Workbook
Privacidade, Dados Pessoais e LGPD

Edição 202412

Sobre o autor

Livro original em inglês (base GDPR):

Leo Besemer
Privacy and Data Protection based on the GDPR: Understanding the General Data Protection Regulation
Van Haren Publishing, 2020

Contato: leo.besemer@certiqa.nl

Adaptação em português (base LGPD)

Revisão em 2021 por:

Daniela Cabella
Primeira certificada como DPO pelo EXIN no continente americano
https://www.linkedin.com/in/danielacabella/

Gisele Kauer
Advogada certificada pelo EXIN (PDPE e ISFS)
https://www.linkedin.com/in/giselekauer

Revisão em 2024 por:

Adrianne Lima
Advogada, líder em Segurança da Informação, DPO desde 2019 e instrutora das trilhas de formação DPO e ISO
https://www.linkedin.com/in/adrianneclima/

Conteúdo

Lista de figuras

EXIN Privacy & Data Protection Essentials based on LGPD

Introdução

Este workbook apresenta um resumo da literatura para os candidatos que estudam para o exame EXIN Privacy & Data Protection Essentials based on LGPD (PDPELGPD), exame em português baseado na Lei Geral de Proteção de Dados Pessoais (LGPD). Este Workbook leva em consideração, entre outras, as seguintes referências: Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018); Resolução CD/ANPD nº 1/2021; Resolução CD/ANPD nº 2/2022; Resolução CD/ANPD nº 4/2023, Resolução CD/ANPD nº 15/2024; Resolução CD/ANPD nº 18/2024; Guia Orientativo ANPD Fev/2024; e Guia Orientativo ANPD Jun/2023. Para informações sobre os requisitos mais recentes para o exame, consulte o Guia de Preparação do EXIN, que pode ser baixado em www.exin.com.

Em um mundo cada vez mais digital, os dados pessoais se tornaram ativos valiosos porque são amplamente utilizados para orientar decisões estratégicas nas empresas e no setor público. Esses dados permitem a personalização de produtos, a criação de campanhas de marketing direcionadas e o desenvolvimento de serviços sob medida. No entanto, a coleta e o armazenamento em larga escala, facilitados por novas tecnologias, também aumentam os desafios de segurança. A proteção dessas informações se tornou essencial com a entrada em vigor da Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709/2018, que exige das organizações práticas rigorosas de governança e segurança.

A LGPD segue uma tendência global, impulsionada pela implementação do Regulamento Geral de Proteção de Dados (RGPD/GDPR) na Europa e pela pressão de organismos internacionais, como a Organização para a Cooperação e Desenvolvimento Econômico (OCDE), para uma proteção de dados mais eficiente. No Brasil, a LGPD, que entrou em vigor em setembro de 2020, exige que todas as organizações dos setores público e privado que tratam dados de pessoas localizadas no Brasil adotem práticas de governança e segurança rigorosas. Isso inclui empresas fora do país que oferecem produtos ou serviços a brasileiros ou realizam qualquer tipo de tratamento de dados em território nacional.

A Autoridade Nacional de Proteção de Dados (ANPD), responsável por fiscalizar o cumprimento da LGPD, já iniciou sua atuação, com um planejamento estratégico vigorando entre 2021 e 2023. A partir disso, a observância às normas da LGPD se tornou imperativa. Além de prevenir sanções administrativas, a conformidade com a LGPD fortalece a confiança de clientes e cidadãos, que cada vez mais exigem a proteção de seus dados como um direito fundamental, assegurado pela Constituição Federal.

A não conformidade legal pode gerar não apenas sanções administrativas, mas também ações judiciais por parte dos titulares, fortalecendo a importância da proteção de dados como um tema central nas discussões sobre privacidade no Brasil e no mundo.

Figura 1. Benefícios em cumprir a LGPD

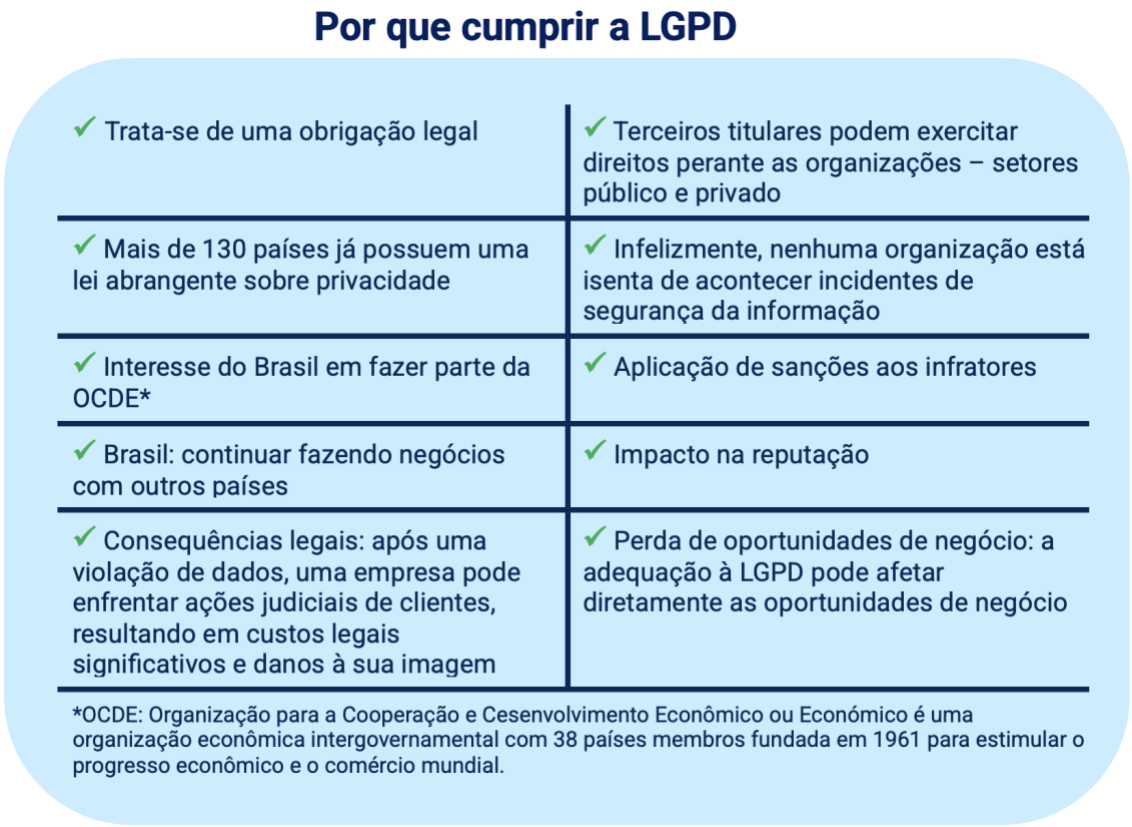

Imagem criada pelo EXIN com base em: Lima, Adrianne (2024). *Por que cumprir a LGPD*.

A certificação EXIN Privacy & Data Protection Essentials based on LGPD (PDPELGPD) pode ser altamente benéfica para profissionais que desejam demonstrar conhecimentos em privacidade de dados e adequação à legislação brasileira de proteção de dados em várias situações, como processos seletivos para vagas de trabalho, propostas de consultoria e participação em licitações. A certificação também facilita o reconhecimento internacional, já que o EXIN é uma organização respeitada no campo de certificações de TI e governança.

A certificação EXIN Privacy & Data Protection Essentials based on LGPD confirma que o profissional compreende os conceitos e princípios básicos de proteção de dados no contexto da LGPD. Isso é especialmente relevante, considerando que a conformidade com a LGPD é uma exigência crescente para empresas e órgãos públicos. Paralelamente a isso, em processos seletivos ou propostas de consultoria, essa certificação pode servir como um diferencial. Para empresas que precisam mostrar compromisso com a privacidade de dados, contar com profissionais certificados reforça a imagem de conformidade, segurança e seriedade.

Portanto, investir nessa certificação pode trazer benefícios não só para a carreira do profissional, mas também para as empresas ou consultorias em que o profissional atua, ao demonstrar um compromisso ativo com a proteção de dados e conformidade legal.

EXIN, dezembro de 2024.

Fundamentos de privacidade

1 Definições e contexto histórico

Neste capítulo, veremos a história da privacidade e proteção de dados e a relação entre os dois conceitos. Com isso, analisaremos algumas definições básicas, já que elas são previstas na Lei Geral de Proteção de Dados Pessoais (LGPD). Alguns dos termos e conceitos são explicitamente definidos no artigo 5º da LGPD e outros são derivados do direito internacional.

1.1 A história das regulações de proteção de dados – contexto internacional

A Declaração Universal dos Direitos Humanos (DUDH) da ONU foi aprovada em 1948 como uma resposta imediata às atrocidades da Segunda Guerra Mundial. Com o objetivo de estabelecer um padrão mínimo de direitos humanos a ser protegido globalmente, a Declaração simbolizou um compromisso internacional para garantir que os horrores da guerra não se repetissem. O artigo 12 da Declaração trata especificamente do direito à privacidade, determinando que

> Ninguém será alvo de ingerências arbitrárias em sua vida privada, família, residência ou correspondência, nem de ataques contra sua honra e reputação. Todos têm direito à proteção legal contra essas interferências ou agressões.
>
> Fonte: Declaração Universal dos Direitos Humanos (DUDH) (art. 12)

Em 1950, o Conselho da Europa criou a Convenção Europeia dos Direitos Humanos, inspirada nos princípios da Declaração Universal da ONU. Essa Convenção incorporou a proteção à vida privada e familiar e ao acesso à informação, ao mesmo tempo em que permitiu a intervenção das autoridades públicas nesses direitos com limites definidos, como segurança nacional, ordem pública, bem-estar econômico, manutenção da ordem, prevenção de crimes, defesa da saúde ou moral, e a proteção dos direitos e liberdades de terceiros. A Convenção foi um marco, consolidando a noção de direito ao respeito pela vida privada e familiar.

Em 1973 e 1974, o Conselho da Europa introduziu as Resoluções nº 22 e nº 29, estabelecendo princípios para a proteção de dados pessoais em bases de dados eletrônicos, tanto no setor público quanto no privado. Em 1979, sete países da Comunidade Europeia, incluindo Dinamarca, França, Alemanha, Luxemburgo e Noruega, implementaram legislações nacionais de privacidade. Áustria, Espanha e Suécia foram além, incorporando a proteção de dados em suas constituições ou criando leis com status constitucional.

Em 1980, a Organização para a Cooperação e Desenvolvimento Econômico (OCDE) adotou as Diretrizes sobre a Proteção da Privacidade e Fluxos Transfronteiriços de Dados Pessoais. Embora fossem apenas recomendações, essas diretrizes representaram um passo significativo para a harmonização das legislações de privacidade e o fluxo internacional de dados.

A busca por fortalecer essas resoluções resultou na criação, em 1981, da Convenção nº 108 pelo Conselho da Europa, o primeiro tratado internacional dedicado à proteção de indivíduos no tratamento automatizado de dados pessoais.

A Diretiva nº 95/46/CE, introduzida em 1995 pela Comissão Europeia, reconheceu que a Convenção nº 108 não cobria todos os aspectos necessários para uma proteção abrangente e

eficaz da privacidade, o que levou à sua substituição. Cinquenta anos após a primeira convenção, a Carta dos Direitos Fundamentais da União Europeia foi proclamada, destacando os artigos 7 e 8, que versam sobre o respeito à vida privada e familiar e a proteção de dados pessoais, respectivamente.

Por fim, em 2016, a introdução do Regulamento Geral sobre a Proteção de Dados (RGPD) (mais conhecido como GDPR) marcou um avanço crucial. Entrando em vigor em 2018, o GDPR substituiu a Diretiva nº 95/46/CE, estabelecendo um marco legal de aplicação direta com o intuito de eliminar disparidades entre as legislações nacionais, ampliar a proteção à privacidade e modernizar as leis para enfrentar os desafios atuais, incluindo aqueles advindos do avanço da internet.

1.2 A história das regulações de proteção de dados – contexto nacional

As bases para a legislação nacional específica de proteção de dados foram construídas principalmente por meio da consolidação do direito à privacidade como um direito fundamental na Constituição Federal de 1988. O artigo 5º, incisos X e XII, assegura a inviolabilidade da intimidade, da vida privada, da honra e da imagem dos indivíduos, bem como o sigilo de correspondências e das comunicações telegráficas e telefônicas, exceto, neste último caso, por determinação judicial.

A década de 1990 trouxe avanços significativos, incluindo decisões importantes do Supremo Tribunal Federal em 1991, que trataram do *habeas data*, garantindo o direito de acesso, retificação e complementação de registros pessoais. Nesse mesmo período, o Código de Defesa do Consumidor destacou a importância da segurança e do direito à informação sobre serviços prestados.

O Código de Defesa do Consumidor (1990) visa salvaguardar os direitos dos consumidores, incluindo a proteção contra publicidade enganosa e abusiva, além de práticas comerciais coercitivas ou desleais. Embora não trate diretamente de dados pessoais, o código estabeleceu um marco para a defesa dos direitos dos consumidores, abrangendo inclusive a proteção da privacidade em transações comerciais.

A Lei de Acesso à Informação (LAI, Lei nº 12.527/2011) representa um pilar essencial na promoção da transparência e governança pública, tendo uma relação importante com a proteção de dados, privacidade e intimidade.

O Marco Civil da Internet, sancionado em 2014 (Lei n. 12.965/2014), estabeleceu diretrizes para a proteção de registros, dados pessoais e comunicações privadas na internet no Brasil. Este marco legal foi crucial para a evolução do direito à privacidade, ao delinear normas para a coleta, uso, armazenamento e tratamento de dados pessoais, além de reforçar a proteção à intimidade e à vida privada.

Em agosto de 2018, a Lei Geral de Proteção de Dados Pessoais (LGPD) (Lei nº 13.709/2018), foi aprovada. Essa lei específica e unificada sobre proteção de dados pessoais coloca o Brasil e as organizações estabelecidas em território nacional em outro patamar no cenário econômico mundial, com um maior nível de confiança por parte do mercado e da comunidade internacional e maior protagonismo na economia digital.

A conformidade com a LGPD não apenas evita multas e outras sanções, mas agrega valor e uma série de benefícios operacionais à organização, como por exemplo:

- Isso colabora para que as empresas evitem violações de dados, economizando tempo e dinheiro que seriam gastos na gestão de incidentes e possíveis sanções[1];
- Com a conformidade às normas de proteção de dados, há aumento da confiança dos consumidores;
- Isso protege as empresas de fraudes e cibercrimes, garantindo a segurança não apenas dos dados pessoais, mas também das informações internas da organização, evitando prejuízos financeiros e danos à imagem da empresa[2].

Além disso, a Constituição Federal foi emendada, mostrando um movimento claro para alinhar a proteção de dados pessoais aos direitos fundamentais dos cidadãos (Emenda Constitucional nº 115, de 10 de fevereiro de 2022). Isso buscou incluir explicitamente a proteção de dados na lei maior do Brasil e garantir que a competência para legislar sobre o tema fosse exclusiva da União, reconhecendo a importância da proteção de dados em nível constitucional.

1.2.1 Cronologia da proteção de dados

Ano	Nome	Sigla
1948	Declaração Universal dos Direitos Humanos	DUDH (UHDR)
1950	Convenção Europeia sobre Direitos Humanos	CEDH (ECHR)
1980	Diretrizes para a Proteção da Privacidade e Fluxos Transfronteiriços de Dados Pessoais	OCDE
1981	Convenção para Proteção de Indivíduos relativamente ao Processamento Automático de Dados Pessoais	ETS 108 = EU Tratado de Estrasburgo (Convenção 108)
1988	Constituição Federal do Brasil	CF
1990	Código de Defesa do Consumidor	CDC
1995	Diretiva n. 95/46/CE relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados	95/46/EC - Diretiva de Privacidade (válida até 25/5/2018)
2002	Carta dos Direitos Fundamentais da União Europeia Código Civil	CEDH (EU Charter) CC
2002	Código Civil Brasileiro	CC
2011	Lei de Acesso à Informação	LAI
2012	Alterações no Código Penal Brasileiro (Lei n.º 12.737/2012 - Crimes Cibernéticos)	Crimes Cibernéticos
2014	Marco Civil da Internet	MCI
2016	Regulamento Geral de Proteção de Dados (EU - 2016/679)	'GDPR' (a partir de 25/5/2018)
2016	Decreto n.º 8.771/2016 - Regulamentação do Marco Civil da Internet	Decreto 8.771
2018	Brasil: Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018)	LGPD
2022	Emenda Constitucional n.º 115 - Inclusão da proteção de dados como direito fundamental	EC 115

[1] IBM. *How to implement the General Data Protection Regulation (GDPR).* Disponível em: https://www.ibm.com/think/topics/general-data-protection-regulation-implementation. Acesso em 21.09.2024.
[2] EDPB. *Data protection benefits for you*. Disponível em: https://www.edpb.europa.eu/sme-data-protection-guide/data-protection-benefits-for-you_en. Acesso em 21.09.2024.

1.3 Escopo material e territorial da LGPD

1.3.1 Escopo material

Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Fonte: Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709/2018 (art. 1º, *caput*)

A LGPD se aplica a dados pessoais apresentados de forma estruturada ou não, desde sistemas de banco de dados totalmente automatizados até arquivos baseados em papel, como os prontuários médicos clássicos ainda usados em algumas clínicas médicas.

Existem algumas exceções: a LGPD não se aplica ao tratamento de dados pessoais de cunho puramente doméstico, ou seja, realizado para fins exclusivamente particulares e não econômicos. A lei também não se aplica ao tratamento feito para cumprir finalidades unicamente jornalísticas e artísticas.

O tratamento de dados pessoais realizado para fins exclusivos de segurança pública, defesa nacional, segurança do Estado e atividades de investigação e repressão de infrações penais será objeto de legislação específica, e a Autoridade Nacional de Proteção de Dados (ANPD) emitirá opiniões técnicas ou recomendações referentes a esses temas e deverá solicitar Relatórios de Impacto à Proteção de Dados (RIPD) aos respectivos responsáveis.

Por fim, não se aplica a LGPD ao tratamento de dados pessoais que não ocorra, de nenhuma forma, em território brasileiro e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados que envolva o Brasil.

1.3.2 Escopo territorial

Art. 3º Esta Lei aplica-se a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que:

- I - a operação de tratamento seja realizada no território nacional;
- II - a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; ou
- III - os dados pessoais objeto do tratamento tenham sido coletados no território nacional.

§ 1º Consideram-se coletados no território nacional os dados pessoais cujo titular nele se encontre no momento da coleta.

Fonte: Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709/2018 (art. 3º, *caput* e § 1º)

Qualquer tratamento de dados pessoais no contexto das atividades de um estabelecimento de um controlador ou de um operador no Brasil deve ser efetuado em conformidade com a LGPD, independentemente do local (no mundo) em que os dados sejam tratados efetivamente (por exemplo, um controlador tem sede no Brasil, mas os dados estão em um servidor de cloud computing no Arizona, EUA).

A LGPD também se aplica ao tratamento relacionado ao comércio (a oferta ou o fornecimento de bens ou serviços) e ao tratamento de dados pessoais de pessoas que estão localizadas no território nacional. Isso tem consequências de longo alcance. Por exemplo, o caso de uma empresa canadense que trata dados pessoais de um cidadão argentino para uma compra online. Se esse cidadão argentino estiver visitando João Pessoa (Brasil) no momento da compra e a empresa canadense estiver oferecendo bens ou serviços para o Brasil de forma intencional (porque eles enviam produtos para o Brasil e apresentam uma versão da Política de Privacidade em português do Brasil, por exemplo), esse tratamento está sujeito à LGPD.

Além disso, a LGPD se aplica ao tratamento de dados pessoais por um controlador não estabelecido em território brasileiro, mas em que "os dados objeto do tratamento tenham sido coletados em território nacional" (LGPD, art. 3º, III).

1.4 Definições

Nos primeiros dispositivos da LGPD, constam os fundamentos do tema de proteção de dados pessoais:

Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos:

- I - o respeito à privacidade;
- II - a autodeterminação informativa;
- III - a liberdade de expressão, de informação, de comunicação e de opinião;
- IV - a inviolabilidade da intimidade, da honra e da imagem;
- V - o desenvolvimento econômico e tecnológico e a inovação;
- VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e
- VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

Fonte: Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709/2018 (art. 2º)

A autodeterminação informativa é um princípio que dá ao indivíduo o controle sobre seus dados pessoais. Isso significa que cada pessoa tem o direito de decidir quais informações sobre si podem ser coletadas, como essas informações podem ser usadas e por quem.

Embora o princípio de autodeterminação informativa não esteja explicitamente mencionado na Constituição Brasileira, ele é implícito no direito à privacidade e proteção de dados, protegido pelo art. 5º, X, da Constituição Federal.

O conceito de autodeterminação informativa tem sua origem no direito alemão, sendo reconhecido pela primeira vez pelo Tribunal Constitucional Federal da Alemanha em 1983, no contexto do censo populacional. Esse momento foi crucial para estabelecer a importância do controle individual sobre os dados pessoais, especialmente em relação à capacidade do Estado de coletar e usar esses dados[3].

A autodeterminação informativa na LGPD é reforçada pelo Capítulo III, especialmente pelo artigo 18, que estabelece direitos fundamentais dos titulares de dados, como o direito à informação, acesso, correção e eliminação de dados, entre outros.

[3] *Decisão do Tribunal Constitucional Federal Alemão (Bundesverfassungsgericht)*. Disponível em: https://www.bundesverfassungsgericht.de/EN/Verfahren/Der-Weg-zur-Entscheidung/der-weg-zur-entscheidung_node.html. Acesso em 21.09.2024.

A disciplina da proteção de dados pessoais está explicitamente ligada à Constituição Federal, que prevê:

Art. 5º. Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:

- IV - é livre a manifestação do pensamento, sendo vedado o anonimato;
- X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;
- XII - é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal;

Fonte: Constituição da República Federativa do Brasil, 1988

A disciplina da proteção de dados pessoais também possui referência ao já previsto, desde 2022, no Código Civil:

CAPÍTULO II - Dos Direitos da Personalidade

Art. 21. A vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma.

Fonte: Código Civil (art. 21)

Nesse sentido, a proteção de dados pessoais é um meio efetivo para garantir o pleno exercício de direitos e liberdades fundamentais das pessoas – dentre eles, a sua privacidade.

1.4.1 Privacidade

A privacidade é definida como o direito ao respeito à vida privada (particular, íntima) e familiar de uma pessoa, sua casa e suas comunicações.

Esse direito abrange a proteção contra a divulgação não autorizada de informações pessoais, bem como a proteção contra vigilância e invasões que possam comprometer a honra, imagem e integridade pessoal.

1.4.2 Proteção de Dados

É importante destacar que a LGPD não protege todo e qualquer tipo de dado, mas somente os dados definidos no art. 5º como “pessoais”.

A proteção de dados refere-se ao conjunto de medidas legais, técnicas e organizacionais que garantem a segurança, confidencialidade, integridade e controle sobre os dados pessoais de indivíduos, protegendo-os contra acessos não autorizados, uso inadequado ou divulgação indevida.

O objetivo central da proteção de dados é assegurar que o tratamento (coleta, armazenamento, uso, compartilhamento, etc.) de informações pessoais seja feito de forma transparente e segura, respeitando os direitos fundamentais à privacidade e à autodeterminação informativa dos titulares dos dados.

Portanto, dados exclusivamente relacionados a estratégias de negócios ou planejamento de novos produtos, por exemplo, podem ser considerados “sigilosos” ou “confidenciais” e devem ser protegidos de acessos indevidos ou não autorizados, mas não são regulados pela LGPD.

1.4.3 Dados pessoais

O art. 5º, inciso I, da LGPD define dados pessoais como:

> Art. 5º Para os fins desta Lei, considera-se:
>
> - I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;
>
> Fonte: Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709/2018 (art. 5º, inciso I)

Dado pessoal significa qualquer informação relativa a uma pessoa natural identificada ou identificável (titular dos dados). Uma pessoa natural identificável é aquela que pode ser identificada, direta ou indiretamente, em particular por referência a um identificador, como um nome, número de identificação, dados de localização ou identificador online, ou a um ou mais fatores específicos de identidade física ou fisiológica e identidade genética, mental, econômica, cultural ou social daquela pessoa natural.

Qualquer informação pode ser tomada literalmente. Isso inclui informações objetivas, como atributos que podem ser medidos – por exemplo, tipo sanguíneo, tamanho do sapato ou a quantidade de álcool no sangue da pessoa. Isso também inclui informações subjetivas, tais como opiniões sobre uma pessoa (por exemplo, Ana é uma boa economista). Para que as informações sejam "dados pessoais", elas não precisam ser verdadeiras ou comprovadas. Mentiras ou dados incorretos sobre uma pessoa ainda podem ser considerados dados pessoais.

