GUIA

AMÉRICA LATINA: LEGISLAÇÕES DE PROTEÇÃO DE DADOS

NÚMERO 11/12

A Year in Privacy

Autores:

Dandara Ramos Silvestre da Silva

Gustavo Henrique Luz Silva

Natália Góis Ribeiro

Odélio Porto Júnior

Rafaella Resck Braoios

Revisão Técnica:

Fernando Bousso

Projeto Gráfico:

Lucas Bittencourt

Eliza Natsuko Shiroma

Fernanda Muchon

Sumário

‹voltar para o índice

INTRODUÇÃO

Nesta edição do *A Year in Privacy* (AYIP) são analisadas as normas de proteção de dados de Argentina, Colômbia, Chile e Peru. É examinado de forma ampla as principais normas de proteção de dados de cada país e seu escopo de aplicação; as bases legais que autorizam o uso de dados pessoais; quais os direitos dos titulares dos dados; as principais obrigações de controladores e operadores; as entidades responsáveis pela fiscalização das normas; e as sanções aplicáveis em caso de descumprimento

‹voltar para o índice

01 Argentina

ARGENTINA[1]

Principais normas e escopo

O direito à proteção de dados pessoais foi introduzido no ordenamento jurídico argentino por meio do artigo 43 da Constituição Federal do país de 1994. O artigo estabelece direitos sobre dados pessoais tratados por entidades públicas ou privadas, sendo eles: o de obter informação sobre os dados tratados, a finalidade de tratamento, e a prerrogativa de exigir a eliminação, retificação ou restrição caso os dados sejam falsos ou discriminatórios.

No ano 2000, foi publicada pelo Congresso Nacional da Argentina a Lei de Proteção de Dados Pessoais, lei nº 25.326 de 2000, que estabelece o sistema geral de proteção de dados pessoais do país. Posteriormente, o Decreto nº 1.558 de 2001, e o Decreto nº 1160 de 2010 determinaram regras adicionais para a implementação da lei.

Além disso, no âmbito criminal, o Código Penal Nacional da Argentina estabelece sanções para aqueles que infringirem disposições sobre confidencialidade, veracidade e integridade de dados pessoais, por meio de multa e restrição de liberdade (artigos 117 e 173 da referida legislação).

No contexto de fiscalização, a Argentina dispunha da Direção Nacional de Proteção de Dados Pessoais para regulamentar o cumprimento da lei nº 25.326. Este órgão foi, posteriormente, substituído pela autoridade argentina de proteção de dados, a Agência de Acesso à Informação Pública (AAIP).

Em 2003 a Argentina foi reconhecida pela União Europeia como um país que oferece um nível adequado de proteção para dados pessoais.

Outras normas do ordenamento jurídico argentino regulam o uso de dados pessoais de forma esparsa. Dentre elas, destaca-se o Código Civil e Comercial Nacional que protege o direito à privacidade (artigos 52 e 1.770); e a Lei de Proteção Integral dos Direitos da Criança e do Adolescente (artigo 22).

Em 2018 a AAIP elaborou projeto de lei para substituir a lei de proteção de dados pessoais vigente, a fim de aproximar o cenário regulatório ao da GDPR europeia. Entretanto, o projeto de lei não foi aprovado pelo Congresso. Posteriormente, em 2020, três novos projetos de lei foram apresentados por diferentes partidos políticos, também com objetivo de atualizar as normas de proteção de dados pessoais da argentina (até o momento, nenhum foi aprovado).

1 ROSATI, Florencia. Argentina – Data Protection Overview. OneTrust – DataGuidance. 2021. Disponível em:<https://www.dataguidance.com/notes/argentina-data-protection-overview>. Acesso em: 21/11/2022.

Quanto ao escopo de aplicação, o tratamento de dados é definido como qualquer operação ou procedimento sistemático, eletrônico ou não, que permita a coleta, integração, triagem, armazenamento, alteração, relação, avaliação, bloqueio, destruição, divulgação ou transferência de dados para terceiros.

Dado pessoal é definido como informação de qualquer natureza que se refira a pessoas singulares ou coletivas, identificadas ou identificáveis por associação (artigo 2º, lei nº 25.326). A lei aplica-se aos operadores e controladores de dados, pessoas físicas ou jurídicas, públicas ou privadas.

A lei argentina de proteção de dados pessoais considera dados sensíveis como informações que revelem: origem racial e étnica; opiniões políticas; crenças religiosas, filosóficas ou morais; filiação sindical; e/ou informações sobre saúde ou vida sexual do titular. A AAIP estabelece, ainda, que os dados biométricos que possam identificar uma pessoa são considerados dados sensíveis.

Quanto o aspecto territorial, a legislação de proteção de dados pessoais da Argentina aplica-se sempre que os dados pessoais são tratados no território da Argentina (artigo 44 da lei nº 25.326).

Bases legais

De acordo com a Seção 5 da lei 25.326, o tratamento de dados pessoais só é legal a partir do consentimento prévio do titular do dado, que deve ser livre, expresso (por escrito ou por outros meios que possam ser equiparados à escrita), e informado.

O consentimento para o tratamento de dados pessoais não é necessário quando o dado:

- é obtido de fontes publicamente acessíveis;
- para cumprimento de obrigação legal;
- os dados pessoais se limitam a nome, documento de identidade, nº de identificação do contribuinte, nº previdenciário, profissão, data de nascimento e domicílio;
- o uso esteja amparado em uma relação contratual, científica ou profissional com o titular dos dados; ou
- refere-se às transações realizadas por entidades financeiras (protegidas por regras de sigilo bancário).

É válido ressaltar que os projetos de lei mencionados trazem outras bases legais como, por exemplo, proteção à vida do titular e legítimo interesse.

Direitos dos titulares

A lei nº 25.326 argentina sobre proteção de dados estabelece os seguintes direitos.

I. Direito de ser informado

O titular dos dados deve ser informado de maneira clara e expressa sobre:

- as finalidades para as quais os dados serão tratados;
- os destinatários ou terceiros;
- a existência do banco de dados, e a identidade e endereço de seu controlador;
- se o fornecimento do dado pessoal é obrigatório, e as consequências de se recusar o fornecimento; e
- a possibilidade de acessar, atualizar, corrigir e excluir seus dados e o mecanismo para fazê-lo.

II. Direito de acesso

O titular têm o direito de solicitar e obter informações sobre seus dados pessoais. O controlador ou operador dos dados deverá fornecer as informações solicitadas no prazo de dez dias corridos a partir da solicitação.

III. Direito de retificação

O titular dos dados pode exigir a retificação e, se for caso, a supressão ou confidencialidade dos dados. O responsável pelo tratamento deve atender esse direito no prazo de cinco dias úteis, a contar do recebimento da reclamação do titular dos dados ou do conhecimento do erro.

IV. Direito de não se submeter a decisões automatizadas

Conforme a Resolução 4/2019, caso o responsável pelo tratamento de dados tome decisões baseadas exclusivamente no tratamento automatizado de dados que produzam efeitos jurídicos danosos ou negativos ao titular, o titular terá o direito de solicitar uma explicação da lógica aplicada nessa decisão.

Caso os direitos não sejam atendidos, o titular pode interpor ação judicial especial de proteção de dados pessoais ou habeas data (artigos 33 a 43 da lei nº 25.326).

Obrigações controlador e operador

A lei nº 25.326 não define um conceito para controlador de dados, apenas estabelecendo que o tratamento de dados pessoais se aplica à "pessoa responsável por um banco de dados". A lei também não define expressamente o conceito de operador de dados.

A legislação argentina define, portanto, algumas obrigações para os responsáveis por tratamento de dados.

I. **Medidas de segurança**
A seção 9 da lei nº 25.326 dispõe que o responsável ou o usuário dos arquivos de dados devem tomar todas as medidas técnicas e organizacionais necessárias para garantir a segurança e confidencialidade dos dados pessoais, a fim de evitar sua alteração, perda, acesso ou tratamento não autorizado. Além disso, a lei proíbe o registro de dados pessoais em arquivos que não atendam aos requisitos técnicos de integridade e segurança.

