NORMA
BRASILEIRA

# ABNT NBR ISO/IEC 29100

Primeira edição
27.03.2020

## Tecnologia da informação — Técnicas de segurança — Estrutura de Privacidade

*Information technology — Security techniques — Privacy framework*

ICS 35.030

ISBN 978-85-07-08534-8

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS

Número de referência
ABNT NBR ISO/IEC 29100:2020
26 páginas



Documento impresso em 31/03/2020 19:50:29, de uso exclusivo de INST. FED. DE EDUC., CIÊNC. E TECN. RIO DE JANEIRO

ABNT
Av.Treze de Maio, 13 - 28º andar
20031-901 - Rio de Janeiro - RJ
Tel.: + 55 21 3974-2300
Fax: + 55 21 3974-2346
abnt@abnt.org.br
www.abnt.org.br

# Sumário

Página

**Figur**



**Tabelas**

# Prefácio Nacional

A Associação Brasileira de Normas Técnicas (ABNT) é o Foro Nacional de Normalização. As Normas Brasileiras, cujo conteúdo é de responsabilidade dos Comitês Brasileiros (ABNT/CB), dos Organismos de Normalização Setorial (ABNT/ONS) e das Comissões de Estudo Especiais (ABNT/CEE), são elaboradas por Comissões de Estudo (CE), formadas pelas partes interessadas no tema objeto da normalização.

Os Documentos Técnicos internacionais adotados são elaborados conforme as regras da ABNT Diretiva 3.

A ABNT chama a atenção para que, apesar de ter sido solicitada manifestação sobre eventuais direitos de patentes durante a Consulta Nacional, estes podem ocorrer e devem ser comunicados à ABNT a qualquer momento (Lei nº 9.279, de 14 de maio de 1996).

Os Documentos Técnicos ABNT, assim como as Normas Internacionais (ISO e IEC), são voluntários e não incluem requisitos contratuais, legais ou estatutários. Os Documentos Técnicos ABNT não substituem Leis, Decretos ou Regulamentos, aos quais os usuários devem atender, tendo precedência sobre qualquer Documento Técnico ABNT.

Ressalta-se que os Documentos Técnicos ABNT podem ser objeto de citação em Regulamentos Técnicos. Nestes casos, os órgãos responsáveis pelos Regulamentos Técnicos podem determinar as datas para exigência dos requisitos de quaisquer Documentos Técnicos ABNT.

A ABNT NBR ISO/IEC 29100 foi elaborada no Comitê Brasileiro de Computadores e Processamento de Dados (ABNT/CB-021), pela Comissão de Estudo de Técnicas de Segurança (CE-021:000.027). O Projeto circulou em Consulta Nacional conforme Edital nº 02, de 17.02.2020 a 17.03.2020.

A ABNT NBR ISO/IEC 29100 é uma adoção idêntica, em conteúdo técnico, estrutura e redação, à ISO/IEC 29100:2011 + Amd.1:2018, que foi elaborada pelo *Technical Committee Information Technology* (ISO/IEC JTC 1), *Subcommittee IT Security Techniques* (SC 27).

Foi incluído um Anexo Nacional, informativo, com o objetivo de fornecer esclarecimentos adicionais sobre as opções de tradução de termos, com a finalidade de manter o alinhamento com a Lei 13.709/2018 (Lei Geral de Proteção de Dados Pessoais – LGPD).

O Escopo da ABNT NBR ISO/IEC 29100 em inglês é o seguinte:

## *Scope*

*This Standard provides a privacy framework which*

— *specifies a common privacy terminology;*

— *defines the actors and their roles in processing personally identifiable information (PII);*

— *describes privacy safeguarding considerations; and*

— *provides references to known privacy principles for information technology.*

*This Standard is applicable to natural persons and organizations involved in specifying, procuring, architecting, designing, developing, testing, maintaining, administering, and operating information and communication technology systems or services where privacy controls are required for the processing of PII.*

# 0 Introdução

Esta Norma fornece uma estrutura de alto nível para a proteção de dados pessoais (DP) dentro de sistemas de tecnologia da informação e de comunicação (TIC). Ela é geral em sua natureza e coloca os aspectos organizacionais, técnicos e processuais em uma estrutura abrangente de privacidade.

A estrutura de privacidade é destinada a ajudar as organizações a estabelecerem os seus requisitos de salvaguarda de DP dentro de um ambiente TIC:

- especificando uma terminologia comum de privacidade;
- especificandoos atores e os seus papéis no tratamento de DP;
- descrevendo os requisitos de salvaguarda da privacidade; e
- referenciando princípios conhecidos de privacidade.

Em algumas jurisdições, as referências deste documento aos requisitos de salvaguarda da privacidade podem ser entendidas como complementares aos requisitos legais para proteção de DP. Devido ao crescente número de tecnologias que processam DP, é importante ter normas de segurança da informação que forneçam uma base de entendimento comum para a proteção dos DP. Esta Norma destina-se a aprimorar as normas existentes de segurança, adicionando um foco pertinente para o tratamento de DP.

O uso comercial e o valor crescentes dos DP, o compartilhamento de DP entre diferentes jurisdições legais e a complexidade cada vez maior dos sistemas de TIC podem tornar difícil para uma organização assegurar a privacidade e alcançar *compliance* com as várias leis aplicáveis. Porém, as partes interessadas na privacidade podem prevenir o surgimento da incerteza e da desconfiança, lidando adequadamente com as questões de privacidade e evitando casos de uso dos DP.

O uso desta Norma irá:

— ajudar no desenho, implementação, operação e manutenção de sistemas de TIC que tratem e protejam DP;

— incentivar soluções inovadoras que possibilitem a proteção de DP dentro dos sistemas de TIC; e

— melhorar os programas de privacidade nas organizações por meio do uso das melhores práticas.

A estrutura de privacidade fornecida nesta Norma pode servir como base para iniciativas adicionais de padronização da privacidade, como:

— uma arquitetura técnica de referência;

— implementação e uso de tecnologias específicas de privacidade e a gestão geral de privacidade;

— controles de privacidade para processos de dados terceirizados;

— avaliações de risco de privacidade; ou

— especificações de engenharia específicas.

Algumas jurisdições podem exigir *compliance* com um ou mais documentos referenciados no ISO/IEC JTC 1/SC27 WG5 Standing Documento 2 (WG 5 SD2) – *Official Privacy Documents References* [3] ou com outras leis e regulamentações aplicáveis, porém, este documento não se destina a ser um modelo de política global, nem uma estrutura legislativa.

# Tecnologia da informação — Técnicas de segurança — Estrutura de Privacidade

## 1 Escopo

Esta Norma fornece uma estrutura de privacidade que

— especifica uma terminologia comum de privacidade;

— especifica os atores e os seus papéis no tratamento de dados pessoais (DP);

— descreve considerações de salvaguarda de privacidade; e

— fornece referências para princípios conhecidos de privacidade para tecnologia da informação.

Esta Norma é aplicável às pessoas naturais e organizações envolvidas na especificação, aquisição, arquitetura, concepção, desenvolvimento, teste, manutenção, administração e operação de sistemas de tecnologia da informação e comunicação ou serviços em que controles de privacidade são necessários para o tratamento de DP.

## 2 Termos e definições

Para os efeitos deste documento, aplicam-se os seguintes termos e definições.

NOTA Para que seja mais fácil a utilização das normas da família ISO/IEC 27000 no contexto específico de privacidade e para integrar os conceitos de privacidade no contexto das normas da família ISO/IEC 27000, a tabela no Anexo A fornece os conceitos da ISO/IEC 27000 que correspondem aos conceitos da ABNT NBR ISO/IEC 29100 usados nesta Norma.

**2.1**
**anonimidade**
característica da informação que não permite que um titular de dados pessoais seja identificado direta ou indiretamente

**2.2**
**anonimização**
processo pelo qual dados pessoais (DP) são irreversivelmente alterados, de forma que um titular de DP não mais pode ser identificado, direta ou indiretamente, seja por um controlador de DP apenas ou em colaboração com qualquer outra parte

**2.3**
**dado anonimizado**
dado que tenha sido produzido como resultado de um processo de anonimização dos dados pessoais

**2.4**
**consentimento**
concordância, específica e informada, dada livremente pelo titular de dados pessoais (DP) para o tratamento de seus DP

**2.5**
**identificabilidade**
condição que resulta na identificação de um titular de dados pessoais (DP), direta ou indiretamente, com base em um dado conjunto de DP

**2.6**
***opt-in***
processo ou tipo de política, pelo qual é requerido que o titular de DP tome uma ação para expressar consentimento prévio e explícito de que seus DP sejam processados para uma determinada finalidade

NOTA Um termo diferente, que é frequentemente usado com o princípio de privacidade "consentimento e escolha", é *opt-out*. Ele descreve um processo ou tipo de política em que o titular de DP é obrigado a tomar uma ação separada, a fim de reter ou retirar o consentimento, ou se opor a um tipo específico de tratamento. O uso de uma política de *opt-out* presume que o controlador de DP tem o direito de tratar os DP da maneira pretendida. Este direito pode ser implícito em alguma ação do titular de DP diferente do consentimento (por exemplo, fazer um pedido em uma loja *online*).