Figura 2. Principais conceitos da LGPD: dados pessoais

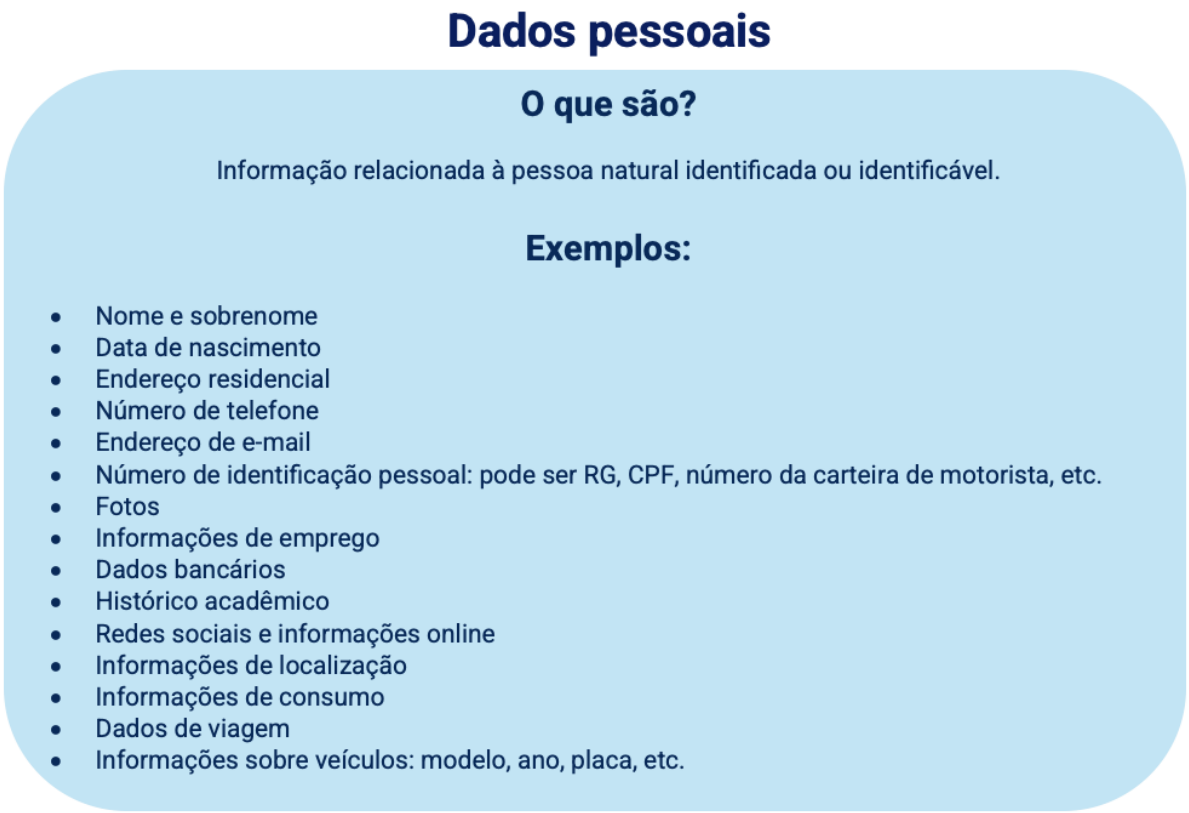

Imagem criada pelo EXIN com base em: Lima, Adrianne (2024). *Principais conceitos da LGPD: dados pessoais*.

Assim, o conceito de dados pessoais não se limita a informações que possam ser consideradas prejudiciais à vida privada e familiar do indivíduo. O meio em que as informações estão contidas também é irrelevante. O conceito de dados pessoais inclui informações disponíveis em qualquer formato: texto, figuras, gráficos, fotografias, vídeo, áudio ou qualquer outro formato possível.

1.4.3.1 Dados pessoais sensíveis

A LGPD classifica como dados pessoais sensíveis (ou de categoria especial) aqueles que revelam informações sobre:

- Origem racial ou étnica;
- Convicção religiosa;
- Opinião política;
- Filiação a sindicato ou organização de caráter religioso, filosófico ou político;
- Dados relacionados à saúde ou à vida sexual;
- Dados genéticos ou biométricos, quando associados a uma pessoa natural.

Esses tipos de dados são considerados sensíveis porque o seu uso inadequado pode levar a discriminação ou outros danos à liberdade e privacidade da pessoa. Por isso, sua coleta, armazenamento e processamento são geralmente sujeitos a restrições legais e medidas de segurança mais rigorosas.

Figura 3. Principais conceitos da LGPD: dados pessoais sensíveis

Imagem criada pelo EXIN com base em: Lima, Adrianne (2024). *Principais conceitos da LGPD: dados pessoais sensíveis.*

Os dados pessoais sensíveis somente podem ser tratados com o devido enquadramento em, no mínimo, uma das hipóteses do art. 11 da LGPD.

1.4.4 Pessoa natural

Tanto o inciso I, quanto V, descrevem o termo “pessoa natural” para o titular:

> Art. 5º Para os fins desta Lei, considera-se:
>
> - I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;
> - V - titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;
>
> Fonte: Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709/2018 (art. 5º, inciso I e V)

Juridicamente, uma pessoa natural é um ser humano, um indivíduo capaz de assumir obrigações e de ter direitos. No Código Civil Brasileiro, a pessoa natural é definida como o ser humano considerado sujeito de direitos e deveres na ordem civil. A capacidade de ser sujeito de direitos começa com o nascimento com vida, mas a lei põe a salvo, desde a concepção, os direitos do nascituro, conforme o artigo 2º do Código Civil. Isso significa que a pessoa natural adquire personalidade jurídica ao nascer, passando a ser titular de direitos e deveres, como a capacidade de contrair obrigações, adquirir bens, entre outros, respeitando os limites estabelecidos pela lei.

Figura 4. Principais conceitos da LGPD: titulares

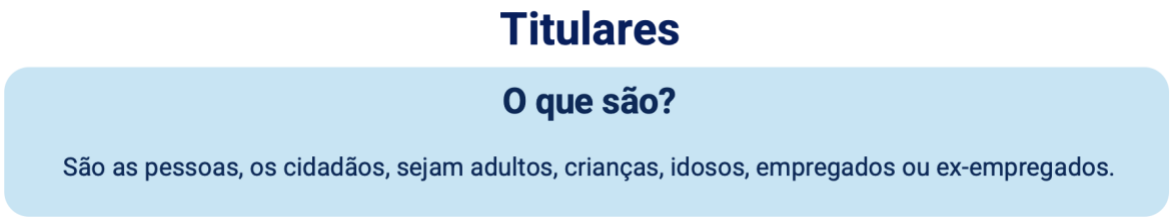

Imagem criada pelo EXIN com base em: Lima, Adrianne (2024). *Principais conceitos da LGPD: titulares.*

A princípio, a LGPD não se aplica a pessoas falecidas, como já ratificou a ANPD em decisão judicial:

> A LGPD se aplica apenas a informações relacionadas a pessoas naturais, ou seja, vivas, identificáveis ou identificadas. Os dados relativos a uma pessoa falecida não constituem dados pessoais para fins de LGPD e, portanto, não estão sujeitos ao nível de proteção da LGPD.
>
> Fonte: Nota Técnica nº 3/2023/CGF/ANPD[4]

1.4.5 Dados pessoais diretos e indiretos

Apesar de não explícitos na LGPD, na prática, há dois tipos de dados pessoais: diretos e indiretos.

1.4.5.1 Dados pessoais diretos

Dados pessoais diretos são dados que podem ser atribuídos diretamente a um indivíduo específico sem o uso de informações adicionais. Por exemplo, a foto, DNA ou impressão digital de um indivíduo. Os nomes podem ser dados pessoais diretos se forem raros, como no caso de um nome incomum. Além disso, títulos específicos que apontam diretamente para uma pessoa, como "o atual ministro da economia do Brasil", são considerados dados pessoais diretos, pois referem-se de maneira clara e imediata a um indivíduo específico.

[4] *Nota Técnica nº 3/2023/CGF/ANPD*. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/NotaTecnica3CGF.ANPD.pdf. Acesso em 21.09.2024.

1.4.5.2 Dados pessoais indiretos

Dados pessoais indiretos são aqueles que, por si só, não identificam diretamente uma pessoa, mas podem ser vinculados a um indivíduo específico quando combinados com outras informações. Por exemplo, uma placa de carro é um dado indireto, pois pode ser associada ao proprietário do veículo através de um banco de dados. Da mesma forma, números como o CPF, o número de previdência social ou o endereço IP são considerados dados pessoais indiretos, uma vez que podem ser relacionados a uma pessoa com o uso de informações adicionais. Mesmo que nem todos possam acessar essas informações para identificar um indivíduo, o fato de ser possível essa associação caracteriza-os como dados pessoais indiretos.

Além disso, nomes comuns como "João da Silva" são considerados dados pessoais indiretos, pois, para identificar uma pessoa específica com esse nome, é necessário utilizar dados adicionais, como data de nascimento ou endereço de residência.

1.4.6 Dados pessoais pseudonimizados

Pseudonimização de dados é o processo de disfarçar identidades. O objetivo desse processo é ser capaz de coletar dados adicionais relacionados ao mesmo indivíduo sem precisar conhecer sua identidade.

Um exemplo pode ser uma câmera registrando quantos carros únicos passam por uma ponte em uma estrada. O número da placa é um dado pessoal indireto. O controlador substituiria cada número da placa por uma chave ou pseudônimo exclusivo, mantendo uma tabela separada vinculando cada chave à placa correspondente (por exemplo, uma planilha Excel com “de x para y”). O controlador pode enviar esses dados pseudonimizados para um operador, mantendo a chave em um local seguro.

Dados pseudonimizados podem ser classificados como um tipo de dados pessoais indiretos, pois são necessários dados complementares para identificar os titulares. Essas informações adicionais (a "chave") ficam acessíveis apenas ao controlador. O processo é reversível, desde que a chave esteja disponível. Por isso, dados pseudonimizados ainda são considerados dados pessoais, já que a identificação do titular continua sendo tecnicamente viável.

Na pseudonimização, o controlador mantém essas informações extras separadamente, em um ambiente seguro e controlado, para possibilitar a reconexão entre os dados pseudonimizados e a identidade do titular sempre que necessário (LGPD, art. 13, § 4º).

1.4.7 Dados anonimizados

Já a anonimização é o processo pelo qual as informações deixam de ter quaisquer vínculos diretos e indiretos às pessoas naturais a quem se relacionavam originalmente. Dados anonimizados, portanto, **não são mais** considerados dados pessoais e a LGPD não se aplica a eles (pois a lei se aplica somente a dados pessoais)[5]. Dados pseudonimizados podem ser anonimizados com a destruição (sem volta) da chave.

Por exemplo, para pesquisas sobre saúde e hábitos alimentares, é chamado um grupo selecionado de titulares de dados. Os nomes, números de telefone e outros dados de identificação dos titulares dos dados são conhecidos e mantidos em um banco de dados, para o qual os titulares dos dados deram sua permissão. Os titulares dos dados são chamados várias vezes durante a pesquisa. Depois que o período da pesquisa termina, todos os dados identificáveis são apagados. Isso significa que os dados não podem mais ser vinculados aos titulares de dados específicos, porque

[5] ANPD. *Estudo técnico sobre a anonimização de dados na LGPD:* análise jurídica. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/estudo_tecnico_sobre_anonimizacao_de_dados_na_lgpd___analise_juridica.pdf e https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/estudo_de_casos_sobre_anonimizacao_de_dados_na_lgpd_.pdf. Acesso em 21.09.2024.

não existe uma chave. Somente dados pessoais mais gerais, como sexo e categoria etária, estão vinculados aos dados sobre saúde e hábitos alimentares. Em outras palavras, os dados estatísticos que resultaram da pesquisa são anonimizados.

1.4.8 Tratamento

No que diz respeito à LGPD, a definição de tratamento é ampla, exemplificativa e aplicável somente a operações com dados pessoais (e não de quaisquer tipos de dados):

> Tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;
>
> Fonte: Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709/2018 (art. 5º, inciso X)

A coleta de dados pessoais é tratamento. O armazenamento de dados pessoais é tratamento. Destruir dados pessoais também é tratamento. Mesmo fazer um backup de um servidor que não é seu, mas contém dados pessoais, seria considerado um tipo de armazenamento, incluído na definição de tratamento.

A LGPD também se aplica ao tratamento de dados pessoais em formatos físicos, como documentos impressos, papéis ou cadernos. Por exemplo, coletar dados pessoais ao preencher uma ficha de cadastro em papel é uma forma de tratamento, assim como o armazenamento de documentos impressos contendo informações pessoais em arquivos ou pastas.

Outros exemplos incluem a reprodução de dados ao fazer cópias de documentos físicos, a distribuição ao enviar informações pessoais impressas por correio, a eliminação ao destruir esses documentos, como rasgá-los ou triturá-los, e a transferência ao mover pastas físicas contendo dados pessoais de um departamento para outro. Dessa forma, o tratamento de dados pessoais, conforme definido pela LGPD, abrange tanto o meio digital quanto o físico.

1.5 Papéis, responsabilidades e partes interessadas (stakeholders)

1.5.1 Agentes de tratamento

A LGPD define no art. 5º, inciso IX, que os agentes de tratamento são o controlador e o operador.

Quando se trata de pessoas jurídicas de direito público, o art. 23 da LGPD remete àquelas mencionadas no parágrafo único do art. 1º da Lei de Acesso à Informação. Isso inclui órgãos da administração direta dos Poderes Executivo, Legislativo e Judiciário, bem como empresas públicas e sociedades de economia mista.

No caso de pessoas jurídicas de direito privado, a LGPD não fornece uma definição específica, sendo necessário recorrer ao Código Civil. De acordo com o art. 44 do Código Civil, as pessoas jurídicas de direito privado incluem: associações, sociedades, fundações, organizações religiosas, partidos políticos e empresas individuais de responsabilidade limitada.

Assim, a LGPD abrange tanto entidades de direito público quanto privado, impondo obrigações e definindo claramente os papéis de controlador e operador, garantindo que o tratamento de dados seja feito de forma segura e em conformidade com as regras estabelecidas.

Ainda, os agentes de tratamento de pequeno porte, segundo o Regulamento de aplicação da Lei nº 13.709, de 14 de agosto de 2018 (LGPD), aprovado pela Resolução CD/ANPD nº 2, de 27 de janeiro de 2022, são definidos como:

- Microempresas (ME);
- Empresas de Pequeno Porte (EPP), conforme o Estatuto Nacional da Microempresa e da Empresa de Pequeno Porte (Lei Complementar nº 123/2006);
- Startups;
- Pessoas jurídicas de direito privado, incluindo as sem fins lucrativos;
- Pessoas naturais que realizam tratamento de dados pessoais, exceto quando realizam tratamento de alto risco ou em grande escala.

Esses agentes são considerados de pequeno porte para fins de aplicação de algumas flexibilizações das obrigações previstas na LGPD. A ANPD estabeleceu critérios de volume de dados tratados, complexidade das operações e risco aos titulares para definir as condições em que esses agentes podem ser considerados de pequeno porte e, portanto, sujeitos a tratamentos diferenciados.

1.5.1.1 Controlador

Controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;

Fonte: Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709/2018 (art. 5º, inciso VI)

O controlador é a pessoa natural ou jurídica responsável pela **determinação das finalidades e meios do tratamento dos dados pessoais**.

É responsabilidade e papel do controlador implementar medidas técnicas e organizacionais apropriadas para cumprir a LGPD, incluindo políticas apropriadas de proteção de dados. Além disso, o controlador deve ser capaz de demonstrar que o processamento é executado de acordo com a LGPD.

É seu papel implementar medidas técnicas e organizacionais apropriadas para garantir o cumprimento da LGPD, além de ser capaz de demonstrar que o tratamento de dados está sendo realizado de acordo com a lei. Entre essas responsabilidades estão a criação de políticas de proteção de dados e o monitoramento contínuo do tratamento.

1.5.1.2 Operador

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

Fonte: Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709/2018 (art. 5º, inciso VII)

Um operador sempre age “em nome do controlador” e deve cumprir as instruções do controlador. O meio mais adequado para definir as instruções do controlador para o operador é através de um contrato firmado entre eles, o qual deve definir claramente as responsabilidades e limites da atuação do operador.

1.5.2 Encarregado pelo tratamento dos dados pessoais ou Data Protection Officer (DPO)

O encarregado pelo tratamento de dados pessoais, também conhecido como Data Protection Officer (DPO), é uma pessoa designada pelo controlador e/ou operador para atuar como canal de comunicação entre esses agentes, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD)[6].

1.5.2.1 Obrigatoriedade de nomeação

A LGPD estabelece a obrigatoriedade de nomeação do DPO pelos agentes de tratamento nos seguintes artigos:

- **Artigo 5º, inciso VIII:** define o encarregado como o responsável pelo canal de comunicação com titulares de dados e a ANPD;
- **Artigo 23:** aplica-se às pessoas jurídicas de direito público, que devem nomear um encarregado conforme as regras da LGPD para garantir a transparência e a boa governança no tratamento de dados;
- **Artigo 41:** estabelece que todos os agentes de tratamento de dados pessoais, sejam controladores ou operadores, devem indicar um encarregado. A exceção para esta obrigatoriedade é prevista para agentes de tratamento de pequeno porte, conforme regulamentação específica da ANPD.

1.5.2.1.1 Exceções à obrigatoriedade de nomeação

De acordo com a Resolução CD/ANPD nº 2, de 27 de janeiro de 2022, agentes de tratamento de pequeno porte não são obrigados a nomear um encarregado. No entanto, eles devem cumprir as seguintes exigências:

- **Artigo 11, §1º:** caso o agente de pequeno porte não nomeie um encarregado, ele deve disponibilizar um canal de comunicação adequado para que os titulares de dados possam exercer seus direitos conforme o artigo 41, §2º, inciso I da LGPD;
- **Artigo 11, §2º:** a indicação voluntária de um encarregado pelos agentes de pequeno porte será considerada uma política de boas práticas e governança, conforme o artigo 52, §1º, inciso IX da LGPD, e poderá ser levada em conta em eventuais processos de sanção ou avaliação de conformidade pela ANPD.

Além disso, o DPO deve reportar à alta gestão, garantindo uma **posição independente**, e sua autonomia deve ser protegida pelos agentes de tratamento:

[6] Alves, Davis; Lima, Adrianne. *Encarregados:* Data Protection Officer (DPO). 2021. Disponível em: https://www.amazon.com.br/Encarregados-Data-Protection-Officer-DPO/dp/B09K49JTDS/ref=tmm_pap_swatch_0?_encoding=UTF8&dib_tag=se&dib=eyJ2IjoiMSJ9.lCSEgylh-0qODxHaoZHrmCZ-l_rFoV5ghkOi6lUeXN42D-SUhVHs2pyt2vKQXvNw.mNC7bAp3UE3lNh2JDe5igS8crDuo5UUMlkvfz49Av80&qid=1727046245&sr=1-3. Acesso em 31.10.2024.

Dos Deveres dos Agentes de Tratamento

Art. 10. O agente de tratamento deverá

- I - prover os meios necessários para o exercício das atribuições do encarregado, neles compreendidos, entre outros, recursos humanos, técnicos e administrativos;
- II - solicitar assistência e orientação do encarregado quando da realização de atividades e tomada de decisões estratégicas referentes ao tratamento de dados pessoais;
- III - garantir ao encarregado a autonomia técnica necessária para cumprir suas atividades, livre de interferências indevidas, especialmente na orientação a respeito das práticas a serem tomadas em relação à proteção de dados pessoais;
- IV - assegurar aos titulares meios céleres, eficazes e adequados para viabilizar a comunicação com o encarregado e o exercício de direitos;
- V - garantir ao encarregado acesso direto às pessoas de maior nível hierárquico dentro da organização, aos responsáveis pela tomada de decisões estratégicas que afetem ou envolvam o tratamento de dados pessoais, bem como às demais áreas da organização.

Fonte: Resolução CD/ANPD nº 18, de 16 de julho de 2024 (art. 10)

1.5.2.2 Tarefas do encarregado ou Data Protection Officer (DPO)

Art. 41, § 2º As atividades do encarregado consistem em:

- I - aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;
- II - receber comunicações da autoridade nacional e adotar providências;
- III - orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e
- IV - executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.

§ 3º A autoridade nacional poderá estabelecer normas complementares sobre a definição e as atribuições do encarregado, inclusive hipóteses de dispensa da necessidade de sua indicação, conforme a natureza e o porte da entidade ou o volume de operações de tratamento de dados.

Fonte: Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709/2018 (art. 41, § 2º e 3º)

Portanto, as principais atribuições obrigatórias do DPO incluem:

- **Aceitar reclamações e comunicações dos titulares dos dados:** o DPO deve atuar como ponto de contato para que os titulares possam exercer seus direitos, como acesso, retificação e exclusão de dados, além de prestar esclarecimentos e adotar providências necessárias em resposta a essas solicitações;
- **Receber comunicações da Autoridade Nacional de Proteção de Dados (ANPD):** o DPO deve ser responsável por receber comunicações da ANPD e assegurar que as medidas adequadas sejam tomadas em resposta a essas comunicações;
- **Orientar funcionários e contratados:** o DPO tem a responsabilidade de instruir colaboradores e prestadores de serviço da organização sobre as práticas de proteção de dados pessoais, especialmente no que diz respeito às atividades de tratamento de dados. Isso inclui esclarecer dúvidas sobre o tratamento de dados, orientar sobre o planejamento de iniciativas que envolvam dados pessoais e assegurar que as operações estejam em conformidade com a LGPD;
- **Executar as demais atribuições legais:** o DPO deve executar todas as demais atribuições que lhe forem determinadas pelo controlador, conforme as exigências da legislação e normas complementares da ANPD.

Além das atribuições obrigatórias, o controlador ou operador podem atribuir outras responsabilidades ao DPO, de acordo com as necessidades da organização e a complexidade das operações de tratamento de dados (Resolução CD/ANPD nº 18, de 16 de julho de 2024). Essas responsabilidades podem incluir:

- **Elaboração e supervisão de políticas internas:** o controlador pode definir que o DPO auxilie na criação e implementação de políticas e procedimentos internos relacionados à proteção de dados, como políticas de segurança da informação e regras de boas práticas de governança;
- **Apoio na gestão de incidentes de segurança:** o DPO pode ser responsável por supervisionar o processo de resposta a incidentes de segurança envolvendo dados pessoais, incluindo a notificação de incidentes à ANPD e a mitigação de riscos;
- **Auxílio no registro de operações de tratamento:** o DPO pode ser encarregado de manter um registro atualizado das operações de tratamento de dados realizadas pela organização, conforme exigido pela LGPD;
- **Assessoria na elaboração de relatórios de impacto:** o DPO pode participar da elaboração de relatórios de impacto à proteção de dados pessoais, especialmente quando o tratamento envolver riscos elevados aos direitos e liberdades dos titulares;
- **Supervisão de transferências internacionais de dados:** o controlador pode definir que o DPO auxilie na avaliação e gestão das transferências internacionais de dados, garantindo que sejam cumpridos os requisitos legais para essas operações;
- **Orientação sobre design de produtos e serviços:** o DPO pode colaborar para garantir que novos produtos ou serviços desenvolvidos pela organização adotem o conceito de privacidade por design (*privacy by design*), garantindo que o tratamento de dados seja minimizado e adequado desde a concepção.

2 Tratamento de dados pessoais

Qualquer operação com dados pessoais está contida na definição de tratamento. O art. 6º da LGPD detalha os princípios do tratamento de dados.

2.1 Princípios de tratamento de dados

O tratamento de dados pessoais precisa estar em conformidade com os princípios elencados na LGPD. Esses princípios são:

- Finalidade;
- Adequação;
- Necessidade;
- Livre acesso;
- Qualidade dos dados;
- Transparência;
- Segurança;
- Prevenção;
- Não discriminação;
- Responsabilização e prestação de contas.

A seguir, cada um desses princípios é abordado separadamente.

2.1.1 Finalidade

Os dados pessoais devem ser tratados para cumprir propósitos legítimos, autorizados por lei, específicos, explícitos e informados ao titular.

A regra geral é que os dados pessoais não devem ser objeto de tratamento posterior incompatível com essas finalidades originais; no entanto, o § 7º do art. 7º da LGPD permite que os dados de acesso público ou tornados manifestamente públicos pelo próprio titular sejam tratados para novas finalidades, desde que: (i) sejam observados os propósitos legítimos e específicos para o novo tratamento, (ii) sejam garantidos meios efetivos para que os titulares possam exercer plenamente seus direitos, e (iii) sejam cumpridos os fundamentos e os princípios da LGPD.

2.1.2 Adequação

Considerando-se o contexto do tratamento, os dados pessoais devem ser tratados de forma compatível com as finalidades informadas ao titular. Esse princípio tem por objetivo garantir a ciência do titular sobre o que é feito com seus dados, bem como possibilitar certo controle e o efetivo exercício de seus direitos, quando aplicável.

Para o cumprimento desse princípio, é importante garantir que a ciência seja dada ao titular em tempo hábil; ou seja, caso um tratamento já tenha sido finalizado e a ciência tenha sido dada posteriormente, como seria possível o titular exercer seu direito de oposição (LGPD, art. 18, § 2º), quando cabível? O exercício desse direito certamente estaria prejudicado.

2.1.3 Necessidade

Os dados pessoais devem ser pertinentes, proporcionais e não excessivos, isto é, **limitados ao mínimo necessário** em relação aos fins para os quais são tratados. Deve-se levar em consideração não apenas os tipos (categorias) de dados pessoais necessários para cumprir as finalidades do tratamento, mas também o volume de dados, se não é possível atender ao mesmo objetivo do tratamento de forma subsidiária, menos invasiva à privacidade, e o período necessário para o cumprimento das finalidades legítimas.

Por exemplo, não é necessário ter permissão de acesso às fotos salvas em um dispositivo móvel para permitir que um usuário jogue um jogo online de "paciência" ou "campo minado". Também não é necessário coletar as intenções de votos de todos os brasileiros para se ter uma ideia da tendência relacionada ao resultado das eleições – basta coletar uma porcentagem proporcional à população de cada estado da federação e do distrito federal.