II. **Registro de banco de dados**
Conforme a seção 3 e 21 da lei nº 25.326 os bancos de dados precisam estar registrados no Registro Nacional de Bancos de Dados Pessoais mantido pela AAIP. No registro, os responsáveis deverão fornecer informações como: o nome e domicílio do responsável; as características e finalidade do registro; a natureza dos dados pessoais; a forma de coleta e atualização dos dados; o destino dos dados e as pessoas físicas ou jurídicas a quem esses dados podem ser transmitidos; a forma como as informações cadastradas podem ser inter-relacionadas; os meios utilizados para garantir a segurança dos dados, com a obrigatoriedade de indicação da categoria de pessoas com acesso ao processo de tratamento da informação; o período de preservação dos dados; e a forma e as condições em que as pessoas podem ter acesso aos dados que lhes digam respeito e os procedimentos a implementar para a retificação ou atualização desses dados.

III. **Transferência internacional**
O artigo 12 da lei nº 25.326 impede a transferência de dados pessoais para país ou organização internacional ou supranacional que não forneça um nível adequado de proteção. Entretanto, destaca-se que a transferência internacional de dados pessoais para países que não oferecem um nível de proteção adequado será permitida quando:

- o titular dos dados consentiu expressamente com tais transferências;
- haja contrato de transferência internacional com cláusulas contratuais padrão; e
- transferência entre empresas do mesmo grupo econômico, se as empresas tiverem instituído normas corporativas globais (binding corporate rules) com conteúdo mínimo estabelecido ou aprovado pela AAIP.

IV. Avaliação de impacto à proteção de dados

O ordenamento jurídico argentino contém um Guia sobre a Avaliação de Impacto de Proteção de Dados, publicado em janeiro de 2020, pelas autoridades de proteção de Dados da Argentina em conjunto com a do Uruguai. O Guia estabelece que é requisito obrigatório para controladores e operadores de dados realizar uma Avaliação de Impacto de Proteção de Dados.

V. Encarregado de proteção de dados

Na legislação argentina de proteção de dados não há obrigação de nomear um encarregado de proteção de dados (data protection officer - DPO). Entretanto, a AAIP recomenda a indicação de um DPO como boa prática.

VI. Dever de notificar incidentes de segurança

A seção G.1.3. do Anexo I e II, incluso à Resolução 47/2018 (contêm as medidas de segurança recomendadas) estabelece que, em caso de violação de segurança, os controladores e operadores devem notificar a AAIP do incidente, a partir de um relatório de incidente de segurança que contém, no mínimo:

- a natureza da violação;
- a categoria de dados pessoais afetados;
- uma identificação dos usuários afetados; e
- as medidas tomadas pelo responsável para mitigar o incidente e as medidas aplicadas para evitar futuros incidentes.

VII. Retenção dos dados

A Seção 4 da lei nº 25.326 estabelece que os dados devem ser eliminados sempre que não forem mais necessários ou relevantes para os fins para os quais foram coletados. O prazo aplicável deve ser determinado caso a caso em função da necessidade e pertinência dos dados.

VIII. Tratamento de dados de crianças e adolescentes

No que concerne o tratamento de dados de crianças e adolescentes, a lei nº 25.326 não dispõe de nenhuma norma específica. A AAIP, por sua vez, estabeleceu que se aplicam as normas do Código Civil e Comercial Nacional (Resolução 4/2019).

O Código Civil e Comercial Nacional define que os menores de 18 anos não têm capacidade jurídica absoluta, e distingue entre menores de 13 anos (não adolescentes) e maiores de 13 anos (adolescentes). No caso de adolescentes entende-se haver uma capacidade jurídica relativa.

Assim, a AAIP entende que adolescentes podem fornecer consentimento caso tenham capacidade de compreender o uso dos dados pessoais com base em suas características psicofísicas, aptidão e nível de

desenvolvimento. Nos demais casos, o responsável legal pelo menor deve fornecer o consentimento. O controlador deve envidar esforços razoáveis para verificar se o consentimento foi dado pelo responsável legal.

IX. Contratos de controlador e operador

O responsável pelo tratamento deve elaborar um contrato que estabeleça que o operador só pode tratar os dados seguindo as instruções do responsável.

A Seção 25 da lei nº 25.326 estabelece que o operador só pode utilizar os dados para as finalidades definidas no contrato. A Seção 11 da lei nº 25.326 define que o controlador e o operador responderão solidariamente pelo cumprimento das obrigações legais e regulamentares perante a AAIP e o titular dos dados. O operador pode ser total ou parcialmente isento de responsabilidade se provar que a causa do dano não pode ser atribuída a ele.

Fiscalização

A **Agência de Acesso à Informação Pública (AAIP)** é a principal autoridade supervisora das normas de proteção de dados pessoais (artigo 19 da lei de Direito de Acesso à Informação Pública nº 27.275).

Em relação às sanções administrativas aplicáveis, o artigo 31 da lei nº 25.326 dispõe que a AAIP pode aplicar:

- advertência;
- suspensão;
- multa (entre mil pesos a cem mil pesos argentinos); e
- encerramento do arquivo, registro ou banco de dados.

A aplicação das sanções deve ser graduada, com base na gravidade e extensão da violação e dos danos decorrentes. Vale destacar que uma das principais limitações na atuação sancionatória da AAIP é que valor máximo de multa a ser aplicável é de apenas cem mil pesos argentinos.

Dentre os casos de sanções aplicadas pela autoridade argentina, pode-se citar como exemplo a aplicação de multa de 80.000 pesos à empresa Rappi Arg SAS[2] por ter negado a um usuário o direito de exclusão previsto na lei nº 25.326 (Resolução nº 32/2021 da AAIP).

2 SANCIÓN a empresas de entregas a domicilio. Argentina.gob.ar. Buenos Aires, 03 de março de 2021. Disponível em: < https://www.argentina.gob.ar/sites/default/files/2021/04/resol-2021-32-apn--dnpdp-aaip_tachas.pdf>. Acesso em 21 de nov de 2022

‹voltar para o índice

Quadro-resumo

Principais normas	• Constituição Federal (art. 43). • Lei nº 25.326 de 2000, principal norma sobre proteção de dados pessoais. • Código Penal Nacional, que estabelece punições para aqueles que infringirem normas de proteção aos dados pessoais. • Código Civil e Comercial Nacional, que protege o direito à privacidade. • Lei de Proteção Integral dos Direitos da Criança e do Adolescente (lei nº 26.061), que garante a proteção dos dados de menores.
Bases legais	• Consentimento. • Exceções ao consentimento: **i.** execução de contrato; **ii.** cumprimento de obrigações legais; **iii.** dados obtidos de fontes publicamente acessíveis; **iv.** dados pessoais se limitam a nome, documento de identidade, nº de identificação do contribuinte, nº previdenciário, profissão, data de nascimento e domicílio; e **v.** transações realizadas por entidades financeiras (protegidas por regras de sigilo bancário).
Direitos dos titulares	• Direito de ser informado. • Direito de acesso aos dados tratados. • Direito de retificação. • Direito de não se submeter a decisões automatizadas.
Obrigações controlador e operador	• Adotar medidas técnicas de segurança. • Realizar o registro do banco de dados na AAIP. • Realizar a transferência internacional de dados apenas nos casos permitidos em lei. • Realizar a Avaliação de Impacto de Proteção de Dados. • Notificar incidentes de segurança. • Reter os dados apenas quando for necessário para cumprir com as finalidades. • Para tratar dados pessoais de crianças e adolescentes, realizar esforços razoáveis para verificar se o consentimento foi dado pelos pais ou responsáveis do titular.
Fiscalização	• A Agência de Acesso à Informação Pública (AAIP) é a principal autoridade supervisora dos regulamentos relacionados à proteção de dados na Argentina. • A AAIP tem como objetivo: (i) verificar as atividades dos controladores de bancos de dados e os dados que eles gerenciam; (ii) avaliar o cumprimento do legislação. • A AAIP também pode aplicar sanções administrativas como multas e encerramento ou cancelamento do arquivo, registro ou banco de dados para aqueles que descumprirem a legislação.

