

**PADRÕES DE PROTEÇÃO DE DADOS
PESSOAIS PARA OS ESTADOS
IBERO-AMERICANOS**

PRÓLOGO

No âmbito do XV Encontro Ibero-Americano de Proteção de Dados, a Rede Ibero-Americana de Proteção de Dados (RIPD ou a Rede) aprovou e apresentou oficialmente os denominados “Padrões de Proteção de Dados dos Estados Ibero-Americanos”, para cumprir com um objetivo longamente almejado por todas as entidades que a integram, bem como para um dos acordos adotados na XXV Cúpula Ibero-Americana de Chefes de Estado e de Governo, celebrada nos dias 28 e 29 de outubro de 2016, na Colômbia, relacionado com solicitar à Rede a elaboração de uma proposta de cooperação efetiva com a proteção de dados pessoais e a privacidade.

O texto ora aprovado, tenta dar respostas para um dos eixos da estratégia acordada pela RIPD em novembro de 2016, em Montevideu, plasmada no documento “RIPD 2020”, que consiste em “encorajar e contribuir para o fortalecimento e a adequação dos processos regulatórios na região, mediante a elaboração de diretrizes que sirvam de parâmetro para futuras regulações ou para a revisão das já existentes.”

Nesse sentido, os Padrões Ibero-Americanos conformam um conjunto de diretrizes orientadoras, que contribuem para a emissão de iniciativas regulatórias de proteção de dados pessoais na região ibero-americana para aqueles países que ainda não contam com esses ordenamentos, ou no caso, para servir de referência na modernização e atualização das legislações existentes.

Entre os objetivos dos Padrões Ibero-Americanos, destacam-se:

- O estabelecimento de um conjunto de princípios e direitos comuns para proteção de dados pessoais, que os Estados Ibero-Americanos podem adotar e desenvolver em sua legislação nacional, com a finalidade de contar com regras homogêneas na região.
- Garantir o efetivo exercício e tutela do direito à proteção de dados pessoais de qualquer pessoa física nos Estados Ibero-Americanos, mediante a determinação de regras comuns que assegurem o devido tratamento de seus dados pessoais.
- Facilitar o fluxo de dados pessoais entre os Estados Ibero-Americanos e fora de suas fronteiras, com o propósito de coadjuvar para o crescimento econômico e social da região.
- Encorajar a cooperação internacional entre as autoridades de controle dos Estados Ibero-Americanos com outras autoridades de controle não pertencentes à região, e autoridades e órgãos internacionais na matéria.

Como antecedentes diretos desses Padrões, por um lado, é possível mencionar a adoção pela própria RIPD, em 2007, no contexto do V Encontro Ibero-Americano de Proteção de Dados, das “Diretivas para a Harmonização da Proteção de Dados na Comunidade Ibero-Americana”. Com elas, pretendia-se estabelecer um “contexto harmonizado” de referência para iniciativas regulatórias nacionais que pudessem surgir na região em matéria de proteção de dados. E, por outro, os padrões aprovados na Conferência Internacional de Autoridades de Privacidade e Proteção de Dados, celebrada em Madri, em 2009, os chamados “Padrões de Madri”, que sem dúvida representaram um avanço na busca por soluções e disposições específicas “que poderiam ser aplicadas independentemente das diferenças que pudessem existir entre os diferentes modelos existentes de proteção de dados e privacidade”.

Na elaboração dos Padrões Ibero-Americanos também foram tomados como referência outros instrumentos internacionais e emblemáticos em matéria de proteção de dados pessoais, como as Diretivas relativas à proteção da intimidade e da circulação transfronteiriça de dados pessoais da Organização para a Cooperação e Desenvolvimento Econômico; o Convênio número 108 do Conselho da Europa, para a proteção das pessoas respeito do tratamento automatizado de dados de caráter pessoal e seu Protocolo; o Marco de Privacidade do Fórum de Cooperação Econômica Ásia-Pacífico, e o Regulamento do Parlamento Europeu e do Conselho, relativo à proteção das pessoas físicas no que respeita ao tratamento de dados pessoais e à livre circulação desses dados, entre outros.

O percurso seguido na elaboração incluiu as seguintes etapas:

- Junho de 2016: no XIV Encontro Ibero-Americano de Proteção de Dados, celebrado em 08 de junho de 2016, em Santa Marta, Colômbia, acordou-se a elaboração dos Padrões Ibero-Americanos a cargo do Instituto Nacional de Transparência, Acesso à Informação e Proteção de Dados Pessoais (INAI), nesse momento em caráter de presidente da Rede.
- Novembro de 2016: no Seminário da RIPD no Centro de Cooperação Espanhola em Montevideu, celebrado nos dias 08 e 09 de novembro em Montevideu, Uruguai, o INAI apresentou aos membros presentes da Rede o anteprojeto de Padrões Ibero-Americanos. Nesse seminário, acordou-se que, durante todo o mês de dezembro de 2016, o anteprojeto de Padrões Ibero-Americanos estaria aberto para comentários e observações dos membros da Rede.
- Maio de 2017: na Oficina da RIPD no Centro de Cooperação Espanhola, em Cartagena de Índias, foi estudado e debatido, do ponto de vista técnico, a versão dos Padrões Ibero-Americanos resultado de todas as contribuições recebidas durante o mês de dezembro de 2016. Nessa oficina participaram as Autoridades membros da RIPD, uma

representação do Supervisor Europeu de Proteção de Dados e da Organização dos Estados Americanos, bem como, mediante videoconferência, a Unidade de Fluxos Internacionais da Comissão Europeia.

- Junho de 2017: no XV Encontro Ibero-Americano de Proteção de Dados, celebrado entre 20 e 22 de junho de 2017, em Santiago do Chile, aprovou-se por unanimidade em sessão fechada do Encontro a versão que resultara dos trabalhos realizados durante a oficina de Cartagena de Índias, sendo formalmente proclamados em Sessão Aberta.

Com a aprovação desses Padrões, a RIPD possui uma ferramenta chave para poder enfrentar com rigor o seguimento e apoio dos futuros desenvolvimentos legislativos na Região, devido a que os Padrões Ibero-Americanos têm a característica de serem um modelo normativo que:

- Responde às necessidades e exigências nacionais e internacionais que demanda o direito à proteção de dados pessoais, em uma sociedade onde as tecnologias da informação e do conhecimento assumem cada vez maior relevância em todas as atividades da vida cotidiana.
- Inclui as melhores práticas nacionais e internacionais na matéria.
- Propõe uma série de padrões flexíveis que possam facilitar sua adoção entre os Estados Ibero-Americanos, sem infringir de qualquer maneira seu direito interno, de maneira tal que esse documento seja uma realidade viva e viável na região ibero-americana, em benefício do próprio titular.
- Garante um nível adequado de proteção dos dados pessoais na região ibero-americana, com o fim de não estabelecer barreiras para sua livre circulação nos Estados Ibero-Americanos e, em consequência, favorecer as atividades comerciais entre a região, bem como com outras regiões econômicas.

Por outro lado, e não menos importante, os Padrões Ibero-Americanos permitirão reforçar a posição da Rede no âmbito internacional. Para isso, iniciativas serão implementadas nos diversos fóruns internacionais (Comissão Europeia, Conferência Internacional de Autoridades de Proteção de Dados e Privacidade, Organização dos Estados Americanos, etc.), tentando procurar a maior difusão possível dos mesmos.

Em definitiva, o trabalho efetuado pelas entidades que integram a RIPD, que levou finalmente à aprovação dos citados Padrões, constitui uma experiência concreta de cooperação que, a nosso critério, pode ser de grande utilidade para outras organizações, por que ficam à inteira disposição de todas as entidades e profissionais que possam se beneficiar deles, em nome de garantir, da maneira mais eficaz, o possível exercício e tutela do direito à proteção de dados, tanto na região ibero-americana como no contexto internacional.

