos:

1) Cláusulas-tipo de proteção de dados pessoais adotadas pela autoridade de proteção de dados pessoais, às quais os responsáveis e os encarregados do tratamento possam aderir, garantindo, através dessa adesão, o cumprimento da legislação em matéria de proteção de dados do país a partir do qual os dados são exportados.

2) Códigos de conduta vinculativos e exigíveis, representativos de uma associação ou entidade setorial, sujeitos a mecanismos de supervisão independentes e eficazes, que assegurem o respeito pela legislação em matéria de proteção de dados do país de onde os dados são exportados, e que devem ser avaliados e aprovados pela autoridade de proteção de dados pessoais do referido país.

3) Normas corporativas vinculativas, que garantam e demonstrem que a legislação em matéria de proteção de dados do país a partir do qual os dados são exportados será respeitada, revistas e aprovadas pela autoridade de proteção de dados pessoais do país de destino dos dados.

4) Certificações que garantam e demonstrem que a legislação em matéria de proteção de dados do país a partir do qual os dados são exportados será respeitada, revistas e aprovadas pela autoridade responsável pela proteção de dados pessoais do referido país.

5) Instrumentos juridicamente vinculativos e exigíveis entre instituições e entidades públicas do Estado.

6) Cláusulas contratuais entre um responsável ou um encarregado do tratamento, do país de onde os dados são exportados, e um destinatário de um país terceiro ou uma organização internacional. Para serem válidas, estas cláusulas deverão ser devidamente autorizadas pela autoridade de proteção de dados pessoais.

c. Na ausência de uma decisão de adequação ou de garantias adequadas, as transferências internacionais de dados poderão realizar-se nos seguintes casos excecionais:

1) Quando o titular tenha dado o seu consentimento expresso para a transferência dos dados, após ter sido informado dos possíveis riscos da mesma.

2) Se dita transferência for indispensável para a celebração ou execução de um contrato, ou de medidas pré-contratuais, relacionadas com o titular dos dados.

3) Por razões de interesse público.

4) Para a formulação, exercício e defesa de reclamações.

5) Para a proteção de interesses vitais do titular dos dados ou de terceiros, nos casos em que o titular se encontre impossibilitado de prestar o seu consentimento.

6) Se for efetuada a partir de um registo público, cujo objetivo seja facilitar a informação e estar aberto à consulta do público em geral, ou de qualquer pessoa que demonstre ter um interesse legítimo, apenas na medida em que sejam cumpridos os requisitos da legislação aplicável para a consulta.

Os casos descritos nos n.ºs 1) e 2) não serão aplicáveis às atividades realizadas por autoridades e instituições públicas do Estado, no exercício de atribuições, competências ou poderes públicos.

d. No caso de que uma transferência internacional de dados pessoais não possa realizar-se através de qualquer um dos mecanismos descritos nas alíneas a), b) e c), poderá ser realizada a título excecional, desde que se verifiquem todas as seguintes condições:

1) Não seja repetitiva.

2) Afete um número limitado de titulares.

3) Seja necessária para satisfazer interesses legítimos e imperativos do responsável pelo tratamento, que se sobreponham aos direitos e liberdades dos titulares. Estes interesses legítimos devem ser comunicados ao titular dos dados.

4) O responsável pelo tratamento tenha oferecido garantias adequadas, de acordo com a situação.

5) Que se informe a autoridade de proteção de dados pessoais.

A exceção d) não será aplicável a atividades realizadas por autoridades e instituições públicas do Estado, no exercício de atribuições, competências ou poderes públicos.

Capítulo VI

Medidas proativas no tratamento de dados pessoais

37. Reconhecimento de medidas proativas

37.1. A legislação nacional dos Estados ibero-americanos aplicável nesta matéria poderá reconhecer e estabelecer medidas que promovam um melhor cumprimento da sua legislação e contribuam para reforçar e melhorar os controlos de proteção de dados pessoais implementados pelo responsável pelo tratamento, entre as quais se podem incluir as que se indicam a seguir no presente capítulo.