**2.7**
**dados pessoais**
**DP**
qualquer informação que (a) possa ser usada para identificar a pessoa natural à qual tal informação se relaciona ou (b) pode estar direta ou indiretamente vinculada a uma pessoa natural

NOTA Para determinar se um titular de DP é identificável, convém que sejam levados em conta todos os meios que possam ser razoavelmente usados pela parte interessada na privacidade, detentora dos dados, ou por qualquer outra parte, para identificar a pessoa natural.

**NOTA BRASILEIRA** O motivo para a tradução do termo "*personally identifiable information (PII)*" por "dados pessoais" (DP) é o uso corrente da expressão "dados pessoais" no Brasil, além de sua adoção pela lei brasileira que trata de privacidade e proteção de dados pessoais (Lei 13.709/2018 – Lei Geral de Proteção de Dados Pessoais – LGPD).

**2.8**
**controlador de DP**
parte(s) interessada(s) na privacidade que determina(m) os objetivos e os meios para o tratamento dos dados pessoais (DP) e que não é(são) pessoa(s) natural(is) que usa(m) os dados para objetivos pessoais

NOTA Um controlador de DP algumas vezes instrui outros (por exemplo, operadores de DP) a tratar DP em seu nome, enquanto a responsabilidade pelo tratamento permanece com o controlador de DP.

**2.9**
**titular de DP**
pessoa natural a quem se referem os dados pessoais (DP)

NOTA Dependendo da jurisdição e da legislação específica de proteção de dados e privacidade, o sinônimo "sujeito dos dados" pode ser usado em vez do termo "titular de DP".

**2.10**
**operador de DP**
parte interessada na privacidade, que faz o tratamento dos dados pessoais (DP) em benefício e de acordo com as instruções de um controlador de DP

**NOTA BRASILEIRA** O motivo para a tradução do termo "*PII processor*" por "operador de DP" é o uso corrente da expressão "operador de DP" no Brasil e sua adoção pela lei brasileira que trata de privacidade e proteção de dados pessoais (Lei 13.709/2018 – Lei Geral de Proteção de Dados Pessoais – LGPD).

**2.11**
**violação de privacidade**
situação onde os dados pessoais são tratados em violação de um ou mais requisitos pertinentes de salvaguarda da privacidade

**2.12**
**controles de privacidade**
medidas que tratam os riscos de privacidade por meio da redução de sua probabilidade ou de suas consequências

NOTA 1 Controles de privacidade incluem medidas organizacionais, físicas e técnicas, por exemplo, políticas, procedimentos, diretrizes, contratos legais, práticas de gestão ou estruturas organizacionais.

NOTA 2 Controle é também usado como um sinônimo de salvaguarda ou contramedida.

**2.13**
**tecnologia de aprimoramento da privacidade**
**TAP**
controle de privacidade que consiste em medidas, produtos ou serviços de tecnologia da informação e da comunicação (TIC), que protegem a privacidade, eliminando ou reduzindo os dados pessoais (DP), ou impedindo o tratamento desnecessário e/ou indesejado de DP, tudo sem perder a funcionalidade do sistema de TIC

NOTA 1 Exemplos de TAP incluem, mas não são limitados a, ferramentas de anonimização e pseudonimização, que eliminam, reduzem, mascaram ou desidentificam DP, ou aquelas que previnem tratamento desnecessário, desautorizado ou indesejável de DP.

NOTA 2 Mascaramento é o processo de obscurecer os elementos de DP.

**2.14**
**política de privacidade**
intenção e orientação geral, regras e compromissos, formalmente expressos pelo controlador de dados pessoais (DP), relativos ao tratamento de DP em uma configuração específica

**2.15**
**preferências de privacidade**
escolhas específicas, feitas por um titular de dados pessoais (DP), sobre como convém que os seus DP sejam tratados para uma finalidade específica

**2.16**
**princípios de privacidade**
conjunto de valores compartilhados, governando a proteção de privacidade de dados pessoais (DP), quando tratados em sistemas de tecnologia da informação e comunicação

**2.17**
**risco de privacidade**
efeito da incerteza sobre a privacidade

NOTA 1 Risco é definido como o “efeito da incerteza sobre os objetivos” nos ABNT ISO Guia 73 e ABNT NBR ISO 31000.

NOTA 2 Incerteza é o estado, mesmo parcial, de deficiência de informação relacionada à compreensão ou conhecimento de um evento, sua consequência ou probabilidade.

**2.18**
**avaliação de impacto de privacidade**
AIP
avaliação de risco de privacidade
processo geral de identificação, análise, avaliação, consulta, comunicação e planejamento do tratamento de impactos potenciais da privacidade em relação à operação de informação de identificação pessoal (DP), estruturado dentro de um sistema de gestão de riscos mais abrangente da organização

[FONTE: ISO/IEC 29134:2017, 3.7, modificado – "avaliação de risco de privacidade" foi acrescentado como um termo aceitável.]

**2.19**
**requisitos de salvaguarda da privacidade**
conjunto de requisitos que uma organização precisa levar em conta ao tratar dados pessoais (DP) em relação à proteção de privacidade de DP

**2.20**
**parte interessada na privacidade**
pessoa natural ou jurídica, autoridade pública, agência ou qualquer outra entidade, que possa afetar, ser afetada ou perceber que é afetada por uma decisão ou atividade relacionada ao tratamento de dados pessoais (DP)

**2.21**
**tratamento de DP**
operação ou conjunto de operações realizadas sobre dados pessoais (DP)

NOTA Exemplos de operações de tratamento de DP incluem, mas não estão limitados a, coleta, armazenamento, alteração, recuperação, consulta, divulgação, anonimização, pseudonimização, disseminação ou disponibilização, exclusão ou destruição de DP.

**2.22**
**pseudonimização**
processo aplicado aos dados pessoais (DP) que substitui informação identificável por um pseudônimo

NOTA 1 Pseudonimização pode ser realizada, tanto pelos titulares de DP, quanto pelos controladores de DP. A pseudonimização pode ser usada pelos titulares de DP para usar consistentemente um recurso ou serviço sem divulgar a sua identidade para este recurso ou serviço (ou entre serviços), ainda assim sendo responsabilizada por este uso.

NOTA 2 A pseudonimização não exclui a possibilidade de que possa haver (um conjunto restrito de) partes interessadas na privacidade, que não sejam o controlador de DP do dado pseudonimizado, que sejam capazes de determinar a identidade do titular de DP, com base no pseudônimo e nos dados conectados a ele.

**2.23**
**uso secundário**
tratamento de dados pessoais (DP) em condições que diferem das iniciais

NOTA Condições que diferem das iniciais poderiam envolver, por exemplo, um novo propósito para tratamento de DP, um novo destinatário de DP etc.

**2.24**
**DP sensíveis**
categoria de dados pessoais (DP) cuja natureza é sensível, como aqueles que se relacionam à esfera mais íntima do titular de DP ou que podem ter um impacto significativo sobre o titular de DP

NOTA Em algumas jurisdições ou em contextos específicos, DP sensíveis são definidos com referência à natureza dos DP e podem consistir em DP que revelem a origem racial, opiniões políticas, crenças religiosas

ou outras, dados pessoais sobre saúde, vida sexual ou condenações criminais, bem como outros DP que possam ser definidos como sensíveis.

**2.25**
**terceiro**
parte interessada na privacidade que não o titular de dados pessoais (DP), o controlador de DP e o operador de DP, e as pessoas naturais que são autorizadas a tratar os dados sob direta autoridade do controlador de DP ou do operador de DP

## 3 Símbolos e termos abreviados

Os seguintes termos abreviados são comuns à ABNT NBR ISO/IEC 29100.

TIC Tecnologia da Informação e Comunicação

TAP Tecnologia de Aprimoramento de Privacidade

DP Dados Pessoais

## 4 Elementos básicos da estrutura de privacidade

### 4.1 Visão geral da estrutura de privacidade

Os seguintes componentes estão relacionados à privacidade e ao tratamento de DP em sistemas de TIC e compõem a estrutura de privacidade descrita nesta Norma:

— atores e papéis;

— interações;

— reconhecimento de DP;

— requisitos de salvaguarda de privacidade;

— políticas de privacidade; e

— controles de privacidade.

Para o desenvolvimento desta estrutura de privacidade, conceitos, definições e recomendações de outras fontes oficiais foram levados em consideração. Estas fontes podem ser encontradas no ISO/IEC JTC 1/SC27 WG5 Documento Padrão 2 (WG 5 SD2) – *Referência Oficial de Documentos de Privacidade* [3].