Os Estados Ibero-Americanos:

- (1) Considerando a proteção das pessoas físicas, relativamente ao tratamento de seus dados pessoais, como direito fundamental reconhecido com categoria máxima na maioria das Constituições Políticas dos Estados Ibero-Americanos, na forma do direito de proteção dos dados pessoais ou *habeas data*, e que, nalguns casos, foi jurisprudencialmente definido por seus Tribunais ou Cortes Constitucionais;
- (2) Determinando que o direito à proteção dos dados pessoais foi conceitualizado em alguns países Ibero-Americanos, legislativamente ou jurisprudencialmente, como direito de natureza diferente dos direitos à vida privada e familiar, à intimidade, à honra, ao bom nome e outros direitos semelhantes, que em conjunto garantem o livre desenvolvimento da personalidade da pessoa física, até se conformarem como direito autônomo, com características e dinâmicas próprias, cujo objeto é a preservação do poder de disposição e do controle que qualquer pessoa física tem respeito da informação que lhe diz respeito, especialmente atendendo ao emprego das tecnologias da informação e das comunicações, que cada vez assumem maior relevância em todos os aspectos da vida cotidiana;
- (3) Assumindo que salvaguardar o direito das pessoas físicas respeito do tratamento de 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 requerem de proteção conforme para resguardar, em sua esfera mais ampla, às pessoas físicas contra intrusões ilegais ou arbitrárias, mesmo daquelas derivadas do tratamento de dados pessoais. O acima mencionado não impede que o direito à proteção dos dados pessoais seja aplicado às pessoas jurídicas, em cumprimento do estabelecido no direito interno dos Estados Ibero-americanos;
- (4) Lembrando que a Rede Ibero-Americana de Proteção de Dados surgiu em virtude do acordo alcançado no Encontro Ibero-Americano de Proteção de Dados, celebrado em La Antigua, Guatemala, entre 01 a 06 de junho de 2003, com a presença de representantes de 14 países ibero-americanos. Esta iniciativa contou, desde o início, com o apoio político refletido na Declaração Final da XIII Cúpula de Chefes de Estado e de Governo dos países Ibero-Americanos, realizada em Santa Cruz de la Sierra, Bolívia, entre 14 e 15 de novembro de 2003, cientes do caráter da proteção de dados pessoais como direito fundamental;

- (5) Tendo em conta que, devido à Resolução adotada na XXV Cúpula Ibero-Americana de Chefes de Estado e de Governo, que teve lugar em Cartagena de Índias, Colômbia, nos dias 28 e 29 de outubro de 2016, reafirmou-se que a adoção, elaboração e impulsionamento de diversos manuais, programas, iniciativas e projetos fortaleceriam a gestão e o impacto das ações de cooperação entre os países da Ibero-América;
- (6) Assumindo que a Rede Ibero-Americana de Proteção de Dados se constitui como fórum permanente de intercâmbio de informação aberto a todos os países membros da Comunidade Ibero-Americana e que possibilita o envolvimento dos setores público, privado e social, com o fim de encorajar desenvolvimentos normativos necessários para garantir uma regulação avançada do direito de proteção dos dados pessoais num contexto democrático e global;
- (7) Lembrando que, em virtude da reunião celebrada em Santa Cruz de la Sierra, Bolívia, entre os dias 03 e 05 de maio de 2006, elaborou-se o documento denominado Diretrizes para a Harmonização da Proteção de Dados na Comunidade Ibero-Americana, que estabelece um conjunto de disposições cujo objeto é contribuir para a elaboração das iniciativas regulamentares de proteção de dados que possam surgir na Comunidade Ibero-Americana, constituindo-se em referência para o desenvolvimento dos presentes Padrões;
- (8) Considerando que a União Europeia tem adotado um novo quadro normativo na matéria, com o objetivo de modernizar suas disposições e garantir maior solidez e coerência na proteção efetiva do direito fundamental à proteção dos dados pessoais na União Europeia e para gerar confiança na sociedade em geral e, por sua vez, facilitar o desenvolvimento da economia digital, tanto no mercado interior como em suas relações globais; quadro normativo que se posiciona como referência obrigatória e determinante na elaboração das legislações nacionais de proteção de dados na Ibero-América;
- (9) Reconhecendo a existência da falta de harmonização nos Estados Ibero-Americanos respeito do reconhecimento, adoção, definição e desenvolvimento das figuras, princípios, direitos e

procedimentos que dão conteúdo ao direito de proteção de dados pessoais em suas legislações nacionais, o qual, sem dúvida, dificulta na atualidade enfrentar os novos desafios na proteção desse direito, derivados da contínua e vertiginosa evolução tecnológica e da globalização em diversos âmbitos;

- (10) Tornando urgente, no âmbito da contínua inovação tecnológica, a adoção de instrumentos regulamentares que, por um lado, garantam a proteção das pessoas físicas em relação ao tratamento de seus dados pessoais e, pelo outro, o livre fluxo dos dados pessoais, que atualmente conformam a base para o desenvolvimento, fortalecimento e intercâmbio de bens e serviços, em uma economia global e digital, sobre os quais são erigidas as economias dos Estados Ibero-Americanos;
- (11) Acordando que, para garantir um alto nível de proteção dos direitos e liberdades das pessoas físicas, entre outras questões, por sua vez, requer-se de nível uniforme e elevado de proteção às pessoas físicas respeito de sua informação pessoal, que responda às necessidades e exigências atuais em um contexto global, com o objetivo de não estabelecer barreiras à livre circulação dos dados pessoais nos Estados Ibero-Americanos e, em consequência, encorajar atividades comerciais entre a região, bem como em outras regiões econômicas;
- (12) Aceitando que, com o propósito de ampliar e fortalecer o regime de proteção às pessoas físicas respeito do tratamento de seus dados pessoais, é imperioso estabelecer um equilíbrio entre os interesses de todos os atores do setor público, privado e social e titulares envolvidos, incluindo o estabelecimento de exceções por questões de interesse público razoáveis e compatíveis com os direitos e liberdades, a fim de evitar incorrer em restrições ou limitações injustificadas ou desproporcionadas, que não estejam em conformidade com os fins perseguidos em sociedades democráticas;
- (13) Cientes dos riscos potenciais que poderiam derivar da esfera das pessoas físicas em função do tratamento de seus dados pessoais em grande escala, efetuado por órgãos públicos e privados e, em particular, considerando a especial vulnerabilidade de crianças e adolescentes, que demandam garantias adequadas e suficientes de proteção perante usos indevidos ou arbitrários de sua informação pessoal, preservando, então, seu interesse superior, o livre desenvolvimento de sua personalidade, sua segurança e outros valores que objeto de máxima proteção por parte dos Estados Ibero-Americanos;

- (14) Acordando que o desenvolvimento tecnológico facilita o tratamento de novas categorias de dados pessoais que apresentam riscos específicos, especialmente o uso inadequado dos mesmos; assim, resulta altamente relevante alcançar um consenso mínimo respeito das categorias de dados pessoais consideradas de caráter sensível ou especialmente protegidas, bem como das regras de tratamento, considerando que as consequências e ingerências negativas que podem derivar do uso indevido deste tipo de dados pessoais podem produzir condições injustas ou discriminatórias para as pessoas físicas;
- (15) Admitindo que nem todos os Estados Ibero-Americanos contam com uma legislação na matéria, situação que pode afetar a preservação e tratamento da informação pessoal, se considerado o acelerado uso das tecnologias da informação que facilitam e possibilitam a comunicação massiva de dados pessoais de maneira 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 nos presentes Padrões, para contar com um contexto regulamentar harmonizado, que ofereça um nível de proteção às pessoas físicas respeito do tratamento de seus dados pessoais e, por sua vez, garantindo o desenvolvimento comercial e econômico da região;
- (17) Admitindo que, atualmente, as bases jurídicas que legitimam qualquer órgão de caráter público ou privado que tratar dados pessoais em seu poder são o consentimento do titular; o cumprimento de uma disposição legal; o cumprimento de ordem judicial, resolução ou mandado fundado e motivado de autoridade pública competente; o exercício de faculdades próprias das autoridades públicas; o reconhecimento ou defesa dos direitos do titular perante autoridades públicas competentes; a execução de contrato ou pré-contrato em que o titular for parte; o cumprimento de obrigação legal aplicável ao responsável; a proteção dos interesses vitais do titular ou de outra pessoa física; o interesse legítimo do órgão público ou privado, ou por razões de interesse público;
- (18) Salientando a necessidade de que os Estados Ibero-Americanos tratem os dados pessoais com os mesmos padrões e regras homogêneas que oferecem aos titulares as mesmas garantias de proteção, através do estabelecimento de um catálogo de princípios de cumprimento obrigatório, que responda aos atuais padrões nacionais e internacionais na matéria, bem como às exigências que

demanda um efetivo exercício e respeito desse direito fundamental;