38. Privacidade desde a conceção e privacidade por predefinição

38.1. O responsável aplicará, desde a conceção, na determinação dos meios de tratamento dos dados pessoais, durante a mesma e antes da recolha dos dados pessoais, medidas preventivas de diversa natureza que permitam aplicar de forma eficaz os princípios, direitos e demais obrigações previstos na legislação nacional do Estado ibero-americano que lhe seja aplicável. Nos tratamentos automatizados, incluindo os realizados através de sistemas de inteligência artificial, as medidas devem prever mecanismos razoáveis de supervisão, rastreabilidade, documentação e gestão de riscos e controlo do funcionamento do sistema, tendo em conta a natureza, o contexto e os possíveis efeitos do tratamento.

38.2. O responsável deverá garantir que os seus programas, serviços, sistemas ou plataformas informáticas, aplicações eletrónicas ou qualquer outra tecnologia que implique o tratamento de dados pessoais cumpram de maneira predefinida ou estejam em conformidade com os princípios, direitos e demais obrigações previstas na legislação nacional do Estado ibero-americano que lhe seja aplicável, especificamente com o objetivo de que apenas seja objeto de tratamento um volume mínimo de dados pessoais e de que a acessibilidade aos mesmos, sem a intervenção do seu titular, seja limitada a um número indeterminado de pessoas.

39. Responsável ou delegado de proteção de dados pessoais

39.1. O responsável e o encarregado do tratamento designarão um responsável ou delegado de proteção de dados pessoais, tendo em conta a sua formação e experiência profissionais, os seus conhecimentos especializados e devidamente acreditados no domínio da proteção de dados pessoais, bem como a sua capacidade para desempenhar as funções descritas no n.º 39.4.

A nomeação de um responsável ou delegado de proteção de dados pessoais será obrigatória nos seguintes casos:

a. Quando se trate de uma autoridade pública. Para estes efeitos, considera-se como autoridade pública não uma autoridade que faz parte do Estado num sentido estrito, mas também os particulares que desenvolvem atividades próprias do Estado através de concessões, licenças ou autorizações, entre outras.

b. Quando se leve a cabo o tratamento de dados pessoais tendo por objeto uma observação habitual e sistemática do comportamento do seu titular.

c. Quando se leve a cabo o tratamentos de dados pessoais que sejam suscetíveis de implicar um risco elevado de afetação do direito à proteção dos dados pessoais dos titulares, tendo em conta, entre outros fatores e a título exemplificativo mas não limitativo, as categorias de dados pessoais tratados, especialmente quando se trate de dados sensíveis, as transferências efetuadas, o número de titulares, o âmbito do tratamento, as tecnologias da informação utilizadas e as finalidades do tratamento.

39.2. O responsável que não se insira em nenhuma das situações contempladas no número anterior poderá designar um responsável pela proteção de dados pessoais, se assim o considerar conveniente.

39.3. O responsável estará obrigado a apoiar o responsável pela proteção dos dados pessoais no desempenho das suas funções, colocando ao seu dispor os recursos necessários para o seu desempenho e para a manutenção e atualização dos seus conhecimentos especializados.

39.4. O responsável pela proteção de dados pessoais terá, entre outras, as seguintes funções:

a. Aconselhar o responsável ou o encarregado do tratamento dos dados sobre as questões que lhe sejam submetidas para apreciação em matéria de proteção de dados pessoais.

b. Coordenar, no âmbito da organização do responsável ou do encarregado do tratamento dos dados, as políticas, programas, ações e outras atividades necessárias para o cumprimento das normas em matéria de dados pessoais.

c. Supervisionar, no âmbito da organização do responsável ou do encarregado do tratamento dos dados, o cumprimento da legislação em matéria de dados pessoais.

d. Colaborar com a autoridade de proteção de dados pessoais e servir de ponto de contacto.

39.5. O responsável e o encarregado do tratamento dos dados garantirão que o responsável ou delegado não receba instruções relativas ao desempenho das suas funções, assegurando-se de que não venha a encontrar-se em situações de conflito de interesses decorrentes de outras atividades, no seio da organização, se for o caso. O responsável ou delegado prestará contas à alta direção ou à autoridade máxima do responsável ou do encarregado do tratamento dos dados.