### 4.2 Atores e papéis

Para os efeitos desta Norma, é importante identificar os atores envolvidos no tratamento de DP. Existem quatro tipo de atores que podem estar envolvidos no tratamento de DP: titulares de DP, controladores de DP, operadores de DP e terceiros.

#### 4.2.1 Titulares de DP

Os titulares de DP fornecem os seus DP para tratamento aos controladores de DP e operadores de DP e, quando não for previsto pela lei aplicável, eles dão consentimento e determinam as suas

preferências de privacidade sobre como convém que os seus DP sejam tratados. Os titulares de DP podem incluir, por exemplo, um funcionário listado no sistema de recursos humanos de uma empresa, o consumidor mencionado em um relatório de crédito e um paciente listado em um prontuário eletrônico. Nem sempre é necessário que a respectiva pessoa natural seja identificada diretamente pelo nome para ser considerada um titular de DP. Se a pessoa natural a quem os DP se relacionam puder ser identificada indiretamente (por exemplo, por meio de um identificador de conta, número de documento de identidade ou mesmo pela combinação de atributos disponíveis), ela será considerada o titular dos DP para esse conjunto de DP.

### 4.2.2 Controladores de DP

Um controlador de DP determina o porquê (propósito) e o como (meios) o tratamento de DP ocorrerá. Convém que o controlador de DP assegure a aderência aos princípios de privacidade desta estrutura durante o tratamento de DP sob seu controle (por exemplo, implementando os controles de privacidade necessários). Pode existir mais de um controlador de DP para o mesmo conjunto de DP ou conjunto de operações de dados realizados sobre os DP (para o mesmo ou diferentes propósitos legítimos). Nestes casos, diferentes controladores de DP devem trabalhar conjuntamente e estabelecer os arranjos necessários para garantir que os princípios de privacidade sejam aderentes durante o tratamento de DP. Um controlador de DP também pode decidir ter todas ou parte das operações de tratamento realizadas por uma parte interessada diferente em seu nome. Convém que os controladores de DP avaliem cuidadosamente se estão processando DP sensíveis e que implementem controles de privacidade e segurança razoáveis e apropriados com base nos requisitos estabelecidos na jurisdição pertinente, bem como em possíveis efeitos adversos para os titulares de DP, identificados durante uma avaliação de risco de privacidade.

### 4.2.3 Operadores de DP

Um operador de DP realiza o tratamento de DP em nome do controlador de DP, agindo em nome dele ou conforme as instruções do controlador de DP, observando os requisitos de privacidade estipulados e implementando os controles de privacidade correspondentes. Em algumas jurisdições o operador de DP é vinculado por um contrato legal.

### 4.2.4 Terceiros

Um terceiro pode receber DP de um controlador de DP ou de um operador de DP. O terceiro não trata DP em nome do controlador de DP. Geralmente, o terceiro se tornará um controlador de DP por si próprio, quando receber os DP em questão.

## 4.3 Interações

Os atores identificados na Seção anterior podem interagir entre si de várias maneiras. Em relação aos fluxos possíveis de DP entre o titular de DP, o controlador de DP e o operador de DP, os seguintes cenários podem ser identificados:

a) o titular de DP fornece DP para um controlador de DP (por exemplo, ao se registrar em um serviço prestado pelo controlador de DP);

b) o controlador de DP fornece DP para um operador de DP, que realiza o tratamento de DP em nome do controlador de DP (por exemplo, como parte de um contrato de terceirização);

c) o titular de DP fornece DP para um operador de DP, que realiza o tratamento de DP em nome do controlador de DP;

d) o controlador de DP fornece ao titular de DP os DP que são relacionados ao titular de DP (por exemplo, respondendo a uma requisição feita pelo titular de DP);

e) o operador de DP fornece DP ao titular de DP (por exemplo, conforme indicado pelo controlador de DP); e

f) o operador de DP fornece DP para o controlador de DP (por exemplo, depois de ter realizado o serviço para o qual foi designado).

Os papéis do titular de DP, controlador de DP, operador de DP e um terceiro neste cenário são ilustrados na Tabela 1.

É necessário distinguir entre operadores de DP e terceiros, porque o controle legal dos DP permanece com o controlador de DP original quando ele é enviado para o operador de DP, enquanto um terceiro pode se tornar um controlador de DP por si só, uma vez que recebeu os DP em questão. Por exemplo, quando um terceiro toma a decisão de transferir DP que recebeu de um controlador de DP para outra parte, ele agirá como um controlador de DP por si só e, portanto, não será mais considerado um terceiro.

No que diz respeito aos possíveis fluxos de DP entre os controladores e operadores de DP, por um lado, e terceiros, por outro, os seguintes cenários podem ser identificados:

a) o controlador de DP fornece DP para um terceiro (por exemplo, no contexto de um acordo comercial); e

b) o operador de DP fornece DP para um terceiro (por exemplo, conforme indicado pelo controlador de DP).

Os papéis do controlador de DP e de um terceiro nestes cenários também estão ilustrados na Tabela 1.

**Tabela 1 – Fluxos de DP possíveis entre o titular de DP, o controlador de DP, o operador de DP e um terceiro, e seus papéis no fluxo**

| | Titular de DP | Controlador de DP | Operador de DP | Terceiro |
|---|---|---|---|---|
| Cenário a) | Provedor de DP | Recebedor de DP | – | – |
| Cenário b) | – | Provedor de DP | Recebedor de DP | – |
| Cenário c) | Provedor de DP | – | Recebedor de DP | – |
| Cenário d) | Recebedor de DP | Provedor de DP | – | – |
| Cenário e) | Recebedor de DP | – | Provedor de DP | – |
| Cenário f) | – | Recebedor de DP | Provedor de DP | – |
| Cenário g) | – | Provedor de DP | – | Recebedor de DP |
| Cenário h) | – | – | Provedor de DP | Recebedor de DP |

## 4.4 Reconhecendo DP

Para determinar se convém que uma pessoa natural seja ou não considerada identificável, vários fatores precisam ser levados em consideração. Em particular, convém que sejam levados em consideração todos os meios que possam ser razoavelmente usados pela parte interessada na privacidade que detém os dados ou por qualquer outra parte para identificar esta pessoa natural. Convém que os sistemas de TIC suportem mecanismos que conscientizem o titular de DP de tais informações e forneçam à pessoa natural os controles apropriados sobre o compartilhamento destas informações. As subseções a seguir fornecem esclarecimentos adicionais sobre como determinar se convém que um titular de DP seja ou não considerado identificável.

### 4.4.1 Identificadores

Em certos casos, a identificabilidade do titular de DP pode ser muito clara (por exemplo, quando a informação contém ou está associada a um identificador que é usado para se referir ou se comunicar com o titular de DP). As informações podem ser consideradas DP pelo menos nos seguintes casos:

— se elas contêm ou estão associadas a um identificador que se refere a uma pessoa natural (por exemplo, ao número do CPF);

— se elas contêm ou estão associadas a um identificador que pode ser relacionado a uma pessoa natural (por exemplo, um número de passaporte, uma conta bancária);

— se elas contêm ou estão associadas a um identificador que pode ser utilizado para estabelecer uma comunicação com uma pessoa natural identificada (por exemplo, uma localização geográfica precisa, um número de telefone); ou

— se elas contêm uma referência que liga os dados a qualquer dos identificadores acima.

### 4.4.2 Outras características distintivas

As informações não precisam necessariamente estar associadas a um identificador para serem consideradas DP. As informações também serão consideradas DP se contiverem ou estiverem associadas a uma característica que distingue uma pessoa natural de outras pessoas naturais (por exemplo, dados biométricos).

Qualquer atributo que assuma um valor que identifique exclusivamente um titular de DP é considerado uma característica distintiva. Observar que o fato de uma determinada característica distinguir uma pessoa natural de outras pessoas naturais pode mudar, dependendo do contexto de uso. Por exemplo, embora o sobrenome de uma pessoa natural possa ser insuficiente para identificar esta pessoa em escala global, muitas vezes será suficiente para distinguir uma pessoa natural em escala de empresa.

Adicionalmente, existem também situações nas quais uma pessoa natural é identificável mesmo se não existir atributo simples que a identifique unicamente. Este é o caso onde uma combinação de vários atributos tomados juntos distingue esta pessoa natural de outras pessoas naturais. Se a pessoa natural for ou não identificável com base em uma combinação de atributos, isto pode também ser dependente de um domínio específico. Por exemplo, a combinação dos atributos “feminino”, “45” e “advogado”, pode ser suficiente para identificar uma pessoa natural em uma companhia específica, porém será sempre insuficiente para identificar uma pessoa natural fora da companhia.

A Tabela 2 fornece alguns exemplos de atributos que poderiam ser considerados DP, dependendo do domínio. Estes exemplos são informativos.