- (19) Reconhecendo que, com o propósito de garantir de maneira efetiva o direito à proteção dos dados pessoais, é preciso adotar um contexto regulamentar que reconheça a qualquer pessoa física, no caráter de titular de seus dados pessoais, a possibilidade de exercer, por regra geral de maneira gratuita e excepcional com custos associados por razões naturais de reprodução, o envio, certificação ou outras, os direitos de acesso, retificação, cancelamento, oposição e portabilidade, inclusive no contexto de tratamentos de dados pessoais efetuados por motores ou buscadores da Internet; direitos que complementam as condições necessárias para que os titulares possam exercer de maneira plena seu direito à autodeterminação informativa;
- (20) Destacando a importância e o papel fundamental desempenhado pelos prestadores de serviços, que tratam dos dados pessoais em nome e por conta do responsável, incluindo aqueles que prestam serviços de cômputo na nuvem e outras matérias, resultando que os Estados Ibero-Americanos devam adotar, em um mundo globalizado, um regime que permita regular este tipo de serviços, com a finalidade de estabelecer uma série de garantias para a proteção dos dados pessoais que devido a seu encargo possuem e tratam, sem isentar o responsável de suas obrigações e responsabilidades que possui perante titulares e autoridades de controle;
- (21) Considerando que o desenvolvimento das novas tecnologias da informação e das comunicações, bem como dos serviços desenvolvidos no contexto da economia digital, contribuem para o crescimento contínuo dos fluxos transfronteiriços de dados pessoais no âmbito da sociedade global, é inescusável a obrigação de estabelecer uma base mínima que facilite e permita a responsáveis e encarregados, como exportadores, realizar transferências internacionais de dados pessoais com total respeito dos direitos dos titulares;
- (22) Tendo em conta que, através da Internet, é possível acessar e obter informação disponível em qualquer país, bem como efetuar seu tratamento, coletar dados de milhões de pessoas sem domicílio físico, circunstância que não deveria constituir fator de impedimento para a efetiva proteção dos direitos e liberdades das pessoas no ciberespaço;

- (23) Reconhecendo a importância de adotar medidas preventivas que permitam ao responsável responder de maneira proativa perante possíveis problemas relacionados com o direito à proteção de dados pessoais, como à adoção de esquemas de autorregulação vinculante ou sistemas de certificação na matéria; à designação de um oficial de proteção de dados pessoais; à elaboração de avaliações de impacto da proteção de dados pessoais e da privacidade de forma predeterminada e por projeto, entre outras, o que resulta essencial no âmbito das tecnologias da informação e das telecomunicações;
- (24) Admitindo a necessidade imperiosa de que cada Estado Ibero-Americano conte com autoridade de controle independente e imparcial em suas faculdades, cujas decisões somente possam ser recorríveis pelo controle judicial, alheia a 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 na matéria, que possua recursos humanos e materiais suficientes para garantir o exercício de seus poderes e o desempenho efetivo de suas funções;
- (25) Reconhecendo que os Estados Ibero-Americanos são obrigados a adotar um regime que garanta aos titulares um conjunto de mecanismos e procedimentos para apresentar suas reclamações perante a autoridade de controle, quando considerarem vulnerados seus direitos à proteção de dados pessoais, bem como de ser indenizados se tiverem sofrido danos e prejuízos como consequência da violação de seu direito;
- (26) Salientando a importância de estabelecer uma base mínima de cooperação internacional entre as autoridades de controle latino-americanas, e entre elas e as de terceiros países, com a finalidade de favorecer e facilitar a aplicação da legislação na matéria e a efetiva proteção dos titulares;

Convieram em adotar os presentes Padrões como máxima prioridade na Comunidade Ibero-Americana para que, com o caráter de diretrizes orientadoras, contribuam para a emissão de iniciativas regulamentares de proteção de dados pessoais na região dos países que ainda não contam com esses ordenamentos, ou no caso, sirvam de referência para a modernização e atualização das legislações existentes, favorecendo a adoção de um contexto regulamentar harmonizado, que ofereça um nível adequado de proteção às pessoas físicas respeito do tratamento de seus dados pessoais e garantindo, por sua vez, o desenvolvimento comercial e econômico da região, em função do seguinte:

Capítulo I Disposições gerais

1. Objeto

1.1. Os presentes Padrões têm como objetivo:

- a. Estabelecer um conjunto de princípios e direitos de proteção de dados pessoais que os Estados Ibero-Americanos poderão adotar e desenvolver em sua legislação nacional, com o fim de garantir o correspondente tratamento dos dados pessoais e contar com regras homogêneas na região.
- b. Aumentar o nível de proteção das pessoas físicas relativamente ao tratamento de seus dados pessoais, bem como entre os Estados Ibero-Americanos, para responder às necessidades e exigências internacionais demandadas pelo direito à proteção de dados pessoais em uma sociedade onde as tecnologias da informação e do conhecimento assumem cada vez maior relevância em todos os momentos da vida cotidiana.
- c. Garantir o efetivo exercício e tutela do direito à proteção dos dados pessoais de qualquer pessoa física nos Estados Ibero-Americanos, mediante o estabelecimento de regras comuns que assegurem o devido tratamento de seus dados pessoais.
- d. Facilitar o fluxo dos dados pessoais entre os Estados Ibero-Americanos e além de suas fronteiras, com o propósito de coadjuvar no crescimento social e econômico da região.
- e. Impulsionar o desenvolvimento de mecanismos de cooperação internacional entre as autoridades de controle dos Estados Ibero-Americanos, autoridades de controle não pertencentes à região e autoridades e entidades internacionais na matéria.

2. Definições

2.1. Aos efeitos dos presentes Padrões se entenderá por:

- a. **Anonimização:** aplicação de medidas de qualquer natureza voltadas a impedir a identificação ou reidentificação de pessoa física sem esforços desproporcionados.
- b. **Consentimento:** manifestação da vontade, livre, específica, inequívoca e informada do titular, através da qual aceita e autoriza o tratamento dos dados pessoais que lhe dizem respeito.
- c. **Dados Pessoais:** qualquer informação referente a uma pessoa física identificada ou identificável, expressa em forma numérica, alfabética, gráfica, fotográfica, alfanumérica, acústica ou de qualquer outro tipo. Considera-se que uma pessoa é identificável quando sua identidade pode ser determinada direta ou

indiretamente, sempre que isso não demandar prazos ou atividades desproporcionadas.

- d. Dados pessoais sensíveis:** aqueles referidos à esfera íntima do titular ou cuja utilização indevida possa originar discriminação ou derivar em risco grave para ele. De maneira enunciativa, consideram-se sensíveis aqueles dados pessoais que podem revelar aspectos como origem racial ou étnica; crenças ou convicções religiosas, filosóficas e morais; filiação sindical; opiniões políticas; dados relativos à saúde, à vida, preferência ou orientação sexual, dados genéticos ou dados biométricos dirigidos a identificar, de maneira unívoca, uma pessoa física.
- e. Encarregado:** prestador de serviços, que com o caráter de pessoa física ou jurídica ou autoridade pública, alheia à organização do responsável, trata dos dados pessoais em nome e por conta dele.
- f. Exportador:** pessoa física ou jurídica de índole privada, autoridade pública, serviços, órgão ou prestador de serviços localizado no território de um Estado que efetuar transferências internacionais de dados pessoais, conforme estabelecido nos presentes Padrões.
- g. Responsável:** pessoa física ou jurídica de índole privada, autoridade pública, serviços ou órgão que, só ou em conjunto com outros, determina fins, meios, alcance e outras questões relacionadas com o tratamento de dados pessoais.
- h. Titular:** pessoa física a quem diz respeito os dados pessoais.
- i. Tratamento:** qualquer operação ou conjunto de operações efetuadas mediante procedimentos físicos ou automatizados, realizadas sobre dados pessoais, relacionadas, de maneira enunciativa mais não limitativa, com a obtenção, acesso, registro, organização, estruturação, adaptação, indexação, modificação, extração, consulta, armazenamento, conservação, elaboração, transferência, difusão, poder, aproveitamento e, em geral, quaisquer usos ou disposições de dados pessoais.