Ainda, caso se deseje saber apenas uma média de quantas pessoas passam por determinada estação de metrô por dia, não é necessário coletar e registrar seus dados pessoais de nenhuma forma – basta contabilizar o número de acessos ao metrô (entradas/saídas) que a catraca registra, de forma anônima, por dia.

Finalmente, caso determinados dados pessoais sejam coletados única e exclusivamente para fins de cumprimento de obrigação legal, por exemplo, eles devem ser eliminados, de forma segura (sem possibilidade de recuperação), após atingido esse propósito.

Podemos dizer, portanto, que a definição do princípio da necessidade, de forma ampla, abrange os princípios da necessidade de forma estrita (menor número de tipos ou categorias de dados pessoais possível), proporcionalidade (menor volume de dados pessoais possível), subsidiariedade (busca do meio menos invasivo à privacidade possível) e temporalidade (tratamento pelo tempo mínimo possível necessário para o cumprimento das finalidades legítimas).

2.1.4 Livre acesso

Os agentes de tratamento devem garantir aos titulares de dados pessoais meios eficazes para que possam realizar consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais. Essas informações podem ser colocadas nas políticas de privacidade dos sites e aplicações, por exemplo.

Para cumprir esse princípio, os controladores e operadores devem implementar mecanismos que permitam aos titulares:

- **Solicitar acesso aos dados pessoais:** o titular deve ser capaz de consultar quais dados a organização possui sobre ele, de forma clara e acessível. Isso inclui informações sobre o tipo de dados coletados, finalidades do tratamento, tempo de retenção e eventuais compartilhamentos com terceiros;
- **Consultar a forma do tratamento:** o controlador deve fornecer informações sobre como os dados pessoais estão sendo processados, incluindo quais operações de tratamento estão sendo realizadas, como coleta, armazenamento, uso e compartilhamento;
- **Consultar a duração do tratamento:** o titular deve ser informado sobre o período pelo qual seus dados pessoais serão mantidos, de acordo com a finalidade original do tratamento ou conforme o exigido por legislação aplicável;
- **Facilidade de solicitação:** a organização deve oferecer canais acessíveis, como formulários online, portais de privacidade ou suporte ao cliente, para que o titular possa exercer seu direito de livre acesso de forma simples e gratuita;
- **Informações sobre a integralidade dos dados:** o controlador deve fornecer ao titular todos os dados pessoais que estão sendo tratados, garantindo que o titular possa verificar a correção, precisão e atualidade dessas informações.

Essas práticas garantem que o livre acesso seja respeitado, proporcionando transparência e controle ao titular sobre o tratamento de seus dados pessoais.

2.1.5 Qualidade dos dados

Os dados pessoais devem ser precisos (exatos), claros, relevantes e atualizados, e todas as medidas razoáveis devem ser tomadas para garantir que eventuais dados incorretos, inexatos, obscuros ou desatualizados sejam retificados.

O atendimento a esse princípio depende da participação tanto do titular de dados como do próprio agente de tratamento. O titular é responsável por verificar seus dados pessoais e corrigi-los ou atualizá-los, sempre que aplicável, e o agente de tratamento também deve, do seu lado, buscar garantir que o titular de dados tenha meios para acessar, atualizar ou retificar seus dados.

Para garantir o cumprimento desse princípio, os agentes de tratamento devem adotar as seguintes medidas:

- **Exatidão dos dados:** o controlador é responsável por garantir que os dados pessoais sejam precisos e corretos, evitando o uso de informações desatualizadas ou incorretas. Isso significa manter processos internos que verifiquem a veracidade dos dados e corrigir qualquer erro quando solicitado ou detectado;
- **Clareza:** os dados pessoais devem ser tratados de forma transparente, garantindo que sejam compreensíveis e acessíveis ao titular, sem ambiguidades. A organização deve utilizar uma linguagem clara ao fornecer informações sobre os dados e evitar complexidade excessiva;
- **Relevância:** os dados coletados e tratados devem ser estritamente necessários e adequados à finalidade a que se destinam. Isso evita o armazenamento de informações irrelevantes ou excessivas, garantindo que apenas os dados pertinentes ao objetivo do tratamento sejam mantidos;
- **Atualização dos dados:** o controlador deve manter os dados atualizados, principalmente em relação a informações que possam mudar com o tempo, como endereço, nome ou estado civil. Isso inclui a criação de mecanismos que permitam ao titular solicitar a atualização de seus dados sempre que necessário;
- **Correção e exclusão:** o titular tem o direito de solicitar a retificação ou exclusão de seus dados pessoais quando esses estiverem incorretos, desatualizados ou desnecessários. O controlador deve disponibilizar canais para que essas solicitações possam ser feitas de forma fácil e eficiente.

2.1.6 Transparência

Os titulares devem ter fácil acesso a informações clara e precisas sobre o tratamento de seus dados pessoais e saber quais são os agentes envolvidos. O nível de detalhamento das informações deve respeitar os segredos comerciais e industriais. Isso significa, por exemplo, mencionar em uma política de privacidade quais categorias de dados (como faixa etária, renda, imóveis em nome próprio) serão levadas em consideração para o estudo da concessão ou não de crédito, mas a forma de valorar e equacionar cada dado é segredo comercial e não deverá ser revelada.

Conforme o art. 17, § 2º da Resolução CD/ANPD nº 19, o controlador que realiza transferência internacional de dados deve disponibilizar, em sua página na internet, um documento em língua portuguesa, redigido em linguagem simples, clara, precisa e acessível, contendo informações detalhadas sobre a forma, duração e finalidade da transferência; o país de destino dos dados; a identificação e contatos do controlador; o uso compartilhado de dados e sua finalidade; as responsabilidades dos agentes envolvidos no tratamento; as medidas de segurança adotadas; além dos direitos dos titulares e como exercê-los, incluindo um canal de fácil acesso e a possibilidade de peticionar contra o controlador perante a ANPD.

O § 3º do mesmo artigo permite que esse documento seja disponibilizado em uma página específica ou integrado de forma destacada à Política de Privacidade ou outro instrumento equivalente. Essas obrigações visam garantir a transparência no tratamento de dados, assegurando que os titulares recebam informações claras e completas, principalmente em relação à transferência internacional de dados, sem comprometer os segredos comerciais da organização.

2.1.7 Segurança

Os agentes de tratamento devem aplicar medidas técnicas e administrativas para garantir a segurança adequada dos dados pessoais contra quaisquer tipos de tratamentos não autorizados, sejam eles acidentais ou ilícitos.

Medidas como treinamento em segurança da informação para os funcionários envolvidos no tratamento, de modo a minimizar falhas humanas, controle de acesso, plano de resposta a incidente testado e implementado com sucesso, criptografia nos dados em trânsito e em repouso, backup, política de segurança da informação completa, atualizada, amplamente divulgada entre os colaboradores e com forte adesão ao seu conteúdo são alguns exemplos que cumprem o princípio da segurança.

Vale ressaltar que as medidas devem levar em consideração os dados pessoais tanto em meio eletrônico como físico (em papel, por exemplo). Recomenda-se seguir o framework da ISO 27001 para implementar controles eficazes de segurança da informação, bem como outras melhores práticas de mercado, como: NIST, CIS Controls, publicações da ENISA, entre outros.

2.1.8 Prevenção

Esse princípio está contido dentro do princípio da segurança, mas a LGPD acabou por dar destaque à prevenção de forma proposital, demonstrando a importância em procurar evitar ao máximo que incidentes com dados pessoais ocorram. Além das medidas de detecção e resposta a incidentes, também é necessário adotar medidas técnicas e administrativas para prevenir que eventuais incidentes ocorram.

Para cumprir o princípio da prevenção estabelecido pela LGPD, é necessário adotar medidas proativas para evitar que incidentes relacionados a dados pessoais aconteçam. Esse princípio vai além da simples detecção e resposta a incidentes, exigindo uma abordagem mais abrangente, com foco na prevenção de riscos antes que eles se concretizem.

Para isso, os agentes de tratamento devem implementar uma combinação de medidas técnicas e administrativas, tais como:

- **Avaliação de riscos:** realizar análises de impacto à proteção de dados (DPIA) para identificar e mitigar possíveis vulnerabilidades em processos que envolvem o tratamento de dados pessoais;
- **Medidas de segurança:** adotar controles técnicos como criptografia, autenticação multifator e monitoramento de redes para proteger os dados contra acessos não autorizados ou vazamentos;
- **Políticas e procedimentos internos:** estabelecer políticas claras de governança de dados e treinamento contínuo para funcionários e contratados, de modo a garantir que todos compreendam a importância da proteção de dados e as melhores práticas a serem adotadas;
- **Privacidade desde a concepção (by design):** incorporar a proteção de dados pessoais desde a fase inicial de desenvolvimento de novos produtos e serviços, de forma que a segurança seja um componente essencial do planejamento e execução de processos;
- **Monitoramento e auditorias regulares:** implementar programas de auditoria periódica e monitoramento contínuo das operações de tratamento de dados, a fim de identificar e corrigir possíveis falhas antes que resultem em incidentes.

2.1.9 Não discriminação

Para cumprir o princípio da não discriminação, a LGPD proíbe expressamente qualquer tratamento de dados pessoais que resulte em discriminação ilícita ou abusiva. Isso significa que, embora algumas formas de classificação e segmentação sejam permitidas, elas devem ser realizadas de maneira que respeitem os limites legais e não violem os direitos dos titulares.

Para garantir a conformidade com esse princípio, as organizações devem adotar as seguintes práticas:

- **Evitar discriminação ilícita:** o tratamento de dados não pode resultar em exclusão, diferenciação ou tratamento injusto com base em características sensíveis, como origem racial ou étnica, convicção religiosa, saúde, orientação sexual, entre outros dados classificados como sensíveis pela LGPD. Isso inclui práticas que possam gerar preconceito, exclusão ou tratamento desigual sem justificativa legal;
- **Classificação lícita e não abusiva:** segmentações de dados que visam, por exemplo, o marketing direcionado são permitidas, desde que baseadas em critérios que não violem os direitos dos titulares. Isso inclui, por exemplo, agrupar públicos-alvo com base em interesses, faixa etária ou perfil de consumo, para o envio de publicidade relevante. O objetivo é facilitar que o titular receba comunicações úteis e deixe de receber ofertas irrelevantes, respeitando sempre o direito de opt-out (recusar o tratamento para marketing).

2.1.10 Responsabilização e prestação de contas

Os agentes de tratamento devem ser capazes de demonstrar, com provas objetivas e eficazes, o cumprimento da legislação de proteção de dados pessoais e o quão eficazes são as medidas técnicas e administrativas adotadas. Por isso, a documentação e o registro de logs de ações que demonstram o cumprimento de direitos do titular, por exemplo, são fundamentais.

3 Limitação de finalidade e hipóteses de legalidade

3.1 Limitação de finalidade e especificação de finalidade

As finalidades do tratamento informadas ao titular de dados (em atendimento ao princípio da transparência) devem ser específicas, explícitas e legítimas. Considerando que a LGPD foi inspirada no GDPR, vamos analisar esses três elementos seguindo as orientações do Working Party 29, endossadas pelo European Data Protection Board.

3.1.1 Finalidades específicas

A fim de determinar se o processamento de dados está em conformidade com a lei e estabelecer quais as salvaguardas de proteção de dados que devem ser aplicadas, a identificação das finalidades específicas é uma pré-condição necessária para a coleta de dados pessoais. A especificação, portanto, estabelece limites para as finalidades para as quais os controladores podem usar os dados pessoais coletados e ajuda a estabelecer as medidas técnicas e administrativas de proteção de dados adequadas e necessárias.

A especificação do propósito requer uma avaliação prévia interna realizada pelo controlador de dados e é uma condição necessária para a prestação de contas. É um primeiro passo fundamental que um controlador deve seguir para garantir a conformidade com a lei de proteção de dados aplicável. O controlador deve identificar quais são as finalidades, documentá-las e demonstrar que realizou essa avaliação interna.

Fonte: Parecer do WP29 sobre limitação de finalidade (§ III.1.1)[7]

Como a coleta de dados pessoais já é em si um tratando de dados pessoais, a finalidade deve ser especificada antes que a coleta ocorra, sempre que possível.

A especificação de finalidade deve ser detalhada o suficiente para determinar que tipo de tratamento está ou não incluído no objetivo do controlador. Finalidades vagas ou gerais, como "melhorar a experiência dos usuários", "fins de marketing" ou "pesquisas futuras", sem maiores detalhes, geralmente não atendem ao critério de serem "específicas". Uma mensagem para o titular dos dados de que "as informações de navegação são tratadas para apresentar anúncios relacionados aos seus interesses" relacionaria exatamente qual é o objetivo e como este é alcançado.

3.1.2 Finalidades explícitas

Os dados pessoais devem ser coletados para fins explícitos. Os objetivos da coleta não devem ser especificados apenas na mente dos agentes responsáveis pela coleta de dados. Eles também devem ser explicitados. Em outras palavras, as finalidades devem ser claramente reveladas, explicadas ou expressas de alguma forma inteligível. Segue-se da análise anterior que isso deve acontecer, o mais tardar, no momento em que ocorra a coleta de dados pessoais.

O propósito maior deste requisito é garantir que os objetivos do tratamento sejam especificados sem imprecisão ou ambiguidade quanto ao seu significado ou intenção. O que se entende deve

[7] Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf. Acesso em 29.10.2024.

ser claro e não deve deixar dúvida ou dificuldade de compreensão. A especificação dos fins deve, em particular, ser expressa de forma a ser entendida da mesma forma não apenas pelo controlador (incluindo todo o pessoal relevante) e por quaisquer terceiros operadores, mas também pelas autoridades de proteção de dados e os titulares de dados em questão. Deve-se tomar cuidado especial para assegurar que qualquer especificação da finalidade seja suficientemente clara para todos os envolvidos, independentemente de suas diferentes origens culturais / linguísticas, nível de compreensão ou necessidades especiais.

Fonte: Parecer do WP29 sobre limitação de finalidade (§ III.1.2)[8]

Ao explicitar a finalidade dessa forma, o controlador atende ao princípio da transparência e deixa claro ao titular como pretende utilizar seus dados pessoais. Finalidades explícitas também beneficiam os operadores e informam as autoridades e quaisquer terceiros interessados, de modo que todos tenham um entendimento comum de como os dados podem ser usados. Isso, por sua vez, reduz o risco de que as expectativas dos titulares de dados e/ou de quaisquer interessados sejam diferentes das expectativas do controlador.

3.1.3 Finalidades legítimas

A exigência de legitimidade significa que as finalidades para o tratamento de dados devem estar de acordo com a lei no sentido mais amplo. Isso inclui todas as formas de direito comum e escrito, legislação primária e secundária, decretos municipais, precedentes judiciais, princípios constitucionais, direitos fundamentais, outros princípios jurídicos, bem como jurisprudência, como tal lei seria interpretada e consideradas pelos tribunais competentes.

Além da legislação de forma geral, o tratamento de dados pessoais deve **sempre** ser baseado em pelo menos uma das hipóteses de legalidade.

3.2 Hipóteses de legalidade para o tratamento

De acordo com o artigo 7º da LGPD, o tratamento de dados pessoais só será lícito se, e na medida em que, **pelo menos uma** das hipóteses de legalidade se aplicar:

[8] Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf. Acesso em 30.03.2017.

Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:

- I - mediante o fornecimento de **consentimento** pelo titular;
- II - para o **cumprimento de obrigação legal ou regulatória** pelo controlador;
- III - pela **administração pública**, para o tratamento e uso compartilhado de dados necessários à **execução de políticas públicas** previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres;
- IV - para a **realização de estudos por órgão de pesquisa**, garantida, sempre que possível, a anonimização dos dados pessoais;
- V - quando necessário para a execução de **contrato** ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;
- VI - para o **exercício regular de direitos** em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);
- VII - para a **proteção da vida** ou da incolumidade física do titular ou de terceiros;
- VIII - para a **tutela da saúde**, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;
- IX - quando necessário para atender aos **interesses legítimos** do controlador ou de terceiros, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou
- X - para a **proteção do crédito**, inclusive quanto ao disposto na legislação pertinente.

Fonte: Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709/2018 (art. 7º, grifo nosso)

A lista de hipóteses de legalidade do tratamento é exaustiva, taxativa, e não exemplificativa. Não são possíveis outros motivos legítimos para o tratamento de dados pessoais sob a LGPD.

Já o tratamento de dados sensíveis não permite a utilização de interesse legítimo nem proteção do crédito como hipóteses de legalidade, mas acrescenta uma hipótese específica, de garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º da LGPD e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais (conforme art. 11 da LGPD).

Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:

- I - quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas;
- II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:
    a) cumprimento de obrigação legal ou regulatória pelo controlador;
    b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;
    c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;
    d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);
    e) proteção da vida ou da incolumidade física do titular ou de terceiro;
    f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou

g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

Fonte: Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709/2018 (art. 11)

3.2.1 Conceitos e fundamentos jurídicos dos requisitos adicionais para tratamento legítimo de dados pessoais

Os artigos 15 e 16 da LGPD trazem conceitos e fundamentos jurídicos que regulam o término do tratamento de dados pessoais e estabelecem os requisitos adicionais para a sua conservação legítima após o fim do tratamento. Esses artigos têm como base os princípios de finalidade, necessidade e transparência, que são essenciais para garantir o uso adequado dos dados e a proteção dos direitos dos titulares.

O artigo 15 define as situações em que o tratamento de dados pessoais deve ser encerrado. O tratamento só pode ser mantido enquanto houver uma justificativa legítima e vinculada à finalidade originalmente estabelecida. As hipóteses de término incluem:

- **Alcance da finalidade:** quando a finalidade para a qual os dados foram coletados for atingida, ou se os dados não forem mais necessários para essa finalidade;
- **Fim do período de tratamento:** quando o prazo estabelecido para o tratamento de dados expira;
- **Solicitação do titular:** o titular pode solicitar o término do tratamento a qualquer momento, incluindo a revogação do consentimento, respeitando-se o interesse público;
- **Determinação da ANPD:** a autoridade reguladora pode determinar o fim do tratamento caso identifique violações à lei.

Essas situações refletem o princípio da limitação da finalidade e do tempo de retenção dos dados, limitando o tratamento a contextos específicos e períodos estritamente necessários.

Apesar de o término ser obrigatório nas hipóteses descritas, o artigo 16 estabelece requisitos adicionais que permitem a conservação legítima dos dados pessoais em situações específicas. Esses fundamentos jurídicos visam conciliar a proteção dos dados com necessidades operacionais e legais do controlador. As hipóteses são:

- **Cumprimento de obrigação legal ou regulatória:** o controlador pode manter os dados para atender a exigências legais, como o armazenamento de informações fiscais ou trabalhistas;
- **Pesquisa:** dados podem ser conservados para fins de pesquisa, desde que anonimizados, quando possível, para proteger a privacidade do titular;
- **Transferência a terceiros:** a transferência de dados a terceiros é permitida, desde que respeite as disposições legais, como o consentimento ou outras bases legais de tratamento;
- **Uso exclusivo do controlador:** os dados podem ser mantidos para uso exclusivo do controlador, desde que sejam anonimizados e não possam ser acessados por terceiros.

Esses requisitos adicionais, especialmente os relacionados à conservação, baseiam-se no princípio da necessidade e no equilíbrio entre os direitos do titular e os interesses legítimos do controlador. A manutenção dos dados, nesses casos, deve ser estritamente vinculada a finalidades legítimas e respeitar a minimização do tratamento de dados pessoais, protegendo os direitos e liberdades dos titulares.

3.2.2 Tratamento de dados com respaldo no legítimo interesse

O controlador deve assegurar que o tratamento de dados pessoais baseado em legítimo interesse atenda a finalidades legítimas, que sejam claras e estejam vinculadas a situações concretas. Isso inclui:

- Apoio e promoção das atividades do controlador (por exemplo, marketing direto e análise de comportamento de clientes);
- Proteção do titular de dados ou prestação de serviços que o beneficiem diretamente (por exemplo, prevenção a fraudes e melhoria de serviços).

O controlador deve documentar essas finalidades em políticas internas e relatórios, assegurando que o tratamento seja adequado às legítimas expectativas do titular.

Além disso, o controlador deve garantir que:

- apenas os dados estritamente necessários à finalidade pretendida sejam tratados. Isso significa implementar práticas de minimização de dados, tratando o mínimo necessário de dados pessoais para atingir o objetivo. Para demonstrar conformidade, o controlador pode:
    - Manter registros claros sobre os dados coletados, sua finalidade e justificativa de necessidade;
    - Realizar auditorias e revisões regulares das operações de tratamento para garantir que nenhum dado excessivo ou irrelevante seja coletado ou mantido.
- haja adoção de medidas de transparência para que os titulares de dados sejam informados sobre o tratamento baseado no legítimo interesse. Isso inclui:
    - Políticas de privacidade claras e acessíveis: o controlador deve publicar um documento, como uma política de privacidade, que informe aos titulares sobre a coleta, uso e armazenamento de seus dados pessoais, explicando claramente o fundamento do legítimo interesse;
    - Canal de comunicação aberto: disponibilizar aos titulares meios para consulta sobre o tratamento de seus dados e sobre seus direitos de oposição, caso não concordem com a justificativa do controlador.

Se solicitado pela ANPD, o controlador deve fornecer um Relatório de Impacto à Proteção de Dados Pessoais (RIPD), que demonstre a avaliação dos riscos do tratamento baseado no legítimo interesse e as medidas de mitigação adotadas. Esse relatório deve incluir:

- Descrição detalhada das finalidades do tratamento de dados;
- Análise dos riscos associados ao tratamento, como violações de privacidade, e as medidas para mitigá-los;
- Prova de conformidade com o princípio da necessidade e proteção dos direitos fundamentais do titular, garantindo que o legítimo interesse do controlador não se sobreponha aos direitos e liberdades dos titulares.

3.2.3 Diferenças de tratamento de dados para pequenas empresas e critérios para enquadramento

A Resolução CD/ANPD nº 2, de 27 de janeiro de 2022, estabelece regras específicas para o tratamento de dados pessoais por agentes de tratamento de pequeno porte, de acordo com a Lei Geral de Proteção de Dados Pessoais (LGPD).

Esses agentes, que incluem microempresas (ME), empresas de pequeno porte (EPP), startups e pessoas naturais que realizam tratamento de dados, possuem um regime mais flexível quanto à aplicação de certas obrigações da LGPD, visando facilitar o cumprimento das normas por essas organizações de menor porte.

Para ser considerado um agente de tratamento de pequeno porte, a organização deve se enquadrar nos seguintes critérios, conforme a Resolução:

- Microempresas (ME) e empresas de pequeno porte (EPP): empresas que se enquadram nas definições da Lei Complementar nº 123/2006;
- Startups: empresas inovadoras que também se encaixam nos parâmetros de pequeno porte e têm como foco o desenvolvimento de novos produtos e serviços, que atendam aos critérios previstos no Capítulo II da Lei Complementar nº 182, de 1º de junho de 2021;
- Pessoas jurídicas sem fins lucrativos, pessoas naturais e entes privados despersonalizados que realizam tratamento de dados pessoais, desde que não realizem tratamento de alto risco ou em grande escala.

A Resolução também destaca que agentes de pequeno porte que realizam tratamento de dados de alto risco ou em grande escala não poderão ser enquadrados nesse regime simplificado.

Os agentes de tratamento de pequeno porte têm direito a algumas flexibilizações em relação às obrigações impostas pela LGPD. Entre as principais diferenças estão:

- **Dispensa de nomeação de Encarregado (Data Protection Officer, DPO):** agentes de pequeno porte não são obrigadas a nomear um Encarregado pelo Tratamento de Dados Pessoais (DPO), mas devem disponibilizar um canal de comunicação para que os titulares de dados possam exercer seus direitos, como acesso, correção ou exclusão de dados. No entanto, a nomeação de um DPO por parte desses agentes é considerada uma boa prática e pode ser levada em conta pela ANPD no caso de processos sancionatórios;
- **Prazo ampliado para atendimento de direitos dos titulares:** agentes de pequeno porte podem ter prazos maiores para responder às solicitações dos titulares de dados, como pedidos de acesso, correção e exclusão. Isso oferece mais tempo para adequação e cumprimento, respeitando as capacidades operacionais limitadas;
- **Registro simplificado das atividades de tratamento:** agentes de pequeno porte podem manter um registro simplificado das operações de tratamento de dados. Isso diminui a carga burocrática para essas organizações;
- **Medidas de segurança adequadas à realidade:** agentes de pequeno porte têm a possibilidade de adotar medidas de segurança da informação proporcionais ao seu tamanho, contexto e capacidade financeira, desde que assegurem a proteção dos dados pessoais tratados.

3.2.4 Tratamento de dados pelo poder público

A LGPD é aplicável ao poder público, com normas específicas, exceto para atividades relacionadas à segurança pública e defesa nacional (LGPD, art. 4º). De acordo com o art. 7º da LGPD, o tratamento de dados realizado pela administração pública é legítimo para o uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres.

Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:

- III - pela **administração pública**, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;

Fonte: Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709/2018 (art. 7º, grifo nosso)

Dessa forma, o tratamento de dados pelo poder público deve atender a finalidades legítimas previstas na legislação e relacionadas ao interesse público. O poder público deve justificar as finalidades do tratamento, e o consentimento não é uma exigência para o tratamento de dados pessoais pelo poder público, sendo uma das possíveis hipóteses de legitimidade. É importante destacar, ainda, que é vedado ao poder público transferir a entidades privadas dados pessoais constantes de bases de dados a que tenha acesso, exceto em casos específicos (LGPD, art. 26, § 1º).