40. Mecanismos de autorregulação

40.1. O responsável pelo tratamento dos dados poderá aderir, de forma voluntária, a regimes de autorregulação vinculativos, que tenham por objetivo, entre outros, contribuir para a correta aplicação da legislação nacional do Estado ibero-americano aplicável a esta matéria e estabelecer procedimentos de resolução de conflitos entre o responsável pelo tratamento e o titular dos dados, sem prejuízo de outros mecanismos estabelecidos pela legislação nacional aplicável a esta matéria, tendo em conta as características específicas dos tratamentos de dados pessoais realizados, bem como o exercício efetivo e o respeito pelos direitos do titular.

40.2. Para efeitos do número anterior, poderão ser desenvolvidos, entre outros, códigos deontológicos e sistemas de certificação, bem como os respetivos selos de confiança, que contribuam para os objetivos indicados no presente número.

40.3. A legislação nacional dos Estados ibero-americanos aplicável nesta matéria estabelecerá as regras pertinentes para a validação, confirmação ou reconhecimento dos mecanismos de autorregulação referidos.

41. Avaliação do impacto na proteção de dados pessoais

41.1. Quando o responsável pretender realizar algum tipo de tratamento de dados pessoais, especialmente através de tecnologias emergentes ou disruptivas, incluindo

sistemas de inteligência artificial, tecnologia biométrica, neurotecnologia, sistemas preditivos e outras tecnologias capazes de produzir tratamentos intensivos, inferenciais ou altamente automatizados de dados pessoais, que, pela sua natureza, âmbito, contexto ou finalidade sejam suscetíveis de implicar um risco elevado para os direitos e liberdades dos titulares, deverá realizar, antes do tratamento dos dados, uma avaliação do impacto das operações de tratamento na proteção dos dados pessoais.

Esta avaliação deverá incluir, pelo menos, o seguinte:

a. Uma descrição sistemática das operações de tratamento revistas, os seus fins e, se for o caso, dos interesses legítimos do responsável pelo tratamento dos dados.

b. A avaliação da necessidade e da proporcionalidade das operações de tratamento de dados a realizar, em função dos fins pretendidos.

c. A avaliação dos riscos para os direitos e liberdades dos titulares dos dados.

d. As medidas previstas para fazer face aos riscos, indicando todas as garantias e mecanismos destinados a assegurar e demonstrar a proteção dos dados pessoais e o cumprimento da legislação aplicável sobre esta matéria.

e. A descrição das medidas de governação algorítmica, bem como das medidas previstas para a supervisão, rastreabilidade, controlo e mitigação dos riscos associados a sistemas automatizados ou de inteligência artificial.

Nos casos em que tal se justifique, o responsável solicitará a opinião dos titulares relativamente ao tratamento a realizar, sem prejuízo do interesse público, comercial ou de segurança que, no seu caso, pudessem implicar.

41.2 A avaliação do impacto na proteção dos dados pessoas deve apresentar-se, em especial, nos seguintes casos:

a. Tratamentos automatizados ou baseados em sistemas de inteligência artificial, incluindo a criação de perfis, que gerem recomendações ou decisões exclusiva ou essencialmente automatizadas, que possam produzir efeitos jurídicos, repercussões significativas semelhantes ou influenciar de forma relevante o comportamento, as decisões, o acesso a direitos, oportunidades, serviços essenciais ou condições de vida das pessoas singulares.

b. Tratamento em grande escala de dados sensíveis ou de categorias especiais de dados.

c. Os tratamentos de alto risco descritos nas presentes Normas.

d. Os tratamentos que impliquem a observação sistemática, em grande escala, em zonas de acesso público.

e. As transferências internacionais de dados pessoais para países não reconhecidos como possuindo um nível de segurança adequado, sempre que não seja possível oferecer alguma das garantias adequadas

reconhecidas no n.º 36.1, alínea b), ou não se comprove a existência de alguma das exceções previstas no n.º 36.1, alínea c).

Nos casos em que o resultado da avaliação de impacto indique que o tratamento dos dados pode implicar um risco elevado, e caso não sejam implementadas as medidas de mitigação adequadas, o responsável será obrigado a consultar a autoridade de proteção de dados pessoais, antes de dar início ao seu tratamento.