3. Âmbito de aplicação subjetivo

3.1. Os presentes Padrões serão aplicáveis às pessoas físicas ou jurídicas de índole privada, autoridades e órgãos públicos, que tratem dados pessoais no exercício de suas atividades e funções.

4. Âmbito de aplicação objetivo

4.1. Os presentes Padrões serão aplicáveis ao tratamento de dados pessoais que estejam em suportes físicos, automatizados total ou parcialmente, ou em ambos suportes, independente da forma ou da modalidade de sua criação, tipo de suporte, processamento,

armazenamento e organização.

4.2. Como regra geral, os presentes Padrões serão aplicáveis aos dados pessoais de pessoas físicas, o que não impede que os Estados Ibero-Americanos, em sua legislação nacional, disponham que a informação das pessoas jurídicas seja salvaguardada segundo o direito à proteção dos dados pessoais, em cumprimento do estabelecido em seu direito interno.

4.3. Os Padrões não serão de aplicação nas seguintes situações:

- a. Quando os dados pessoais estiverem destinados a atividades exclusivamente no âmbito da vida familiar ou doméstica da pessoa física, isto é, quando da utilização de dados pessoais em ambiente de amizade, parentesco ou grupo pessoal próximo, e quando não tiverem como propósito divulgação ou utilização comercial.
- b. A informação anônima, isto é, aquela que não estiver relacionada com uma pessoa física identificada ou identificável, bem como os dados pessoais submetidos a processo de anonimização, de forma tal que o titular não possa ser identificado ou reidentificado.

4.4. A legislação nacional dos Estados Ibero-Americanos aplicável na matéria poderá estabelecer categorias de dados pessoais nas quais não poderá ser aplicado o regime de proteção previsto nos presentes Padrões, em cumprimento do direito interno.

5. Âmbito de aplicação territorial

5.1. Os Padrões serão de aplicação no tratamento de dados pessoais efetuado:

- a. Por responsável ou encarregado estabelecido em território dos Estados Ibero-Americanos.
- b. Por responsável ou encarregado não estabelecido em território dos Estados Ibero-Americanos, quando as atividades do tratamento estiverem relacionadas com a oferta de bens ou serviços dirigidos aos residentes dos Estados Ibero-Americanos, ou, relacionadas com o controle de seu comportamento, na medida em que este acontecer nos Estados Ibero-Americanos.
- c. Por responsável ou encarregado não estabelecido em um Estado Ibero-Americano, mas que lhe for aplicável a legislação nacional desse Estado, derivado da celebração de contrato ou em virtude do direito internacional público.
- d. Por responsável ou encarregado não estabelecido em território dos Estados Ibero-Americanos e que utilizar ou empregar meios,

automatizados ou não, localizados nesse território para tratar dados pessoais, exceto que esses meios sejam utilizados somente com fins de trânsito.

5.2. Aos efeitos dos presentes Padrões, se entenderá por estabelecimento o lugar da administração central ou principal do responsável ou encarregado, que deverá ser determinado em função de critérios objetivos e compreender o exercício efetivo e real das atividades de gestão que determinem as principais decisões, quanto aos fins e meios do tratamento de dados pessoais que realizar através de modalidades estáveis.

5.3. A presença e 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 critérios determinantes para a definição do estabelecimento principal do responsável ou encarregado.

5.4. Quando for realizado o tratamento de dados pessoais por grupo empresarial, o estabelecimento principal da empresa que exercer o controle deve ser considerado o estabelecimento principal do grupo empresarial, exceto quando os fins e meios do tratamento forem efetivamente determinados por outra das empresas do grupo.

6. Exceções gerais ao direito à proteção de dados pessoais.

6.1. A legislação nacional dos Estados Ibero-Americanos aplicável na matéria poderá limitar o direito à proteção de dados para preservar a segurança nacional, a segurança pública, a proteção da saúde pública, a proteção dos direitos e das liberdades de terceiros, bem como por questões de interesse público.

6.2. As limitações e restrições serão reconhecidas de maneira expressa na lei, com o propósito de oferecer certeza suficiente aos titulares sobre a natureza e alcance da medida.

6.3. Qualquer lei que tiver como propósito limitar o direito à proteção de dados pessoais conterà, no mínimo, disposições relativas:

- a. À finalidade do tratamento.
- b. Às categorias de dados pessoais correspondentes.
- c. Ao alcance das limitações estabelecidas.
- d. Às garantias adequadas para evitar acessos ou transferências ilícitas ou desproporcionadas.

- e. À determinação do responsável ou responsáveis.
- f. Aos prazos de conservação dos dados pessoais.
- g. Aos possíveis riscos para os direitos e liberdades dos titulares.
- h. Ao direito dos titulares a serem informados sobre a limitação, salvo que for prejudicial ou incompatível com os fins desta.

6.4. As leis serão as necessárias, adequadas e proporcionais em uma sociedade democrática, e deverão respeitar os direitos e as liberdades fundamentais dos titulares.

7. Consideração do direito de proteção de dados pessoais

7.1. Os Estados Ibero-Americanos poderão isentar, em seu direito interno, do cumprimento dos princípios e direitos previstos nos presentes Padrões, exclusivamente na medida em que for necessário conciliar o direito à proteção de dados pessoais com outros direitos e liberdades fundamentais.

7.2. Essa isenção demandará um exercício de consideração, com a finalidade de determinar a necessidade, idoneidade e proporcionalidade da restrição ou exceção, conforme as regras e critérios que estabeleçam os Estados Ibero-Americanos em seu direito interno.

8. Tratamento de dados pessoais de crianças e adolescentes

8.1. No tratamento de dados pessoais relativos a crianças e adolescentes, os Estados Ibero-Americanos privilegiarão a proteção do interesse superior deles, conforme a Convenção sobre os Direitos da Criança e outros instrumentos internacionais que procurem seu bem-estar e proteção integral.

8.2. Os Estados Ibero-Americanos encorajarão, na formação acadêmica das crianças e adolescentes, o uso responsável, adequado e seguro das tecnologias da informação e comunicação, e os eventuais riscos que enfrentam em ambientes digitais respeito do tratamento inadequado de seus dados pessoais, bem como o respeito de seus direitos e liberdades.

9. Tratamento de dados pessoais de caráter sensível

9.1. Por regra geral, o responsável não poderá tratar dados pessoais sensíveis, exceto em quaisquer das seguintes hipóteses:

- a. Que forem estritamente necessários para o exercício e cumprimento das atribuições e obrigações expressamente previstas nas normas que regulam sua atuação.

- b. Dar cumprimento a um mandado legal.
- c. Contar com o consentimento expresso e por escrito do titular.
- d. Forem necessários por motivos de segurança nacional, segurança pública, ordem pública, saúde pública ou salvaguarda de direitos e liberdades de terceiros.

9.2. A legislação nacional dos Estados Ibero-Americanos aplicável na matéria poderá estabelecer exceções, garantias e condições adicionais para garantir o devido tratamento dos dados pessoais sensíveis, conforme seu direito interno.

Capítulo II

Princípios de proteção de dados pessoais

10. Princípios aplicáveis ao tratamento de dados pessoais

10.1. No tratamento dos dados pessoais, o responsável respeitará os princípios de legitimação, licitude, lealdade, transparência, finalidade, proporcionalidade, qualidade, responsabilidade, segurança e confidencialidade.