**Tabela 2 – Exemplos de atributos que podem ser usados para identificar pessoas naturais**

| Exemplos |
|---|
| Idade ou necessidades especiais de pessoas naturais vulneráveis |
| Alegações de conduta criminosa |
| Qualquer informação coletada durante serviços de saúde |
| Conta bancária ou número de cartão de crédito |
| Identificador biométrico |
| Extratos de cartão de crédito |
| Condenações criminais ou delitos cometidos |
| Relatórios de investigação criminal |
| Número do cliente |
| Data de nascimento |
| Informação de diagnóstico de saúde |
| Deficiências |
| Contas médicas |
| Salários dos empregados e arquivos dos recursos humanos |
| Perfil financeiro |
| Gênero |
| Posição no GPS |
| Trajetória no GPS |
| Endereço residencial |
| Endereço IP |
| Localização fornecida por sistemas de telecomunicação |
| Histórico médico |
| Nome |
| Identificadores nacionais (por exemplo, número do passaporte) |
| Endereço de *e-mail* pessoal |
| Número de identificação pessoal (PIN) ou senha |
| Interesses pessoais derivados do rastreamento do uso de *websites* |
| Perfil pessoal ou comportamental |
| Número do telefone pessoal |
| Fotografia ou vídeo identificado a uma pessoa natural |
| Preferências de produtos ou serviços |
| Origem étnica ou racial |
| Crenças religiosas ou filosóficas |
| Orientação sexual |
| Filiação sindical |
| Contas de serviços públicos |

### 4.4.3 Informação que é ou pode ser vinculada a um titular de DP

Se as informações em questão não identificarem um titular de DP, convém que se determine se são ligadas, ou podem ser ligadas, à identidade de uma pessoa natural.

Uma vez que a relação com uma pessoa natural identificável é estabelecida, é necessário decidir se a informação diz alguma coisa sobre essa pessoa, por exemplo, se ela se refere às suas características ou comportamento. Exemplos incluem registros médicos, perfis financeiros ou interesses pessoais derivados do rastreamento do uso de *websites*. Além disso, declarações simples de atributos sobre uma pessoa natural, como idade ou sexo, podem qualificar as informações vinculadas como DP. Independentemente disso, se o relacionamento com uma pessoa natural identificável puder ser estabelecido, essas informações também devem ser tratadas como DP.

### 4.4.4 Dados pseudonimizados

Para restringir a capacidade dos controladores e operadores de DP de identificar o titular de DP, as informações de identidade podem ser substituídas por pseudônimos. Essa substituição geralmente é executada por um provedor de DP antes de transmitir os DP para um recebedor de DP, em particular nos cenários a, b, c, g e h da Tabela 1.

Certos processos de negócios dependem de operadores designados que executam a substituição e controlam a tabela ou função de atribuição. Geralmente, este é o caso em que dados sensíveis precisam ser tratados por partes interessadas na privacidade que não os coletaram.

A substituição é considerada pseudonimização, desde que:

a) os atributos restantes ligados ao pseudônimo não sejam suficientes para identificar o titular de DP a quem eles se relacionam; e

b) a atribuição de pseudônimo seja tal que não seja possível ser revertida por esforços razoáveis das partes interessadas na privacidade, exceto aquelas que a realizou.

A pseudonimização retém a capacidade de vinculação. Dados diferentes associados ao mesmo pseudônimo podem ser vinculados. Quanto maior o conjunto de dados associado a um determinado pseudônimo, maior é o risco de que a propriedade a) seja violada. Além disso, quanto menor o grupo de pessoas naturais ao qual um conjunto de dados pseudonimizados se relaciona, maior é a probabilidade de identificação de um titular de DP. Convém que atributos contidos diretamente nas informações em questão e atributos que podem ser facilmente vinculados a essas informações (por exemplo, usando um mecanismo de pesquisa ou referência cruzada com outros bancos de dados) sejam levados em conta ao determinar se as informações estão relacionadas a um titular de DP.

A pseudonimização contrasta com a anonimização. Os processos de anonimização também cumprem as propriedades a) e b) acima, mas destroem a capacidade de vinculação. Durante a anonimização, informações de identidade são apagadas ou substituídas por pseudônimos para os quais a função ou tabela de atribuição é destruída. Assim, os dados anonimizados não são mais DP.

### 4.4.5 Metadados

Os DP podem ser armazenados em um sistema de TIC, de modo que não sejam prontamente visíveis para o usuário do sistema (isto é, para o titular de DP). Os exemplos incluem o nome do titular de DP armazenado como metadados nas propriedades de um documento e comentários ou registro de alterações armazenados como metadados em um documento de processamento de texto. Se o titular de DP tiver conhecimento da existência de DP ou do tratamento de DP para esta finalidade, ele pode preferir que os DP não sejam tratados desta maneira ou sejam compartilhados publicamente.

### 4.4.6 DP não solicitados

Os DP não solicitados por um controlador de DP ou operador de DP (isto é, obtidos não intencionalmente) também podem estar armazenados em um sistema TIC. Por exemplo, um titular de DP poderia,

potencialmente, fornecer os DP para um controlador de DP que não foram solicitados ou procurados pelo controlador (por exemplo, DP adicionais fornecidos no contexto de um formulário de *feedback* anônimo em um *site*). O risco de coletar DP não solicitados pode ser reduzido considerando-se medidas de salvaguarda de privacidade no momento do projeto do sistema (também chamado de conceito de "*privacy by design*").

### 4.4.7 DP sensíveis

A sensibilidade se estende a todos os DP dos quais DP sensíveis podem ser derivados. Por exemplo, as prescrições médicas podem revelar informações detalhadas sobre a saúde do titular de DP. Mesmo que os DP não contenham informações diretas sobre a orientação sexual ou saúde do titular de DP, se eles puderem ser usados para inferir nessas informações, os DP poderiam ser sensíveis. Para os efeitos desta Norma, os DP devem ser tratados como sensíveis onde tal inferência e conhecimento da identidade do titular de DP for razoavelmente possível.

Em algumas jurisdições, o que constitui os DP sensíveis também é definido explicitamente na legislação. Os exemplos incluem informações que revelam raça, origem étnica, crenças religiosas ou filosóficas, opiniões políticas, associação a sindicatos, estilo de vida ou orientação sexual e saúde física ou mental do titular de DP. Em outras jurisdições, os DP sensíveis podem incluir informações que podem facilitar o roubo de identidade ou resultar em danos financeiros significativos à pessoa natural (por exemplo, números de cartão de crédito, informações de contas bancárias ou identificadores emitidos pelo governo, como números de passaporte, números de previdência social ou números de carteira de motorista) e informações que poderiam ser usadas para determinar a localização em tempo real do titular de DP.

O tratamento dos DP sensíveis requer precauções especiais. Em algumas jurisdições, o tratamento dos DP sensíveis pode ser proibido pela lei aplicável, mesmo com o consentimento por *opt-in* do titular de DP. Algumas jurisdições podem exigir a implementação de controles específicos nos quais determinados tipos de DP sensíveis são tratados (por exemplo, um requisito para criptografar os DP médicos ao transmiti-los por uma rede pública).

## 4.5 Requisitos de salvaguarda de privacidade

As organizações são motivadas a proteger os DP por diversas razões: para proteger a privacidade do titular de DP, para atender aos requisitos legais e regulamentares, para praticar a responsabilidade corporativa, para aumentar a confiança do consumidor etc. O objetivo desta seção é fornecer uma visão geral dos diferentes fatores que podem influenciar os requisitos de salvaguarda de privacidade que são relevantes para uma determinada organização ou partes interessadas na privacidade que tratam os DP.

Os requisitos de salvaguarda de privacidade podem relacionar-se a muitos aspectos diferentes do tratamento de DP, por exemplo, a coleta e retenção de DP, a transferência de DP para terceiros, a relação contratual entre os controladores de DP e operadores de DP, a transferência internacional de DP etc. Requisitos de salvaguarda de privacidade também podem variar em especificidade. Eles podem ter uma natureza muito geral, por exemplo, consistindo em uma enumeração de princípios de privacidade de alto nível que se espera que uma organização leve em consideração ao processar DP. No entanto, os requisitos de salvaguarda de privacidade também podem envolver restrições muito específicas ao processamento de certos tipos de DP ou exigir a implementação de controles específicos de privacidade.

Convém que o projeto de qualquer sistema de TIC que envolva o tratamento de DP seja precedido por uma identificação dos requisitos de salvaguarda de privacidade pertinentes. Convém que as implicações de privacidade de sistemas de TIC novos ou substancialmente modificados envolvendo o

tratamento de DP sejam resolvidas antes que esses sistemas de TIC sejam implementados. As organizações executam rotineiramente atividades amplas de gestão de riscos e desenvolvem perfis de risco relacionados aos seus sistemas de TIC.