‹voltar para o índice

02 Colômbia

COLÔMBIA[3]

Principais normas e escopo

Na Colômbia, a proteção de dados pessoais é um direito garantido constitucionalmente pelo artigo 15 da Constituição Política da Colômbia, que estabelece de forma geral que no tratamento de dados pessoais devem ser respeitadas a liberdade e demais garantias previstas na constituição.

Em 2008, foi promulgada a Lei de Habeas Data (lei nº 1.266 de 2008), que regula o tratamento de dados contidos em bases financeira, creditícias, comerciais, de serviços e provenientes de outros países. Apesar do avanço representado por essa lei, o seu conteúdo é essencialmente orientado a proteção de dados comerciais e financeiros, deixando um vácuo normativo em relação aos demais tipos de dados pessoais.[4]

Para ampliar o direito a proteção de dados na Colômbia, em 2012, foi estabelecida a Lei Estatutária nº 1.581 de 2012, que garante o devido tratamento dos dados pessoais registrados em qualquer banco de dados, seja ele operado por entidades públicas ou privadas. Sendo a lei também parcialmente regulamentada pelo Decreto nº 1.377 de 2013, que visa à sua complementação e a facilitação de sua implementação, trazendo disposições complementares sobre diversos aspectos importantes, como a necessidade de autorização do titular para o tratamento de seus dados, exercício de direitos, políticas e avisos de privacidade e transferências internacionais.

A lei nº 1.581 é aplicada a qualquer tratamento de dados pessoais realizados no território colombiano, também, sendo aplicável nas hipóteses nas quais a legislação colombiana for aplicável ao agente responsável pelo tratamento em virtude de normas ou tratados internacionais (art 2º da lei nº 1.581). Entretanto, a legislação colombiana exclui de sua aplicação as bases de dados e arquivos utilizados para as seguintes finalidades:

- exclusivamente para fins pessoais e domésticos;
- segurança e defesa nacional, bem como para prevenção, detecção, monitoramento e controle de lavagem de recursos e financiamento de terrorismo;
- inteligência e contraespionagem;

3 PARDO, Carolina. Colombia – Data Protection Overview. OneTrust – DataGuidance. 2021. Disponível em:< https://www.dataguidance.com/notes/colombia-data-protection-overview>. Acesso em: 21/11/2022.

4 ROJAS BEJARANO, M. Evolución del derecho de protección de datos personales en Colombia respecto a estándares internacionales. Novum Jus, 2014, pag. 13. Disponível em: https://novumjus.ucatolica.edu.co/article/view/652. Acesso em: 18 nov. 2022.

- informações jornalísticas e editoriais;
- regulamentados pela lei de habeas data; e
- regulamentado pela lei de censo demográfico.

Em relação à aplicação extraterritorial da lei, o Tribunal Constitucional, responsável pelo controle constitucional da legislação de proteção de dados na Colômbia, estendeu a aplicação da lei nº 1.581 para o tratamento de dados de titulares residentes na Colômbia, mesmo quando realizado fora dos limites territoriais do país[5]. Com essa ampliação, a corte teve como objetivo estender a proteção garantida pela legislação aos titulares.

Bases legais

Em relação às hipóteses legais que autorizam o tratamento de dados pessoais, a legislação colombiana estabelece o consentimento como base legal prioritária. Sendo assim, os responsáveis pelo tratamento devem obter o consentimento qualificado dos titulares dos dados para realizar qualquer uso de dados pessoais. Para ser válido o consentimento deverá (i) ser concedido antes ou simultaneamente ao tratamento, e (ii) informado, devendo ser oferecido ao titular informações suficientes sobre os meios e os propósitos pelos quais os dados serão utilizados, contato do controlador, os direitos, os meios de exercê-los, como acessar a política de proteção de dados do controlador.

Entretanto, não é necessário a coleta de consentimentos nos casos em que os dados pessoais:

- sejam requeridos por entidades públicas ou administrativas, no exercício de suas funções legais ou por ordem judicial;
- sejam de natureza pública;
- em casos de urgência médica ou sanitária;
- sejam utilizados para finalidades históricas, estatísticas ou científicas
- estejam relacionados com o registro civil.

Caso o tratamento envolva dados pessoais sensíveis – considerados pela legislação colombiana como aqueles que afetem a privacidade do titular ou cujo uso indevido possa gerar discriminação (dados relativos à saúde e vida sexual, dados biométricos, dados que revelem origem racial ou étnica, orientação política, convicções religiosas ou filosóficas, filiação a sindicatos, organizações sociais, de direitos humanos ou organizações que promovam os interesses de um partido político ou assegurem direitos e garantias dos partidos da oposição) – o consentimento deverá ser também expresso, ou seja, é necessária uma manifestação inequívoca do titular sobre a

5 Corte Constitucional da República Colombiana, Sentencia C-748-11. Disponível em https://www.corteconstitucional.gov.co/relatoria/2011/c-748-11.htm. Acesso em: 18 nov. 2022.

sua concordância para que essa categoria de dados seja utilizada pela organização. Devendo, ainda, o responsável pelo tratamento informar ao titular sobre o caráter não obrigatório do consentimento e sobre o caráter sensível dos dados coletados.

No caso de tratamento de dados sensíveis, a lei dita não haver necessidade de coletar o consentimento do titular quando (i) o tratamento de dados é necessário para garantir um interesse vital do titular que está física ou legalmente incapacitado; (ii) o tratamento é realizado durante o exercício das atividades de associações sem fins lucrativos; (iii) é necessário para o exercício ou defesa de direitos em processos judiciais; ou (iv) tem finalidades históricas, estatísticas ou científicas, desde que a identidade do titular seja suprimida .

Direito dos titulares

A lei nº 1.581 estabelece, em seu artigo 8º, um rol de direitos que podem ser exercidos pelo titular dos dados pessoais:

I. **Direito de retificação**
Possibilita aos titulares conhecer, atualizar e retificar dados pessoais parciais ou inexatos, ou cujo tratamento seja expressamente proibido ou não tenha sido autorizado.

II. **Direito de acesso**
Que prevê que o titular dos dados pode acessar livremente seus dados pessoais tratados pelo agente.

III. **Direito de revogação do consentimento e exclusão**
Também, é dada a faculdade ao titular de requerer a revogação do consentimento e/ou solicitar a exclusão de dados, quando o tratamento não estiver em conformidade a legislação.

IV. **Direito de ser informado**
O titular também possui o direito de ser informado sobre as finalidades do tratamento.

Por fim, também garante o artigo 8º da lei a possibilidade de os titulares de requerem um comprovante da autorização concedida para o tratamento de dados realizado pelo titular. Além de estabelecer que os titulares, podem submeter, à autoridade competente, reclamações por violação das disposições nas legislações aplicáveis.

Obrigações controlador e operador

A legislação colombiana define como controladores dos dados pessoais a pessoa física ou jurídica, pública ou privada que, isoladamente ou em associação com outras, controla a base de dados e/ou o tratamento dos dados. O artigo 17 da lei nº 1.581 estabelece uma série de obrigações que devem ser atendidas pelos controladores, entre elas:

- obter e registar o consentimento do titular para o tratamento de seus dados pessoais;
- informar aos titulares sobre as finalidades do tratamento e sobre os seus direitos;
- manter o titular informado sobre alterações relativas ao tratamento de seus dados;
- retificar dados pessoais incorretos e comunicar os operadores sobre tais atualizações;
- exigir dos operadores de dados o respeito pelas condições de segurança dos dados pessoais e pela privacidade de seus titulares; e
- informar os operadores sobre eventuais requisições de dados pessoais.