Os prazos e procedimentos para exercício dos direitos do titular perante o poder público observarão o disposto em legislação específica, diferentemente do que ocorre com empresas privadas. Por exemplo, o prazo de cinco anos para registro de incidentes de segurança se aplica a empresas privadas, mas não se aplica às entidades previstas no art. 23 da LGPD (poder público), que devem seguir as regras específicas de guarda permanente para documentos, conforme definido pela tabela de temporalidade aplicável ou pelo Conselho Nacional de Arquivo. De acordo com o texto da própria Lei:

Art. 23. O tratamento de dados pessoais pelas pessoas jurídicas de direito público referidas no parágrafo único do art. 1º da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação), deverá ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público, desde que:

- I - sejam informadas as hipóteses em que, no exercício de suas competências, realizam o tratamento de dados pessoais, fornecendo informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos; [...]
- III - seja indicado um encarregado quando realizarem operações de tratamento de dados pessoais, nos termos do art. 39 desta Lei;
- IV – [...]

§ 1º A autoridade nacional poderá dispor sobre as formas de publicidade das operações de tratamento.

§ 2º O disposto nesta Lei não dispensa as pessoas jurídicas mencionadas no caput deste artigo de instituir as autoridades de que trata a Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação).

§ 3º Os prazos e procedimentos para exercício dos direitos do titular perante o Poder Público observarão o disposto em legislação específica, em especial as disposições constantes da Lei nº 9.507, de 12 de novembro de 1997 (Lei do Habeas Data) , da Lei nº 9.784, de 29 de janeiro de 1999 (Lei Geral do Processo Administrativo) , e da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação).

§ 4º Os serviços notariais e de registro exercidos em caráter privado, por delegação do Poder Público, terão o mesmo tratamento dispensado às pessoas jurídicas referidas no caput deste artigo, nos termos desta Lei.

§ 5º Os órgãos notariais e de registro devem fornecer acesso aos dados por meio eletrônico para a administração pública, tendo em vista as finalidades de que trata o caput deste artigo.

Fonte: Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709/2018 (art. 23)

Por fim, o art. 32 da LGPD estabelece que a Autoridade Nacional de Proteção de Dados (ANPD) pode solicitar que agentes do poder público publiquem Relatório de Impacto à Proteção de Dados Pessoais (RIPD) e adotem padrões adequados ao tratamento dos dados.

4 Direitos dos titulares dos dados

Desde o histórico de privacidade e proteção de dados, vimos que os direitos fundamentais do titular dos dados são considerados de extrema importância. A LGPD declara que deve haver uma razão legal para o tratamento.

O objetivo do tratamento deve ser claramente especificado. E mesmo assim, se houver outros meios além do tratamento de dados pessoais para atingir o objetivo especificado, esses outros meios deverão ser utilizados.

Mesmo quando todos os requisitos são atendidos, o agente de tratamento deve sempre equilibrar os direitos fundamentais do titular de dados com os objetivos do tratamento. Não é de admirar que uma seção relativamente grande da LGPD seja dedicada aos direitos do titular.

4.1 Informação transparente

O princípio da transparência está intrinsecamente relacionado aos direitos dos titulares conforme a LGPD, garantindo que as pessoas tenham acesso claro e facilitado às informações sobre como seus dados pessoais estão sendo tratados. Esse princípio assegura que o controlador seja transparente em relação às finalidades, forma de tratamento e compartilhamento de dados, além de permitir que o titular tenha pleno controle sobre seus dados.

Os direitos dos titulares, descritos principalmente no art. 18 da LGPD, reforçam a importância da transparência ao garantir o direito de acesso, correção, anonimização, eliminação e portabilidade dos dados. Para cumprir esses direitos, o controlador deve ser capaz de fornecer informações de forma clara e acessível, assegurando que o titular tenha total compreensão sobre a existência do tratamento, os agentes envolvidos e a possibilidade de revogação de consentimento. Além disso, o art. 19 exige que o controlador forneça a confirmação da existência do tratamento e o acesso aos dados em formato simplificado e imediato, o que exemplifica a aplicação prática do princípio da transparência no contexto da proteção de dados.

4.2 Informação sobre o tratamento

Art. 9º O titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca de, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso:

- I - finalidade específica do tratamento;
- II - forma e duração do tratamento, observados os segredos comercial e industrial;
- III - identificação do controlador;
- IV - informações de contato do controlador;
- V - informações acerca do uso compartilhado de dados pelo controlador e a finalidade;
- VI - responsabilidades dos agentes que realizarão o tratamento; e
- VII - direitos do titular, com menção explícita aos direitos contidos no art. 18 desta Lei.

Fonte: Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709/2018 (art. 9º)

4.3 Direto de acesso e confirmação sobre o tratamento

Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição:

- I - confirmação da existência de tratamento;
- II - acesso aos dados;

Fonte: Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709/2018 (art. 18)

O titular dos dados pode solicitar ao controlador a confirmação de existência de tratamento de seus dados ou o acesso aos dados pessoais. Cabe destacar que os controladores podem (e geralmente devem) exigir que os titulares de dados forneçam prova de identidade ao solicitarem a confirmação do tratamento ou, o que é mais crítico, o acesso aos dados pessoais. Isso ajuda a limitar o risco de terceiros obterem acesso ilegal a esses dados, o que configuraria um incidente de segurança.

Como vimos, segundo o fundamento da autodeterminação informativa, o titular dos dados tem, a qualquer momento, o direito de obter informações do controlador sobre se os dados pessoais relativos a ele estão sendo tratados ou não.

O controlador deve fornecer essa confirmação de forma simplificada e imediata. Caso o titular deseje mais detalhes, o controlador deverá apresentar uma declaração completa, dentro de até 15 dias, que informe a origem dos dados, os critérios utilizados no tratamento, e a finalidade, respeitando os segredos comercial e industrial.

Quando o tratamento tiver origem no consentimento do titular ou em contrato, o titular tem direito a obter do controlador uma cópia dos dados gratuitamente (LGPD, art. 19, § 3º).

4.4 Outros Direitos

4.4.1 Direito à correção

Naturalmente, quando um titular de dados tem acesso aos próprios dados pessoais que estão sob responsabilidade do controlador, ele pode verificar eventualmente que os dados estão incorretos, inexatos ou desatualizados. Nesse caso, o titular dos dados pode exigir uma correção.

4.4.2 Direito à eliminação

Os titulares de dados têm o direito de ter seus dados "apagados" (eliminados) quando sejam considerados desnecessários, excessivos ou tratados em desconformidade com a LGPD, ou quando sejam tratados com base no consentimento e já não estejam mais sujeitos a nenhuma hipótese de retenção.

Contudo, o artigo 16 da LGPD prevê que, mesmo após o término do tratamento, os dados pessoais poderão ser conservados em algumas situações específicas, como para:

- Cumprimento de obrigação legal ou regulatória pelo controlador;
- Estudo por órgão de pesquisa, desde que os dados sejam anonimizados, sempre que possível;
- Transferência a terceiros, respeitando os requisitos da LGPD;
- Uso exclusivo do controlador, desde que os dados sejam anonimizados e não acessíveis por terceiros.

Essas exceções garantem que, em determinadas circunstâncias, a eliminação dos dados não seja possível e/ou obrigatória, protegendo interesses legais e de pesquisa.

4.4.3 Direito à anonimização

O titular pode requisitar que os dados desnecessários (inclusive por já não haver mais base legal para o tratamento ou retenção), excessivos ou tratados em desconformidade com a LGPD passem por um processo de anonimização. Isso significa que os atributos que podem identificar direta ou indiretamente o titular serão eliminados de forma segura (sem retorno), e os dados remanescentes não identificarão mais o titular original, deixando de se enquadrar na definição de "dado pessoal" da lei. Tais dados remanescentes podem ser úteis, por exemplo, para a composição de estatísticas.

A anonimização pode ser uma alternativa para o titular que deseja proteger sua privacidade. Na área financeira, por exemplo, a legislação impõe a obrigatoriedade de retenção de dados por um período determinado para fins de auditoria e fiscalização. A Resolução CMN nº 4.474/2016 do Conselho Monetário Nacional (CMN) exige que instituições financeiras mantenham registros de transações por cinco anos, conforme o art. 1º, para assegurar a conformidade com normas de prevenção à lavagem de dinheiro e para eventuais auditorias fiscais. Se um cliente encerra sua conta e solicita a eliminação de seus dados pessoais, o banco pode argumentar que os dados precisam ser preservados para cumprir essas obrigações legais. Nesse cenário, o cliente pode solicitar a anonimização, o que permitiria à instituição financeira continuar mantendo as informações relevantes (como transações financeiras) sem identificar diretamente o cliente.

4.4.4 Direito ao bloqueio do tratamento

O titular poderá requisitar que o tratamento dos dados considerados desnecessários, excessivos ou tratados em desconformidade com a LGPD seja bloqueado, ou seja, suspenso temporariamente.

Nesse caso, ao invés de eliminar ou anonimizar os dados, o titular pode optar por solicitar que o controlador interrompa o tratamento em determinadas circunstâncias, como:

- Quando há uma disputa sobre a legitimidade do tratamento de dados e o titular precisa que o processamento seja interrompido até que a questão seja resolvida;
- Quando os dados são considerados excessivos ou desnecessários, mas o titular quer manter a possibilidade de revisão antes de pedir a eliminação ou anonimização;
- Quando há suspeita de que os dados tenham sido tratados em desconformidade com a LGPD, o que pode justificar a suspensão do tratamento até que seja verificada a regularidade do uso dos dados.

O bloqueio é útil quando o titular deseja uma suspensão temporária do tratamento, aguardando uma eventual correção ou decisão posterior, sem que os dados sejam imediatamente eliminados ou anonimizados.

4.4.5 Direito à portabilidade dos dados

O titular tem o direito de ter seus dados pessoais brutos transferidos para outro fornecedor de produto ou serviço mediante requerimento expresso e observando os segredos comercial e industrial.

O objetivo é garantir a liberdade de escolha do titular, permitindo que seus dados sejam levados para outro fornecedor sem prejuízo ao exercício de seus direitos. A portabilidade deverá ser feita de acordo com a regulamentação da ANPD, que definirá as normas e formatos que facilitem essa transferência, sem comprometer a integridade e segurança dos dados.

4.4.6 Direito à revogação do consentimento

O consentimento na LGPD deve ser obtido de forma explícita e estar relacionado a finalidades determinadas, sendo considerado nulo no caso de autorizações genéricas ou se houver qualquer vício de consentimento.

Cabe ao controlador o ônus da prova de que o consentimento foi obtido adequadamente, conforme o art. 8º, § 2º da LGPD. O consentimento pode ser dado por escrito ou por outro meio que demonstre claramente a manifestação de vontade do titular. Quando concedido por escrito, deve ser incluído em cláusula destacada das demais cláusulas contratuais (LGPD, art. 8º, § 1º).

O titular pode revogar o consentimento a qualquer momento, por meio de um procedimento gratuito e facilitado, conforme o art. 8º, § 5º, sendo que os tratamentos realizados anteriormente permanecem válidos até que o titular solicite a eliminação dos dados, como previsto no art. 18, inciso VI.

O controlador deve interromper o tratamento dos dados quando o consentimento for revogado, exceto quando houver outras bases legais para o tratamento. Em caso de alterações nas informações fornecidas ao titular, como aquelas previstas nos incisos I, II, III ou V do art. 9º, o controlador é obrigado a informar o titular, que poderá revogar o consentimento se discordar das modificações.

Além disso, o titular tem o direito de ser informado sobre a possibilidade de não fornecer consentimento e as consequências da negativa (LGPD, art. 18), assegurando que o consentimento seja sempre informado, livre e com controle total sobre o tratamento de seus dados pessoais.

4.4.7 Direito ao peticionamento

No que diz respeito aos seus dados pessoais sob responsabilidade do controlador, o titular pode realizar requerimentos em face do controlador tanto perante a ANPD como perante os órgãos de defesa do consumidor, como forma de proteção e exercício de seus direitos de maneira administrativa. Caso o titular não esteja satisfeito com as respostas ou ações, ele também pode recorrer à via judicial, conforme garantido pela legislação brasileira, para assegurar o cumprimento de seus direitos.

4.4.8 Direito à oposição ao tratamento

O titular pode requisitar que o tratamento feito com base em uma das hipóteses de dispensa do consentimento e que esteja em desconformidade com a LGPD seja impedido de ser realizado, se estiver em desconformidade com a LGPD ou afetar seus direitos e liberdades. A oposição é especialmente relevante quando o tratamento for realizado com base em interesse legítimo do controlador, e o titular tem o direito de questionar o uso de seus dados e solicitar a interrupção do tratamento, caso considere que seus direitos estão sendo violados.

4.4.9 Direito à revisão de decisões automatizadas

As decisões tomadas unicamente com base em tratamento automatizado de dados pessoais e que afetem os interesses do titular dos dados poderão ser revisadas – incluindo-se as decisões que tem por finalidade definir o perfil pessoal, profissional, de consumo e de crédito do titular, ou aspectos da sua personalidade.

O titular tem o direito de entender os critérios utilizados na tomada de decisões automatizadas, podendo solicitar a revisão de forma que garanta mais transparência e a oportunidade de contestar qualquer erro ou injustiça resultante do tratamento automatizado de dados (LGPD, art. 20).

5 Incidentes com dados pessoais e procedimentos relacionados

5.1 O conceito de incidentes com dados pessoais

A LGPD exige que os agentes de tratamento, como controladores e operadores, adotem medidas preventivas para proteger os titulares de eventuais danos causados por suas atividades. Em caso de um incidente de segurança, o controlador deve avaliar o ocorrido, identificar as possíveis consequências e determinar se é necessário notificar a ANPD e os titulares afetados.

De acordo com o art. 3º, inciso XII, do Regulamento de Comunicação de Incidente de Segurança (Resolução CD/ANPD nº 15/2024), incidente de segurança significa "qualquer evento adverso confirmado, relacionado à violação das propriedades de confidencialidade, integridade, disponibilidade e autenticidade da segurança de dados pessoais".

Os quatro pilares da segurança da informação são autenticidade, confidencialidade, disponibilidade e integridade. Esses pilares são definidos da seguinte maneira:

- II - autenticidade: propriedade pela qual se assegura que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, equipamento, sistema, órgão ou entidade;
- V - confidencialidade: propriedade pela qual se assegura que o dado pessoal não esteja disponível ou não seja revelado a pessoas, empresas, sistemas, órgãos ou entidades não autorizados;
- XI - disponibilidade: propriedade pela qual se assegura que o dado pessoal esteja acessível e utilizável, sob demanda, por uma pessoa natural ou determinado sistema, órgão ou entidade devidamente autorizados;
- XIII - integridade: propriedade pela qual se assegura que o dado pessoal não foi modificado ou destruído de maneira não autorizada ou acidental;

Fonte: Resolução CD/ANPD nº 15/2024 (art. 3º)

O incidente de segurança pode ocorrer por meio de ações voluntárias ou acidentais, resultando em divulgação, alteração, perda ou acesso não autorizado a dados pessoais, independentemente do meio em que estão armazenados. Exemplos incluem o envio de dados pessoais ao destinatário errado, invasões de sistemas que armazenam informações como nome, CPF ou dados financeiros, e o furto de dispositivos contendo esses dados. Esses incidentes também podem envolver ransomware, acessos não autorizados a dados pessoais sensíveis (como informações de saúde), ou a publicação inadvertida de dados dos titulares, como endereços ou números de identificação.

Nem todos os incidentes envolvem dados pessoais — se o evento afetar dados anonimizados, dados corporativos ou segredos comerciais, a notificação à ANPD não é necessária. É crucial verificar se o incidente comprometeu dados pessoais para aplicar a LGPD corretamente.

O controlador é responsável por identificar, tratar e avaliar os riscos associados aos incidentes, adotando medidas para mitigar possíveis danos. Por exemplo, um incêndio em um data center que destrua dados pessoais viola o pilar da disponibilidade, constituindo um incidente de segurança. Da mesma forma, a exclusão acidental e irreversível de dados pessoais por um operador afeta a disponibilidade e representa outro exemplo de incidente com dados pessoais.

5.2 Procedimento sobre como agir quando ocorre incidente de segurança com dados pessoais e notificação de um incidente com dados pessoais à ANPD e ao titular de dados

De acordo com o artigo 48 da LGPD, a obrigação de comunicar incidentes de segurança à Autoridade Nacional de Proteção de Dados (ANPD) e aos titulares cabe ao controlador. Isso significa que, caso o incidente com dados pessoais ocorra no âmbito da operação do operador, este tem obrigação de comunicar o controlador para que o controlador, então, tome as devidas providências e comunique a ANPD e os titulares, quando cabível.

A comunicação é exigida apenas para incidentes que possam acarretar risco ou dano relevante aos titulares, como perdas financeiras, danos à reputação, roubo de identidade ou fraudes.

Um incidente de segurança deve ser comunicado se atender cumulativamente a três critérios:

- Ocorrência confirmada pelo controlador;
- Envolvimento de dados pessoais sujeitos à LGPD;
- Potencial para risco ou dano relevante aos titulares.

Conforme o art. 5º, o incidente pode acarretar risco ou dano relevante aos titulares quando afetar significativamente os direitos fundamentais e interesses dos titulares e envolver ao menos um dos seguintes elementos:

- Dados pessoais sensíveis;
- Dados de crianças, adolescentes ou idosos;
- Dados financeiros;
- Dados de autenticação em sistemas;
- Dados protegidos por sigilo legal, judicial ou profissional;
- Dados em larga escala.

O incidente que afeta significativamente os direitos dos titulares pode resultar em impedimento do exercício de direitos e uso de serviços ou causar danos materiais ou morais, como discriminação, violação da integridade física, fraudes financeiras ou roubo de identidade.
Um incidente envolvendo dados em larga escala é aquele que abrange um número significativo de titulares, considerando o volume de dados, duração, frequência e a extensão geográfica.

Incidentes que não se enquadrem nesses critérios, como quando os dados estavam criptografados ou foram tomadas medidas eficazes para minimizar o risco, não precisam ser comunicados à ANPD ou aos titulares. No entanto, mesmo esses incidentes devem ser reportados pelo operador ao controlador, em respeito ao princípio da responsabilização e prestação de contas, para que o controlador possa avaliar medidas para melhorar a segurança.

A comunicação à ANPD deve ser feita pelo controlador em até três dias úteis a partir do conhecimento do incidente, e deve incluir informações como: a descrição dos dados afetados, o número de titulares, as medidas de segurança adotadas, os riscos e impactos, além das ações para mitigar os efeitos.

O controlador pode complementar as informações em até vinte dias úteis, se necessário. A comunicação deve ser realizada por meio de formulário eletrônico disponibilizado pela ANPD e enviada pelo encarregado ou representante do controlador.

O controlador deve manter o registro de incidentes de segurança, mesmo daqueles que não foram comunicados à ANPD e aos titulares, por um período mínimo de cinco anos a partir da data do registro. Esse registro deve incluir informações como a data de conhecimento do incidente, a descrição das circunstâncias, a natureza e a categoria dos dados afetados, o número de titulares

impactados, a avaliação dos riscos e os possíveis danos, além das medidas de correção e mitigação adotadas. Se o incidente foi comunicado, a forma e o conteúdo da comunicação também devem ser registrados; caso contrário, os motivos da ausência de comunicação devem constar.

O prazo de cinco anos não se aplica às entidades previstas no art. 23 da LGPD (Poder Público), que devem seguir as regras específicas de guarda permanente para documentos, conforme definido pela tabela de temporalidade aplicável ou pelo Conselho Nacional de Arquivo. Essas informações são essenciais para assegurar o cumprimento do princípio da responsabilização e garantir a rastreabilidade dos eventos de segurança.

O texto da comunicação deverá conter, no mínimo, as seguintes informações:

- I - a descrição da natureza dos dados pessoais afetados;
- II - as informações sobre os titulares envolvidos;
- III - a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial;
- IV - os riscos relacionados ao incidente;
- V - os motivos da demora, no caso de a comunicação não ter sido imediata; e
- VI - as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.

Fonte: Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709/2018 (art. 48, §1º)

Ao analisar a comunicação, a ANPD deverá verificar a gravidade do incidente e poderá, caso necessário para a salvaguarda dos direitos dos titulares, determinar ao controlador a adoção de providências, como a ampla divulgação do fato em meios de comunicação e medidas para reverter ou mitigar os efeitos do incidente.

A LGPD estabelece, ainda, que, na análise da gravidade do incidente, a ANPD deverá avaliar eventuais provas de que os agentes de tratamento adotaram medidas técnicas adequadas para tornar os dados pessoais afetados no âmbito e nos limites técnicos de seus serviços, ininteligíveis, para terceiros não autorizados a acessá-los, pois essas medidas devem reduzir o nível de impacto aos titulares e, consequentemente, também devem reduzir o nível de gravidade do incidente.

Figura 5. Violação de segurança e impacto financeiro

Imagem criada pelo EXIN com base em: Lima, Adrianne (2024). *Impacto financeiro*; IBM (2022). *Cost of a Data Breach Report*.

Organizando a proteção de dados

6 Importância da proteção de dados para a organização

Quase todas as organizações tratam dados pessoais. Para uma organização que trata dados pessoais, a proteção de dados não é apenas "um requisito da lei" ou "importante para evitar multas", mas algo diretamente vinculado à sua reputação e à confiança do cliente/consumidor.

O tratamento de dados pessoais realizado de maneira adequada significa garantia de qualidade, gerenciamento de segurança e governança.

Os parágrafos a seguir destacam alguns dos requisitos que não podem faltar para o que tratamento de dados pessoais seja considerado adequado.

6.1 Requisitos para o tratamento adequado

6.1.1 Programa de Governança em Privacidade (PGP)

Governança refere-se ao conjunto de processos, regras e práticas utilizadas para administrar e controlar uma organização ou sistema, visando garantir que suas operações sejam realizadas de maneira eficiente, ética e alinhada com seus objetivos e valores.

A ISO 37000:2021, que trata da governança de organizações, por exemplo, fornece um referencial global sobre práticas de governança eficazes. Ela estabelece princípios para garantir a integridade e a sustentabilidade das operações, promovendo uma liderança ética e responsável. A governança corporativa é definida como o sistema pelo qual as organizações são dirigidas e controladas, com foco em transparência, equidade, responsabilidade e prestação de contas.

A Lei das Sociedades por Ações (Lei n. 6.404/1976), por exemplo, estabelece bases legais para práticas de governança no Brasil, regulando a forma como as empresas devem proteger os interesses dos acionistas. Além disso, o Código Brasileiro de Governança Corporativa (Instituto Brasileiro de Governança Corporativa, IBGC) e o Código de Melhores Práticas de Governança Corporativa oferecem diretrizes para promover governança sólida e responsável nas organizações.

A governança em privacidade envolve práticas de conformidade com as leis de proteção de dados, como a Lei Geral de Proteção de Dados Pessoais (LGPD) no Brasil e o Regulamento Geral de Proteção de Dados (GDPR) na União Europeia.

O art. 50 da LGPD encoraja controladores e operadores a estabelecer regras de boas práticas e governança para proteger dados pessoais, adaptadas à estrutura, escala e sensibilidade dos dados, sendo compreendido como Programa de Governança em Privacidade (PGP).

A governança em privacidade também abrange avaliações contínuas de impacto e risco, monitoramento de conformidade e planos de resposta a incidentes, conforme recomendado pelas

diretrizes da Autoridade Nacional de Proteção de Dados (ANPD) e boas práticas de mercado sobre medidas de segurança da informação.

A governança corporativa está diretamente relacionada ao PGP, pois ambos visam assegurar a transparência, responsabilidade e conformidade nas operações da organização. Ao integrar o PGP à estrutura de governança corporativa, a organização garante que a proteção de dados pessoais seja tratada como um elemento essencial para a gestão de riscos e para a tomada de decisões estratégicas. Isso não só fortalece a confiança dos titulares de dados e demais partes interessadas, mas também melhora a resiliência organizacional, promovendo uma cultura de responsabilidade e conformidade contínua com as normas legais e regulamentares, como a LGPD.

Um PGP deve incluir, no mínimo, os seguintes elementos:

- Comprometimento do controlador em adotar políticas e processos internos que assegurem o cumprimento das normas e boas práticas de proteção de dados pessoais;
- Aplicabilidade a todos os dados pessoais sob o controle do controlador, independentemente da forma de coleta;
- Adaptação à estrutura, escala, volume das operações e à sensibilidade dos dados tratados;
- Políticas e salvaguardas baseadas em avaliação de impactos e riscos à privacidade;
- Transparência e mecanismos de participação do titular, visando estabelecer uma relação de confiança;
- Integração com a governança geral da organização, com supervisão interna e externa;
- Planos de resposta a incidentes e remediação;
- Atualização constante, com monitoramento contínuo e avaliações periódicas.

Além disso, o controlador deve ser capaz de demonstrar a efetividade do programa à ANPD ou a outras entidades, e as regras de boas práticas devem ser publicadas e atualizadas regularmente.

6.1.2 Cumprimento dos princípios relativos ao tratamento de dados pessoais

Os princípios de proteção de dados estabelecidos no artigo 6º da LGPD não apenas devem cumpridos como deve haver formas efetivas (documentadas) de comprovar esse cumprimento. O objetivo deve ser claro, detalhado e especificado, e pelo menos uma das possíveis “hipóteses legais para o tratamento” deve ser aplicada. Os direitos do titular de dados devem ser garantidos e medidas adequadas de proteção de dados devem ser aplicadas.