O objetivo desta consulta é conseguir que a autoridade de proteção de dados pessoais assessore o responsável pelo seu tratamento. Para este efeito, o responsável pelo tratamento deverá partilhar com a referida autoridade a avaliação de impacto sobre a proteção de dados realizada, bem como toda a informação que se considere necessária.

Capítulo VII
Autoridades de proteção de dados pessoais

42. Autoridades de proteção de dados pessoais

42.1. A legislação sobre a proteção dos dados pessoais deverá prever a existência de uma ou mais autoridades de proteção de dados pessoais, com o objetivo de supervisionar e assegurar o cumprimento da regulamentação, e de garantir o respeito pelos direitos e liberdades das pessoas singulares.

42.2. As autoridades de proteção de dados pessoais devem gozar de plena autonomia em relação à legislação e à regulamentação que as regule. Dita plena autonomia deve garantir, como mínimo, o cumprimento do seu objetivo e o exercício das suas faculdades, atribuições, competências e poderes de forma imparcial e independente e alheia a qualquer influência externa, direta ou indireta, sem requerer nem admitir qualquer ordem ou instrução.

Embora o grau máximo de autonomia reconhecido pelo marco jurídico de cada Estado ibero-americano possa constituir o modelo mais eficaz para a conceção das autoridades, nos casos em que tal não seja viável estas poderão ser dotadas de uma autonomia funcionalmente eficaz, que lhes garanta o cumprimento do seu objetivo e o pleno exercício das suas funções.

42.3. O órgão máximo de direção de ditas autoridades poderá ser de composição unipessoal ou colegial.

O membro ou os membros dos órgãos de direção das autoridades deverão possuir a experiência e os conhecimentos especializados e necessários em matéria de direito e proteção de dados pessoais, especialmente no referente à supervisão regulatória e à cooperação internacional.

O processo de seleção deverá ser transparente e garantir a sua imparcialidade e credibilidade, bem como assegurar que se trata de um processo de seleção de perfil técnico, baseado essencialmente no mérito.

A pessoa ou pessoas nomeadas só poderão ser destituídas por motivos graves previstos na legislação nacional, de acordo com as regras do devido processo legal, ou caso deixem de cumprir as condições exigidas para o exercício das suas funções.

O membro ou os membros dos órgãos de direção da autoridade deverão abster-se de qualquer ação incompatível com as suas responsabilidades durante o período de vigência do seu mandato.

42.4. Para além das funções mencionadas ao longo das presentes Normas, as autoridades de proteção de dados pessoais deverão dispor das competências, atribuições, poderes e autoridade adequados para alcançar os seus objetivos.

A estrutura das autoridades de proteção de dados deverá refletir, na legislação pertinente, os elementos que lhes permitam, como mínimo:

a. Investigar, supervisionar ou fiscalizar o cumprimento da regulamentação.

b. Determinar medidas cautelares provisórias, proporcionais e passíveis de revisão, como instrumento preventivo e urgente.

c. Proferir decisões.

d. Sancionar a prática de infrações.

e. Garantir o exercício dos direitos dos titulares dos dados.

f. Emitir regulamentos.

g. Interpretar a regulamentação.

h. Conceber e implementar políticas públicas.

i. Conceber e implementar programas de reforço de capacidades.

j. Construir e promover uma cultura de proteção de dados.

k. Criar e promover o conhecimento.

l. Cooperar a nível internacional com outras autoridades.

No exercício das suas funções, as autoridades de proteção de dados deverão implementar políticas destinadas a prestar a atenção adequada à tutela dos grupos vulneráveis, de acordo com as suas necessidades, de modo a permitir-lhes o exercício efetivo dos seus direitos.

42.5. As decisões e atuações da autoridade de proteção de dados, no exercício das suas funções, competências, atribuições, prerrogativas e poderes, exclusivamente, estarão sujeitas a revisão judicial, pelo que a legislação nacional deverá adotar as disposições necessárias para o garantir.

42.6. As autoridades de proteção de dados pessoais deverão dispor dos recursos humanos e materiais necessários ao cumprimento das suas funções.

Cada Estado ibero-americano deverá garantir que os controlos financeiros a que a autoridade de proteção de dados pessoais está sujeita não prejudiquem a sua plena autonomia e independência, pelo que esta deverá dispor de um orçamento público, independentemente da existência de outras fontes de financiamento que possa ter.