11. Princípio de legitimação

11.1. Como regra geral, o responsável só poderá tratar dados pessoais quando surgir alguma das seguintes hipóteses:

- a. O titular brindar seu consentimento para uma ou várias finalidades específicas.
- b. O tratamento for necessário para cumprir ordem judicial, resolução ou mandado fundado e motivado de autoridade pública competente.
- c. O tratamento for necessário para o exercício de faculdades próprias das autoridades públicas ou realizado em virtude de habilitação legal.
- d. O tratamento for necessário para o reconhecimento ou defesa dos direitos do titular perante autoridade pública.
- e. O tratamento for necessário para a execução de contrato ou pré-contrato, em que o titular for parte.
- f. O tratamento for necessário para cumprir uma obrigação legal aplicável ao responsável.
- g. O tratamento for necessário para proteger interesses vitais do titular ou de outra pessoa física.
- h. O tratamento for necessário por motivos de interesse público estabelecidos ou previstos na lei.
- i. O tratamento for necessário para atender aos interesses legítimos perseguidos pelo responsável ou por terceiros, sempre que sobre

esses interesses não prevaleçam os interesses ou direitos e liberdades fundamentais do titular que requer da proteção de dados pessoais, especialmente quando o titular for criança ou adolescente. O acima mencionado não será aplicável em tratamentos de dados pessoais realizados por autoridades públicas no exercício de suas funções.

11.2. Tratando-se desse último inciso, entender-se-á amparado pelo interesse legítimo o tratamento de dados pessoais de contato imprescindíveis para a localização de pessoas físicas que prestam serviços ao responsável, com a finalidade de manter qualquer tipo de relação com esta.

12. Condições para o consentimento

12.1. Quando for necessário obter o consentimento do titular, o responsável demonstrará, de maneira indubitável, que o titular ofereceu seu consentimento, seja através de declaração ou de ação afirmativa clara.

12.2. Sempre que for preciso consentimento para tratamento de dados pessoais, o titular poderá revogá-lo em qualquer momento. Para esse fim, o responsável estabelecerá mecanismos simples, ágeis, eficazes e gratuitos.

13. Consentimento para tratamento de dados pessoais de crianças e adolescentes

13.1. Na obtenção do consentimento de crianças e adolescentes, o responsável obterá a autorização do titular do poder familiar ou tutela, conforme disposto nas regras de representação previstas no direito interno dos Estados Ibero-Americanos, ou no caso, solicitará diretamente autorização ao menor de idade, se o direito interno de cada Estado Ibero-Americano estabelecer idade mínima para a concessão direta e sem qualquer representação do titular do poder familiar ou tutela.

13.2. O responsável realizará esforços razoáveis para verificar se o consentimento foi concedido pelo titular do poder familiar ou tutela, ou então, pelo menor diretamente atendendo sua idade de acordo com o direito interno de cada Estado Ibero-Americano considerando a tecnologia disponível.

14. Princípio de licitude

14.1. O responsável tratará os dados pessoais que estiverem em seu poder com rigoroso apego e cumprimento do previsto no direito interno do Estado Ibero-Americano que for aplicável, do direito internacional e dos direitos e liberdades das pessoas.

14.2. O tratamento de dados pessoais realizado por autoridades públicas ficará sujeito às faculdades ou atribuições que o direito interno do Estado Ibero-Americano correspondente lhes conferir expressamente, além do previsto no número acima nos presentes Padrões.

15. Princípio de lealdade

15.1. O responsável tratará os dados pessoais que estiverem em seu poder priorizando a proteção dos interesses do titular e se abstendo de tratá-los através de meios enganosos ou fraudulentos.

15.2. Aos efeitos dos presentes Padrões, serão considerados desleais os tratamentos de dados pessoais que envolvam discriminação injusta ou arbitrária contra os titulares.

16. Princípio de transparência

16.1. O responsável informará ao titular sobre a existência e características principais do tratamento a que serão submetidos seus dados pessoais, a fim de poder tomar decisões informadas ao respeito.

16.2. O responsável proporcionará ao titular, no mínimo, a seguinte informação:

- a. Identidade e dados de contato.
- b. As finalidades do tratamento que receberão seus dados pessoais.
- c. Comunicações nacionais ou internacionais de dados pessoais que tencione realizar, incluindo destinatários e finalidades que motivam sua realização.
- d. A existência, forma e mecanismos ou procedimentos através dos quais exercerá os direitos de acesso, retificação, cancelamento, oposição e portabilidade.
- e. No caso, a origem dos dados pessoais quando o responsável não os obtiver diretamente do titular.

16.3. A informação proporcionada ao intitular deve ser suficiente e de fácil acesso, bem como redigida e estruturada em linguagem clara, simples e de fácil compreensão para os titulares aos quais estará dirigida, especialmente se tratando de crianças e adolescentes.

16.4. Todo responsável contará com políticas transparentes para os tratamentos de dados pessoais que realizar.

17. Princípio de finalidade

17.1. Todo tratamento de dados pessoais estará limitado ao cumprimento de finalidades determinadas, explícitas e legítimas.

17.2. O responsável não poderá tratar os dados pessoais em seu poder com fins diferentes dos que motivaram seu tratamento original, exceto pela ocorrência de alguma das causas que possibilitam um novo tratamento dos dados, conforme o princípio de legitimação.

17.3. O tratamento posterior de dados pessoais com fins de arquivamento, pesquisa científica e histórica, ou com fins estatísticos, todos eles em favor do interesse público, não será considerado incompatível com as finalidades iniciais.

18. Princípio de proporcionalidade

18.1 O responsável somente tratará os dados pessoais que forem adequados, pertinentes e limitados para o mínimo necessário em relação às finalidades que justifiquem seu tratamento.

19. Princípio de qualidade

19.1. O responsável adotará as medidas necessárias para manter exatos, completos e atualizados os dados pessoais em seu poder, de maneira tal a não alterar sua veracidade, conforme requerido para o cumprimento das finalidades que motivaram o tratamento.

19.2. Quando os dados pessoais já não sejam necessários para o cumprimento das finalidades que motivaram o tratamento, o responsável os suprimirá ou eliminará de seus arquivos, registros, bases de dados, dossiês ou sistemas de informação, ou no caso, deverá submetê-los a um procedimento de anonimização.

19.3. Na supressão dos dados pessoais, o responsável implementará métodos e técnicas orientadas à sua eliminação definitiva e segura.

19.4. Os dados pessoais somente serão conservados durante o prazo necessário para o cumprimento das finalidades que justifiquem seu tratamento, ou aquelas relacionadas com exigências legais aplicáveis ao responsável. Porém, a legislação nacional dos Estados Ibero-Americanos aplicável na matéria poderá estabelecer exceções respeito do prazo de conservação dos dados pessoais, respeitando totalmente os direitos e garantias do titular.

20. Princípio de responsabilidade

20.1. O responsável implementará os mecanismos necessários para demonstrar o cumprimento dos princípios e obrigações estabelecidas nos presentes Padrões, bem como prestará contas sobre o tratamento de dados

personais em seu poder para o titular e a autoridade de controle, para o que poderá empregar padrões, melhores práticas nacionais ou internacionais, esquemas de autorregulação, sistemas de certificação ou quaisquer outros mecanismos que determinar adequado para tais fins.

20.2. O acima mencionado corresponderá quando os dados pessoais forem tratados por encarregado em nome e por conta do responsável, bem como no momento de realizar transferências de dados pessoais.

20.3. Entre os mecanismos que o responsável poderá adotar para cumprir com o princípio de responsabilidade encontram-se, de maneira enunciativa mais não limitativa, os seguintes:

- a. Alocação de recursos para instrumentação de programas e políticas de proteção de dados pessoais.
- b. Implementação de sistemas de gestão de riscos associados com o tratamento de dados pessoais.
- c. Elaboração de políticas e programas de proteção de dados pessoais obrigatórios e exigíveis ao interior da organização do responsável.
- d. Pôr em prática um programa de capacitação e atualização do pessoal sobre obrigações em matéria de proteção de dados pessoais.
- e. Rever de maneira periódica as políticas e programas de segurança de dados pessoais, para determinar as modificações requeridas.
- 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 dúvidas e reclamações dos titulares.