6.1.3 Estrutura legal

O controlador, como agente que determina as finalidades e a forma de tratamento, é obrigado a implementar medidas técnicas e organizacionais apropriadas para assegurar que o tratamento seja realizado de acordo com a LGPD, não apenas no âmbito de sua operação, mas também de quaisquer operadores que eventualmente contrate. E, para garantir que o nível de proteção de dados se mantenha o mesmo em toda a cadeia de tratamento, é fundamental que o controlador também garanta, por meio do contrato com o operador, previsões de que o operador somente poderá terceirizar parte do tratamento (para um suboperador) em casos já previstos e autorizados no contrato ou, caso contrário, a terceirização deverá ser autorizada pelo controlador antes de ocorrer.

O operador somente deverá tratar os dados pessoais baseado nas instruções documentadas do controlador. A melhor forma de documentar essas instruções do controlador ao operador é através de um contrato que defina:

- o objeto do tratamento;
- a duração do tratamento;
- a natureza e o objetivo do tratamento, como definido pelo controlador;
- os tipos de dados pessoais envolvidos;
- as categorias de titulares de dados afetados;
- as obrigações, responsabilidades e direitos dos agentes de tratamento.

Durante a relação entre controlador e operador, é importante que ambos consigam **demonstrar conformidade** com os requisitos da LGPD, e isso pode ser feito por meio da **documentação de provas de conformidade**.

6.1.4 Relatório de Impacto à Proteção de Dados Pessoais (RIPD)

Pela lei, realizar um Relatório de Impacto à Proteção de Dados Pessoais (RIPD) não é obrigatório para todos os tipos de tratamento, mas somente para aqueles que podem gerar riscos às liberdades civis e aos direitos fundamentais dos titulares. Ainda assim, para os casos que não geram esses riscos, é uma boa prática documentar a análise e fundamentação do motivo pelo qual o tratamento não se encaixa nessa obrigatoriedade, e muitas vezes isso pode ser realizado no próprio formato de um RIPD.

Segundo a LGPD (Lei nº 13.709/2018), o RIPD é obrigatório em casos de tratamento de dados pessoais sensíveis ou quando o tratamento for baseado no legítimo interesse do controlador, conforme previsto no art. 38.

Adicionalmente, o art. 32 estabelece que a ANPD pode solicitar que agentes do Poder Público publiquem relatórios de impacto à proteção de dados pessoais e adotem padrões adequados ao tratamento desses dados. O que um RIPD compreende e seus objetivos são discutidos mais detalhadamente em 8.3 Relatório de Impacto à Proteção de Dados Pessoais (RIPD).

6.2 Tipos requeridos de administração

De acordo com o princípio da responsabilização e prestação de contas, o agente de tratamento deve manter registros capazes de demonstrar e comprovar a adoção de medidas eficazes para a proteção de dados pessoais. Nesse sentido, há dois tipos de registros que são fundamentais.

6.2.1 Registro de atividades de tratamento

O controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse. Tal registro também é conhecido como Records of Processing Activities (ROPA), devido ao previsto no art. 30 do GDPR.

Os agentes de tratamento de pequeno porte podem cumprir a obrigação de elaboração e manutenção de registro das operações de tratamento de dados pessoais de forma simplificada (Resolução CD/ANPD nº 2/2022)[9].

[9] *ANPD divulga modelo de registro simplificado de operações com dados pessoais para Agentes de Tratamento de Pequeno Porte (ATPP)*. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-divulga-modelo-de-registro-simplificado-de-operacoes-com-dados-pessoais-para-agentes-de-tratamento-de-pequeno-porte-atpp. Acesso em 22.09.2024.

Embora a LGPD não detalhe explicitamente todas as informações que devem constar no registro de operações de tratamento de dados pessoais, o modelo simplificado da ANPD para agentes de tratamento de pequeno porte oferece diretrizes importantes. Esses elementos são úteis para garantir conformidade com a lei e a transparência no tratamento de dados pessoais. Aqui estão os principais pontos que devem ser incluídos no registro, tendo em vista a Resolução CD/ANPD nº 2/2022:

- **Informações de contato:** identificar a organização, CNPJ, principal atividade, e o responsável pela gestão dos dados, incluindo contatos como e-mail e telefone;
- **Categorias de titulares:** especificar a quem pertencem os dados, como titulares em geral, crianças, adolescentes ou idosos;
- **Tipos de dados pessoais tratados:** listar os dados pessoais tratados, como nome, endereço, RG, CPF, telefone, entre outros;
- **Medidas de segurança:** descrever as medidas de segurança adotadas para proteger os dados pessoais, como controle de acesso, backups, criptografia, etc;
- **Compartilhamento:** detalhar o fluxo de compartilhamento de dados com terceiros, como empresas parceiras ou prestadores de serviços;
- **Período de armazenamento:** informar por quanto tempo os dados serão mantidos, conforme a finalidade do tratamento;
- **Processo, finalidade e hipótese legal:** descrever o processo de tratamento, a finalidade (por exemplo, seleção de candidatos) e a base legal que justifica o tratamento (como consentimento ou cumprimento de obrigação legal);
- **Observações:** inserir informações adicionais, como transferências internacionais de dados ou outros pontos relevantes para o tratamento de dados.

6.2.2 Registro de incidentes com dados pessoais

O controlador deve manter o registro de incidentes de segurança, mesmo daqueles que não foram comunicados à ANPD e aos titulares, por um período mínimo de cinco anos a partir da data do registro[10].

Algumas das informações que devem ser registradas são:

- I - a data de conhecimento do incidente;
- II - a descrição geral das circunstâncias em que o incidente ocorreu;
- III - a natureza e a categoria de dados afetados;
- IV - o número de titulares afetados;
- V - a avaliação do risco e os possíveis danos aos titulares;
- VI - as medidas de correção e mitigação dos efeitos do incidente, quando aplicável;
- VII - a forma e o conteúdo da comunicação, se o incidente tiver sido comunicado à ANPD e aos titulares; e
- VIII - os motivos da ausência de comunicação, quando for o caso.

Fonte: Regulamento de Comunicação de Incidente de Segurança com Dados Pessoais, aprovada pela Resolução CD/ANPD nº 15, de 24 de abril de 2024 (art. 10, § 1º)

[10] Conforme o Regulamento de Comunicação de Incidente de Segurança com Dados Pessoais, aprovado pela Resolução CD/ANPD nº 15, de 24 de abril de 2024 (art. 10).

7 Autoridade Nacional de Proteção de Dados (ANPD)

De acordo com o artigo 5º, inciso XIX da Lei nº 13.853, de 2019, e com os artigos 55-A e 55-B da Lei Geral de Proteção de Dados Pessoais (redação dada pela Lei nº 14.460, de 2022), a ANPD é uma autarquia de natureza especial, dotada de autonomia técnica e decisória, com patrimônio próprio e com sede e foro no Distrito Federal. A ANPD tem autonomia técnica e decisória e é responsável por zelar, implementar e fiscalizar o cumprimento da LGPD em todo o território nacional.

A ANPD é composta por um Conselho Diretor, órgão máximo de direção, um Conselho Nacional de Proteção de Dados Pessoais e da Privacidade, a Corregedoria, a Ouvidoria, a Procuradoria e unidades administrativas ou especializadas necessárias à aplicação da LGPD (conforme o art. 55-C da LGPD).

7.1 Responsabilidades gerais da ANPD

A principal responsabilidade da Autoridade Nacional de Proteção de Dados (ANPD) é zelar pela proteção dos dados pessoais, nos termos da legislação (LGPD, art. 55-J, inciso I), ou seja, **fiscalizar e fazer cumprir a aplicação** da LGPD com o objetivo de **proteger** os direitos e liberdades fundamentais das pessoas naturais em relação ao tratamento. Outra importante responsabilidade é promover a conscientização pública e a compreensão dos riscos, regras, salvaguardas e direitos em relação ao tratamento de dados pessoais.

A ANPD tem papel central na implementação, fiscalização e promoção da LGPD no Brasil. Suas atribuições estão descritas na LGPD, no artigo 55-J, e são fundamentais para garantir a proteção de dados pessoais e o respeito aos direitos dos titulares. Aqui estão suas principais responsabilidades:

1. Zelar pela proteção de dados pessoais
A ANPD é responsável por garantir a aplicação da LGPD, assegurando a proteção dos dados pessoais no Brasil. Isso inclui monitorar e regular o tratamento de dados, promovendo a conformidade entre controladores e operadores de dados.
2. Fiscalização e aplicação de sanções
A ANPD fiscaliza o cumprimento da LGPD e aplica sanções quando necessário. Ela pode realizar auditorias e investigações sobre violações à lei, incluindo denúncias e petições de titulares de dados. As sanções são aplicadas por meio de processos administrativos que garantem o direito ao contraditório e ampla defesa.
3. Análise de denúncias e petições
A ANPD analisa denúncias e petições apresentadas por titulares de dados pessoais contra controladores. Quando os titulares não obtêm respostas adequadas dos controladores, podem recorrer à ANPD para mediar e investigar o caso, como previsto no art. 55-J, V e art. 18, §1º da LGPD.
4. Promoção de conscientização
A ANPD também atua para educar a população sobre as normas de proteção de dados, promovendo ações de conscientização e elaborando estudos sobre boas práticas nacionais e internacionais de privacidade. Ela incentiva a adoção de padrões que facilitem o exercício dos direitos dos titulares.

5. Gerenciamento de incidentes de segurança
Cabe à ANPD receber comunicações de incidentes de segurança com dados pessoais, analisá-los e, se necessário, aplicar sanções aos controladores. Ela também define procedimentos para a comunicação desses incidentes aos titulares, quando eles representarem risco ou dano relevante.
6. Estabelecimento de normas e diretrizes
A ANPD tem a responsabilidade de estabelecer normas e padrões, como cláusulas-padrão contratuais e Normas Corporativas Globais (NCG), além de verificar a conformidade de selos, certificados e códigos de conduta relacionados à proteção de dados.
7. Promoção de cooperação internacional
A ANPD também promove cooperação internacional, colaborando com autoridades de proteção de dados de outros países para fortalecer a privacidade e proteção de dados pessoais no Brasil e no exterior.

Essas funções garantem que a ANPD atue tanto de forma preventiva quanto remediadora, promovendo a proteção de dados pessoais e assegurando que os agentes de tratamento cumpram as disposições da LGPD, enquanto educa e conscientiza a população sobre seus direitos.

Algumas consultas complementares relativas à ANPD são:

- **Resolução CD/ANPD nº 1, de 28 de outubro de 2021:** aprova o Regulamento do Processo de Fiscalização e do Processo Administrativo Sancionador no âmbito da Autoridade Nacional de Proteção de Dados;
- **Resolução CD/ANPD nº 4, de 24 de fevereiro de 2023:** altera a Resolução CD/ANPD Nº 1, de 28 de outubro de 2021, que aprova o Regulamento do Processo de Fiscalização e do Processo Administrativo Sancionador no âmbito da Autoridade Nacional de Proteção de Dados;
- **Resolução CD/ANPD nº 15, de 24 de abril de 2024:** aprova o Regulamento de Comunicação de Incidente de Segurança;
- **Decreto n. 10.474/2020:** aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão e das Funções de Confiança da Autoridade Nacional de Proteção de Dados e remaneja e transforma cargos em comissão e funções de confiança.

7.1.1 Poderes de investigação da ANPD

O artigo 55-J, inciso IV, da LGPD concede à ANPD poder de fiscalizar e aplicar sanções em caso de tratamento de dados pessoais que viole a legislação. Dentre as previsões do artigo citado, as responsabilidades da ANPD incluem:

- Fiscalizar e aplicar sanções em caso de tratamento de dados realizado em descumprimento à legislação, mediante processo administrativo que assegure o contraditório, a ampla defesa e o direito de recurso;
- Realizar auditorias, ou determinar sua realização, no âmbito das atividades de fiscalização;
- Solicitar ao controlador Relatório de Impacto à Proteção de Dados Pessoais (RIPD), inclusive quando o tratamento tiver como fundamento seu interesse legítimo;
- Realizar auditoria para verificação de aspectos discriminatórios em tratamento automatizado de dados pessoais.

7.1.2 Poderes corretivos da ANPD

Os artigos 52 e 55-J da LGPD, juntamente com a Resolução CD/ANPD nº 1/2021, estabelecem os seguintes poderes corretivos para a ANPD:

- Advertência, com indicação de prazo para adoção de medidas corretivas;
- Multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração;
- Multa diária, observado o limite total do valor acima;
- Publicização da infração após devidamente apurada e confirmada a sua ocorrência;
- Bloqueio dos dados pessoais a que se refere a infração até a sua regularização;
- Eliminação dos dados pessoais a que se refere a infração;
- Suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador;
- Suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período;
- Proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados.

Além disso, conforme previsto na Resolução CD/ANPD Nº 1/2021, a aplicação de sanções segue um processo administrativo sancionador, garantindo a observância dos princípios de legalidade, proporcionalidade e contraditório, com:

- monitoramento contínuo das atividades dos agentes de tratamento;
- aplicação progressiva de sanções, desde advertências até multas e bloqueios, conforme a gravidade da infração;
- auditorias e análises para assegurar a conformidade com a LGPD.

Essas disposições reforçam o papel da ANPD na correção de infrações e no alinhamento das operações de tratamento de dados com os requisitos da LGPD.

O processo administrativo sancionador da ANPD segue etapas detalhadas na LGPD e na Resolução CD/ANPD nº 1/2021. Aqui está um resumo das principais fases:

1. Início do processo
O processo pode ser instaurado de ofício pela ANPD por meio de denúncia, petição de titular, ou com base em programas de fiscalização. Antes da instauração, pode ocorrer uma fase de procedimento preparatório para apurar preliminarmente indícios de infração.
2. Lavratura do auto de infração
Caso sejam encontrados indícios suficientes de infração, a ANPD lavra um auto de infração, detalhando a pessoa física ou jurídica autuada, os fatos e a legislação violada.
3. Defesa do autuado
O autuado é intimado para apresentar sua defesa em até 10 dias úteis. Nessa fase, o autuado pode juntar documentos, provas e informações para contestar a acusação.
4. Instrução do processo
A ANPD pode realizar diligências e juntar novas provas, além de solicitar a participação de terceiros interessados. O autuado também pode solicitar a produção de provas adicionais, como perícias.
5. Decisão de primeira instância
Após a fase de instrução, é elaborado um relatório de instrução, e a ANPD profere sua decisão de primeira instância, que pode aplicar sanções, como multas, advertências ou bloqueios. A decisão é publicada no Diário Oficial.

6. Recurso
O autuado pode apresentar recurso ao Conselho Diretor da ANPD em até 10 dias úteis, o que suspende a decisão de primeira instância até o julgamento. A decisão do Conselho Diretor é definitiva na esfera administrativa.
7. Cumprimento da decisão
Se o recurso for negado ou não houver recurso, o autuado deve cumprir a decisão. No caso de multa, o não pagamento pode resultar em inscrição na Dívida Ativa da União.
8. Revisão
A qualquer momento, pode ser solicitado um pedido de revisão do processo, caso surjam novos fatos ou elementos que justifiquem a reavaliação da sanção imposta. Contudo, a revisão não pode agravar a penalidade inicial.

7.1.3 Papéis e responsabilidades relacionadas a incidentes de segurança com dados pessoais

Ao receber uma notificação de incidente de segurança com dados pessoais, a ANPD deve avaliar a gravidade do ocorrido, verificando como as medidas de proteção de dados foram implementadas pelos controladores e operadores envolvidos. Essa análise considera os riscos para os titulares, como possíveis violações de direitos fundamentais, e as medidas mitigadoras adotadas ou que ainda devem ser implementadas para prevenir maiores danos. Cabe ao controlador investigar o incidente, avaliar os riscos e adotar medidas de mitigação para minimizar os efeitos negativos sobre os titulares dos dados e terceiros.

A ANPD tem poderes adicionais para fiscalizar e aplicar sanções caso os controladores ou operadores não cumpram a LGPD (art. 55-J da LGPD). Isso inclui, conforme o Decreto 10.474/2020, a capacidade de monitorar, orientar e, se necessário, reprimir práticas inadequadas, além de estabelecer compromissos para eliminar irregularidades (art. 2º, XVII). Ademais, no processo de fiscalização, a ANPD pode solicitar auditorias e exigir que sejam realizadas medidas corretivas para garantir a conformidade legal.

7.1.3.1 Condições gerais para a imposição de sanções administrativas

As sanções administrativas devem ser proporcionais e dissuasivas, levando em consideração as peculiaridades do caso concreto.

7.1.3.2 Proporcional

Quando a ANPD decidir impor uma sanção administrativa, além de outras medidas, ela deve dar a devida atenção às circunstâncias.

Os critérios para essa decisão são:

- A gravidade e a natureza das infrações e dos direitos pessoais afetados;
- A boa-fé do infrator;
- A vantagem auferida ou pretendida pelo infrator;
- A condição econômica do infrator;
- A reincidência;
- O grau do dano;
- A cooperação do infrator;
- A adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano, voltados ao tratamento seguro e adequado de dados;
- A adoção de política de boas práticas e governança;
- A pronta adoção de medidas corretivas; e
- A proporcionalidade entre a gravidade da falta e a intensidade da sanção.

A cooperação com a ANPD para remediar uma infração e mitigar os possíveis efeitos adversos da infração poderá ser favorável aos controladores e operadores.

7.1.3.3 Dissuasivo

Uma sanção também deve ser dissuasiva. Qualquer que seja o custo da implementação de medidas para cumprir a LGPD em uma organização, nenhuma empresa deve arriscar ignorar as regras, porque as multas vão muito além do que custará a conformidade. Ainda assim, a intenção é incentivar as empresas a cumprir a LGPD, e não as destruir financeiramente.

7.2 Transferência internacional de dados

7.2.1 Definição

A transferência de dados é, segundo o inciso X do artigo 5º da LGPD, um tipo de tratamento, pois constitui uma operação realizada com dados pessoais. Já a transferência internacional de dados é definida pelo inciso XV do mesmo artigo como:

> Transferência internacional de dados: transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro
>
> Fonte: Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709/2018 (art. 5º, inciso XV)

7.3 Normas aplicáveis à transferência internacional de dados

De acordo com o Regulamento de Transferência Internacional de Dados (aprovado pela Resolução CD/ANPD nº 19, de 23 de agosto de 2024), a transferência internacional de dados deve atender a propósitos legítimos, específicos e informados ao titular, e é permitida somente quando amparada em uma das hipóteses legais previstas nos artigos 7º e 11 da LGPD.

Entre os mecanismos válidos para essa transferência estão: transferências de dados entre fronteiras para um destinatário em um país terceiro considerado como uma "jurisdição adequada" (LGPD, artigo 33, I) ou se a parte ou partes que exportam os dados tiverem implementado um mecanismo legal de transferência de dados, como o uso de cláusulas-padrão contratuais ou Normas Corporativas Globais (NCG) (salvaguardas previstas no artigo 33, II a IX).

Além disso, o Regulamento reforça que a transferência internacional deve ser limitada ao mínimo necessário para o cumprimento das finalidades específicas, ou seja, apenas os dados pertinentes e proporcionais devem ser transferidos.

7.3.1 Transferências para país ou organismo avaliado pela ANPD como adequado

> Art. 33. A transferência internacional de dados pessoais somente é permitida nos seguintes casos:
>
> - I - para países ou organismos internacionais que proporcionem grau de proteção de dados pessoais adequado ao previsto nesta Lei;
>
> Fonte: Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709/2018 (art. 33)

A ANPD precisa analisar e garantir que o país ou organismo destinatário dos dados pessoais objeto de transferência apresenta um nível adequado de proteção de dados pessoais em razão de sua legislação interna ou dos compromissos internacionais assumidos, conforme evidenciado no Artigo 34:

Art. 34. O nível de proteção de dados do país estrangeiro ou do organismo internacional mencionado no inciso I do *caput* do art. 33 desta Lei será avaliado pela autoridade nacional, que levará em consideração:

- I - as normas gerais e setoriais da legislação em vigor no país de destino ou no organismo internacional;
- II - a natureza dos dados;
- III - a observância dos princípios gerais de proteção de dados pessoais e direitos dos titulares previstos na LGPD;
- IV - a adoção de medidas de segurança previstas em regulamento;
- V - a existência de garantias judiciais e institucionais para o respeito aos direitos de proteção de dados pessoais; e
- VI - outras circunstâncias específicas relativas à transferência.

Fonte: Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709/2018 (art. 34)

7.3.2 Transferências sujeitas a salvaguardas apropriadas

Na ausência de uma aprovação do país ou organismo internacional pela ANPD, o controlador ou o operador deve tomar medidas para compensar a falta de proteção de dados em um país terceiro por meio de aplicação de salvaguardas (garantias) apropriadas para o titular dos dados.

Essas salvaguardas adequadas podem consistir na utilização de cláusulas contratuais específicas para determinada transferência, Normas Corporativas Globais (NCG), cláusulas-padrão contratuais, bem como selos, certificados e códigos de conduta regularmente emitidos.

A definição do conteúdo de cláusulas-padrão contratuais e a verificação de cláusulas contratuais específicas para uma determinada transferência, NCG ou selos, certificados e códigos de conduta são definidas pela ANPD, conforme a Resolução CD/ANPD nº 19/2024.

Essas salvaguardas devem garantir a conformidade com os requisitos de proteção de dados e os direitos dos titulares de dados adequados ao tratamento em conformidade com a LGPD.

7.3.3 Normas Corporativas Globais (NCG)

As NCG (Binding Corporate Rules, BCR) têm origem nas regras corporativas vinculantes, instituídas pelo GDPR:

Um grupo de empresas, ou um grupo de empresas envolvidas numa atividade econômica conjunta, deve poder utilizar as regras empresariais vinculantes aprovadas para as suas transferências internacionais da União para organizações pertencentes ao mesmo grupo de empresas ou grupo de empresas uma atividade econômica conjunta, desde que tais regras corporativas incluam todos os princípios essenciais e direitos aplicáveis para garantir as salvaguardas apropriadas para transferências ou categorias de transferências de dados pessoais.

Fonte: item 110 do Preâmbulo do GDPR

Segundo o Regulamento de Transferência Internacional de Dados da ANPD, as NCG são diretrizes internas que regulam a transferência internacional de dados pessoais entre diferentes entidades pertencentes a um mesmo grupo empresarial ou conglomerado.

Essas normas têm caráter vinculante para todos os membros que as subscrevem, garantindo que, independentemente do país em que uma entidade do grupo esteja localizada, as práticas de tratamento de dados pessoais estejam em conformidade com as exigências da Lei Geral de Proteção de Dados Pessoais (LGPD) e outras regulamentações internacionais aplicáveis.

Conforme o art. 25 do Regulamento de Transferência Internacional de Dados da ANPD, essas NCG são válidas apenas para transferências envolvendo organizações ou países cobertos por elas. Além disso, para serem aceitas, as NCG devem estar vinculadas a um Programa de Governança em Privacidade (PGP), atendendo às exigências mínimas descritas no art. 50, § 2º da LGPD, que incluem práticas como a gestão de riscos, a responsabilização dos controladores e políticas de privacidade robustas.

Essencialmente, as NCG oferecem uma estrutura segura para transferências internacionais de dados dentro de grupos empresariais, garantindo que os dados pessoais sejam protegidos de acordo com padrões adequados, independentemente do local de tratamento.

Dentre os requisitos da LGPD, as NCG devem especificar pelo menos:

- Descrição das transferências internacionais de dados para as quais o instrumento se aplica, incluindo as categorias de dados pessoais, a operação de tratamento e suas finalidades, a hipótese legal e os tipos de titulares de dados;
- Identificação dos países para os quais os dados podem ser transferidos;
- Estrutura do grupo ou conglomerado de empresas, contendo a lista de entidades vinculadas, o papel exercido por cada uma delas no tratamento e os dados de contato de cada organização que efetue tratamento de dados pessoais;
- Determinação da natureza vinculante da norma corporativa global para todos os integrantes do grupo ou conglomerado de empresas que as subscreverem, inclusive para seus funcionários;
- Delimitação de responsabilidades pelo tratamento, com a indicação da entidade responsável;
- Indicação dos direitos dos titulares aplicáveis e os meios para o seu exercício, incluindo canal de fácil acesso e o direito de peticionar contra o controlador perante a ANPD, após comprovada pelo titular a apresentação de reclamação ao controlador não solucionada no prazo estabelecido em regulamentação;
- Regras sobre o processo de revisão das Normas Corporativas Globais (NCG) e previsão de submissão à prévia aprovação da ANPD; e
- Previsão de comunicação à ANPD em caso de alterações nas garantias apresentadas como suficientes de observância dos princípios, dos direitos do titular e do regime de proteção de dados previsto na LGPD, especialmente na hipótese em que um dos membros do grupo ou conglomerado de empresas estiver submetido a determinação legal de outro país que impeça o cumprimento das normas corporativas.

8 Aspectos da qualidade

8.1 Proteção de dados desde a concepção (by design) e por padrão (by default)

> Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito. [Essas medidas] deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução.
>
> Fonte: Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709/2018 (art. 46, *caput* e § 2º)

Com este artigo, a LGPD faz do princípio de proteção de dados **desde a concepção** (by design) um **requisito legal**, e não apenas uma maneira eficaz de cumprir as obrigações relacionadas à segurança dos dados. O controlador é responsável pela implementação de um conjunto completo de medidas técnicas e administrativas **apropriadas**.

O controlador deve implementar medidas técnicas e administrativas apropriadas para garantir que, **por padrão** (by default), apenas sejam tratados os dados pessoais estritamente necessários para cada finalidade específica do tratamento. Isso se aplica à quantidade de dados pessoais coletados, à extensão de seu tratamento, ao período de armazenamento e à acessibilidade.