A gestão de riscos é definida como “atividades coordenadas para dirigir e controlar uma organização no que se refere a riscos” (ABNT ISO Guia 73:2009). O processo de gestão de riscos de privacidade compreende os seguintes processos:

— estabelecer o contexto, compreendendo a organização (por exemplo, tratamento de DP, responsabilidades), o ambiente técnico e os fatores que influenciam a gestão de riscos de privacidade (ou seja, fatores legais e regulatórios, fatores contratuais, fatores comerciais e outros fatores);

— avaliação de riscos, identificando, analisando e avaliando os riscos para os titulares de DP (riscos que podem ser adversamente afetados);

— tratamento de risco, determinando os requisitos de salvaguarda de privacidade e identificando e implementando controles de privacidade para evitar ou reduzir os riscos para os titulares de DP;

— comunicação e consulta, obtendo informações das partes interessadas, obtendo consenso sobre cada processo de gestão de riscos, informando os titulares de DP e comunicando sobre riscos e controles; e

— monitoramento e análise crítica, acompanhando os riscos e controles, e melhorando o processo.

Uma entrega pode ser uma avaliação de impacto de privacidade, que é o componente da gestão de riscos que se concentra em garantir *compliance* aos requisitos da legislação de privacidade e proteção de dados, e em avaliar as implicações de programas novos ou substancialmente alterados para a privacidade. Convém que as avaliações de impacto de privacidade sejam enquadradas na estrutura de gestão de riscos mais ampla de uma organização.

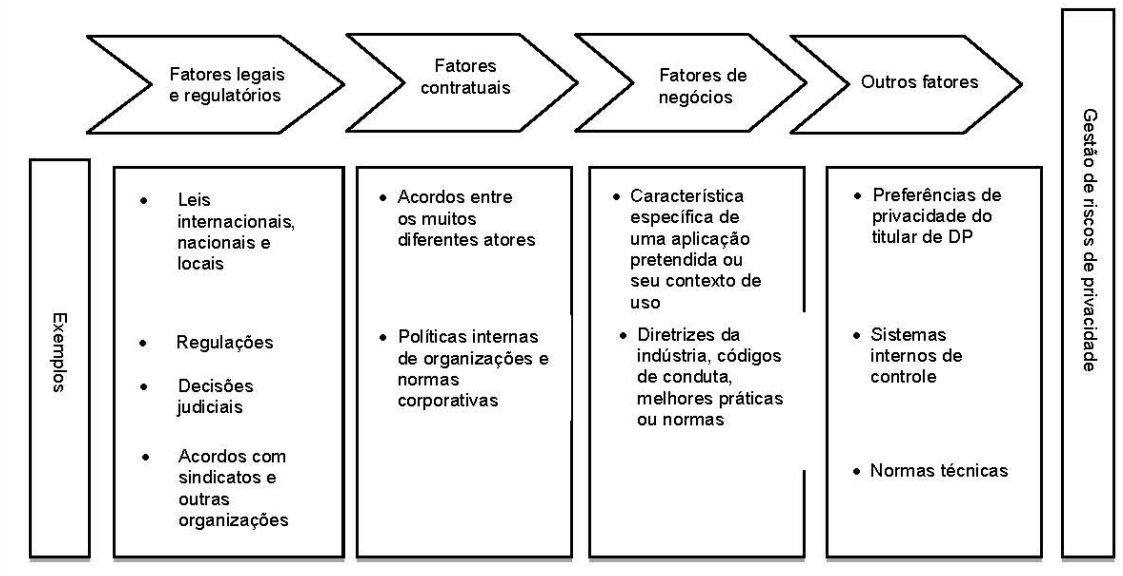


**Figura 1 – Fatores que influenciam a gestão de riscos de privacidade**

Requisitos de salvaguarda da privacidade são identificados como parte do processo geral de gestão de riscos de privacidade, que é influenciado pelos seguintes fatores (conforme ilustrado na Figura 1 e descrito abaixo):

— fatores legais e regulatórios para a salvaguarda da privacidade da pessoa natural e para a proteção dos seus DP;

— fatores contratuais, como acordos entre os muitos diferentes atores, políticas internas de organizações e normas corporativas;

— fatores de negócios predeterminados por uma aplicação de negócios específica ou em um contexto de caso de uso específico; e

— outros fatores que podem afetar o projeto de sistemas de TIC e os requisitos de salvaguarda de privacidade associados.

### 4.5.1 Fatores legais e regulatórios

Os requisitos de salvaguarda de privacidade são frequentemente refletidos em (1) leis internacionais, nacionais e locais, (2) regulações (3) decisões judiciais ou (4) acordos negociados com conselhos de trabalho ou outras organizações trabalhistas. Alguns exemplos de legislações local e nacional incluem leis de proteção de dados, leis de proteção ao consumidor, leis de notificação de violação, leis de retenção de dados e leis trabalhistas. O direito internacional pertinente pode conter regras que afetem a transferência transfronteiriça de DP. Convém que os controladores de DP estejam cientes de todos os requisitos pertinentes de salvaguarda de privacidade decorrentes de fatores legais ou regulatórios. Para atingir este objetivo, eles podem coordenar em conjunto com especialistas jurídicos. Embora em muitas jurisdições o controlador de DP seja o responsável final pela garantia de *compliance*, convém que todos os atores envolvidos no tratamento de DP adotem uma abordagem proativa na identificação de requisitos pertinentes de salvaguarda de privacidade decorrentes de fatores legais ou outros.

### 4.5.2 Fatores contratuais

As obrigações contratuais também podem influenciar os requisitos de salvaguarda da privacidade. Estas obrigações podem resultar de acordos entre os muitos diferentes atores, como operadores de DP, controladores de DP e terceiros. Por exemplo, uma parte interessada de privacidade pode requerer que terceiros usem controles de privacidade específicos e concordem com os requisitos específicos de eliminação de DP antes que os DP sejam transferidos para eles. Os requisitos de salvaguarda da privacidade também podem ser o resultado de políticas da empresa e de regras corporativas vinculantes que a parte interessada da privacidade estabeleceu para si, por exemplo, para proteger a sua marca de publicidade negativa no caso de violação da privacidade.

Em princípio, convém que qualquer parte que tenha acesso aos DP esteja ciente de suas obrigações pelo(s) respectivo(s) controlador(es) de DP, de uma maneira formalizada, por exemplo, pela inclusão nos acordos com terceiros. Tais acordos provavelmente contêm vários requisitos de salvaguarda de privacidade que os recipientes de DP precisarão levar em conta. Em certas jurisdições, autoridades nacionais e regionais podem ter instrumentos legais e contratuais estabelecidos que possibilitem a transferência de DP para terceiros.

### 4.5.3 Fatores de negócio

Os requisitos de salvaguarda de privacidade também podem ser influenciados por fatores de negócios, os quais incluem as características específicas de uma aplicação prevista ou o seu contexto de uso. Fatores de negócio podem variar largamente de acordo com o tipo de partes interessadas na

privacidade e o tipo de negócio. Por exemplo, eles podem relacionar-se ao setor no qual a organização atua (por exemplo, padrões para a indústria, códigos de conduta, melhores práticas, normas) ou à natureza do seu modelo de negócio (por exemplo, serviços *online* que operam 24 por 7, serviços de compartilhamento de informações, aplicações bancárias).

Muitos fatores de negócios não têm impacto direto nos requisitos de salvaguarda de privacidade como tal. O uso previsto de DP provavelmente pode afetar a implementação de políticas de privacidade de uma organização, bem como a escolha de controles de privacidade. Entretanto, convém que a organização não altere os princípios de privacidade que ela subscreve, por causa disto. Por exemplo, oferecer um determinado serviço pode requerer que um provedor de serviços colete DP adicionais ou permita que mais de seus funcionários acessem determinados tipos de DP. Entretanto, convém que um controlador de DP que tenha assinado os princípios contidos nesta estrutura avalie cuidadosamente quais tipos de DP são estritamente necessários para fornecer o serviço (princípio de limitação de coleta) e para limitar a operação de DP por seus funcionários, que precisam ter acesso para cumprir as suas obrigações (princípio da minimização de dados).

### 4.5.4 Outros fatores

O fator mais importante a ser considerado pelas organizações na identificação dos requisitos de salvaguarda da privacidade refere-se às preferências de privacidade dos titulares de DP. A disposição pessoal de uma pessoa natural em relação à privacidade e quais riscos uma pessoa natural considera podem depender de vários fatores, incluindo o entendimento da pessoa natural sobre a tecnologia usada, os seus antecedentes, as informações fornecidas, o propósito da transação, a natureza da experiência passada dessa pessoa e os fatores sociopsicológicos.

Convém que os projetistas de sistemas de TIC tentem entender as prováveis preocupações de privacidade de um titular de DP e entender os tipos de DP que serão tratados por meio de seu sistema. Assim como um desenvolvedor de sistema, ou um aplicativo ou provedor de serviços estuda o público-alvo de clientes para as expectativas de uso e seus desejos e necessidades, é importante tentar entender as expectativas e preferências das pessoas naturais relevantes em relação à privacidade. Embora nem sempre seja possível para os projetistas de sistemas de TIC fornecer aos titulares de DP as opções que correspondam às suas preferências de privacidade, essa é uma consideração importante no projeto.