20.4. O responsável conferirá e avaliará em forma permanente os mecanismos que, para tal efeito, adotar voluntariamente para cumprir com o princípio de responsabilidade, com o objeto de medir seu nível de eficácia quanto ao cumprimento da legislação nacional aplicável.

21. Princípio de segurança

21.1. O responsável estabelecerá e manterá, independentemente do tipo de tratamento que efetuar, medidas de índole administrativa, física e técnica suficientes para garantir a confidencialidade, integridade e disponibilidade dos dados pessoais.

21.2. Para a determinação das medidas citadas no número acima, o responsável considerará os seguintes fatores:

- a. O risco para os direitos e liberdades dos titulares, em particular, pelo valor potencial quantitativo e qualitativo que pudessem ter os dados pessoais tratados para terceiras pessoas não autorizadas para sua posse.
- b. O estado da técnica.
- c. Os custos de aplicação.
- d. A natureza dos dados pessoais tratados, especialmente dados pessoais sensíveis.
- e. Alcance, contexto e finalidades do tratamento.
- f. Transferências internacionais de dados pessoais realizadas ou que pretendam ser realizadas.
- g. Número de titulares.
- h. Possíveis consequências para os titulares derivadas de vulneração.
- i. Vulnerações prévias acontecidas no tratamento de dados pessoais.

21.3. O responsável realizará um conjunto de ações visando garantir o estabelecimento, implementação, operação, monitoração, revisão, manutenção e melhoria contínua das medidas de segurança aplicáveis ao tratamento dos dados pessoais, de maneira periódica.

22. Notificação de vulnerações na segurança dos dados pessoais

22.1. Quando o responsável tiver conhecimento de vulneração na segurança dos dados pessoais acontecida em qualquer fase do tratamento, entendida como qualquer dano, perda, alteração, destruição, acesso, e em geral, qualquer uso ilícito ou não autorizado de dados pessoais, mesmo quando acontecer de maneira acidental, notificará à autoridade de controle e aos titulares afetados nesse acontecimento imediatamente.

22.2. O acima mencionado não resultará aplicável quando o responsável puder demonstrar, atendendo ao princípio de responsabilidade proativa, a improbabilidade de vulneração da segurança acontecida, ou que ela não representa risco para os direitos e liberdades dos titulares envolvidos.

22.3. A notificação realizada pelo responsável para os titulares afetados estará redigida em linguagem clara e simples.

22.4. A notificação referida nos números acima conterà, no mínimo, a seguinte informação:

- a. Natureza do incidente.

- b. Dados pessoais comprometidos.
- c. Ações de correção realizadas de forma imediata.
- d. Recomendações para o titular sobre medidas que poderia adotar para proteger seus interesses.
- e. Meios disponíveis para o titular para obter mais informações sobre a questão.

22.5. O responsável documentará qualquer vulneração à segurança de dados pessoais acontecida em qualquer fase do tratamento, identificando, de maneira enunciativa mais não limitativa, a data em que aconteceu; o motivo da vulneração; os fatos relacionados e seus efeitos e medidas corretivas implementadas de forma imediata e definitiva, que estarão à disposição da autoridade de controle.

22.6. A legislação nacional dos Estados Ibero-Americanos aplicável na matéria estabelecerá os efeitos das notificações de vulnerações de segurança realizadas pelo responsável à autoridade de controle, no referente a procedimentos, forma e condições de intervenção, com o propósito de preservar os interesses, direitos e liberdades dos titulares afetados.

23. Princípio de confidencialidade

23.1. O responsável estabelecerá controles ou mecanismos para que quem intervir em qualquer fase do tratamento dos dados pessoais mantenha e respeite sua confidencialidade, obrigação que continuará, inclusive, após finalizar sua relação com o titular.

Capítulo III Direitos do titular

24. Direitos ARCO

24.1. Em todo momento, o titular ou seu representante poderão solicitar ao responsável o acesso, retificação, cancelamento, oposição e portabilidade dos dados pessoais relacionados.

24.2. O exercício de quaisquer dos direitos referidos no número acima não é requisito prévio, nem impede o exercício de outro.

25. Direito de acesso

25.1. O titular terá direito de solicitar o acesso a seus dados pessoais em poder do responsável, bem como de conhecer qualquer informação relacionada com as condições gerais e específicas de seu

tratamento.

26. Direito de retificação

26.1. O titular terá direito de obter do responsável a retificação ou correção de seus dados pessoais, quando esses resultarem inexatos, incompletos ou não se encontrarem atualizados.

27. Direito de cancelamento

27.1. O titular terá direito de solicitar o cancelamento ou supressão de seus dados pessoais de arquivos, registros, processos e sistemas do responsável, a fim de que já não estejam em seu poder e deixem de ser tratados por este último.

28. Direito de oposição

28.1. O titular poderá se opor ao tratamento de seus dados pessoais quando:

- a. Existir razão legítima derivada de situação particular.
- b. O tratamento de seus dados pessoais tiver como objetivo marketing direto, incluída a elaboração de perfis, na medida em que estiver relacionada com essa atividade.

28.2 Tratando-se do inciso acima, quando o titular se opuser ao tratamento com fins de marketing direto, seus dados pessoais deixarão de ser tratados para esses fins.

29. Direito a não ser objeto de decisões individuais automatizadas

29.1. O titular terá direito de não ser objeto de decisões que possam produzir efeitos jurídicos ou o afetem de maneira significativa, baseados somente em tratamentos automatizados destinados a avaliar, sem intervenção humana, determinados aspectos pessoais ou analisar ou prever, em particular, seu rendimento profissional, situação econômica, estado de saúde, preferências sexuais, confiabilidade ou comportamento.

29.2. O previsto no número acima não será aplicável quando o tratamento automatizado de dados pessoais for necessário para a celebração ou execução de contrato entre o titular e o responsável; estiver autorizado pelo direito interno dos Estados Ibero-Americanos, ou tiver como base o consentimento demonstrável do titular.

29.3. Contudo, quando for necessário para a relação contratual ou o titular tiver manifestado seu consentimento, terá direito de obter intervenção humana; receber uma explicação sobre a decisão tomada; expressar seu ponto de vista e impugnar a decisão.

29.4. O responsável não poderá realizar tratamentos automatizados de dados pessoais que tiverem como efeito a discriminação dos titulares por origem racial ou étnica; crenças ou convicções religiosas, filosóficas e morais; filiação sindical; opiniões políticas; dados relativos à saúde, à vida, preferência ou orientação sexual, bem como dados genéticos ou dados biométricos.

30. Direito à portabilidade dos dados pessoais

30.1. Ao tratar dados pessoais por via eletrônica ou meios automatizados, o titular terá direito de obter cópia dos dados pessoais que informou ao responsável ou que são alvo de tratamento, em formato eletrônico estruturado, de uso comum e leitura mecânica, que permita continuar utilizando-os e transferi-los para outro responsável, em caso necessário.

30.2. O titular poderá solicitar que seus dados pessoais sejam transferidos diretamente de responsável para responsável, quando isso for tecnicamente possível.

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

30.4. Sem prejuízo de outros direitos do titular, o direito à portabilidade dos dados pessoais não resultará procedente quando for informação inferida, derivada, criada, gerada ou obtida a partir da análise ou tratamento efetuado pelo responsável com base nos dados pessoais informados pelo titular, como o caso dos dados pessoais submetidos a um processo de personalização, recomendação, categorização ou criação de perfis.

31. Direito à limitação do tratamento dos dados pessoais

31.1. O titular terá direito a que o tratamento dos dados pessoais se limite ao armazenamento durante o período decorrido entre uma solicitação de retificação ou oposição até a resolução pelo responsável.