Além disso, o conjunto de medidas técnicas e administrativas apropriadas é necessário para integrar as salvaguardas necessárias ao tratamento para proteger os direitos dos titulares de dados. Dessa forma, uma ligação jurídica é definida entre os princípios de segurança de dados e a privacidade, com o objetivo de garantir a efetividade do direito humano à privacidade.

8.1.1 Os sete princípios de privacidade desde a concepção (by design)

A ideia de privacidade desde a concepção (by design) foi desenvolvida por Ann Cavoukian, PhD., ex-Comissária de Informações e Privacidade, em Ontário, Canadá. Em uma publicação sobre os princípios, ela escreveu:

> Privacidade desde a concepção (by design) é um conceito que desenvolvi nos anos 90, para abordar os efeitos sempre crescentes e sistêmicos das Tecnologias de Informação e Comunicação e dos sistemas de dados em rede em larga escala. A privacidade desde a concepção (by design) promove a visão de que o futuro da privacidade não pode ser assegurado apenas pelo cumprimento de estruturas regulatórias; em vez disso, a garantia da privacidade deve idealmente se tornar o modo de operação padrão de uma organização.
>
> Fonte: Cavoukian, Ann (2011). Privacy by Design, the 7 Foundational Principles: Implementation and Mapping of Fair Information Practices[11]

[11] Cavoukian, Ann (2011). *Privacy by Design, the 7 Foundational Principles:* Implementation and Mapping of Fair Information Practices. Disponível em: https://privacy.ucsc.edu/resources/privacy-by-design---foundational-principles.pdf. Acesso em 31.10.2024.

O framework de privacidade desde a concepção (by design) é composto por sete princípios, que serão explorados nos próximos parágrafos.

8.1.1.1 Proativo, não reativo; preventivo, não corretivo

A abordagem de privacidade desde a concepção (by design) é caracterizada por medidas proativas em vez de reativas. Ele antecipa e evita eventos invasivos à privacidade antes que eles aconteçam. A privacidade desde a concepção (by design) não espera que os riscos à privacidade se concretizem, nem oferece remédios para resolver infrações à privacidade depois de terem ocorrido - ele visa **impedir** que ocorram. Em resumo, a privacidade desde a concepção (by design) vem antes do fato, não depois.

8.1.1.2 Privacidade como configuração padrão (by default)

Todos podem ter certeza de uma coisa: as regras padrão. A privacidade desde a concepção (by design) busca oferecer o máximo grau de privacidade, garantindo que os dados pessoais sejam protegidos automaticamente em qualquer sistema de TI ou prática comercial. Se um indivíduo não faz nada, sua privacidade permanece intacta. Nenhuma ação é necessária por parte de um titular de dados para proteger sua privacidade. Privacidade e proteção de dados são incorporadas ao sistema, por padrão.

8.1.1.3 Privacidade incorporada ao design

A privacidade desde a concepção (by design) está incorporada ao design e à arquitetura de sistemas de TI e práticas de negócios. Não é acoplada como um complemento após o fato. O resultado é que a privacidade se torna um componente essencial da funcionalidade principal que será entregue. A privacidade é parte integrante do sistema, sem diminuir suas funcionalidades.

8.1.1.4 Funcionalidade total: soma positiva, não soma zero

A privacidade desde a concepção (by design) busca acomodar todos os interesses e objetivos legítimos de uma maneira positiva para todos, não por meio de uma abordagem de soma zero, em que compensações desnecessárias são feitas. A privacidade desde a concepção (by design) evita a pretensão de falsas dicotomias, como privacidade versus segurança, demonstrando que é possível ter ambas.

8.1.1.5 Segurança de ponta a ponta: proteção total do ciclo de vida dos dados

A privacidade desde a concepção (by design), tendo sido incorporada ao sistema antes do primeiro elemento da informação que está sendo coletada, se estende com segurança durante todo o ciclo de vida dos dados envolvidos – medidas de segurança fortes são essenciais à privacidade, do início ao fim. Isso garante que todos os dados sejam retidos com segurança e, em seguida, destruídos com segurança (sem possibilidade de recuperação) no final do processo, em tempo hábil. Assim, a privacidade desde a concepção (by design) garante o gerenciamento do ciclo de vida de dados pessoais seguro e de ponta a ponta.

8.1.1.6 Visibilidade e transparência

A privacidade desde a concepção (by design) procura assegurar a todas as partes interessadas que, seja qual for a prática ou tecnologia de negócio envolvida, ela está, de fato, operando de acordo com as promessas e objetivos declarados, sujeita à verificação independente. Seus componentes e operações permanecem visíveis e transparentes para usuários e provedores.

8.1.1.7 Respeito pela privacidade do usuário

Acima de tudo, a privacidade desde a concepção (by design), exige que os arquitetos e operadores mantenham os interesses do indivíduo (usuário) em primeiro lugar, oferecendo medidas como padrões de privacidade fortes, notificação apropriada e capacitando opções fáceis de usar. O objetivo é garantir que se mantenha o foco no usuário.

8.1.2 Benefícios da aplicação dos princípios de privacidade desde a concepção (by design) e por padrão (by default)

Adotar uma abordagem de proteção de dados desde a concepção (by design) é uma ferramenta essencial para minimizar os riscos à privacidade e criar confiança[12]. Criar projetos, processos, produtos ou sistemas com a privacidade em mente desde o início pode levar a benefícios que incluem:

- Problemas potenciais são identificados em um estágio inicial, quando resolvê-los será sempre mais simples e menos dispendioso;
- Maior conscientização sobre privacidade e proteção de dados em toda a organização;
- As organizações são mais propensas a cumprir suas obrigações legais e menos propensas a violar a legislação de proteção de dados;
- É menos provável que as ações sejam invasivas à privacidade e tenham um impacto negativo nos indivíduos.

A implementação dos princípios de privacy by design, conforme descritos por Cavoukian (2011), se alinha diretamente com as resoluções 1/2021 e 4/2023 da ANPD, reforçando a importância de uma abordagem proativa à proteção de dados e conformidade com a Lei Geral de Proteção de Dados Pessoais (LGPD):

1. Prevenção de riscos e sanções
Princípio: proativo, não reativo; preventivo, não corretivo
O primeiro princípio do privacy by design visa a adoção de medidas preventivas, antecipando riscos antes que se concretizem. Ao demonstrar a aplicação do privacy by design, a organização pode reduzir significativamente o risco de incidentes e, por consequência, evitar sanções severas.
2. Conformidade contínua
Princípio: privacidade como configuração padrão (by default)
Esse princípio exige que os sistemas e processos sejam projetados para proteger os dados por padrão, sem a necessidade de qualquer ação por parte dos titulares. A Resolução 4/2023, que regula a dosimetria das sanções, considera a "implementação de medidas corretivas" como um fator atenuante na aplicação de multas (art. 13, III). Manter a conformidade contínua demonstra que a organização já adota práticas que limitam o tratamento de dados ao estritamente necessário, o que pode facilitar a defesa em um processo administrativo sancionador.
3. Segurança e confiança
Princípio: segurança de ponta a ponta – proteção total do ciclo de vida dos dados
O princípio de segurança de ponta a ponta garante que os dados estejam protegidos desde o momento da coleta até sua destruição. Esse conceito é reforçado pela Resolução 1/2021, que determina que os agentes de tratamento devem adotar medidas de segurança técnicas e administrativas para proteger os dados pessoais (LGPD, art. 46). No processo de fiscalização, a organização que já adota essa abordagem demonstra estar em conformidade com a exigência de proteção contínua e adequada dos dados.
4. Mitigação de sanções
Princípio: funcionalidade total – soma positiva, não soma zero
A soma positiva propõe que a privacidade pode ser alcançada em conjunto com outros objetivos organizacionais, sem sacrificar a funcionalidade. A Resolução 4/2023 (art. 13, II) reconhece a implementação de políticas de boas práticas e governança como uma atenuante para sanções. A adoção do privacy by design, que busca acomodar privacidade e funcionalidade, pode ser vista pela ANPD como um indicativo de que a organização se esforça para manter boas práticas de conformidade com a LGPD, o que pode mitigar penalidades.

[12] Disponível em: https://ico.org.uk/. Acesso em: 25.04.2017.

5. Transparência e visibilidade
Princípio: visibilidade e transparência
O privacy by design também enfatiza a importância da transparência e da visibilidade das operações de tratamento de dados, permitindo auditorias e verificações. A Resolução 1/2021 estabelece que as atividades de tratamento de dados devem ser conduzidas com base em critérios de transparência e controle (art. 17, VI), e o agente regulado deve manter sistemas de rastreamento que permitam verificar o uso adequado dos dados (art. 5º, II). Durante uma fiscalização, organizações que mantêm um registro claro e acessível de suas operações de tratamento estarão em uma posição vantajosa para demonstrar conformidade e cooperar com as autoridades, o que pode influenciar positivamente o resultado do processo administrativo sancionador.

8.2 Contratos entre controlador e operador

Conforme visto no item 8.1 acima, o artigo 46 da LGPD exige que tanto o controlador como o operador implementem medidas técnicas e administrativas apropriadas e garantam que essas precauções permaneçam em vigor durante o tratamento, na verdade, implementando um dos princípios da proteção de dados desde a concepção (by design): o de segurança de ponta-a-ponta.

Dessa forma, quando um operador é contratado para executar o tratamento ou parte do tratamento em nome do controlador, o contrato por escrito entre esses agentes deve garantir que o mesmo nível de segurança e conformidade em proteção de dados seja aplicado em toda a cadeia de tratamento[13].

8.2.1 Cláusulas do contrato

A LGPD não determina o conteúdo específico que deveria constar no contrato entre Controlador e Operador. No entanto, o artigo 28(3) do GDPR (Regulamento em que nossa lei se inspirou), determina que esse contrato (ou outro ato jurídico que vincule os agentes de tratamento) deve estipular, em especial, que o operador ("tratador", no GDPR):

(a) processe os dados pessoais apenas conforme as instruções documentadas do controlador, incluindo no que diz respeito às transferências de dados pessoais para um país terceiro ou uma organização internacional;
(b) assegure que as pessoas autorizadas a tratar os dados pessoais se comprometeram com a confidencialidade ou estejam sujeitas a uma obrigação legal adequada de confidencialidade;
(c) adote todas as medidas técnicas e administrativas de segurança do tratamento, conforme determinado pelo artigo 46 da LGPD;
(d) respeite as condições impostas pelo Controlador para contratar outro operador (também chamado de "suboperador");
(e) auxilie o controlador, por meio de medidas técnicas e administrativas apropriadas, na medida do possível, no cumprimento da obrigação do controlador de responder aos pedidos de exercício dos direitos de titulares de dados;
(f) auxilie o controlador a garantir o cumprimento das obrigações de segurança, notificações às autoridades, notificações aos titulares de dados e elaboração de Relatório de Impacto à Proteção de Dados Pessoais (RIPD), considerando a natureza do tratamento e as informações de que dispõe;

[13] Alcassa, Flávia. Lima; Lima, Adrianne; Samaniego, Daniela; Baronosvky, Thainá (2021). *LGPD para contratos:* Adequando contratos e documentos à Lei Geral de Proteção de Dados Pessoais. Disponível em: https://www.amazon.com.br/Lgpd-para-contratos-Adequando-documentos/dp/6553620253/ref=tmm_pap_swatch_0?_encoding=UTF8&qid=1628523947&sr=1-1. Acesso em 31.10.2024.

(g) à escolha do controlador, suprima ou devolva todos os dados pessoais ao controlador após o termo da prestação de serviços relacionados ao tratamento e elimine eventuais cópias existentes, a menos que a legislação exija a conservação dos dados pessoais, e
(h) disponibilize ao controlador todas as informações necessárias para demonstrar o cumprimento das obrigações estabelecidas, permitindo e contribuindo para as auditorias, incluindo as inspeções realizadas pelo controlador ou por outro auditor à mando do controlador.
(i) Ressalta-se que esse conteúdo, ainda que seja determinado pela legislação europeia (GDPR), tem sido amplamente adotado pelo mercado brasileiro na ausência de orientação pela LGPD ou pela ANPD.

8.2.1.1 Exemplo

A tabela a seguir mostra um exemplo do conteúdo que um contrato de tratamento de dados entre o controlador e o operador deveria abordar:

Conteúdo	Referência GDPR (podem ser aplicadas analogamente ao cenário brasileiro)	Referência LGPD
Escopo e finalidade do contrato	Artigo 4(2) definições: processamento (tratamento)	Artigo 5º, I e X, definições e finalidade de tratamento
Dados cobertos pelo acordo	Artigo 4(1) dados pessoais Artigo 9 / item 10 categorias especiais de dados pessoais (dados sensíveis)	Artigo 5º, II e III, definição de dados pessoais e sensíveis
Segurança geral e salvaguardas no tratamento de dados	Artigo 32 segurança do processamento (tratamento)	Artigo 46 medidas de segurança
Medidas técnicas e administrativas	Artigo 28, 3, “a” até “h”	Artigo 46 medidas de segurança técnicas e administrativas Resolução CD/ANPD nº 2/2022
Monitoramento da segurança da informação e proteção de dados	Artigo 35 avaliação (relatório) de impacto sobre proteção de dados	Artigo 5º, XVII, e artigo 38 relatório de impacto
Violação de segurança da informação e incidente com dados pessoais	Artigo 33(2) notificação de um incidente com dados pessoais à autoridade e aos titulares	Artigo 48 comunicação de incidente de segurança Resolução nº15/2024, que aprovou o Regulamento de Comunicação de Incidente de Segurança (RCIS)
Correção, exclusão e bloqueio / obrigações específicas para auxiliar o controlador	Artigo 32 segurança de processamento artigo 36 consulta prévia	Artigo 7º e artigo 18 direitos dos titulares e dever de assistência
Acordo com outro operador de dados	Artigo 28(2) e (4) subprocessador (suboperador)	Artigo 39 contratação de operadores

Transferência de dados	Rec. (112), (113) Artigo 47 regras corporativas vinculantes (Normas Corporativas Globais, NCG) Artigo 49 exceções para situações específicas; o capítulo V transfere (..) para países terceiros ou organizações internacionais.	Artigo 33 a 36 transferência internacional de dados Resolução CD/ANPD nº 19/2024, que aprova o Regulamento de Transferência Internacional de Dados
Outras obrigações	Artigo 39 tarefas do DPO (1b)... sensibilização e formação do pessoal envolvido nas operações de processamento (tratamento)	Artigo 41 e artigo 42 responsabilidade do encarregado (Data Protection Officer, DPO) Resolução CD/ANPD nº 18/2024, que aprova o Regulamento sobre a atuação do encarregado pelo tratamento de dados pessoais
Os direitos de controle dos controladores	Artigo 4(7) controlador Artigo 28(3f) suporte ao controlador	
Retorno e exclusão dos dados pessoais	Artigo 28(3g) eliminar ou devolver	Artigo 18, VI e VII, eliminação de dados
Dever de confidencialidade	Artigo 28(3b) confidencialidade	
Duração	Artigo 28(3) duração do processamento (tratamento) Artigo 5 princípios relativos ao processamento (tratamento) de dados pessoais (1) (e) limitação de armazenamento	Artigo 15 limitação de armazenamento
Prevalência	No caso de cláusulas conflitantes, legislação tem prevalência	Artigo 63 aplicação subsidiária das normas da LGPD em caso de conflito

8.3 Relatório de Impacto à Proteção de Dados Pessoais (RIPD)

O primeiro princípio de proteção de dados desde a concepção (by design) requer que o controlador antecipe e evite eventos danosos às liberdades civis e direitos fundamentais (com destaque para a privacidade) e antes que eles ocorram.

A LGPD inclui essa determinação no artigo 5º, XVII:

> Relatório de impacto à proteção de dados pessoais: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco.
>
> Fonte: Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709/2018 (art. 5º, inciso XVII)

Segundo a ANPD, o Relatório de Impacto à Proteção de Dados Pessoais (RIPD) é a documentação que contém a descrição dos processos de tratamento de dados pessoais que podem gerar alto risco à garantia dos princípios gerais de proteção de dados pessoais previstos na LGPD e às liberdades civis e aos direitos fundamentais do titular de dados. Deve conter, ainda, as medidas, salvaguardas e mecanismos de mitigação de risco, nos termos dos artigos 5º, inciso XVII, e 38 da Lei nº 13.709, de 14 de agosto de 2018, a Lei Geral de Proteção de Dados Pessoais (LGPD)[14].

A LGPD não exige que um RIPD seja executado para cada operação de tratamento. Na realidade, o texto da lei é bem sucinto sobre a matéria. Em resumo, é importante haver a elaboração do RIPD nas seguintes situações:

- Em iniciativas e tratamentos que possam gerar riscos às liberdades civis e aos direitos fundamentais dos titulares (art. 5º, XVII);
- Em operações de tratamento efetuadas para fins exclusivos de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais (art. 4º, § 3º);
- Quando o tratamento tiver como fundamento a hipótese de interesse legítimo (art. 10, § 3º);
- Para agentes do Poder Público, incluindo determinação quanto à publicação do RIPD (art. 32); e
- Para controladores em geral, quanto às suas operações de tratamento, incluindo as que envolvam dados pessoais sensíveis (art. 38).

Os controladores podem, quando aplicável, utilizar como referência o conceito de tratamento de alto risco estabelecido no art. 4º do Regulamento de aplicação da LGPD para agentes de tratamento de pequeno porte, aprovado pela Resolução nº 2/2022.

Conforme esse artigo, o tratamento será considerado de alto risco se, no caso específico, for identificada a presença de, pelo menos, um critério geral (“ampla escala” ou “impactar significativamente os interesses e direitos fundamentais dos titulares”) e um critério específico (“emprego de tecnologias emergentes ou inovadoras”, “monitoramento ou vigilância de áreas públicas”, “decisões baseadas exclusivamente em tratamento automatizado de dados pessoais” ou “uso de dados pessoais sensíveis ou de dados pessoais de crianças, adolescentes e idosos”).

Levando em conta esses critérios, recomenda-se elaborar o RIPD, por exemplo, se o tratamento de dados pessoais envolver um número substancial de titulares (“ampla escala”, critério geral) e dados pessoais sensíveis (critério específico). Outro exemplo é uma decisão baseada exclusivamente em tratamento automatizado de dados pessoais (critério específico), que possa resultar na negativa de um direito ou no acesso a um serviço (“impactar significativamente interesses e direitos”, critério geral).

É importante destacar que, para a elaboração do RIPD, esses critérios não são exaustivos, permitindo ao controlador identificar alto risco em circunstâncias distintas das mencionadas. Assim, em observância ao princípio da responsabilidade e prestação de contas, cabe ao controlador avaliar as condições relevantes de cada caso, a fim de identificar os riscos envolvidos e as medidas de prevenção e segurança adequadas, considerando os potenciais impactos nas liberdades e direitos fundamentais dos titulares, bem como a probabilidade de ocorrência desses riscos.

[14] Autoridade Nacional de Proteção de Dados (ANPD), *Relatório de Impacto à Proteção de Dados Pessoais (RIPD)*, 2023. Disponível em: https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/relatorio-de-impacto-a-protecao-de-dados-pessoais-ripd#p3. Acesso em 22.09.2024.

Figura 6. Tratamento de alto risco (art. 4º, Resolução CD/ANPD nº 2/2022)

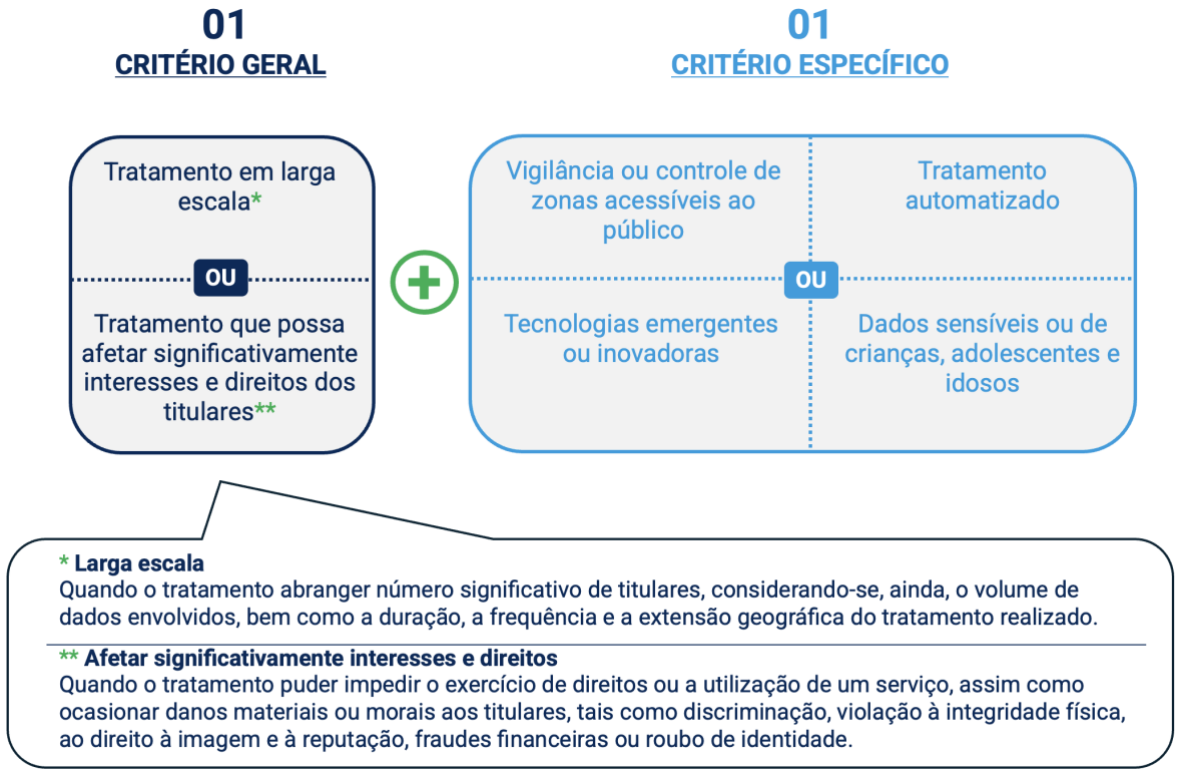

Imagem criada pelo EXIN com base em: Autoridade Nacional de Proteção de Dados (ANPD), *Relatório de Impacto à Proteção de Dados Pessoais (RIPD)*, 2023. Disponível em: https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/relatorio-de-impacto-a-protecao-de-dados-pessoais-ripd#p3. Acesso em 31.10.2024.

Ainda no artigo 38, parágrafo único, da LGPD, afirma-se que o relatório deverá conter, no mínimo:

(a) a descrição dos tipos de dados coletados;
(b) a metodologia utilizada para a coleta e para a garantia da segurança das informações; e
(c) a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados.

É possível aplicar, por analogia, algumas orientações europeias sobre o DPIA. Por exemplo, não há impeditivo legal na LGPD para que um RIPD pode enderece um conjunto de operações de tratamento semelhantes de uma só vez. Isso significa que **um único RIPD poderia ser usado para avaliar várias operações de tratamento que são semelhantes em termos dos riscos apresentados**, desde que seja dada consideração adequada à natureza específica, ao escopo, ao contexto e às finalidades do tratamento. Isso pode significar, por exemplo, um único relatório para onde uma tecnologia semelhante é usada com a finalidade de coletar o mesmo tipo de dados para os mesmos fins.

Aplicando-se a abordagem de *privacy by design*, o RIPD deve ser realizado **antes de ser realizado o tratamento** (art. 46, §2). Isso porque a análise evidenciará eventuais riscos às liberdades civis e aos direitos fundamentais em uma fase em que menos danoso (ao titular de dados) mitigar esses riscos, assim como é também e menos custoso e mais fácil para o agente corrigir o projeto de um novo produto ou serviço em fase embrionária.

O RIPD, portanto, deve ser iniciado **o mais cedo possível** no projeto da operação de tratamento, mesmo que algumas das operações de tratamento ainda sejam desconhecidas. À medida que o RIPD for atualizado durante todo o projeto de ciclo de vida, ele garantirá que a proteção de dados e a privacidade sejam consideradas e que sejam criadas soluções que promovam a conformidade.

Também é necessário repetir etapas individuais dessa avaliação à medida que o processo de desenvolvimento avança, porque a seleção de certas medidas técnicas ou administrativas pode afetar a gravidade ou a probabilidade dos riscos representados pelo tratamento.

Figura 7. Relatório de Impacto à Proteção de Dados Pessoais (RIPD)

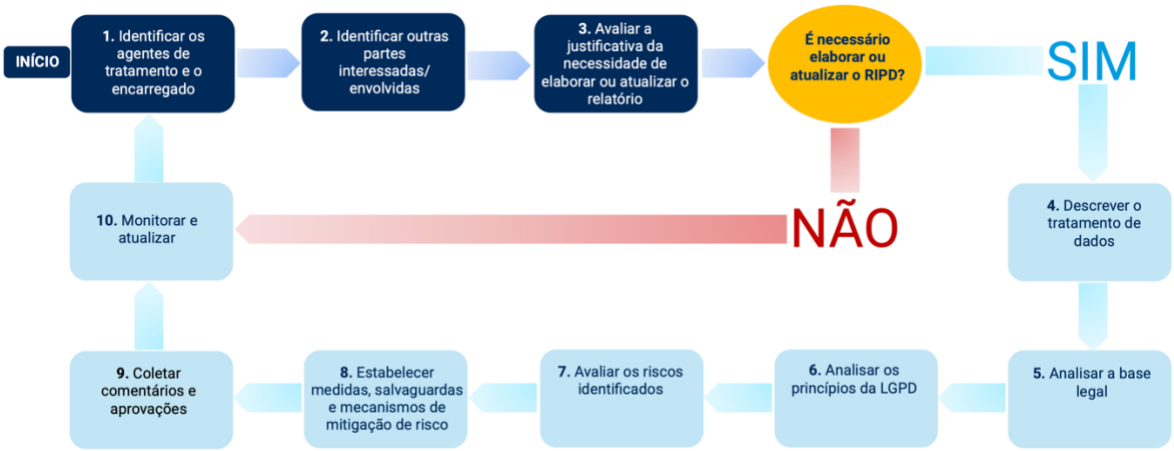

Imagem criada pelo EXIN com base em: Autoridade Nacional de Proteção de Dados (ANPD), *Relatório de Impacto à Proteção de Dados Pessoais (RIPD)*, 2023. Disponível em: https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/relatorio-de-impacto-a-protecao-de-dados-pessoais-ripd#p3. Acesso em 31.10.2024.