Também o artigo 25 da lei nº 1.581 estabelece que os controladores de dados pessoais devem registrar cada banco de dados que contenham dados pessoais no Cadastro Nacional de Bancos de Dados, diretório público administrado pela autoridade de proteção de dados colombiana, a Superintendencia de Industria y Comercio (SIC).

Por fim, os controladores, de acordo com o Decreto nº 1.377, também devem divulgar, aos titulares, políticas de tratamento e avisos de privacidade, em meio físico ou eletrônico. Estes documentos devem possibilitar o acesso a informações sobre (i) a identidade do controlador; (ii) o tratamento de dados realizado; (iii) os direitos dos titulares e as formas de exercê-los; e (iv) a data de vigência da política e o prazo de tratamento da base de dados.

Já o papel de operador de dados pessoais, é definido, pelo artigo 3º da lei nº 1.581, como a pessoa física ou jurídica, pública ou privada que, isoladamente ou em associação com outros, processa dados pessoais em nome do controlador de dados. As obrigações impostas aos operadores são descritas no artigo 18 da mesma lei, a qual estabelece que cabe aos operadores:

- atualizar as informações prestadas pelos controladores de dados em até 5 (cinco) dias úteis a partir de seu recebimento;
- anotar na base de dados sempre que existir uma reclamação em curso, ou em casos de notificação pela autoridade competente sobre processos judiciais relacionados com a qualidade dos dados pessoais;
- abster-se de divulgar informação que seja alvo de discussão por parte do

titular, e cujo bloqueio tenha sido determinado pela autoridade de proteção de dados;

- permitir o acesso à informação apenas às pessoas que a ela possam ter acesso.

Tanto o artigo 17 como o artigo 18 da legislação de proteção de dados estabelecem as seguintes obrigações, que devem ser cumpridas simultaneamente por controladores e operadores de dados pessoais:

- garantir o pleno e efetivo exercício do direito de habeas data;
- assegurar condições de segurança da informação suficientes para prevenir a sua adulteração, perda, consulta, utilização ou acesso não autorizado, ou fraudulento;
- adotar políticas e procedimentos para garantir o adequado cumprimento da legislação; e
- cumprir exigências da autoridade de proteção de dados, além de informá-la sobre violações de dados pessoais.

Fiscalização

A lei de proteção de dados pessoais colombiana atribuiu as funções de autoridade à Superintendência de Indústria e Comércio (SIC), um órgão da administração pública federal. A SIC já existia anteriormente, sendo o órgão responsável por realizar a regulação da propriedade industrial, proteção do consumidor, proteção da concorrência e regulamentação da metrologia legal na Colômbia. Com a atribuição de regulação de temas de proteção de dados, em 2012, a SIC criou uma pasta específica nomeada "Delegação de Proteção de Dados Pessoais".

O artigo 21 da lei nº 1.581 indica as responsabilidades e deveres atribuídos à SIC, a seguir listadas:

- zelar pelo cumprimento da legislação sobre proteção de dados pessoais;
- realizar investigações, de ofício ou a pedido de uma das partes e, a partir delas, ordenar as providências necessárias;
- providenciar o bloqueio temporário dos dados quando identificado risco de violação de direitos fundamentais;
- promover e divulgar os direitos dos titulares, e implementar campanhas educativas;
- dar instruções sobre as medidas e procedimentos necessários para adequação das operações realizadas por controladores e operadores;
- solicitar aos agentes de tratamento de dados informações necessárias ao efetivo exercício das suas funções;
- emitir declarações de conformidade sobre transferências internacionais de dados;

- gerir o Cadastro Público Nacional de Bases de Dados;
- recomendar ajustes nos regulamentos para que estejam em linha com a evolução tecnológica;
- exigir a colaboração de entidades internacionais ou estrangeiras quando os direitos dos titulares forem afetados fora do território colombiano.

Caso seja constatada a inobservância do disposto na legislação aplicável, por parte de controladores ou operadores de dados pessoais, a SIC poderá aplicar as sanções previstas na lei nº 1.581:

- a aplicação de multas de natureza pessoal ou institucional até o equivalente a 2.000 (dois mil) salários-mínimos mensais, podendo as multas serem aplicadas em caráter sucessivo;
- a suspensão das atividades relacionadas ao tratamento pelo prazo de até 6 (seis) meses;
- o encerramento temporário das operações relacionadas com o tratamento; e
- o encerramento imediato e definitivo da operação que implique o tratamento de dados sensíveis.

Entretanto, as sanções indicadas na legislação de proteção de dados apenas podem ser aplicadas a entidades privadas, não tendo a SIC legitimidade para impor sanções às autoridades públicas, as quais devem ser investigadas pela Procuradoria-Geral da Nação.

Em relação à autonomia administrativa do órgão, a SIC compõe a administração indireta da Colômbia, possuindo personalidade jurídica própria e não estando submetida a nenhum controle hierárquico.

Como exemplo de atuação fiscalizatória da SIC, cita-se o caso em que a empresa Avantel foi sancionada por consultar o score de crédito sem o consentimento prévio dos titulares. A empresa sofreu uma multa de aproximadamente U$ 55.000 dólares, tendo a SIC também imposto a obrigação de adoção de medidas internas para garantia do controle de acesso aos dados de score de crédito.[6]

6 MOLANO, María del Pilar Duplat. Sanctions imposed by the supeirntendence of industry and commerce of colombia for breaches in data protection law. Disponível em:<https://www.pmabogados.co/uncategorized/sanctions-imposed-by-the-supeirntendence-of-industry-and-commerce-of--colombia-for-breaches-in-data-protection-law/?lang=en>. Acesso em: 21/11/2022.

Quadro-resumo

Principais normas	• Lei Estatutária nº 1.581 de 2012. • Decreto nº 1.377 de 2013. • Constituição Política da Colômbia. • Lei de Habeas Data (lei nº 1.266 de 2008). • Decreto nº 1.727 de 2009. • Decreto nº 2.952 de 2010.
Bases legais	• Consentimento. • Exceções ao consentimento: i. dados requeridos por entidades públicas ou administrativas; ii. dados de natureza pública; de urgência médica ou sanitária; iii. finalidades históricas, estatísticas ou científicas; e iv. dados relacionados com o registro civil.
Direitos dos titulares	• Direito de retificação. • Direito de acesso. • Direito de revogação do consentimento. • Direito de exclusão. • Direito de ser informado. • Direito de solicitar a comprovação do consentimento. • Direito de reclamar à autoridade competente.
Obrigações controlador e operador	• Obter e registar o consentimento. • Prestar informações aos titulares. • Retificar dados pessoais. • Exigir dos operadores de dados o cumprimento da lei. • Informar os operadores sobre eventuais requisições de dados pessoais. • Divulgar, aos titulares, políticas de tratamento e avisos de privacidade. • Registrar banco de dados que contenham dados pessoais. • Atualizar as informações prestadas pelos controladores. • Anotar reclamação em curso ou notificação da autoridade na base dados. • Não divulgar informação sobre eventuais discussões relacionadas a base de dados. • Restringir o acesso à informação. • Garantir o exercício do direito de habeas data. • Assegurar a segurança dos dados. • Adotar manual interno de políticas e procedimentos para garantir o cumprimento da legislação. • Cumprir instruções e exigências da autoridade de proteção de dados, além de informá-la sobre casos de violações de dados pessoais.
Fiscalização	• Superintendência de Indústria e Comércio (SIC). • A SIC pode aplicar sanções administrativas: i. multa; ii. suspensão das atividades por 6 meses; iii. encerramento temporário do tratamento; e iv. encerramento imediato do tratamento.