Exemplos de preferências de privacidade poderiam incluir uma preferência por anonimato ou pseudonimato, a capacidade de restringir quem pode acessar os DP específicos ou a capacidade de restringir a finalidade para a qual os DP serão tratados. Convém que, na medida do possível, o titular de DP tenha uma escolha de preferências para o tratamento de seus dados, por exemplo, se os DP são usados para propósitos secundários, como *marketing*. A capacidade de expressar preferências favoráveis à privacidade pode ser implementada usando a interface gráfica do usuário do sistema TIC. Ela pode ajudar o titular de DP a fazer uma escolha, apresentando um conjunto de opções predefinidas para preferências de privacidade comuns em linguagem facilmente compreensível. A implementação da interface do usuário pode ser baseada em elementos como caixas de seleção ou menus suspensos.

Além dos fatores listados nas seções anteriores, ainda há outros fatores que podem influenciar o projeto de sistemas de TIC e os requisitos de proteção de privacidade associados. Por exemplo, os requisitos de proteção da privacidade podem ser influenciados por sistemas de controle interno ou normas técnicas adotadas por uma organização (por exemplo, uma norma voluntária, como uma Norma Brasileira).

## 4.6 Políticas de privacidade

Convém que a alta direção da organização envolvida no tratamento de DP estabeleça uma política de privacidade. Convém que a política de privacidade:

— seja apropriada ao objetivo da organização;

— forneça a estrutura para a determinação de objetivos;

— inclua um compromisso em satisfazer os requisitos aplicáveis de salvaguarda da privacidade;

— inclua um compromisso com a melhoria contínua;

— seja comunicada dentro da organização; e

— esteja disponível para as partes interessadas, conforme apropriado.

Convém que a organização documente a sua política de privacidade por escrito. Onde uma organização que processa DP é um operador de DP, essas políticas podem ser determinadas em grande parte pelo controlador de DP. Convém que a política de privacidade seja complementada por regras e obrigações mais detalhadas das diferentes partes interessadas envolvidas no tratamento de DP (por exemplo, procedimentos para departamentos ou funcionários específicos). Além disso, convém que os controles usados para impor a política de privacidade em uma configuração específica (por exemplo, controle de acesso, disposições de aviso, auditorias etc.) sejam claramente documentados.

O termo “política de privacidade” é frequentemente usado para se referir a políticas de privacidade internas e externas. Uma política de privacidade interna documenta os objetivos, regras, obrigações, restrições e/ou controles adotados por uma organização para atender aos requisitos de proteção de privacidade pertinentes para o tratamento de DP. Uma política de privacidade externa fornece às pessoas de fora da organização um aviso das práticas de privacidade da organização, bem como outras informações pertinentes, como identidade e endereço oficial do controlador de DP, pontos de contato dos quais os titulares de DP podem obter informações adicionais etc. No contexto desta estrutura, o termo “política de privacidade” é usado para se referir à política de privacidade interna de uma organização. As políticas de privacidade externas são chamadas de avisos.

## 4.7 Controles de privacidade

Convém que as organizações identifiquem e implementem controles de privacidade para atender aos requisitos de proteção de privacidade identificados pelo processo de avaliação e tratamento de risco de privacidade. Além disso, convém que os controles de privacidade identificados e implementados sejam documentados como parte da avaliação de risco de privacidade da organização. Certos tipos de tratamento de DP podem exigir controles específicos para os quais a necessidade só se torna aparente uma vez que um tratamento previsto tenha sido cuidadosamente analisado. Uma avaliação de risco de privacidade pode ajudar as organizações a identificar os riscos específicos de violação de privacidade envolvidos em uma operação planejada.

Convém que esforços sejam feitos pelas organizações para desenvolver os seus controles de privacidade como parte de uma abordagem geral de “*privacy by design*”, isto é, convém que a *compliance* com privacidade seja levada em conta na fase de projeto dos sistemas de tratamento de DP, em vez de ser implementada em um estágio subsequente.

No que diz respeito aos controles de segurança da informação, é importante observar que nem todo tratamento de DP requer o mesmo nível ou tipo de proteção. Convém que as organizações façam a

distinção das operações de tratamento de DP, de acordo com os riscos específicos que apresentam, para ajudar a determinar quais controles de segurança da informação são apropriados em cada situação. A gestão de riscos é um método central neste processo, e convém que a identificação de controles de privacidade seja parte integrante da estrutura de gestão de segurança da informação de uma organização.

# 5 Os princípios de privacidade da ABNT NBR ISO/IEC 29100

## 5.1 Visão geral dos princípios de privacidade

Os princípios de privacidade descritos nesta Norma foram derivados de princípios existentes desenvolvidos por vários países e organizações internacionais. Esta estrutura se concentra na implementação dos princípios de privacidade em sistemas de TIC e no desenvolvimento de sistemas de gestão de privacidade a serem implementados nos sistemas de TIC da organização. Convém que esses princípios de privacidade sejam usados para orientar a concepção, o desenvolvimento e a implementação de políticas de privacidade e controles de privacidade. Além disso, eles podem ser usados como uma linha de base no monitoramento e medição de questões de desempenho, *benchmarking* e auditoria de programas de gestão de privacidade em uma organização.

Apesar das diferenças nos fatores sociais, culturais, legais e econômicos que podem limitar a aplicação desses princípios em alguns contextos, recomenda-se a aplicação de todos os princípios estabelecidos nesta Norma. Convém que exceções a esses princípios sejam limitadas.

Os seguintes princípios de privacidade formam a base para esta Norma.

**Tabela 3 – Os princípios de privacidade da ABNT NBR ISO/IEC 29100**

| |
|---|
| 1. Consentimento e escolha |
| 2. Legitimidade e especificação de objetivo |
| 3. Limitação de coleta |
| 4. Minimização de dados |
| 5. Uso, retenção e limitação da divulgação |
| 6. Precisão e qualidade |
| 7. Abertura, transparência e notificação |
| 8. Participação individual e acesso |
| 9. Responsabilização |
| 10. Segurança da informação |
| 11. *Compliance* com a privacidade |

## 5.2 Consentimento e escolha

Aderir ao princípio do consentimento significa:

— apresentar ao titular de DP a escolha de permitir ou não o tratamento de seus DP, exceto quando o titular de DP não puder livremente reter o consentimento ou onde a legislação aplicável permitir especificamente o tratamento de DP sem o consentimento da pessoa natural. A escolha do titular de DP deve ser dada livremente, específica e com conhecimento;

— obter o consentimento *opt-in* de aceitação do titular de DP para coletar ou processar os DP sensíveis, exceto onde a lei aplicável permitir o processamento de DP sensível sem o consentimento da pessoa natural;

— informar aos titulares de DP, antes de obter o consentimento, sobre os seus direitos sob o princípio de participação e acesso individual;

— fornecer aos titulares de DP, antes da obtenção do consentimento, as informações indicadas pelo princípio da abertura, transparência e notificação; e

— explicar aos titulares de DP as implicações da concessão ou retenção do consentimento.

Convém que sejam tomadas providências para que os titulares de DP tenham a oportunidade de escolher como os seus DP são tratados e permitir que um titular de DP retire o seu consentimento com facilidade e sem ônus. Convém que este pedido seja tratado de acordo com a política de privacidade. Mesmo se o consentimento for retirado, o controlador de DP pode precisar reter certos DP por um período de tempo para cumprir as obrigações legais ou contratuais (por exemplo, responsabilização e retenção de dados). Nos casos em que o tratamento das informações pessoais de identificação não se baseia no consentimento, mas sim em outra base jurídica, convém que o titular de DP seja notificado sempre que possível. Quando o titular de DP tiver a capacidade de retirar o consentimento e tiver escolhido fazê-lo, convém que este DP seja dispensado de ser tratado para qualquer finalidade não legalmente obrigatória.

Para um controlador de DP, aderir ao princípio de escolha significa:

— fornecer aos titulares de DP mecanismos claros, proeminentes, facilmente compreensíveis, mecanismos acessíveis e inteligíveis para exercer a escolha e dar o consentimento em relação ao tratamento de seus DP no momento da coleta, primeiro uso ou assim que praticável depois disso; e

— implementar as preferências do titular de DP conforme expressas em seu consentimento.

Além disso, disposições adicionais podem ser estabelecidas para o tratamento de DP, além do consentimento (por exemplo, o desempenho de um contrato, o interesse vital do titular de DP ou o cumprimento da lei). A lei aplicável, em alguns casos, prevê que o consentimento do titular de DP não constitui uma base legal suficiente para tratar DP (por exemplo, o consentimento de um menor de idade dado sem a aprovação de um pai ou responsável). Além disso, requisitos adicionais para a transferência de DP internacionalmente precisam ser considerados. É responsabilidade do controlador de DP estar em *compliance* com estas disposições adicionais antes de tratar ou transferir dados.