O fato de que o RIPD pode precisar ser atualizado uma vez que o tratamento tenha realmente iniciado **não** é uma razão válida para adiar ou não executar um RIPD. Em alguns casos, o RIPD será um processo contínuo, por exemplo, quando uma operação de tratamento é dinâmica e está sujeita a alterações contínuas. Executar um RIPD é um processo contínuo, não um exercício único.

Considerando as atribuições legais definidas nos artigos 5º, inciso VIII, e 41 da LGPD, é desejável que o encarregado seja consultado na elaboração e na análise das conclusões do RIPD. O controlador também poderá consultar outros membros de sua organização, eventuais operadores ou o público externo, incluindo, entre outros, especialistas e titulares de dados pessoais.

8.3.1 Objetivos de um RIPD

Existem vários motivos para realizar um RIPD – como a ideia de prevenção, conforme vista em um dos princípios de privacidade desde a concepção (by design), bem como a obrigação de documentar a conformidade, e outros. Em detalhes, um RIPD ajudará a:

- evitar mudanças dispendiosas nos processos, redesenho de sistemas ou encerramento de projetos;
- reduzir as consequências da supervisão e fiscalização;
- melhorar a qualidade dos dados;
- melhorar a prestação de serviços;
- melhorar a tomada de decisão;
- aumentar a conscientização sobre privacidade em uma organização;
- melhorar a viabilidade do projeto;
- melhorar a comunicação em relação à privacidade e proteção de dados pessoais, e
- reforçar a confiança dos titulares de dados na forma como os dados pessoais são tratados e a privacidade é respeitada.

8.3.2 Tópicos de um RIPD

Além do previsto no artigo 8 da LGPD, segundo a ANPD, são importantes as seguintes informações adicionais no RIPD:

a) Identificação dos agentes de tratamento e do encarregado;
b) Outras partes interessadas/envolvidas. Informar se foram consultadas na elaboração do RIPD e pareceres emitidos;
c) Justificativa da necessidade de elaboração do relatório (por exemplo: alto risco, solicitação da ANPD, gestão de riscos e prevenção, outros);
d) Projeto/Processo que justifica a elaboração do RIPD;
e) Sistemas de informação relacionados ao projeto/processo que justifica a elaboração do RIPD;
f) Tratamento de dados;
   i. Descrição do tratamento (desde a coleta até a eliminação);
   ii. Dados pessoais (informar todos os tipos de dados pessoais tratados, de forma completa);
   iii. Dados pessoais sensíveis (informar todos os tipos de dados pessoais sensíveis tratados, de forma completa);
   iv. Categorias de titulares (por exemplo, clientes, funcionários do controlador, filhos de funcionários do controlador, funcionários de clientes, autores de ações judiciais, beneficiários de apólices, terceiros prestadores de serviços);
   v. Dados de crianças e adolescentes ou de outra categoria de vulneráveis, como idosos, se houver;
   vi. Volume de dados pessoais tratados e número de titulares envolvidos no tratamento;
   vii. Fonte de coleta;
   viii. Finalidade do tratamento (Justifique a finalidade de tratamento para cada dado);
   ix. Informar quais são os compartilhamentos internos e externos (inclusive transferência internacional, se houver);
   x. Política de armazenamento (descrever os prazos de retenção e métodos de descarte);
g) Análise de hipótese legal. Justifique a escolha da hipótese legal para cada finalidade de tratamento;
h) Análise de princípios da LGPD;
i) Riscos identificados ao titular;
j) Resultado apurado com base na metodologia utilizada pelo agente de tratamento;
k) Medidas, salvaguardas e mecanismos de mitigação de risco;
l) Comentários e aprovações.

Fonte: Relatório de Impacto à Proteção de Dados Pessoais (RIPD)[15]

8.4 Gestão do Ciclo de Vida dos Dados (GCVD)

Independentemente de os dados serem gerados por e dentro da organização ou coletados pela organização por meio de terceiros (cliente, fornecedor, parceiro), a única maneira de protegê-los é entendê-los. Eles contêm informações pessoais de qualquer tipo, como sobre clientes, funcionários, comunicações confidenciais, informações de identificação pessoal, informações sobre saúde ou dados financeiros. Em cada um desses casos, havendo possibilidade de identificação direta ou indireta do titular dos dados, a LGPD se aplica, exigindo proteção apropriada a partir do momento em que os dados são coletados.

Exige-se uma estrutura de privacidade e segurança nos fundamentos de qualquer projeto. Os dados mudam ao longo de toda a sua vida útil e muitas vezes são armazenados por anos, seja

[15] Autoridade Nacional de Proteção de Dados (ANPD), *Relatório de Impacto à Proteção de Dados Pessoais (RIPD)*, 2023. Disponível em: https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/relatorio-de-impacto-a-protecao-de-dados-pessoais-ripd#p3. Acesso em 31.10.2024.

para registro ou por comodidade. Com a LGPD, no entanto, este último está se tornando um risco e um hábito caro.

8.4.1 Finalidade da Gestão do Ciclo de Vida dos Dados (GCVD)

A Gestão do Ciclo de Vida dos Dados (GCVD) é um processo que ajuda as organizações a gerenciar o fluxo de dados em todo o seu ciclo de vida: criação, uso, compartilhamento, arquivamento e exclusão.

Rastrear dados com precisão em todo o ciclo de vida da informação é a base de uma estratégia de proteção de dados e ajuda a determinar onde aplicar os controles de segurança.

8.4.2 Compreendendo os fluxos de dados

Os vários requisitos da LGPD exigem que uma empresa saiba:

- exatamente onde seus dados e, em particular, os dados pessoais se encontram;
- para quais finalidades os dados devem ser coletados ou criados;
- por quais razões os dados devem ser retidos;
- em que prazo ou em que situação os dados devem ser excluídos.

8.4.2.1 Coleta de dados

Desde o início, é importante ter em mente quais dados pessoais são necessários para os fins do tratamento pretendido. A LGPD requer um motivo para manter os dados pessoais armazenados; portanto, a qualquer momento, deve ser claro e fácil demonstrar ao menos:

- com que finalidade ou finalidades as informações foram coletadas;
- em que momento (inclusive a data) os titulares dos dados foram informados da coleta e da sua finalidade;
- se o consentimento foi adquirido para o tratamento pretendido;
- em caso positivo, se esse consentimento ainda é válido (e não retirado);
- outro fundamento legal para o tratamento existente.

Na prática, cada “pedaço” de informação precisa de numerosas etiquetas indicando porque existe e por quanto tempo continuará existindo.

8.4.2.2 Estrutura das permissões

Qualquer coleta de dados, mas uma coleta de dados pessoais em particular, precisa de uma estrutura de permissões, definindo claramente quais funcionários precisam, por conta de sua função na organização, acessar quais dados pessoais.

No entanto, as coisas mudam. Um bom programa deve avaliar e revisar continuamente quem precisa acessar que tipo ou tipos de informação. Controladores e operadores devem trabalhar com seus colegas de TI para automatizar controles em todos os sistemas corporativos. Eles devem facilitar para que os funcionários façam a coisa certa contra a coisa errada. Eles devem evitar que os funcionários tenham consequências negativas através de suas ações, até mesmo uma simples negligência em fazer alguma coisa.

Depois que a estrutura de permissões estiver em vigor, ela deve ser mantida por meio de avaliações regulares e contínuas.

8.4.2.3 Construir regras de retenção e exclusão

Um dos princípios fundamentais da LGPD é a necessidade, que significa limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados (artigo 6º, III, LGPD). Na prática, isso leva a um equilíbrio contínuo entre quais dados manter, por qual razão, e quais dados descartar de maneira segura.

Armazenar dados pessoais é um fardo para qualquer organização. É preciso muito esforço para manter os dados seguros, completos e atualizados, e ainda mais esforços para responder às solicitações dos titulares de dados, solicitando informações sobre o tratamento de seus dados e para lidar com reclamações referentes a seus direitos. Adicionalmente, há sempre a ameaça de uma violação de dados pessoais, com os procedimentos resultantes, o risco para os titulares de dados e o risco de dados para a empresa, como perda de reputação, custo de reparações e possíveis multas.

Há muitas obrigações legais em relação à retenção de dados pessoais por um determinado período. Por exemplo, considere-se registros de clientes, como vendas e transações financeiras, garantias ou informações de recursos humanos, como currículo, histórico de pagamento ou informações tributárias.

A boa Gestão do Ciclo de Vida dos Dados (GCVD):

- fornece as ferramentas para gerenciar o fluxo de dados em um sistema de informações;
- mantém rastreamento dos dados a partir do momento em que são coletados ou gerados até o momento em que são excluídos, porque não há **motivo** para retê-los.

8.5 Auditoria de Proteção de Dados

O artigo 55-J, inciso XVI, da LGPD menciona que a Autoridade Nacional de Proteção de Dados (ANPD) poderá realizar auditoria sobre o tratamento de dados pessoais efetuado pelos agentes de tratamento, para monitorar a conformidade com a LGPD.

Além das auditorias da ANPD, é comum que os próprios agentes de tratamento prevejam em contrato a possibilidade de realização de auditorias, especialmente de um controlador em relação ao operador, para verificação do nível de aderência às previsões contratuais e à conformidade em matéria de proteção de dados pessoais.

De acordo com a autora Adrianne Lima[16], com a LGPD, "as organizações devem analisar riscos e implementar medidas que visem mitigar ou reduzir a possibilidade de suas bases de dados serem objeto de roubo, perda ou uso indevido".

Ainda segundo Lima (2022), faz parte da governança em privacidade, prevista na LGPD, compreender seus processos internos (por exemplo, processos seletivos de candidatos às vagas de trabalho e análise de perfis de consumidores) e externos (por exemplo, com prestadores de serviço e fornecedores) que envolvam dados pessoais.

[16] Lima, Adrianne (2022). *A importância das auditorias em privacidade*. Disponível em: https://bd.tjdft.jus.br/items/c6cb82ce-ea36-4389-8864-8f619045a9eb. Acesso em 22.09.2024.

A realização de auditorias e avaliações periódicas de processos e fluxos com dados pessoais possui fundamentação na LGPD, principalmente: no artigo 20, § 2º; artigo 50, § 1º e § 2º, I, h; artigo 55-J, incisos IV e XVI da LGPD; e no artigo 2º, XVI, do Decreto n. 10.474/2020. Também se identifica a fundamentação no artigo 33, §2º, 70, 71, 72, §1º, 74, §2º e 161, parágrafo único, da Constituição Federal. Além de haver previsões técnicas de boas práticas nas normas da ISO/IEC, como ISO-27007, ISO-27008 e ISO 19011.

Fonte: Lima, Adrianne (2022). A importância das auditorias em privacidade.

De acordo com a ANPD, e em conformidade com o art. 50, I, da LGPD, o Programa de Governança em Privacidade (PGP) deve:

f) estar integrado à estrutura geral de governança da instituição, além de estabelecer e aplicar mecanismos de supervisão internos e externos;
[...]
h) ser atualizado constantemente com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas.

Fonte: Programa de Governança em Privacidade do MCom, Ministério das Comunicações[17]

Assim, em caso de uma auditoria pela ANPD ou órgão responsável pelo segmento, ou caso aconteça uma violação de dados, é necessário que se apresentem documentos que detalhem os fluxos de dados e os níveis de risco assumidos pela organização (Lima, 2022).

Nesse sentido, a Resolução CD/ANPD nº 1/2021 determina que:

Art. 5º Os agentes regulados submetem-se à fiscalização da ANPD e têm os seguintes deveres, dentre outros:

- I - fornecer cópia de documentos, físicos ou digitais, dados e informações relevantes para a avaliação das atividades de tratamento de dados pessoais, no prazo, local, formato e demais condições estabelecidas pela ANPD;
- II - permitir o acesso às instalações, equipamentos, aplicativos, facilidades, sistemas, ferramentas e recursos tecnológicos, documentos, dados e informações de natureza técnica, operacional e outras relevantes para a avaliação das atividades de tratamento de dados pessoais, em seu poder ou em poder de terceiros;
- III - possibilitar que a ANPD tenha conhecimento dos sistemas de informação utilizados para tratamento de dados e informações, bem como de sua rastreabilidade, atualização e substituição, disponibilizando os dados e as informações oriundos destes instrumentos;
- IV - submeter-se a auditorias realizadas ou determinadas pela ANPD;
- V - manter os documentos físicos ou digitais, os dados e as informações durante os prazos estabelecidos na legislação e em regulamentação específica, bem como durante todo o prazo de tramitação de processos administrativos nos quais sejam necessários; e
- VI - disponibilizar, sempre que requisitado, representante apto a oferecer suporte à atuação da ANPD, com conhecimento e autonomia para prestar dados, informações e outros aspectos relativos a seu objeto.
  [...]

[17] Ministério das Comunicações. *Programa de Governança em Privacidade do MCom*. Disponível em: https://www.gov.br/mcom/pt-br/arquivos/governanca/mcom-programa-de-governanca-em-privacidade-lgpd. Acesso em: 30.10.2024.

- § 4º O agente regulado, por intermédio de representante indicado, poderá acompanhar a auditoria da ANPD, ressalvados os casos em que a prévia notificação ou o acompanhamento presencial sejam incompatíveis com a natureza da apuração ou em que o sigilo seja necessário para garantir a sua eficácia.

Fonte: Resolução CD/ANPD nº 1/2021 (art. 5º, I-VI e § 4º)

Por fim, Lima (2022) expõe que, para a aplicação de sanções administrativas, poderá ser considerado, como eventual atenuante, o que a organização implementava a respeito do PGP, além da documentação a respeito dos processos, tecnologias utilizadas e fluxos de dados (LGPD, artigo 52). A ANPD determina que o não cumprimento dos deveres estabelecidos poderá caracterizar obstrução à atividade de fiscalização, sujeitando o infrator a medidas repressivas, sem prejuízo da adoção das medidas necessárias com o objetivo de concluir a ação de fiscalização obstruída por parte da ANPD (Resolução CD/ANPD nº 1/2021, art. 6º).

8.5.1 Finalidade de uma auditoria

A finalidade de um processo de auditoria de proteção de dados é testar, avaliar e reavaliar regularmente a eficácia de medidas técnicas e administrativas para garantir a conformidade com a LGPD, incluindo a segurança do tratamento.

Normalmente, uma auditoria revelará, por exemplo, **lacunas** nas políticas de privacidade que precisam ser abordadas para aprimorar a governança de privacidade de dados. No mínimo, uma auditoria tornará a proteção de dados pessoais o "tópico da semana", aumentando a conscientização em toda a organização.

De um modo geral, dois tipos de auditorias de privacidade podem ser distinguidos: uma auditoria de adequação e uma auditoria de conformidade.

8.5.1.1 Auditoria de adequação

Uma auditoria de adequação visa:

- assegurar que haja políticas de proteção de dados adequadas em uma dada organização e que sejam de fato aplicadas a todas as instâncias de tratamento de dados pessoais, incluindo conjuntos de dados históricos, backups e equipamentos obsoletos;
- avaliar se estas políticas são adequadas para atender aos requisitos da LGPD e outras leis e regulamentos de proteção de dados possivelmente aplicáveis.

Isso requer um entendimento e um mapeamento completos dos fluxos de dados em toda a organização, e é mais do que apenas revisar todas as políticas, procedimentos, códigos de conduta e diretrizes da organização que afetam o manuseio de dados pessoais durante seu ciclo de vida. A auditoria de adequação deve ser feita dentro da empresa e com todos os terceiros envolvidos, inclusive operadores.

8.5.1.2 Auditoria de Conformidade

Após a conclusão da auditoria de adequação, a próxima etapa poderá ser, e talvez até deva ser, uma auditoria de conformidade, para determinar se a organização está de fato cumprindo as políticas e procedimentos identificados durante e, talvez, aprimorada como resultado da auditoria de adequação.

Uma auditoria de conformidade requer uma investigação de como os dados pessoais são tratados **na prática** dentro das várias unidades de negócios, entre departamentos e ao lidar com terceiros.

Uma auditoria abrangente de conformidade também deve examinar fatores como:

- Se a organização oferece treinamento de conformidade de proteção de dados;
- Como as políticas de proteção de dados são disseminadas para os funcionários;
- Como as reclamações de violações de políticas são tratadas.

A profundidade da auditoria de conformidade dependerá dos riscos percebidos em relação a infrações legais e envolvendo o tratamento de dados pessoais.

8.5.2 Conteúdo de um plano de auditoria

Em 2024, o Tribunal de Contas da União aplicou um questionário para cada organização federal, estadual e municipal fiscalizada[18], sendo que também podemos considerar alguns aspectos aqui:

1. Desenvolvimento de programas de auditoria (planejamento)
• **Objetivo:** defina que o objetivo da auditoria é verificar a conformidade da organização com a LGPD, focando em áreas críticas como governança de dados, segurança da informação e gerenciamento de riscos. • **Prazos:** estabeleça um prazo realista para a conclusão da auditoria, incluindo etapas como coleta de informações, análise e elaboração do relatório final. • **Contatos e comunicação:** determine os pontos de contato dentro da organização (responsáveis pelo tratamento de dados, TI, jurídico) para facilitar o fluxo de informações.
2. Descrição da abordagem e o escopo da auditoria

• **Escopo:** Defina que a auditoria abrangerá áreas como:
  ○ Governança de proteção de dados
  ○ Gestão de acesso e segurança da informação
  ○ Proteção de dados pessoais sensíveis
  ○ Treinamento e conscientização dos colaboradores
• **Horizontal/Vertical:** decida se a abordagem será:
  ○ Horizontal: cobrirá processos transversais (por exemplo, como os dados são coletados e tratados em vários departamentos).
  ○ Vertical: Focará em departamentos específicos (como Recursos Humanos ou Marketing).
• **Foco na adequação ou conformidade:** identifique se a auditoria é para verificar adequação inicial ou conformidade contínua.

3. Preparativos e reunião de evidências
• **Documentação interna:** solicite as políticas de proteção de dados, normas de segurança da informação e documentos de procedimentos internos. • **Contratos e acordos:** revise os contratos com terceiros, como operadores de dados ou provedores de serviços, para verificar se há cláusulas adequadas de proteção de dados e conformidade com a LGPD. • **Treinamentos e conscientização:** avalie os materiais de treinamento e conscientização sobre a LGPD e segurança de dados oferecidos aos funcionários.
4. Execução da auditoria
• **Método:** utilize um questionário de autoavaliação baseado nos tópicos críticos de conformidade com a LGPD, como o controle de acesso a dados, a gestão de registros e a resposta a incidentes de segurança. • **Evidências:** peça por evidências documentais para confirmar as respostas fornecidas pela organização, como relatórios de auditoria anteriores, registros de incidentes de segurança e provas de consentimento dos titulares de dados.

[18] Tribunal de Contas da União. *Fiscalização de tecnologia da informação:* Fiscalização sobre a implementação dos dispositivos da LGPD na União, nos Estados e nos Municípios. Disponível em: https://portal.tcu.gov.br/fiscalizacao-de-tecnologia-da-informacao/atuacao/fiscalizacoes/auditoria-sobre-lgpd/. Acesso em 22.09.2024.

5. Relatório
• **Conclusão geral:** apresente uma visão geral da situação da organização em relação à LGPD, destacando pontos fortes e áreas de não conformidade. • **Áreas de boas práticas:** identifique práticas que estão em linha com as melhores práticas de proteção de dados, como a existência de políticas robustas e a realização de treinamentos regulares. • **Áreas para melhoria:** indique as áreas onde a organização pode melhorar, como a necessidade de atualizar contratos com fornecedores ou a implementação de controles de acesso mais rigorosos.
6. Acompanhamento
• **Monitoramento contínuo:** recomende a criação de um plano de acompanhamento para garantir que as melhorias sugeridas sejam implementadas. Estabeleça prazos para revisões periódicas e atualizações nas políticas de privacidade e segurança.

Exemplos de perguntas ou tópicos a serem abordados:

Governança de proteção de dados
• A organização tem um DPO (Encarregado) nomeado? • Existe uma política clara de governança de dados?
Segurança da informação
• Quais são as principais medidas técnicas e administrativas adotadas para garantir a segurança dos dados pessoais? • A organização realiza avaliações regulares de riscos de segurança?
Gestão de acessos
• Como a organização gerencia o acesso aos dados pessoais? • Existe controle de acesso baseado em funções?
Treinamento e conscientização
• Os funcionários recebem treinamento regular sobre LGPD e proteção de dados? • Existe um programa de conscientização sobre a importância da proteção de dados?
Gerenciamento de registros e consentimento
• A organização mantém registros adequados sobre o tratamento de dados pessoais? • Os consentimentos dos titulares de dados estão devidamente documentados?

8.6 Práticas relacionadas a aplicações do uso de dados, marketing e mídias sociais

8.6.1 O uso de informações de mídia social em atividades de marketing

Não há muito tempo, havia três métodos de informar ao público sobre o produto ou serviço que um vendedor estava tentando vender:

- Comprar publicidade cara;
- Pedir à mídia para contar sua história;
- Contratar uma enorme força de vendas para incomodar as pessoas diretamente sobre o produto.

Nenhum desses métodos foi realmente eficaz. Todos os três métodos foram baseados em interromper as pessoas no que estavam fazendo, esperando que elas pudessem ver o produto e pensar: “é isso o que tenho procurado” e, se assim fosse, então elas se lembrariam de quem anunciava e aonde deveriam ir para encontrar esse produto.

Com a internet, existem opções melhores para que seu produto seja notado. Dos produtores e consumidores, as pessoas se tornaram “prosumidores”[19], realizando o design de produtos, criticando e consumindo, gastando dinheiro. Tornou-se fácil criar um site, escrever um blog, publicar conteúdo e mídia (fotos, som, vídeo) nas mídias sociais. Não apenas os fornecedores, mas praticamente todos podem publicar seu próprio conteúdo, que seus consumidores desejam comprar.

Com as mídias sociais, todos podem entrar em contato com outras pessoas conectadas a essas mídias sociais, em qualquer lugar do mundo. Só com o Facebook e seus mais de 1,5 bilhão de usuários, um vasto mercado global está aberto.

Com essas mudanças soando na era digital, o negócio está se tornando "multicanal" e interativo. Os fornecedores escrevem sobre seus produtos como jornalistas, e as pessoas reagem a isso indicando que gostam do que veem, gostam do que está sendo produzido, do que está sendo oferecido. Claro, se elas não gostarem, elas não hesitarão em dizer ao mundo sobre isso também - muitas vezes em termos bastante contundentes.

Finalmente, um novo conceito de vendas está surgindo. Muitas pessoas acham importante o que as outras pessoas e, em particular, seus amigos, acham do produto que estão procurando. A mensagem de que "76% dos seus amigos gostam deste produto” prova ser um incentivo para comprar. Mesmo que não haja como verificar essa afirmação, todos parecemos acreditar.

Os consumidores podem ser divididos em grupos com gostos semelhantes, interesses semelhantes e outros grupos relevantes. Ao verificar uma loja on-line, todos nos deparamos com comentários como "compradores do <produto que você acabou de ver> também compraram: <estes outros produtos>". Mensagens como essa provam ser um facilitador de vendas muito forte, desde que o consumidor-alvo tenha gostos e interesses semelhantes aos dos "outros compradores".

8.6.2 Uso da internet no campo do marketing

Para que essa nova economia, mais digital, funcione, as empresas precisam de informações sobre potenciais compradores. Na prática, isso significa que eles precisam de informações sobre o maior número possível de consumidores. Que tipo de consumidor é esse? O tipo "radical", precisando de equipamentos e roupas de boa qualidade para o ar livre? O tipo "eu quero a mais nova tecnologia"? Ou talvez o tipo de melhor relação preço / desempenho, ou melhor, o tipo de comprador que busca o preço mais baixo garantido.

Perfis como esse demandam muitos dados sobre pessoas e seu comportamento. Como essas empresas obtêm essa informação?

8.6.3 Cookies

Um cookie é apenas um arquivo de texto (geralmente pequeno), armazenado no computador do usuário. Os cookies mais comuns são:

- Cookies de sessão;
- Cookies persistentes;
- Cookies de rastreamento.

8.6.3.1 Cookies de sessão

Os cookies de sessão permitem que os usuários sejam reconhecidos dentro de um site, de modo que qualquer alteração de página ou seleção de item ou de dados que o usuário faça seja lembrada de uma página para outra. O exemplo mais comum é o recurso de carrinho de compras

[19] Para mais informações, verifique: https://pt.wikipedia.org/wiki/Prosumer.

de qualquer loja virtual. Sempre que os itens são selecionados, a seleção é armazenada no cookie da sessão, por isso é lembrada até que o usuário esteja pronto para fazer checkout.