‹voltar para o índice

03 Chile

Chile[7]

Principais normas e escopo

O Chile foi o primeiro país da América Latina a aprovar uma lei de proteção de dados, em 1999, a lei nº 19.628, que é aplicável ao setor público e privado. No entanto, ainda que tenha passado por atualizações ao longo do tempo, a lei não trata de temas relacionados a autoridade supervisora, transferência internacional de dados e não define sanções efetivas, entre outros elementos. Em 2018, a proteção de dados pessoais foi incorporada como um direito fundamental na Constituição chilena.

Projetos de emenda à lei de proteção de dados estão sendo discutidos no legislativo, e em outubro de 2021 o Governo alterou o Projeto de Lei nº 11144-07 (principal projeto de emenda à lei) e incorporou a criação de uma agência de proteção dos dados pessoais, aplicação de multas e sanções, e novas bases jurídicas para o tratamento de dados pessoais, como execução de contrato e o legítimo interesse.

Bases legais

A lei nº 19.628 determina, em seu artigo 4º, que o tratamento de dados pessoais somente poderá ocorrer quando o titular expressamente consentir ou quando houver disposição legal autorizando o tratamento. A autorização para o tratamento de dados mediante consentimento deve ser feita por escrito, bem como sua revogação, e é requisito para o consentimento que o titular esteja devidamente informado sobre o propósito do armazenamento de seus dados pessoais e da possibilidade de comunicação ao público.

Ainda no artigo 4º, é mencionado que o consentimento não é necessário para o tratamento de dados pessoais nas seguintes hipóteses:

- provenientes de fontes publicamente acessíveis;
- registros médicos; e
- dados pessoais relativos a obrigações econômicas, financeiras, bancárias ou comerciais.

Sobre dados pessoais sensíveis, a lei os define como sendo dados que se referem às características físicas ou morais das pessoas, a fatos/circunstâncias de sua vida privada e íntima, tais como hábitos pessoais, origem racial, ideologia e opiniões políticas, entre outros (art. 2º, "g" da lei nº 19.628). Quanto ao tratamento desses dados, o artigo 10 da lei nº 19.628 veda qualquer tratamento

7 GATICA, Macarena; URZA, Jaime. Chile - Data Protection Overview. 2022. Disponível em:< https://www.dataguidance.com/notes/chile-data-protection-overview>. Acessado em: 21/11/2022.

desta categoria, salvo quando a lei autorizar, houver consentimento do titular ou caso os dados sejam necessários para a concessão de benefícios de saúde.

Direitos dos titulares

A lei nº 19.628 assegura aos titulares os seguintes direitos em seu artigo 12:

I. **Direito de acesso**
Os titulares possuem o direito de solicitar e acessar os dados pessoais objetos de tratamento, e podem buscar informações sobre seus dados pessoais tratados, a origem dos dados, com quem são compartilhados, a finalidade de armazenamento, o período de retenção. No mais, caso os dados constem em uma base a que tenham acesso várias entidades, o titular pode exercer o direito de acesso a partir de qualquer uma delas (artigo 14 da lei nº 19.628).

Também é disposto que o direito de acesso deve ser concedido gratuitamente, mas não há previsão explícita quanto aos requisitos para o formato do pedido – apenas é informado que, perante um pedido de dados pessoais através de rede eletrônica, devem ser registradas (i) a identificação do requerente, (ii) o motivo e a finalidade do pedido e (iii) o tipo de dado que será transmitido. O responsável pelo tratamento deve avaliar a admissibilidade do pedido, entretanto a responsabilidade do pedido fica a cargo de quem o fizer, ou seja, do titular dos dados.

II. **Direito à retificação**
Os dados pessoais podem ser retificados quando estiverem errados, inexatos ou incompletos. Ainda, caso os dados pessoais retificados tenham sido previamente comunicados a terceiros, o responsável pelo banco de dados deve notificá-los sobre a retificação. Havendo modificações em seus dados pessoais, o titular pode solicitar uma cópia do registro atualizado.

III. **Direito à eliminação**
Os titulares têm direito à eliminação de seus dados pessoais quando (i) seu armazenamento não tem uma base legal adequada, (ii) os dados se encontrarem desatualizados, (iii) sempre que o titular tiver fornecido voluntariamente os seus dados pessoais, ou (iv) seus dados pessoais sejam utilizados para comunicações comerciais e o titular dos dados não pretende continuar a constar no registro do responsável pelo tratamento. Para a eliminação, é válida a mesma regra da retificação: caso os dados pessoais eliminados tenham sido previamente comunicados a terceiros, o responsável pelo banco de dados deve notificá-los.

IV. **Direito de bloqueio**
Bloqueio refere-se à suspensão temporária de qualquer operação de tratamento de dados. Os titulares possuem o direito ao bloqueio aos dados

pessoais sempre que tiver fornecido os dados voluntariamente, ou caso os dados sejam usados para comunicações comerciais, e o titular não se interessar em receber essas comunicações. De modo geral, deverá haver bloqueio dos dados sempre que não for possível demonstrar sua exatidão ou cuja validade seja duvidosa.

Os direitos previstos acima não podem ser requeridos quando visarem impedir ou dificultar a fiscalização de órgãos públicos, afetarem uma exigência de sigilo estabelecida em disposição legal ou regulamentar, ou quando afetarem a segurança ou o interesse nacional.

Caso o responsável pelo tratamento dos dados pessoais não responda ao pedido do titular no prazo de dois dias úteis, ou caso haja recusa por motivos que não sejam a segurança nacional e o interesse nacional, o titular pode recorrer perante um tribunal (artigo 16 da lei nº 19.628).

Tomada a decisão de que o responsável não atendeu legalmente à solicitação do titular para exercer seus direitos, um prazo razoável será definido para a exigência do cumprimento. Adicionalmente, podem ser aplicadas multas de uma a dez unidades mensais de imposto – que variam aproximadamente entre 30€ a 340€.

Obrigações controlador e operador

O controlador dos dados pessoais é definido como pessoa física ou jurídica, pública ou privada, que tem poder de decidir sobre as finalidades e meios de tratamento dos dados pessoais, independente se os dados serão tratados diretamente por si ou por intermédio de um terceiro (artigo 2º da lei nº 19.628). Não há definição legal de operador dos dados na lei.

A lei nº 19.628 estabelece como obrigações para quem trata dados pessoais:

- Obrigação de sigilo sobre dados pessoais, quando estes forem provenientes de fontes não acessíveis ao público;
- Os dados pessoais devem ser usados apenas para os fins para quais os foram coletados, a menos que sejam provenientes de fontes acessíveis ao público;
- O controlador deve adotar medidas técnicas e organizacionais de segurança para tratar dados pessoais; e
- O responsável pelo tratamento deve conservar os dados pessoais com a devida diligência, sendo responsável pelos danos causados.

Quanto ao último ponto citado acima, é disposto em lei que o responsável pelo tratamento deverá indenizar o titular quando tratar indevidamente seus dados pessoais e lhe causar dano (artigo 23 da lei nº 19.628). A lei não menciona o dever de se realizar relatório de impacto à proteção de dados pessoais.

Fiscalização

O Chile ainda não possui uma autoridade pública específica para fiscalizar a proteção de dados no país. Dada a ausência de uma autoridade específica, outras autoridades reivindicaram competência para regular esse tema, como a Comissão para Mercado Financeiro e o Conselho de Transparência do Chile. Adicionalmente, em dezembro de 2021 entrou em vigor a Lei do Consumidor nº 21.938, que confere ao Serviço Nacional do Consumidor ("SERNAC") poderes de fiscalização relativos ao tratamento dos dados pessoais no âmbito das relações de consumo – e desde que tais faculdades não sejam competências legais de outra agência reguladora.