Além disso, deverá garantir-se que cada autoridade possa escolher e dispor livremente do seu pessoal, o qual dependerá exclusivamente do órgão de direção da autoridade de proteção de dados pessoais.

Capítulo VIII
Reclamações e sanções

43. Regime de reclamações e de imposição de sanções

43.1. Qualquer titular de dados terá direito a apresentar a sua reclamação perante a autoridade de proteção de dados pessoais, bem como de recorrer à tutela judicial para fazer valer os seus direitos, em conformidade com a legislação nacional do Estado ibero-americano aplicável sobre esta matéria.

43.2. A legislação nacional dos Estados Ibero-americanos aplicável nesta matéria estabelecerá um regime que permita ao titular apresentar uma reclamação junto da autoridade de proteção de dados pessoais, quando considere que o tratamento dos seus dados viola a legislação nacional aplicável, bem como solicitar a tutela judicial.

43.3. A legislação nacional dos Estados ibero-americanos aplicável nesta matéria estabelecerá um regime que permita a adoção de medidas corretivas e a aplicação de sanções às condutas que contravenham o disposto nas legislações nacionais correspondentes, indicando, pelo menos, o limite máximo e os critérios objetivos para fixar as sanções correspondentes com base na natureza, gravidade, duração da infração e nas suas consequências, bem como as medidas implementadas pelo responsável pelo tratamento para garantir o cumprimento das suas obrigações nesta matéria.

Capítulo IX
Direito a indemnização

44. Regime de reclamações e de imposição de sanções

44.1. A legislação nacional dos Estados ibero-americanos aplicável nesta matéria reconhecerá o direito do titular a ser indemnizado nos casos em que tenha sofrido danos e prejuízos em consequência de uma violação do seu direito à proteção dos seus dados pessoais.

44.2. A legislação nacional dos Estados ibero-americanos indicará a autoridade competente para apreciar este tipo de ações interpostas pelo titular afetado, bem como os prazos, requisitos e condições da pertinente indemnização, caso a ação seja considerada procedente.

Capítulo X

45. Estabelecimento de mecanismos de cooperação internacional

45.1. Os Estados ibero-americanos poderão adotar mecanismos de cooperação internacional que facilitem a aplicação das legislações nacionais aplicáveis sobre esta matéria, os quais poderão incluir, a título exemplificativo mas não exaustivo:

a. O estabelecimento de mecanismos que permitam reforçar a assistência e a cooperação internacional na aplicação das respetivas legislações nacionais sobre esta matéria.

b. A assistência mútua entre as autoridades de controlo através da notificação e remissão de reclamações, da assistência em investigações e do intercâmbio de informação.

c. A adoção de mecanismos orientados para o conhecimento e a partilha das melhores práticas e experiências em matéria de proteção de dados pessoais, incluindo em matéria de conflitos de jurisdição com países terceiros.

45.2. Além disso, no âmbito das ações de cooperação internacional, poderão ser estabelecidos vínculos com redes, foros, mecanismos e espaços de cooperação, entre outros, que permitam partilhar experiências regulatórias e casos significativos, facilitar a assistência mútua, adotar posições comuns sobre fenómenos disruptivos e temas emergentes, promover a interoperabilidade normativa, conceber estratégias comuns de mitigação contra a fragmentação normativa e promover protocolos que facilitem a simplificação administrativa, no âmbito da proteção de dados.

Disposições transitórias

Única. Para a implementação efetiva da legislação, regulamentos e normas, em geral, relativos ao tratamento de dados pessoais, incluindo quaisquer alterações ou reformas, é determinante proporcionar aos responsáveis e aos encarregados as condições necessárias para o cumprimento da legislação e para que dito cumprimento seja sustentável ao longo do tempo.

Uma dessas condições reside na temporalidade da regulamentação, mais concretamente no estabelecimento de prazos razoáveis entre a publicação da regulamentação e a sua entrada em vigor, tendo em consideração o conjunto de implicações materiais, financeiras, humanas e regulamentares que, de um modo geral, esta regulamentação costuma comportar.

RED IBEROAMERICANA DE PROTECCION DE DATOS