## 5.3 Especificação e legitimidade de objetivo

Aderir ao princípio da especificação e legitimidade de objetivo significa:

— assegurar que o(s) objetivo(s) esteja(m) em conformidade com a legislação aplicável e conte(m) com uma base jurídica permissível;

— comunicar o(s) objetivo(s) ao titular de DP antes do momento em que a informação é coletada ou usada pela primeira vez para um novo objetivo;

— usar linguagem para esta especificação que seja clara e apropriadamente adaptada às circunstâncias; e

— se aplicável, dar explicações suficientes para a necessidade de tratar os DP sensíveis.

Com relação aos DP sensíveis, regras mais rigorosas podem ser aplicadas ao objetivo do tratamento. Uma finalidade pode requerer uma base legal ou uma autorização específica de uma autoridade de proteção de dados ou de uma autoridade governamental. Se a(s) finalidade(s) do tratamento de DP não estiver(em) de acordo com a lei aplicável, convém que o tratamento não ocorra.

## 5.4 Limitação de coleta

Aderir ao princípio de limitação de coleta significa:

— limitar a coleta de DP àquilo que está dentro dos limites da lei aplicável e estritamente necessário para o(s) objetivos(s) especificado(s).

Não convém que as organizações coletem DP indiscriminadamente. Convém que tanto a quantidade quanto o tipo de DP coletado sejam limitados ao necessário para cumprir o(s) objetivo(s) especificado(s) pelo controlador de DP. Convém que as organizações considerem cuidadosamente quais DP serão necessários para realizar uma finalidade específica antes de prosseguir com a coleta de DP. Convém que as organizações documentem o tipo de DP coletado, bem como a sua justificativa para fazê-lo, como parte de suas políticas e práticas de manuseio de informações.

Um controlador de DP pode desejar coletar os DP adicionais para outros objetivos que não o fornecimento de um serviço específico solicitado pelo titular de DP (por exemplo, para fins de *marketing* direto). Dependendo da jurisdição, estas informações adicionais só podem ser coletadas com o consentimento do titular de DP. Também é possível que a coleta de determinadas informações seja exigida pela lei aplicável. Sempre que possível, convém que o titular de DP tenha a capacidade de escolher entre fornecer ou não essas informações. Convém que o titular de DP também seja claramente informado do fato de que sua resposta a tais solicitações de informações adicionais pode ser opcional.

## 5.5 Minimização de dados

A minimização de dados está intimamente ligada ao princípio de “limitação de coleta”, mas vai além disso. Enquanto a “limitação de coleta” refere-se aos dados limitados que estão sendo coletados em relação à finalidade especificada, a “minimização de dados” minimiza estritamente o tratamento de DP.

Aderir ao princípio de minimização de dados significa conceber e implementar procedimentos de tratamento de dados e sistemas de TIC, de forma a:

— minimizar os DP tratados e o número de partes interessadas na privacidade e pessoas a quem são divulgado os DP ou que têm permissão para tratá-los;

— assegurar a adoção de um princípio de “necessidade de conhecer” (ou seja, convém que seja permitido tratar apenas os DP necessários para o desempenho de suas funções oficiais, no âmbito do objetivo legítimo do tratamento de DP);

— usar ou oferecer como opções-padrão, sempre que possível, interações e transações que não envolvam a identificação de titulares de DP, reduzam a observabilidade de seus comportamentos e limitem a vinculação de DP coletados; e

— de modo seguro, descartar os DP sempre que for prático fazê-lo, em particular quando o objetivo para o tratamento dos DP tiver expirado, e quando não houver requisitos legais para mantê-los.

## 5.6 Limitação de uso, retenção e divulgação

Aderir ao princípio de limitação de uso, retenção e divulgação significa:

— limitar o uso, retenção e divulgação (incluindo a transferência) de DP ao que é necessário para cumprir objetivos específicos, explícitos e legítimos;

— limitar o uso de DP aos objetivos especificados pelo controlador de DP antes da coleta, a menos que um objetivo diferente seja explicitamente exigido pela lei aplicável;

— reter os DP somente pelo tempo necessário para cumprir os objetivos declarados e, posteriormente, destruí-los ou anonimizá-los com segurança; e

— bloquear (ou seja, arquivar, proteger e isentar os DP de tratamento adicional) qualquer DP quando e por quanto tempo as finalidades estabelecidas tiverem expirado, mas onde a retenção for exigida pelas leis aplicáveis.

Quando os DP são transferidos internacionalmente, convém que o controlador de DP esteja ciente de quaisquer requisitos nacionais ou locais adicionais específicos para transferências internacionais.

## 5.7 Precisão e qualidade

Aderir ao princípio da precisão e qualidade significa:

— assegurar que os DP tratados sejam precisos, completos, atualizados (a menos que haja uma base legítima para manter os dados desatualizados), adequados e pertinentes para o objetivo de uso;

— assegurar a confiabilidade dos DP recolhidos a partir de uma fonte que não seja o titular de DP antes de ser tratado;

— verificar, por meios apropriados, a validade e a exatidão das reivindicações feitas pelo titular de DP antes de fazer qualquer alteração nos DP (a fim de assegurar que as alterações sejam devidamente autorizadas), quando for apropriado fazê-lo;

— estabelecer procedimentos de coleta de DP para ajudar a garantir a precisão e a qualidade; e

— estabelecer mecanismos de controle para verificar periodicamente a precisão e a qualidade dos DP coletados e armazenados.

Este princípio é particularmente importante nos casos em que os dados possam ser utilizados para conceder ou negar um benefício significativo à pessoa natural ou em que os dados imprecisos possam, de outra forma, resultar em danos significativos para a pessoa natural.

## 5.8 Abertura, transparência e notificação

Aderir ao princípio de abertura, transparência e notificação significa:

— fornecer aos titulares de DP informações claras e de fácil acesso sobre as políticas, procedimentos e práticas do controlador de DP em relação ao tratamento de DP;

— incluir em notificações o fato de que os DP estão sendo tratados, o objetivo para o qual isto é feito, os tipos de partes interessadas na privacidade a quem os DP podem ser divulgados e a identidade do controlador de DP, incluindo informações sobre como entrar em contato com o controlador de DP;

— divulgar as escolhas e os meios oferecidos pelo controlador de DP aos titulares de DP para fins de limitação do tratamento e acesso, correção e remoção de suas informações; e

— notificar aos titulares de DP quando ocorrerem mudanças importantes nos procedimentos de tratamento de DP.

Transparência, incluindo informações gerais sobre a lógica subjacente ao tratamento de DP, pode ser necessária, particularmente se o tratamento envolver uma decisão que afete o titular de DP. Convém que as partes interessadas na privacidade que tratam os DP disponibilizem informações específicas sobre as suas políticas e práticas relacionadas à gestão de DP prontamente disponíveis ao público. Convém que todas as obrigações contratuais que afetem o tratamento de DP sejam documentadas e comunicadas internamente, conforme apropriado. Convém que elas também sejam comunicadas externamente, na medida em que essas obrigações não sejam confidenciais.

Além disso, convém que o propósito do tratamento de DP seja suficientemente detalhado para permitir que o titular de DP compreenda:

— os DP especificados requeridos para o objetivo especificado;

— o objetivo especificado para a coleta de DP;

— o tratamento especificado (incluindo mecanismos de coleta, comunicação e armazenamento);

— os tipos de pessoas naturais autorizadas que terão acesso aos DP e para quem os DP podem ser transferidos; e

— os requisitos de retenção e descarte de DP especificados.

## 5.9 Acesso e participação individual

Aderir ao princípio de acesso e participação individual significa:

— dar aos titulares de DP a capacidade de acessar e analisar criticamente os seus DP, desde que a sua identidade seja primeiramente autenticada com um nível apropriado de garantia e tal acesso não seja proibido pela lei aplicável;

— permitir que os responsáveis pelos DP questionem a exatidão e a integridade dos DP e que sejam aperfeiçoados, corrigidos ou removidos conforme apropriado e possível no contexto específico;

— fornecer qualquer emenda, correção ou remoção aos operadores de DP e terceiros para os quais os DP foram divulgados, quando eles são conhecidos; e

— estabelecer procedimentos para permitir que os titulares de DP exerçam estes direitos de forma simples, rápida e eficiente, o que não implica atrasos ou custos indevidos.

Convém que o controlador de DP aplique controles apropriados para garantir que os titulares de DP acessem estritamente os seus próprios DP que não outros de titulares de DP, a menos que a pessoa natural que acessa esteja agindo sob autoridade em nome de um titular de DP incapaz de

exercer o seu direito de acesso. A lei aplicável pode fornecer à pessoa natural o direito de acessar, analisar criticamente e contestar o tratamento de DP sob certas circunstâncias. Quando uma disputa não é resolvida satisfatoriamente para a pessoa natural, convém que o conteúdo da disputa não resolvida seja registrado pela organização. Quando apropriado, convém que a existência da disputa não resolvida seja transmitida aos operadores de DP e a terceiros que tenham acesso às informações em questão.