Quadro-resumo

Principais normas	• Lei nº 19.628 sobre proteção de dados pessoais. • Lei nº 21.236 sobre diretos dos consumidores.
Bases legais	• Consentimento. • Obrigação legal • Exceções ao consentimento: i. provenientes de fontes publicamente acessíveis; ii. registros médicos; e iii. dados pessoais relativos a obrigações econômicas, financeiras, bancárias ou comerciais.
Direitos dos titulares	• Acesso e informação quanto ao tratamento, finalidade, origem e destino dos dados. • Retificação dos dados. • Eliminação dos dados. • Bloqueio dos dados.
Obrigações controlador e operador	• Obrigação de sigilo sobre dados pessoais. • Utilização dos dados para as finalidades que justificaram a coleta. • Adoção de medidas técnicas e organizacionais de segurança. • Conservação dos dados pessoais com a devida diligência.
Fiscalização	• Não apresenta uma autoridade de proteção de dados centralizada. • Comissão para Mercado Financeiro. • Conselho de Transparência do Chile. • Serviço Nacional do Consumidor ("SERNAC").

‹voltar para o índice

04 Peru

Peru[8]

Principais normas e escopo

A Constituição Política do Peru de 1993 positiva o direito à privacidade e à proteção de dados em seu artigo 2(6), o que serviu de base constitucional para a criação da Lei de Proteção de Dados Pessoais do país ("LPDP" – lei nº 29.733), promulgada em junho de 2011. A lei é regulamentada pelo Decreto Supremo nº 003-2013-JUS, de março de 2013 ("Decreto").

Como forma de garantir esses direitos fundamentais, a Constituição Peruana também dispõe sobre o remédio constitucional do habeas data, que prevê que todos os indivíduos têm o direito de acessar, atualizar, cancelar ou retificar suas informações pessoais armazenadas ou registradas, sejam elas manuais, mecânicas ou informáticas, em arquivos, bancos de dados e registros de entidades públicas ou privadas, que prestem serviços ou acessem a terceiros (art. 200(3) da Constituição).

Vale mencionar outros 3 normativos que compõem o ecossistema de proteção de dados peruano, quais sejam. A lei nº 27.489, de junho de 2001, que regula birôs de crédito, fornecendo um *framework* legal para a utilização de informações de pessoas físicas pelo mercado para fins de avaliação creditícia e cálculo de nível de risco.

A lei nº 30.096, de outubro de 2013, que dispõe sobre Crimes Cibernéticos, como forma de prevenir e punir condutas ilegais que afetem os sistemas de informação por meio do uso de tecnologias de informação ou telecomunicações. No que diz respeito à proteção de dados, sanciona, entre outras coisas, a criação, acesso, alteração, exclusão ou interceptação de dados ou sistemas informáticos.

E o Decreto de Emergência nº 007-2020, de janeiro de 2020, que aprova o Marco de Confiança Digital como meio de estabelecer certas obrigações para entidades públicas e privadas que atuam como provedores de serviços digitais. Estas obrigações incluem a comunicação à Autoridade Nacional de Proteção de Dados do Peru da ocorrência de um incidente de segurança digital envolvendo dados pessoais, bem como a implementação de medidas de segurança técnicas, organizacionais e legais para garantir a confidencialidade da informação transmitida através dos seus serviços de comunicações.

Por fim, a Autoridade Nacional de Proteção de Dados do Peru também dispõe da prerrogativa de editar diretrizes e opiniões consultivas para orientar o

8 TOVAR, Teresa; BULEJE, Crosbby. Chile - Data Protection Overview. 2022. Disponível em:< https://www.dataguidance.com/notes/peru-data-protection-overview>. Acessado em: 21/11/2022.

mercado peruano sobre as melhores práticas em termos de segurança da informação e proteção de dados pessoais, bem como de regulamentar pontos da LPDP por meio de resoluções.

As normas sobre proteção de dados se aplicam a informação sobre uma pessoa natural que a identifique ou a torne identificável, que seja armazenada em bases de dados públicas ou privadas. E, se aplica a dados sensíveis, definidos como: dados biométricos; origem racial e étnica; dados econômicos (renda etc.); opiniões ou convicções políticas, religiosas, filosóficas ou morais; filiação sindical; e informações relacionadas à saúde ou à vida sexual.

A LPDP também se aplica nas seguintes situações:

- quando o tratamento de dados é realizado em um estabelecimento localizado no território peruano que pertence a um controlador de dados;
- quando o tratamento de dados for realizado por um operador de dados, independentemente de sua localização, em nome de um controlador de dados estabelecido no território peruano;
- quando o controlador de dados ou operador de dados não estiver estabelecido no território peruano, mas a lei é aplicável a ele por disposições contratuais ou lei internacional; e
- quando o responsável pelo tratamento não estiver estabelecido em território peruano, mas utilizar-se de meios localizados no Peru para o tratamento de dados pessoais, a menos que tais meios sejam utilizados apenas para fins de trânsito que não impliquem em efetivo tratamento.

Vale ressaltar que o escopo de aplicação da LPDP não inclui:

- dados armazenados, ou destinados a serem armazenados, em bancos de dados criados por indivíduos para fins familiares ou privados; ou
- dados armazenados, ou destinados a serem armazenados, em bases de dados da administração pública, quando o seu tratamento seja necessário para o cumprimento das funções atribuídas por lei a essa administração pública, desde que tais funções estejam relacionadas com a defesa nacional, a segurança pública ou o desenvolvimento de atividades para a investigação de atividades criminosas e repressão ao crime.

Bases legais

A LPDP traz o **consentimento** como base legal principal para a realização de operações de tratamentos de dados pessoais. Para que um consentimento seja considerado válido, nos termos da LPDP, ele deverá ser prévio, informado, expresso e inequívoco. Consentimento tácito ou consentimento geral não são permitidos de acordo com a LPDP.

Quando dados sensíveis estão envolvidos, o consentimento deve ser dado por escrito.

O consentimento deve conter, no mínimo, as seguintes informações:

- a existência do banco de dados, a identidade e endereço do controlador e operador;
- a finalidade do tratamento de dados;
- a identidade dos destinatários da informação;
- indicação de quais questões são obrigatórias ou opcionais, se for o caso;
- as consequências de fornecer ou não fornecer dados pessoais;
- o período de retenção dos dados pessoais; e
- a possibilidade e os mecanismos disponíveis para permitir que os titulares dos dados exerçam os seus direitos de proteção de dados dispostos na LPDP.

Há diversas exceções ao consentimento expressas na lei, dentre elas:

- quando o tratamento for relacionado com a saúde de um titular de dados (p. ex. situação de risco, prevenção, diagnóstico ou tratamento médico ou cirúrgico do titular dos dados; por razões de saúde pública; ou para estudos epidemiológicos ou análogos);
- quando estiver relacionado com a solvência financeira ou capacidade creditícia de uma pessoa;
- quando for necessário para a execução de uma relação contratual em que o titular dos dados seja parte;
- quando o dado pessoal tiver sido anonimizado;
- quando o dado pessoal estiver armazenado em fontes publicamente acessíveis;
- quando se tratar do exercício do direito fundamental à liberdade de informação; e
- quando for necessário para a prevenção da lavagem de dinheiro e financiamento do terrorismo.

O **legítimo interesse do titular dos dados** tem um escopo de aplicação indeterminado por falta de jurisprudência das cortes peruanas sobre o tema, devendo ser interpretado de forma restrita.

A **obrigação legal** também é uma base legal independente que pode ser aplicável.

Direitos dos titulares

A LPDP prevê os direitos dos titulares de dados pessoais descritos abaixo.

I. **Direito de ser informado**
O titular dos dados deve ser informado de maneira clara e expressa sobre:

- as finalidades para as quais os dados serão tratados;
- com quem são compartilhados;
- a existência do banco de dados, a identidade e endereço de seu controlador;
- se o fornecimento do dado pessoal é obrigatório, e as consequências de se recusar o fornecimento;
- o período de retenção dos dados pessoais; e
- a possibilidade de exercer os direitos listados na LPDP.