31.2. O titular terá direito à limitação do tratamento de seus dados pessoais quando esses forem desnecessários para o responsável, mas precisar deles para formular uma reclamação.

32. Exercício dos direitos ARCO e de portabilidade

32.1. O responsável estabelecerá meios e procedimentos simples, rápidos, acessíveis e gratuitos que permitam ao titular exercer seus direitos de acesso, retificação, cancelamento, oposição e portabilidade.

32.2. A legislação nacional dos Estados Ibero-Americanos aplicável na matéria estabelecerá requerimentos, prazos, termos e condições nos quais os titulares poderão exercer seus direitos de acesso, retificação, cancelamento, oposição e portabilidade, bem como as causas de improcedência no exercício que podem ser, de maneira enunciativa mais não limitativa:

- a. Quando o tratamento for necessário para cumprir um objetivo importante de interesse público.
- b. Quando o tratamento for necessário para exercer as funções próprias das autoridades públicas.
- c. Quando o responsável consignar que possui motivos legítimos para que o tratamento prevaleça sobre interesses, direitos e liberdades do titular.
- d. Quando o tratamento for necessário para cumprir com disposição legal.
- e. Quando os dados pessoais forem necessários para manter ou cumprir uma relação jurídica ou contratual.

32.3. A legislação nacional dos Estados Ibero-Americanos aplicável na matéria poderá reconhecer que pessoas físicas, vinculadas com falecidos ou designados por eles, possam exercer os direitos referidos no presente padrão, respeito dos dados pessoais de falecido que lhes digam respeito.

32.4. A legislação nacional dos Estados Ibero-Americanos aplicável na matéria reconhecerá o direito do titular de não concordar ou impugnar respostas concedidas pelo responsável perante uma solicitação de exercício dos direitos aludidos no presente número, ou perante sua falta de resposta junto a autoridade de controle e, no caso, perante instâncias judiciais, conforme o direito interno de cada Estado Ibero-Americano.

Capítulo IV Encarregado

33. Alcance do encarregado

33.1. O encarregado realizará atividades de tratamento dos dados pessoais sem possuir nenhum poder de decisão sobre o seu alcance e conteúdo, bem como limitará suas atuações aos termos previstos pelo

responsável.

34. Formalização da prestação de serviços do encarregado

34.1. A prestação de serviços entre o responsável e o encarregado será formalizada mediante assinatura de contrato ou qualquer outro instrumento jurídico que considerarem os Estados Ibero-Americanos na legislação nacional aplicável na matéria.

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

34.3. O contrato ou instrumento jurídico estabelecerá, no mínimo, as seguintes cláusulas gerais relacionadas com os serviços prestados pelo encarregado:

- a. Realizar o tratamento dos dados pessoais conforme as instruções do responsável.
- b. Abster-se de tratar dados pessoais para fins diferentes dos instruídos pelo responsável.
- c. Implementar medidas de segurança conforme os instrumentos jurídicos aplicáveis.
- d. Informar o responsável do acontecimento de vulneração nos dados pessoais que tratar por suas instruções.
- e. Preservar a confidencialidade dos dados pessoais tratados.
- f. Suprimir, devolver ou comunicar para um novo encarregado designado pelo responsável os dados pessoais objeto de tratamento, uma vez cumprida a relação jurídica com o responsável ou por instruções desse, exceto que disposição legal exigir a conservação dos dados pessoais ou que o responsável autorizar sua comunicação a outro encarregado.
- g. Abster-se de transferir dados pessoais, salvo no caso em que o responsável assim estabelecer, ou a comunicação derivar de uma subcontratação, ou por pedido expresso da autoridade de controle.
- h. Permitir ao responsável ou autoridade de controle inspeções e verificações no local.
- i. Gerar, atualizar e conservar a documentação necessária e que permita a acreditação de suas obrigações.
- j. Colaborar com o responsável em tudo o relativo ao cumprimento da legislação nacional do Estado Ibero-Americano que for aplicável na matéria.

34.4. Quando o encarregado descumprir as instruções do responsável e decidir por si mesmo sobre o alcance, conteúdo, meios e outras questões do tratamento dos dados pessoais assumirá o caráter de responsável, conforme a legislação nacional do Estado Ibero-Americano que for aplicável na matéria.

35. Subcontratação de serviços

35.1. Por sua vez, o encarregado poderá subcontratar serviços que compreendam o tratamento de dados pessoais, sempre que existir autorização prévia por escrito, específica ou geral do responsável, ou for estipulado expressamente no contrato ou instrumento jurídico subscrito entre este e o encarregado.

35.2. O subcontratado assumirá o caráter de encarregado, nos termos estipulados pela legislação nacional do Estado Ibero-Americano aplicável na matéria.

35.3. O encarregado formalizará a prestação de serviços do subcontratado através de contrato ou de quaisquer outros instrumentos jurídicos determinados pela legislação nacional do Estado Ibero-Americano que for aplicável na matéria.

35.4. Quando o subcontratado descumprir suas obrigações e responsabilidades respeito do tratamento dos dados pessoais, conforme instruído pelo encarregado, assumirá o caráter de responsável segundo a legislação nacional do Estado Ibero-Americano que for aplicável na matéria.

Capítulo V

Transferências internacionais de dados pessoais

36. Regras gerais para transferências de dados pessoais

36.1. O responsável e o encarregado poderão realizar transferências internacionais de dados pessoais em quaisquer dos seguintes casos:

- a. O país, parte de seu território, setor, atividade ou organização internacional destinatária dos dados pessoais tiver sido reconhecido com nível adequado de proteção de dados pessoais por parte do país transferente, conforme a legislação nacional desse que resultar aplicável na matéria, ou então, o país destinatário ou vários setores dele consignarem condições mínimas e suficientes para garantir um adequado nível de proteção dos dados pessoais.

- b. O exportador ofereça garantias suficientes do tratamento dos dados pessoais no país destinatário, e este, por sua vez, acreditar o cumprimento das condições mínimas e suficientes estabelecidas na legislação nacional de cada Estado Ibero-Americano aplicável na matéria.
- c. Exportador e destinatário subscreverem cláusulas contratuais ou qualquer outro instrumento jurídico que ofereça garantias suficientes e que permita demonstrar o alcance do tratamento dos dados pessoais, das obrigações e responsabilidades assumidas pelas partes e dos direitos dos titulares. A autoridade de controle poderá validar cláusulas contratuais ou instrumentos jurídicos segundo determinar na legislação nacional dos Estados Ibero-Americanos aplicável na matéria.
- d. Exportador e destinatário adotarem um esquema de autorregulação vinculante ou mecanismo de certificação aprovado, sempre que seja conforme as disposições previstas na legislação nacional do Estado Ibero-Americano aplicável na matéria, que o exportador estará obrigado a observar.
- e. A autoridade de controle do Estado Ibero-Americano do país do exportador autorizar a transferência, em termos da legislação nacional que for aplicável na matéria.

36.2. A legislação nacional dos Estados Ibero-Americanos aplicável na matéria poderá estabelecer expressamente limites às transferências internacionais de categorias de dados pessoais por razões de segurança, segurança pública, proteção à saúde pública, proteção dos direitos e liberdades de terceiros, bem como questões de interesse público.

Capítulo VI

Medidas proativas no tratamento de dados pessoais

37. Reconhecimento de medidas proativas

37.1. A legislação nacional dos Estados Ibero-Americanos aplicável na matéria poderá reconhecer e estabelecer medidas que promovam o melhor cumprimento de sua legislação e coadjuvem no fortalecimento e aumento dos controles de proteção de dados pessoais implementados pelo responsável, entre os quais poderão se encontrar as indicadas abaixo no presente Capítulo.

38. Privacidade por projeto e privacidade por defeito

38.1. O responsável aplicará, a partir do projeto, na determinação dos meios de tratamento dos dados pessoais, durante e antes de solicitar os dados pessoais, medidas preventivas de diversa natureza que permitam aplicar de maneira efetiva princípios, direitos e outras obrigações previstas

na legislação nacional do Estado Ibero-Americano que lhe for aplicável.