Ao fazer logon em um site, um cookie de sessão na memória do computador do usuário retém as informações de que o logon foi bem-sucedido, pois o site não tem como lembrar que você fez logon. Ao sair do site, o que usualmente significa fechar o navegador, o cookie da sessão é apagado da memória do computador do usuário e, como resultado, ele é desconectado.

8.6.3.2 Cookies persistentes

Os cookies persistentes permanecem no disco rígido do usuário até serem apagados pelo usuário ou até expirarem. Os cookies persistentes podem oferecer serviços simples ao usuário como visitante recorrente. Por exemplo, para manter a seleção de idioma do usuário. Quando o usuário revisitar esse site, ele oferecerá, com base nas informações do cookie, o conteúdo no idioma escolhido durante a visita anterior.

Esse tipo de cookie pode tornar a experiência do visitante do site mais pessoal. Por exemplo, um usuário usa um site de reservas para reservar um voo barato para a Inglaterra. Para que as transações (financeiras e com a companhia aérea) sejam bem-sucedidas, o usuário deve preencher informações pessoais (nome, endereço, número do passaporte, detalhes do cartão de crédito). Na próxima vez que o usuário visitar o site, a combinação dessas informações poderá levar a uma saudação mais pessoal, como "Bom dia, <nome>", mas também a ofertas de outras viagens, seguro de viagem, ofertas de bons equipamentos para caminhadas, malas de viagem, e mais. Tudo com base nas informações coletadas da viagem reservada e, se aplicável, nas viagens reservadas anteriormente.

Não há necessidade de salvar informações no cookie. De fato, um identificador único é suficiente para reconhecer o usuário (ou pelo menos seu dispositivo ou browser) e vincular esse identificador a um banco de dados.

8.6.3.3 Cookies de rastreamento

Um cookie de rastreamento geralmente é chamado de cookie de terceiros. Ele é colocado no disco rígido de um usuário por um site de um domínio diferente daquele que o usuário está visitando.

Assim como acontece com os cookies padrão, os cookies de terceiros colocados no computador do usuário possibilitam salvar algumas informações sobre o usuário para uso posterior. Entretanto, os cookies de terceiros, são geralmente definidos por redes de publicidade nas quais um site pode se inscrever.

O objetivo dos cookies é acompanhar quais páginas uma pessoa está visitando, construindo um perfil da pessoa com base em interesses. O perfil pode ser adicionado usando informações de outros sites em sua rede. Ele não está vinculado a detalhes pessoais conhecidos do site, mas apenas exibe anúncios ao perfil do usuário para que eles sejam os mais relevantes possível.

8.6.4 Outras informações de perfil: o preço dos serviços "gratuitos"

Redes sociais e buscadores na internet sabem quase tudo o que há para saber sobre os usuários de seus produtos gratuitos. Um exemplo disso é o disposto na Política de Privacidade do Facebook:

> As informações que coletamos e tratamos sobre você dependem do seu uso dos nossos. Por exemplo, coletamos informações diferentes se você vende móveis no Marketplace ou publica um reels no Instagram. Quando você usa nossos Produtos, coletamos algumas informações sobre você, **mesmo que não tenha uma conta.**

Estas são as informações que coletamos:
Sua atividade e as informações que você fornece;
As informações coletadas sobre amigos, seguidores e outras conexões;
As informações de apps, de navegadores e de dispositivos;
Informações de parceiros, fornecedores e outros terceiros.

Fonte: Política de Privacidade do Facebook (grifo nosso)[20]

Já os buscadores na internet combinam informações do LinkedIn, históricos de uso da funcionalidade dos mapas e postagens. É comum os buscadores saberem quais pessoas estão pesquisando ou comprando ativamente e quais palavras ou frases elas usam para encontrá-las. Eles sabem para cada um de seus usuários o que provavelmente comprarão em breve, o que precisarão comprar agora, mais tarde, hoje, amanhã e muito mais.

Um exemplo é o constante na Política de Privacidade da Google[21], que informa que a organização coleta:

- **Informações pessoais:** nome, endereço de e-mail, número de telefone, informações de pagamento;
- **Dados de atividade:** termos de pesquisa, vídeos assistidos, interações em sites e apps;
- **Informações de localização:** dados de GPS, endereços de IP;
- **Informações de dispositivos:** modelo do dispositivo, sistema operacional, navegador, endereço IP;
- **Cookies e tecnologias de rastreamento:** histórico de navegação, identificadores únicos de dispositivo.

8.6.5 Perspectiva de proteção de dados

A LGPD não impede a inovação e o tratamento de dados pessoais – apenas determina princípios, bases legais e outros parâmetros e limites para que essas operações ocorram de modo sustentável a longo prazo, sem que causem riscos às liberdades civis e aos direitos fundamentais dos titulares de dados pessoais.

8.6.5.1 Cookies

Os cookies de sessão normalmente são necessários para efetuar a transmissão de uma comunicação eletrônica através de uma rede de comunicações eletrônicas, ou para fornecer um serviço da sociedade da informação requerido pelo utilizador final, ou ainda para a medição do público na web, desde que essa medição seja efetuada pelo fornecedor do serviço da sociedade da informação solicitado pelo utilizador final. Para cumprir tais finalidades, podem ser armazenados sem o consentimento expresso do usuário, como no carrinho de compras on-line discutido anteriormente.

Para outros cookies, é necessário o consentimento nos moldes definidos pela LGPD. Esse consentimento deve ser livre, informado e inequívoco. A novidade da vez (e que tem sido bastante utilizada) é que os usuários finais podem expressar o consentimento (ou retirá-lo) facilmente pelas configurações do navegador. Isso ajuda a minimizar a sobrecarga de banners e pop-ups.

8.6.5.2 Criação de Perfil

Não há dúvida de que a LGPD se aplica à criação de perfil, conforme descrito no artigo 20. Por conseguinte, o titular dos dados tem o direito de solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus

[20] Facebook. *Política de Privacidade do Facebook*. Disponível em: https://www.facebook.com/privacy/policy/. Acesso em 22.09.2024.
[21] Google. *Política de Privacidade do Google*. Disponível em: https://policies.google.com/privacy?hl=pt-BR&fg=1#infocollect. Acesso em 22.09.2024.

interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade.
No mesmo dispositivo, a LGPD ainda determina que:

§ 1º O controlador deverá fornecer, sempre que solicitadas, informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, observados os segredos comercial e industrial.

§ 2º Em caso de não oferecimento de informações de que trata o [parágrafo anterior] baseado na observância de segredo comercial e industrial, a autoridade nacional poderá realizar auditoria para verificação de aspectos discriminatórios em tratamento automatizado de dados pessoais.

Fonte: Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709/2018 (art. 20, § 1º e 2º)

Tanto é assim que o artigo 12, § 2º, prevê:

§ 2º Poderão ser igualmente considerados como dados pessoais, para os fins desta Lei, aqueles utilizados para formação do perfil comportamental de determinada pessoa natural, se identificada.

Fonte: Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709/2018 (art. 12, § 2º)

Ainda há muitos serviços "gratuitos", oferecendo conteúdo ou outros produtos ou serviços gratuitos, desde que o usuário autorize a coleta de informações sobre ele, seus interesses e gostos para "selecionar propaganda apropriada". A LGPD não mudará isso, mas pelo menos nos dará a chance de realizar essa operação de modo mais consciente e com proteção dos dados pessoais.

Cabe ao titular dos dados ter cuidado com as informações reveladas às empresas que oferecem serviços gratuitos. O ponto é que a maioria das pessoas está acostumada a concordar com declarações longas sem realmente lê-las. A LGPD proíbe a declaração longa e ilegível e requer uma linguagem simples e clara, explicando para qual finalidade os dados pessoais coletados devem ser usados.

8.7 Big Data

O tratamento atual de grandes quantidades de informações de pessoas para a criação de perfis traz um grande desafio. O desafio é justamente encontrar um equilíbrio entre as preocupações com a proteção da privacidade e das liberdades pessoais e a possibilidade de apoiar o desenvolvimento econômico e tecnológico e a inovação com o uso dos dados.

E não são apenas as organizações que desejam que os dados sejam utilizados – os próprios titulares demandam esse tipo tratamento para a entrega de valor e conveniência a si próprio! A personalização facilita uma série de atividades e faz com que o titular se sinta especial com determinadas customizações.

É necessário que essa entrega de valor e conveniência seja acompanhada de uma preocupação atenta para que se evitem, no tratamento dos dados pessoais, problemas como a discriminação, a manipulação e supressão de direitos e liberdades fundamentais, a vigilância e repressão, e o cometimento de crimes decorrentes do acesso indevido às informações pessoais.

Se conseguirmos garantir que os dados pessoais serão tratados da forma correta (de acordo com a legislação) e em benefício (direto ou indireto) dos próprios titulares, por exemplo, estaremos no caminho certo.

A respeito da mineração de dados em Big Data, especialmente envolvendo dados públicos, confidenciais, sigilosos e protegidos por direitos autorais, alguns pontos importantes podem ser considerados, os quais serão apresentados a seguir.

8.7.1 Dados públicos

A mineração de dados públicos é geralmente menos controversa, desde que os dados sejam acessados conforme regulamentações específicas e respeitem princípios de transparência e interesse público. No entanto, o desafio é garantir que a agregação desses dados não leve a reidentificação de indivíduos, o que poderia violar leis de privacidade, como a LGPD.

Ao tratar de dados públicos, é fundamental equilibrar transparência e privacidade. A transparência é necessária para assegurar a responsabilidade pública, permitindo que a sociedade tenha acesso às informações para monitorar o governo e garantir uma governança eficiente. Por outro lado, a privacidade deve ser resguardada para proteger os dados pessoais e os direitos fundamentais dos indivíduos.

Mesmo que os dados sejam públicos, o tratamento deles deve seguir os princípios da Lei Geral de Proteção de Dados Pessoais (LGPD), especialmente no que diz respeito à anonimização e à não violação dos direitos dos titulares. A ANPD reforça que, ao processar dados públicos, as organizações devem garantir que o uso dessas informações não comprometa a privacidade, respeitando o direito dos cidadãos à confidencialidade em determinados contextos.

Esse equilíbrio é necessário para evitar riscos de discriminação, vigilância indevida ou exposição de dados sensíveis, preservando, ao mesmo tempo, o interesse público e a transparência governamental.

8.7.2 Dados confidenciais e sigilosos

Esses dados exigem um nível elevado de segurança no tratamento. A legislação, como a LGPD e diretrizes da ANPD, determina que as organizações implementem medidas técnicas e administrativas robustas para evitar vazamentos ou acessos não autorizados. O uso de tais dados em mineração deve ser justificado, e métodos de anonimização e pseudonimização são frequentemente recomendados para mitigar riscos.

Dados confidenciais e sigilosos apresentam um grande desafio para as organizações, especialmente no contexto do uso de ferramentas de Inteligência Artificial (IA), como o ChatGPT. A crescente integração dessas ferramentas no ambiente corporativo introduz o risco de que empregados, intencional ou inadvertidamente, insiram informações confidenciais, restritas ou sensíveis em plataformas de IA, expondo a empresa a violações de segurança e sigilo.

Essas ferramentas muitas vezes operam com processamento em nuvem, o que pode resultar em armazenamento ou tratamento externo de dados, levantando preocupações sobre a proteção de propriedade intelectual, informações estratégicas e dados pessoais confidenciais. Além disso, a falta de controle sobre como esses dados são processados e retidos por plataformas de IA aumenta o risco de vazamento ou comprometimento da confidencialidade.

Portanto, as organizações precisam adotar medidas rigorosas para monitorar e regular o uso de IA no local de trabalho. Isso inclui a capacitação dos empregados sobre os riscos do uso indevido de dados sensíveis em plataformas de IA, além da implementação de políticas de governança que restrinjam o uso dessas ferramentas para fins que possam expor dados confidenciais ou sigilosos.

8.7.3 Dados com direitos autorais

A mineração de dados protegidos por direitos autorais pode ser controversa. Em muitos casos, o uso desses dados requer licenciamento ou permissões explícitas. A utilização de dados sem as devidas autorizações pode configurar violação de direitos autorais, especialmente em setores como mídia e cultura, onde os dados são frequentemente reutilizados em análises e produções.

8.7.4 Equilíbrio entre privacidade e inovação

A mineração de grandes volumes de dados pode levar a inovações tecnológicas e novos insights, mas sempre é necessário equilibrar esse potencial com as preocupações de privacidade e proteção de dados, conforme destacado pela Estratégia Brasileira de Inteligência Artificial (EBIA) do MCTI[22]. A ANPD reforça que as tecnologias emergentes devem seguir os princípios de privacy by design para garantir que a privacidade dos dados seja preservada desde o início do processo de coleta e tratamento.

A mineração de dados em grandes volumes, seja no contexto de dados pessoais ou de dados públicos e confidenciais, deve sempre considerar os regulamentos de proteção de dados e os direitos dos titulares, conforme previsto pela LGPD e resoluções da ANPD.

8.8 Privacidade de dados e Inteligência Artificial (IA)

8.8.1 Relação e importância da privacidade e proteção de dados pessoais nos sistemas de IA

A relação entre privacidade, proteção de dados pessoais e sistemas de inteligência artificial (IA) é uma questão central no Projeto de Lei 2338/2023. Esse projeto, conhecido como "PL da Inteligência Artificial", busca estabelecer regras claras para o uso de IA visando garantir que o tratamento de dados pessoais seja seguro e respeite os direitos dos titulares, como previsto na Lei Geral de Proteção de Dados Pessoais (LGPD).

Um dos principais pontos do PL é a necessidade de proteger os dados pessoais no uso de IA, especialmente em setores sensíveis como saúde, educação e segurança pública. A privacidade é fundamental, pois sistemas de IA processam grandes volumes de dados, muitas vezes com impacto direto sobre as liberdades individuais e direitos fundamentais. O PL visa garantir que as tecnologias de IA sejam usadas de forma ética e transparente, alinhadas aos princípios da LGPD, como a minimização de dados e a proteção contra usos indevidos ou não autorizados.

Além disso, a Autoridade Nacional de Proteção de Dados (ANPD) propôs sugestões ao projeto para reforçar a proteção dos dados pessoais, recomendando normas específicas para sistemas de IA de alto risco, especialmente em ambientes de testes, como sandboxes[23]. O foco está em evitar fragmentações regulatórias e garantir que a ANPD tenha o papel central na regulamentação, o que manteria a coerência com a LGPD.

[22] Ministério da Ciência, Tecnologia e Inovação. *Inteligência Artificial*. Disponível em: https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/transformacaodigital/inteligencia-artificial. Acesso em 22.09.2024.
[23] Análise preliminar do Projeto de Lei nº 2338/2023, que dispõe sobre o uso da Inteligência Artificial. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/analise-preliminar-do-pl-2338_2023-formatado-ascom.pdf. Acesso em 22.09.2024.

A ANPD destacou, na oportunidade, algumas preocupações em relação à privacidade e proteção de dados pessoais nos sistemas de Inteligência Artificial (IA) no contexto do Projeto de Lei (PL) 2338/2023:

- **Tutela dos direitos dos titulares:** o PL 2338/2023 aborda direitos como o direito à informação, explicação, contestação e revisão de decisões automatizadas. Esses direitos se relacionam diretamente com os direitos dos titulares previstos na Lei Geral de Proteção de Dados Pessoais (LGPD), como o direito de acesso e revisão de decisões automatizadas. Isso sugere que as pessoas afetadas por sistemas de IA devem ter clareza sobre como seus dados estão sendo utilizados e as consequências das decisões baseadas em IA;
- **Riscos associados aos sistemas de IA de alto risco:** o PL classifica alguns sistemas de IA como de "alto risco" ou "risco excessivo", especialmente aqueles que lidam com grandes volumes de dados pessoais sensíveis ou que impactam significativamente os direitos fundamentais. A ANPD destaca a importância de garantir que esses sistemas sejam desenvolvidos e operados com salvaguardas adequadas para proteger os dados pessoais e os direitos fundamentais;
- **Mecanismos de governança:** a avaliação de impacto algorítmico (AIA) proposta no PL é semelhante ao Relatório de Impacto à Proteção de Dados Pessoais (RIPD) previsto na LGPD. Ambos os instrumentos têm como objetivo identificar e mitigar os riscos que o uso de IA pode representar aos titulares de dados, promovendo a conformidade com os marcos regulatórios;
- **Discriminação e não discriminação:** tanto o PL quanto a LGPD tratam do princípio da não-discriminação. A ANPD tem competência para auditar e verificar se há aspectos discriminatórios no tratamento automatizado de dados pessoais, e o PL reforça a proibição de discriminação em sistemas de IA;
- **Interação entre o PL e a LGPD:** a ANPD observa a necessidade de harmonizar as disposições do PL com as da LGPD, para evitar conflitos ou sobreposições de regulamentações, especialmente em relação aos direitos dos titulares e aos mecanismos de governança.

Portanto, a privacidade e a proteção de dados são pilares essenciais na regulamentação de IA, sendo crucial garantir que o desenvolvimento tecnológico seja equilibrado com a segurança e o respeito aos direitos dos titulares.

8.8.2 Principais requisitos para a incorporação da privacidade e proteção de dados em produtos e serviços de consumo

A consolidação entre a Lei Geral de Proteção de Dados Pessoais (LGPD) e o Código de Defesa do Consumidor (CDC) estabelece uma base robusta para garantir a privacidade e a proteção de dados pessoais no contexto de produtos e serviços de consumo no Brasil. Enquanto a LGPD traz regulamentações específicas sobre o tratamento de dados pessoais, o CDC oferece uma proteção mais ampla aos consumidores, garantindo direitos relacionados à informação e à segurança, como pode ser visto a seguir:

1. Princípios da transparência
• A LGPD (art. 6º, VI) estabelece que o tratamento de dados pessoais deve seguir o princípio da transparência, garantindo que os titulares tenham acesso claro e adequado às informações sobre como seus dados são tratados. • O CDC (art. 6º, III) reforça o direito à informação clara e adequada sobre os produtos e serviços, o que inclui o tratamento de dados pessoais. Ambas as leis exigem que o consumidor seja informado de maneira transparente sobre como seus dados serão utilizados.

2. Segurança e riscos
• A LGPD (art. 46) impõe aos controladores de dados a obrigação de adotar medidas de segurança para evitar acessos não autorizados e violações de dados. • Da mesma forma, o CDC (art. 6º, I) garante que os produtos e serviços fornecidos ao consumidor não coloquem em risco sua segurança, o que inclui a proteção contra vazamentos de dados ou uso indevido de informações pessoais.
3. Proteção contra abusos
Ambas as legislações preveem proteção contra práticas abusivas: • A LGPD regula o uso adequado e transparente de dados. • O CDC (art. 39) proíbe práticas abusivas que possam lesar o consumidor, como o uso de dados para fins não autorizados ou a coleta excessiva de informações.
4. Responsabilidade objetiva
Tanto a LGPD quanto o CDC atribuem responsabilidades claras aos controladores de dados e fornecedores de serviços: • A LGPD (art. 45) estabelece que o controlador é responsabilizado por danos causados a titulares de dados em caso de descumprimento da legislação. • O CDC (art. 12 e 14) impõe responsabilidade objetiva às empresas que prejudicarem o consumidor, incluindo danos causados por falhas na segurança de dados.
5. Práticas no comércio eletrônico
As práticas de comércio eletrônico são amplamente cobertas pelo Decreto nº 7.962/2013, que regulamenta a contratação no comércio eletrônico no Brasil. Este decreto, aliado à LGPD e ao CDC, garante a proteção dos dados pessoais e a segurança das informações dos consumidores em transações online. As empresas que operam no e-commerce devem fornecer informações claras sobre o tratamento de dados, implementar medidas de segurança e garantir os direitos dos consumidores quanto ao acesso e correção de suas informações pessoais.

8.8.3 Sandbox Regulatório da ANPD e IA no Programa de Privacidade

O Sandbox Regulatório da ANPD é uma iniciativa criada para promover a inovação em proteção de dados pessoais, permitindo que empresas e outras organizações testem produtos, serviços e tecnologias em um ambiente controlado, com flexibilidade regulatória. A ideia é impulsionar o desenvolvimento de soluções que respeitem a LGPD, ao mesmo tempo em que oferecem oportunidades para ajustes e melhorias antes de uma implementação em larga escala.

8.8.3.1 O que é o Sandbox Regulatório da ANPD

O Sandbox regulatório permite que organizações que estejam inovando no uso de dados pessoais possam operar com regras específicas e adaptadas, sob a supervisão da ANPD, por um período limitado de tempo. Isso incentiva a criação de novas tecnologias, garantindo que as soluções inovadoras estejam em conformidade com os princípios da LGPD. O objetivo é proporcionar um ambiente de experimentação controlada, onde a ANPD pode monitorar e avaliar os impactos e desafios de novas tecnologias em relação à privacidade.

8.8.3.2 IA no Programa de Privacidade

No contexto de Inteligência Artificial, o Sandbox regulatório da ANPD pode ser fundamental para permitir que startups e empresas mais estabelecidas experimentem algoritmos de IA com dados pessoais, sem o risco de sanções imediatas, desde que sejam cumpridos os requisitos de transparência, segurança e minimização de dados. Um dos principais desafios com a IA é garantir que os algoritmos não violem os direitos dos titulares, como a discriminação ou o uso excessivo de dados pessoais.

Esse programa de Sandbox também pode testar soluções que utilizam IA para reforçar a segurança e a privacidade dos dados, explorando como ferramentas automatizadas podem melhorar a detecção de violações e aprimorar o gerenciamento de consentimentos dos usuários.

- **Flexibilidade para inovação:** empresas que participam do Sandbox têm a oportunidade de desenvolver novas tecnologias, incluindo aquelas relacionadas à IA, sob supervisão da ANPD, assegurando que novos produtos possam ser testados sem infringir imediatamente as regras rígidas da LGPD;
- **Desafios e benefícios da IA:** IA apresenta desafios únicos no tratamento de dados, como a possibilidade de discriminação algorítmica ou decisões automatizadas sem supervisão humana. O Sandbox permite que esses desafios sejam enfrentados em um ambiente seguro, com acompanhamento da ANPD;
- **Equilíbrio entre inovação e conformidade:** o uso de IA em dados pessoais deve equilibrar a inovação com o respeito aos direitos dos titulares, como o princípio da privacidade desde a concepção (by design) e o controle do titular sobre seus dados;
- **Privacidade e segurança integradas:** o programa permite a criação de soluções que integram a privacidade desde o design, como esperado pela LGPD, e isso pode incluir ferramentas de IA que auxiliam no gerenciamento seguro e eficiente de grandes volumes de dados pessoais.

Essa iniciativa fomenta o desenvolvimento tecnológico e a aplicação de IA, ao mesmo tempo em que protege os dados pessoais em conformidade com os regulamentos de proteção de dados.

Para inserir uma iniciativa de uma organização sob o Sandbox Regulatório da ANPD, a organização deve seguir alguns passos que envolvem o planejamento estratégico, adesão aos critérios da ANPD, e a integração de aspectos inovadores no tratamento de dados pessoais.

Como inserir a iniciativa:

1. Identificação do projeto inovador
A organização deve identificar uma solução ou tecnologia que utiliza dados pessoais de forma inovadora e que pode se beneficiar da flexibilidade regulatória do Sandbox. Isso pode incluir projetos envolvendo Inteligência Artificial, Internet das Coisas, blockchain, ou novos métodos de coleta e processamento de dados, desde que haja um potencial benefício para o setor de proteção de dados.
2. Aplicação à ANPD
A organização precisa submeter uma proposta detalhada à ANPD, explicando o projeto, suas características inovadoras, o escopo de dados a serem tratados, e como o projeto pode ajudar a cumprir ou superar os requisitos da Lei Geral de Proteção de Dados Pessoais (LGPD).
3. Justificativa e objetivos
A proposta deve destacar como a participação no Sandbox permitirá que a organização experimente soluções de forma segura e controlada, contribuindo para o avanço da proteção de dados. Deve ser demonstrado que o projeto tem potencial de fornecer insights para futuras regulamentações ou práticas de mercado.
4. Medidas de conformidade
Mesmo sob o Sandbox, a organização precisa demonstrar que está tomando medidas para proteger os dados pessoais, como aplicar os princípios de privacy by design e by default, garantindo que os titulares dos dados permaneçam protegidos durante a fase de testes.
5. Monitoramento e relatórios
A organização deve se comprometer a reportar periodicamente os resultados à ANPD, incluindo avaliações sobre a conformidade, impactos na privacidade, e ajustes realizados durante a fase de teste.
6. Exemplo de introdução
"Visando a inovação no tratamento de dados pessoais e a conformidade com a Lei Geral de Proteção de Dados Pessoais (LGPD), a [Nome da Organização] submeteu seu projeto de [descrição do projeto] para participar do Sandbox Regulatório da ANPD. Este ambiente controlado permitirá que testemos soluções tecnológicas inovadoras, como [exemplo de tecnologia, como IA ou blockchain], enquanto garantimos a segurança e a privacidade dos titulares de dados. Nosso objetivo é contribuir para o avanço das práticas regulatórias de proteção de dados no Brasil, oferecendo soluções que possam ser amplamente adotadas em mercados futuros."

7. Benefícios
• Flexibilidade para testar soluções inovadoras. • Segurança jurídica ao operar sob regras específicas. • Contribuição para o avanço das regulamentações em proteção de dados.

Dessa forma, a organização alinha seu projeto com os objetivos do Sandbox e garante a conformidade com as exigências da ANPD.

Contato EXIN

www.exin.com