Para atender ao direito dos titulares de serem informados, a LPDP prevê que uma política de privacidade facilmente acessível e identificável no site dos agentes de tratamentos serve para atender a esse requisito da lei.

II. **Direito de acesso**
O titular dos dados têm o direito de acessar à informação sobre si que é tratada em bancos de dados privados ou da administração pública, a forma como os seus dados pessoais foram coletados, os motivos da coleta e a pedido de quem foram coletados, bem como as transferências efetuadas ou previstas.

É importante salientar que os responsáveis pelo tratamento de dados devem responder a um pedido de acesso sem demora injustificada e, em qualquer caso, no prazo de 20 dias úteis a contar da solicitação. O prazo poderá ser prorrogado por mais 20 dias úteis, se necessário.

III. **Direito de retificação e de eliminação**
Os titulares dos dados têm o direito de retificar e de eliminar os dados pessoais sobre si que são tratados, quando:

- os dados pessoais forem parciais ou totalmente incompletos ou imprecisos;
- for notado um erro ou omissão;
- não for mais necessário ou relevante para a finalidade para a qual foram coletados; ou
- o prazo estabelecido para tratamento dos dados ter expirado.

É importante salientar que os responsáveis pelo tratamento de dados devem responder a um pedido de retificação sem demora injustificada e, em qualquer caso, no prazo de dez dias úteis a contar da solicitação.

IV. Direito de oposição

Os titulares dos dados têm o direito de se opor ao tratamento de dados pessoais quando:

- não existir lei que obrigue à realização do tratamento de dados pessoais contestado;
- houver motivos legítimos e fundamentados, devido a uma situação pessoal específica; ou
- os dados pessoais forem obtidos de fontes públicas, e o titular dos dados não tiver consentido com a referida coleta de dados.

É importante salientar que os responsáveis pelo tratamento de dados devem responder a um pedido de oposição sem demora injustificada e, em qualquer caso, no prazo de dez dias úteis a contar da solicitação. O prazo poderá ser prorrogado por mais dez dias úteis, se necessário.

V. Direito de não se submeter a decisões automatizadas

Os titulares dos dados têm o direito de não serem objeto de decisão com efeitos jurídicos sobre eles, ou que os afete de forma significativa, baseada no tratamento de dados pessoais destinado a avaliar determinados aspectos da sua personalidade ou conduta (no entanto, existem algumas exceções, p.ex., no âmbito da negociação de um acordo ou avaliação para adesão a uma entidade pública).

VI. Direito à portabilidade

O Decreto regulamentador da LPDP estabelece implicitamente o direito à portabilidade ao afirmar que qualquer que seja o formato utilizado para fornecer aos titulares das informações solicitadas, este formato deve ser claro, legível e inteligível, sem o uso de senhas ou códigos que exijam outros mecanismos para acessar as informações.

VII. Direito à tutela

No caso de o controlador ou o encarregado de banco de dados pessoais negar ao titular de dados pessoais, total ou parcialmente, o exercício dos direitos estabelecidos na LPDP, este poderá recorrer à Autoridade Nacional de Proteção de Dados Pessoais do Peru por meio de uma reclamação, ou ao Poder Judiciário por meio de uma ação de habeas data.

VIII. Direito à indenização

O titular de dados pessoais que são afetados em consequência do descumprimento da LDP por parte do controlador ou pelo encarregado do tratamento de dados pessoais ou por terceiros, tem direito a obter a correspondente indenização, nos termos da lei peruana.

IX. Direito à revogação do consentimento

O titular dos dados pessoais pode revogar o seu consentimento para o tratamento dos seus dados pessoais a qualquer momento, sem justificação

prévia e sem efeitos retroativos. Para a revogação do consentimento, serão observados os mesmos requisitos observados pela ocasião de sua obtenção pelo controlador, podendo estes ser mais simples, se assim tiver sido indicado naquele momento.

5.4. Obrigações de controlador e operador

As principais obrigações dos controladores de dados incluem:

- registrar bases de dados perante a Autoridade;
- tratar dados pessoais com uma base legal adequada;
- não coletar dados pessoais usando meios fraudulentos, ilegais ou injustos;
- coletar dados apenas quando necessários e pertinentes para as finalidades informadas aos titulares dos dados;
- permitir o exercício dos direitos dos titulares dos dados de forma facilitada e gratuita;
- eliminar dados pessoais quando já não sejam mais necessários ou relevantes para a finalidade para a qual foram coletados ou quando o prazo para o seu tratamento tenha acabado, salvo se anonimizados ou dissociados;
- adotar medidas técnicas, organizacionais e legais que garantam a segurança dos dados e impeçam sua alteração, tratamento ou acesso não autorizado;
- manter a confidencialidade dos dados pessoais; e
- permitir à Autoridade peruana de proteção de dados acesso à base de dados e fornecer-lhe a informação necessária no âmbito de um processo administrativo.

Os operadores de dados têm as mesmas obrigações que os controladores de dados. Além disso, devem cumprir os princípios de proteção de dados pessoais dispostos na LPDP.

I. **Obrigatoriedade de registros perante a autoridade**
De acordo com a LPDP, o controlador responsável pelo tratamento de dados pessoais é obrigado a registrar as suas bases de dados pessoais no Registro Nacional de Proteção de Dados Pessoais, mantido pela Autoridade de Proteção de Dados do Peru. Ademais, as transferências internacionais de dados pessoais devem ser notificadas à Autoridade. Por fim, destaca-se que os códigos de conduta podem ser registados junto à Autoridade, embora não seja obrigatório.

II. **Indicação de encarregado**
Não há exigência legal expressa quanto à necessidade de indicação de DPO no Peru.

III. Transferência internacional de dados pessoais

A LPDP estabelece que, se o país destinatário dos dados não tiver um nível de proteção adequado, o exportador de dados deve garantir que o tratamento dos dados pessoais será feito de acordo com o nível de proteção adequado nos termos da legislação peruana. Esta disposição não é aplicável nos seguintes casos:

- a transmissão de dados pessoais é realizada no âmbito de cooperação judicial internacional ou da aplicação de comércio internacional a esse respeito;
- cooperação internacional entre agências de inteligência;
- quando os dados pessoais sejam necessários para a celebração de uma relação contratual com o titular dos dados;
- quando se referir a transferências bancárias e de segurança;
- quando a transferência for efetuada para fins de proteção, prevenção, diagnóstico e tratamento médico do titular dos dados; e
- quando o titular dos dados tiver dado o seu consentimento para a transferência dos seus dados nestas condições.

As transferências internacionais de dados devem ser comunicadas à Autoridade, incluindo a informação necessária para tais transferências e o registro da base de dados.

IV. Registro de atividades de tratamento de dados pessoais

Nos termos da LPDP, não é exigido que os controladores de dados mantenham registros internos das atividades de tratamento de dados pessoais.

De acordo com a LPDP, não é expressamente exigido que os controladores de dados elaborem relatórios de impacto à proteção de dados. No entanto, vale destacar que cabe aos controladores de dados realizar uma avaliação de risco para determinar as medidas de segurança, legais e organizacionais necessárias para os tratamentos de dados pessoais.

As leis e regulamentos de proteção de dados do Peru não dispõem de forma específica sobre prazos de retenção de dados aplicáveis aos agentes de tratamento de dados pessoais. Destaca-se que o Decreto regulamentador da LPDP prevê que os controladores de dados podem conservar, por até dois anos, os dados pessoais fornecidos no âmbito de um contrato de tratamento de dados. Essa disposição também se aplica à subcontratação da prestação de serviços de tratamento de dados pessoais a um operador de dados.

V. Notificação de incidente

Não há obrigatoriedade de notificação de incidentes de segurança que envolvam dados pessoais, exceto no caso das empresas do setor bancário,

em que a notificação não é feita à Autoridade de Proteção de Dados do Peru, mas à Superintendência de Bancos, Seguros e Administradoras de Fundos de Pensões.