38.2. O responsável garantirá que seus programas, serviços, sistemas ou plataformas informáticas, aplicações eletrônicas ou qualquer outra tecnologia que impliquem tratamento de dados pessoais, cumpram por defeito ou se ajustem aos princípios, direitos e outras obrigações previstas na legislação nacional do Estado Ibero-Americano que lhe for aplicável. Especificamente, somente com o fim de serem objeto de tratamento os mínimos dados pessoais e limitar a acessibilidade deles, sem a intervenção do titular, a um número indeterminado de pessoas.

39. Oficial de proteção de dados pessoais

39.1. O responsável designará um oficial de proteção de dados pessoais ou figura equivalente, nos casos estabelecidos pela legislação nacional dos Estados Ibero-Americanos aplicável na matéria e quando:

- a. For autoridade pública.
- b. Realizar tratamentos de dados pessoais que tiverem como objeto a observação habitual e sistemática da conduta do titular.
- c. Realizar tratamentos de dados pessoais onde for provável um alto risco de afetação do direito à proteção de dados pessoais dos titulares, considerando, entre outros fatores e de maneira enunciativa mais não limitativa, categorias de dados pessoais tratados, especialmente se tratando de dados sensíveis; transferências efetuadas; número de titulares; alcance do tratamento; tecnologias de informação utilizadas ou finalidades destes.

39.2. O responsável que não se encontrar nalguma das causas previstas no número acima, poderá designar um oficial de proteção de dados pessoais, se assim estimar conveniente.

39.3. O responsável estará obrigado a apoiar o oficial de proteção de dados pessoais no desempenho de suas funções, facilitando os recursos necessários para seu desempenho e para a manutenção de seus conhecimentos especializados e a atualização desses.

39.4. O oficial de proteção de dados pessoais terá, no mínimo, as seguintes funções:

- a. Assessorar o responsável respeito dos temas submetidos a sua consideração em matéria de proteção de dados pessoais.
- b. Coordenar, no interior da organização do responsável, políticas, programas, ações e outras atividades que correspondam com o

cumprimento da legislação nacional do Estado Ibero-Americano que resultar aplicável na matéria.

- c. Supervisionar no interior da organização do responsável o cumprimento da legislação nacional do Estado Ibero-Americano que resultar aplicável na matéria.

40. Mecanismos de autorregulação

40.1. O responsável poderá se aderir, de maneira voluntária, a esquemas de autorregulação vinculante, cujos objetos forem, entre outros, contribuir para a correta aplicação da legislação nacional do Estado Ibero-Americano que resultar aplicável na matéria e estabelecer procedimentos de resolução de conflitos entre o responsável e o titular, sem prejuízo de outros mecanismos estabelecidos pela legislação nacional da matéria aplicável, considerando as características específicas dos tratamentos de dados pessoais realizados, bem como o efetivo exercício e respeito dos direitos do titular.

40.2. Aos efeitos do número acima, será possível desenvolver, entre outros, códigos deontológicos e sistemas de certificação e seus respectivos selos de confiança, que contribuam para os objetivos assinalados no presente número.

40.3. A legislação nacional dos Estados Ibero-Americanos aplicável na matéria estabelecerá regras que correspondam para a validação, confirmação ou reconhecimento dos mecanismos de autorregulação aludidos.

41. Avaliação de impacto na proteção de dados pessoais

41.1. Quando o responsável pretenda realizar um tipo de tratamento de dados pessoais que, por sua natureza, alcance, contexto ou finalidades, envolva a probabilidade de um alto risco de afetação do direito à proteção de dados pessoais dos titulares, realizará, de maneira prévia à implementação, uma avaliação do impacto na proteção dos dados pessoais.

41.2. A legislação nacional dos Estados Ibero-Americanos que for aplicável na matéria assinalará aqueles tratamentos que demandem avaliação de impacto na proteção de dados pessoais; o conteúdo dessas, as hipóteses nas quais corresponder a apresentação do resultado perante autoridade de controle, bem como os requerimentos da apresentação, entre outras questões.

Capítulo VII Autoridades de controle

42. Natureza das autoridades de controle e supervisão

42.1. Em cada Estado Ibero-Americano deverá existir uma ou mais autoridades de controle em matéria de proteção de dados pessoais com plena autonomia, conforme a legislação nacional aplicável na matéria.

42.2. As autoridades de controle poderão ser órgãos unipessoais ou pluripessoais; atuarão com caráter imparcial e independente em seus poderes, bem como serão alheias a qualquer influência externa, seja direta ou indireta, e não solicitarão nem admitirão ordem nem instrução alguma.

42.3. O membro ou os membros dos órgãos de direção das autoridades de controle contarão com experiência e aptidões, especialmente respeito do âmbito de proteção de dados pessoais, necessários para cumprir suas funções e exercer seus poderes. Serão nomeados, mediante procedimento transparente em virtude da legislação nacional aplicável, e somente poderão ser removidos por causas graves estabelecidas no direito interno de cada Estado Ibero-Americano, conforme as regras do devido processo.

42.4. A legislação nacional dos Estados Ibero-Americanos que resultar aplicável na matéria deverá conceder às autoridades de controle poderes suficientes de investigação, supervisão, resolução, promoção, sanção e outros que resultarem necessários para garantir seu efetivo cumprimento, bem como o exercício e respeito efetivo do direito à proteção de dados pessoais.

42.5. As decisões das autoridades de controle somente estarão sujeitas ao controle jurisdicional, conforme os mecanismos estabelecidos na legislação nacional dos Estados Ibero-Americanos que for aplicável na matéria e seu direito interno.

42.6. As autoridades de controle contarão com os recursos humanos e materiais necessários para o cumprimento de suas funções.

Capítulo VIII Reclamações e Sanções

43. Regime de reclamações e imposição de sanções

43.1. Todo titular terá direito de apresentar sua reclamação perante uma autoridade de controle, bem como de recorrer da tutela judicial para tornar efetivos seus direitos, conforme a legislação nacional

do Estado Ibero-Americano aplicável na matéria.

43.2. A legislação nacional dos Estados Ibero-Americanos aplicável na matéria estabelecerá regime que permitirá ao titular apresentar uma reclamação perante a autoridade de controle quando considerar que o tratamento de seus dados pessoais infringe o regulamento nacional na matéria, assim como solicitar tutela judicial.

43.3. A legislação nacional dos Estados Ibero-Americanos aplicável na matéria estabelecerá regime que permita adotar medidas corretivas e sancionar condutas que contravenham o disposto nas legislações nacionais correspondentes, indicando, no mínimo, o limite máximo e os critérios objetivos para fixar as correspondentes sanções a partir da natureza, gravidade, duração da infração e suas consequências, bem como as medidas implementadas pelo responsável para garantir o cumprimento de suas obrigações na matéria.

Capítulo IX Direito de indenização

44. Reparação do dano

44.1. A legislação nacional dos Estados Ibero-Americanos aplicável na matéria reconhecerá o direito do titular de ser indenizado quando tiver sofrido danos e prejuízos, como consequência de uma violação de seu direito à proteção de dados pessoais.

44.2. O direito interno dos Estados Ibero-Americanos indicará a autoridade competente para receber este tipo de ações apresentadas pelo titular afetado, bem como prazos, requerimentos e termos através dos quais será indenizado, em caso de corresponder.

Capítulo X Cooperação internacional

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 correspondentes na matéria, os quais poderão compreender, de maneira enunciativa mais não limitativa:

- a. O estabelecimento de mecanismos que permitam reforçar a assistência e cooperação internacional na aplicação das respectivas legislações nacionais na matéria.

20 de junho de 2017

- b. A assistência entre as autoridades de controle através da notificação e remissão de reclamações, assistência em investigações e intercâmbio de informação.
- c. A adoção de mecanismos voltados para o conhecimento e intercâmbio das melhores práticas e experiências em matéria de proteção de dados pessoais, inclusive no relativo a conflitos de jurisdição com terceiros países.