### 5.10 Responsabilização

O tratamento de DP implica no dever de zelar e adotar medidas concretas e práticas para a sua proteção. Aderir ao princípio da responsabilização significa:

— documentar e comunicar oportunamente todas as políticas, procedimentos e boas práticas relacionadas à privacidade;

— atribuir a um indivíduo específico dentro da organização (que pode, por sua vez, delegar a outros em sua organização, conforme apropriado) a tarefa de implementar as políticas, procedimentos e boas práticas relacionadas à privacidade;

— ao transferir os DP para terceiros, garantir que o terceiro destinatário seja obrigado a fornecer um nível equivalente de proteção da privacidade por meios contratuais ou outros, como políticas mandatórias internas (a lei aplicável pode conter requisitos adicionais relativos a transferências de dados internacionais);

— fornecer treinamento adequado para o pessoal do controlador de DP que terá acesso aos DP;

— estabelecer procedimentos internos eficientes de tratamento de reclamações e de recurso para uso pelos responsáveis pelos DP;

— informar os titulares de DP sobre violações de privacidade que possam causar danos substanciais a eles (a menos que seja proibido, por exemplo, enquanto se trabalha com a aplicação da lei), bem como as medidas tomadas para a resolução;

— notificar todas as partes interessadas pertinentes sobre a violação de privacidade, conforme exigido em algumas jurisdições (por exemplo, as autoridades de proteção de dados) e dependendo do nível de risco;

— permitir que um DP prejudicado tenha acesso a sanções e/ou recursos adequados e eficazes, como retificação, expurgo ou restituição, se uma violação de privacidade ocorrer; e

— considerar procedimentos para compensação de situações em que será difícil ou impossível recuperar o *status* de privacidade da pessoa natural de volta a uma posição como se nada tivesse ocorrido.

Convém que as medidas para remediar uma violação da privacidade sejam proporcionais aos riscos associados à violação, porém convém que elas sejam implementadas o mais rápido possível (a menos que seja proibido, como, por exemplo, uma interferência em uma investigação legal).

Estabelecer procedimentos de reparação é uma parte importante do estabelecimento da responsabilização. A reparação fornece um meio para o titular de DP manter o controlador de DP responsável pelo uso indevido de DP. A restituição é uma forma de reparação que implica a compensação do titular de DP prejudicado. Isto é importante não apenas na situação de roubo de identidade, danos à reputação ou uso indevido de DP, mas também onde erros foram cometidos na modificação ou alteração dos respectivos DP.

Onde existem os processos de reparação, os titulares de DP podem se sentir mais confiantes ao entrar em uma transação, porque o risco percebido para a pessoa natural em relação ao resultado é efetivamente reduzido. Para alguns serviços, a reparação é mais fácil de obter (por exemplo, perdas financeiras) do que para outros (por exemplo, uma identidade roubada, danos à imagem ou reputação da pessoa natural), onde a capacidade de quantificar e compensar a perda pode ser um pouco mais difícil. A correção funciona melhor quando baseada na transparência e honestidade. Os tipos necessários de medidas de reparação podem ser regidos por lei.

## 5.11 Segurança da informação

Aderir ao princípio da segurança da informação significa:

— proteger os DP sob sua autoridade com controles apropriados nos níveis operacional, funcional e estratégico, para assegurar a integridade, confidencialidade e disponibilidade dos DP, e proteger contra riscos como acesso não autorizado, destruição, uso, modificação ou divulgação não autorizados por todo o seu ciclo de vida;

— escolher operadores de DP que apresentem garantias suficientes da aplicação de controles organizacionais, físicos e técnicos no tratamento de dados e que assegurem *compliance* com esses controles;

— basear estes controles em requisitos legais aplicáveis, normas de segurança, resultados de análises de riscos sistemáticas, como descrito na ABNT NBR ISO 31000, e resultados de análises de custo/benefício;

— implementar os controles proporcionalmente à probabilidade e severidade das possíveis consequências, à sensitividade dos DP, ao número de titulares de DP que podem ser afetados e ao contexto em que isto se insere;

— limitar o acesso aos DP apenas àqueles que necessitam deles para o cumprimento de suas obrigações e às necessidades de acesso para a execução das funções que desempenham;

— solucionar os riscos e vulnerabilidades que são descobertos pelos processos de auditoria e pelas avaliações de riscos de privacidade; e

— submeter os controles a análises críticas periódicas e novas análises em um processo contínuo de gestão de riscos.

## 5.12 *Compliance* com a privacidade

Aderir ao princípio de *compliance* com a privacidade significa:

— verificar e demonstrar que o tratamento atende aos requisitos de proteção de dados e de garantia da privacidade por meio de auditorias periódicas com auditores internos ou terceiros credenciados para esta atividade;

— ter controles internos apropriados e mecanismos de supervisão independentes implementados que assegurem *compliance* com a legislação relevante sobre privacidade e com os procedimentos e políticas de segurança, proteção de dados e privacidade; e

— desenvolver e manter análises de riscos de privacidade, de forma a avaliar se os programas e as iniciativas de entrega de serviços, que envolvem o tratamento de DP, estão em *compliance* com os requisitos de proteção de dados e requisitos de privacidade.

A legislação aplicável pode determinar que uma ou mais autoridades supervisoras sejam responsáveis pelo monitoramento do *compliance* com as leis de proteção de dados aplicáveis. Nestes casos, aderir ao princípio de *compliance* com a privacidade também significa cooperar com estas autoridades supervisoras e observar suas diretrizes e requisições.

# Anexo A
(informativo)

# Correspondência entre os conceitos da ABNT NBR ISO/IEC 29100 e os conceitos da ISO/IEC 27000

Para facilitar a utilização da família de normas ISO/IEC 27000 no contexto específico de privacidade e para integrar conceitos de privacidade no contexto da ISO/IEC 27000, a Tabela A.1 apresenta as relações entre os seus principais conceitos.

**Tabela A.1 – Correspondência entre os conceitos da ABNT NBR ISO/IEC 29100 e os conceitos da ISO/IEC 27000**

| Conceitos da ABNT NBR ISO/IEC 29100 | Correspondência com os conceitos da ISO/IEC 27000 |
|---|---|
| Parte interessada pela privacidade | Parte interessada |
| DP (dados pessoais) | Ativo de informação |
| Violação de privacidade | Incidente de segurança da informação |
| Controle de privacidade | Controle |
| Risco de privacidade | Risco |
| Gestão de riscos de privacidade | Gestão de riscos |
| Requisitos de proteção de privacidade | Objetivos de controle |

# Anexo NA
(informativo)

## Esclarecimentos sobre as opções de tradução

A privacidade das informações pessoais no Brasil é regulamentada pela Lei 13.709/2018 (Lei Geral de Proteção de Dados Pessoais – LGPD).

Para a tradução dos termos técnicos de privacidade desta Norma, de forma a facilitar o seu entendimento e aplicação por organizações que tratam informações no País ou que estão sujeitas à jurisdição da lei brasileira, foram utilizados termos equivalentes apresentados na referida lei, ao invés da tradução literal.

Desta forma, PII (*personally identifiable information*) é traduzido como DP (Dados Pessoais); *PII processor* como operador de DP; *PII principal* como titular de DP, *PII processing* como tratamento de DP, e assim por diante, como indicado nas respectivas Notas Brasileiras.

O verbo "tratar" foi utilizado para traduzir "*process*", quando este verbo foi empregado em sentido diretamente relacionado ao tratamento de DP.

Por outro lado, as palavras "*data*" e "*information*", isoladas dos termos técnicos de privacidade, foram traduzidas literalmente, de modo a preservar a distinção entre estes dois termos apresentada nas Normas Brasileiras.

Termos em inglês de uso corrente no Brasil, como "*opt-in*", "*opt-out*", "*privacy by design*" e "*compliance*", foram mantidos na forma original.

Nesta Norma, foram incorporadas as alterações estabelecidas na ISO/IEC 29100, AMD 1: Clarifications (06-2018), que, entre outros, excluiu as seguintes definições:

**2.6**
**identificar**
estabelecer o vínculo entre um titular de dados pessoais (DP) e os DP ou um conjunto de DP

**2.7**
**identidade**
conjunto de atributos que tornam possível identificar um titular de dados pessoais

# Bibliografia

[1] ABNT ISO Guia 73, *Gestão de riscos - Vocabulário*

[2] ABNT NBR ISO 31000, *Gestão de riscos - Princípios e diretrizes*

[3] ISO/IEC JTC 1/SC 27 WG 5 Standing Document 2 (WG 5 SD 2) - Official Privacy Documents References, disponível em *http://www.jtc1sc27.din.de*