Ressalta-se que a Diretriz de Segurança da Autoridade peruana recomenda, para fins de cumprimento do dever de segurança, que qualquer violação de dados deve ser informada aos titulares dos dados assim que for confirmada.

VI. Crianças e adolescentes

O Decreto regulamentador da LPDP estabelece que o tratamento de dados pessoais de crianças e adolescentes exige:

- consentimento livre, prévio, expresso e informado se o titular for maior de 14 anos e menor de 18 anos, ou de seus representantes legais (pais ou responsáveis) se o titular for menor de 14 anos;
- que as informações fornecidas a eles no momento da obtenção de seu consentimento sejam expressas em uma linguagem compreensível;
- que o consentimento obtido não se destine a oferecer bens ou serviços proibidos a crianças e adolescentes (por exemplo, álcool ou conteúdo impróprio);
- que os dados pessoais dos menores que permitam obter informação sobre os membros do seu grupo familiar (p. ex., informações sobre renda) não podem ser coletados sem o consentimento dos titulares desses dados; e
- que os tratamentos de dados sejam realizados respeitando princípios gerais de proteção de dados pessoais, como a proporcionalidade, que estabelece que todos os atos de tratamento de dados devem ser adequados, relevantes e não excessivos para os fins para os quais os dados foram coletados.

VII. Contratos

Não existe nenhuma disposição expressa na LPDP que obrigue os agentes de tratamento de dados a celebrar contratos formais escritos. No entanto, o Decreto regulamentador da LPDP sugere que os contratos escritos podem ser um bom mecanismo para obrigar os operadores de dados a assumir todas as obrigações impostas pela LPDP e, assim, garantir que as informações pessoais sejam tratadas de acordo com a lei peruana.

5.5. Fiscalização

A autoridade de proteção de dados do Peru é a Autoridade Nacional de Proteção de Dados Pessoais (*Autoridad Nacional de Protección de Datos Personales*). Suas principais competências são:

- representar o país perante instâncias internacionais relativas à proteção de dados pessoais;
- gerir e manter atualizado o Registro Nacional de Proteção de Dados Pessoais;
- realizar campanhas de promoção sobre a proteção de dados pessoais;
- fiscalizar o cumprimento da LPDP;
- esclarecer dúvidas sobre proteção de dados pessoais e o significado da regulamentação em vigor na matéria; e
- receber, apurar e dar resposta às reclamações dos titulares dos dados relativas à violação dos direitos que lhes digam respeito e emitir as medidas cautelares ou corretivas estabelecidas no Decreto regulamentador e demais regulamentos expedidos pela Autoridade.

As possíveis sanções por violação dos padrões de proteção de dados variam dependendo da natureza ou escala da infração:

- para infrações menores, multas de até 5 unidades fiscais (aprox. 32,5 mil reais);
- para infrações graves, multas de até 50 unidades fiscais (aprox. 324 mil reais); e
- para infrações muito graves, multas de até 100 unidades fiscais (aprox. 648 mil reais).

A Autoridade peruana também está autorizada a aplicar multas adicionais de até 62 mil reais se o infrator, apesar de ser responsabilizado pela infração, não remediar a prática ilegal. Estas multas adicionais são aplicáveis em complemento à responsabilidade civil e criminal.

A Autoridade peruana tem sido muito proativa no cumprimento da LPDP. Em 2021, auditou 335 entidades públicas e privadas, dentre bancos, agências de crédito e estabelecimentos de saúde; realizou apuração de infrações que resultaram em mais de 100 decisões em processos sancionatórios e aplicação de penalidades pecuniárias num montante total de 1.380 unidades tributárias (aprox. 1,5 milhões de euros). O montante de multas pecuniárias aplicadas a diferentes entidades privadas e públicas em 2021 quase triplicou o valor aplicado antes do início da pandemia e é esperado que essa tendência se mantenha.

Quadro-resumo

Principais normas	• Constituição Política do Peru. • Lei nº 29.733/2011 – Lei de Proteção de Dados Pessoais. • Decreto Supremo nº 003-2013-JUS, que regulamentada a LPDP. • Lei nº 27.489/2001, que regula birôs de crédito. • Lei nº 30.096/2013 sobre crimes cibernéticos. • Decreto de Emergência nº 007-2020 – Marco da Confiança Digital.
Bases legais	• Consentimento. • Exceções ao consentimento: **i.** cumprimento de obrigação legal; **ii.** legítimo interesse do titular de dados; **iii.** tratamento relacionado com a saúde; **iv.** solvência financeira ou capacidade creditícia de uma pessoa; **v.** contrato em que o titular seja parte; **vi.** quando tiver o dado pessoal tiver sido anonimizado; **vii.** dados de fontes publicamente acessíveis; **viii.** exercício do direito fundamental à liberdade de informação; e **ix.** prevenção da lavagem de dinheiro e financiamento do terrorismo.
Direitos dos titulares	• Ser informado. • Acesso. • Retificação e eliminação. • Oposição. • Não se submeter a decisões automatizadas. • Portabilidade. • Tutela. • Indenização. • Revogação do consentimento.
Obrigações controlador e operador	• Registrar bases de dados perante a Autoridade. • Tratar dados pessoais com uma base legal adequada. • Não coletar dados pessoais usando meios fraudulentos, ilegais ou injustos. • Coletar dados apenas quando necessários e pertinentes para as finalidades informadas aos titulares dos dados. • Permitir o exercício dos direitos dos titulares dos dados de forma facilitada e gratuita. • Eliminar dados pessoais quando já não sejam mais necessários ou relevantes para a finalidade para a qual foram coletados ou quando o prazo para o seu tratamento tenha acabado, salvo se anonimizados ou dissociados. • Adotar medidas técnicas, organizacionais e legais que garantam a segurança dos dados e impeçam sua alteração, tratamento ou acesso não autorizado. • Manter a confidencialidade dos dados pessoais. • Permitir à Autoridade peruana de proteção de dados acesso à base de dados e fornecer-lhe a informação necessária no âmbito de um processo administrativo.
Fiscalização	• A Autoridade de Proteção de dados do Peru é a Autoridade Nacional de Proteção de Dados Pessoais. É incumbida de fiscalizar e fazer valer a LPDP no Peru, podendo aplicar sanções, bem como de gerir o Registro Nacional de Proteção de Dados Pessoais.

‹voltar para o índice

Conclusão

Verifica-se como a estrutura normativa de proteção de dados pessoais da Argentina, Colômbia, Chile e Peru apresentam semelhanças gerais significativas. Em graus distintos percebe-se como as legislações desses países tiveram algum nível de influência da legislação europeia de proteção de dados, seja pela Diretiva anterior (95/46/CE) ou pela GDPR (2016/679).

Destaca-se a ênfase no consentimento como base para tratamento de dados pessoais em todos os países. Dentre os direitos previstos, destaca-se que todos os países preveem o direito do titular de obter informações sobre como seus dados pessoais são tratados e o direito de retificar seus dados. Outro destaque interessante é a exigência encontrada na Argentina, Colômbia e Peru para que os controladores registrem a existência de seus bancos de dados nas autoridades de proteção de dados.

Quanto às diferenças, chama a atenção o fato de o Chile não ter uma autoridade de proteção de dados própria, apesar de haver discussão legislativa no país para criação de uma. Os valores das multas aplicáveis também apresentam variação significativa, destacando-se o baixo valor das multas na Argentina.

Conforme observou-se, as leis de cada um dos países estão passando ou passaram por alterações significativas. Nesse sentido, interessante acompanhar essa evolução para avaliar qual será o nível de aproximação das legislações de proteção de dados na América Latina, e verificar como elas podem vir a se diferenciar da legislação europeia, a qual possui forte influência no continente.

b/luz

deixa com a gente

Para saber mais, acesse nosso site ou
nos acompanhe nas redes sociais.

baptistaluz.com.br