Guia Orientativo sobre a

PRIVACIDADE E A PROTEÇÃO DE DADOS PESSOAIS

para a Administração Pública do Município de São Paulo

CIDADE DE SÃO PAULO
CONTROLADORIA GERAL DO MUNICÍPIO

CIDADE DE SÃO PAULO
CONTROLADORIA GERAL DO MUNICÍPIO

Guia Orientativo sobre a

PRIVACIDADE E A PROTEÇÃO DE DADOS PESSOAIS

para a Administração Pública do Município de São Paulo

Kelvin Peroli
Luís Felipe Giacomello
Marcus Vinicius Serricchio Fontan

São Paulo,
Janeiro de 2023

Prefeitura do Município de São Paulo

Prefeito

Ricardo Nunes

Controladoria Geral do Município

Controlador Geral do Município

Encarregado pela Proteção de Dados Pessoais da Prefeitura do Município

Daniel Falcão

Chefe de Gabinete

Thalita Abdala Aris

Coordenadoria de Promoção da Integridade

Coordenador da Coordenadoria de Promoção da Integridade

José Maurício Linhares Barreto Neto

Autores

Kelvin Peroli

Luís Felipe Giacomello

Marcus Vinicius Serricchio Fontan

Diagramação

Marília Miquelin de Oliveira

Versão 1

Janeiro de 2023

Este Guia Orientativo foi elaborado em cumprimento aos termos do Decreto Municipal nº 59.767, de 15 de setembro de 2020, que regulamenta a aplicação da Lei Federal nº 13.709, de 14 de agosto de 2018, no âmbito do Poder Executivo do Município de São Paulo.

Controlador Geral do Município

Encarregado pela Proteção de Dados Pessoais da Prefeitura do Município

Daniel Falcão

Lista de Abreviaturas e Siglas

ABNT – Associação Brasileira de Normas Técnicas

ADI – Ação Direta de Inconstitucionalidade

ADPF – Arguição de Descumprimento de Preceito Fundamental

AMLURB – Autoridade Municipal de Limpeza Urbana do Município de São Paulo

ANPD – Autoridade Nacional de Proteção de Dados

ANS – Acordo de Nível de Serviço

BYOD – "*Bring Your Own Device*" (traga o seu próprio dispositivo)

CET – Companhia de Engenharia de Tráfego do Município de São Paulo

CFCI – Centro de Formação de Controle Interno da Controladoria Geral do Município de São Paulo

CGM/SP – Controladoria Geral do Município de São Paulo

COHAB/SP – Companhia Metropolitana de Habitação de São Paulo

CRFB/88 – Constituição da República Federativa do Brasil

ECA – Estatuto da Criança e do Adolescente

EUA – Estados Unidos da América

HD – "*Hard Disk*" (disco rígido)

HSPM – Hospital do Servidor Público Municipal de São Paulo

HTTPS – "*Hyper Text Transfer Protocol Secure*" (Protocolo de Transferência de Hipertexto Seguro)

FTMSP – Fundação Theatro Municipal de São Paulo

IEC – *"International Electrotechnical Commission*" (Comissão Internacional de Eletrotécnica)

IN – Instrução Normativa

IPREM – Instituto de Previdência Municipal de São Paulo

ISO – "*International Organization for Standardization*" (Organização Internacional de Normatização)

LAI – Lei de Acesso à Informação

LGPD – Lei Geral de Proteção de Dados Pessoais

MCI – Marco Civil da Internet

NBR – Norma Brasileira

PMSP – Prefeitura do Município de São Paulo

PRODAM – Empresa de Tecnologia da Informação e Comunicação do Município de São Paulo

PSI – Política de Segurança da Informação

RGPD – Regulamento Geral de Proteção de Dados da União Europeia

RIPD – Relatório de Impacto à Proteção de Dados

RJET – Regime Jurídico Emergencial e Transitório das relações jurídicas de Direito Privado

SFMSP – Serviço Funerário do Município de São Paulo

SGSI – Sistema de Gestão de Segurança da Informação

SLA – "*Service Level Agreement*" (Acordo de Nível de Serviço)

SMIT – Secretaria Municipal de Inovação e Tecnologia do Município de São Paulo

SP – Município de São Paulo

SP Negócios – São Paulo Negócios

SP Parcerias – São Paulo Parcerias

SP Regula – Agência Reguladora de Serviços Públicos do Município de São Paulo

SPCine – Empresa de Cinema e Audiovisual de São Paulo

SPDA – Companhia São Paulo de Desenvolvimento e Mobilização de Ativos

SPOBRAS – São Paulo Obras

SPSEC – Companhia Paulistana de Securitização

SPTrans – São Paulo Transporte

SPTuris – São Paulo Turismo

SPUrbanismo – São Paulo Urbanismo

STF – Supremo Tribunal Federal

TCE/SP – Tribunal de Contas do Estado de São Paulo

TLS – "*Transport Layer Security*" (Segurança da Camada de Transporte)

UE – União Europeia

Lista de Tabelas

Sumário

Apresentação

O trato com os direitos à privacidade e à proteção de dados pessoais está presente, no dia a dia, de todos os agentes públicos. Esses direitos fazem parte do convívio em sociedade e podem ser contextualizados em cada uma das situações do quotidiano que envolvam relações sociais.

Fundamental o início deste Guia Orientativo com a seguinte questão:

"Eu, agente público, trato dados pessoais?" Um bom dia aos colegas de trabalho, um *e-mail* enviado ou respondido, ou mesmo qualquer tipo de contato já indica a assertiva de que, em qualquer contexto de relações sociais, existe o tratamento de dados pessoais e a expectativa, de cada um, da não-interferência ou, se necessário, da mínima interferência, pelo outro, em sua privacidade e em seus dados pessoais.

Uma outra questão, a este ponto:

"Devo me preocupar?" A resposta, sem dúvidas, é que sim – o que significa que a sua conduta, permeada pelos valores da ética, deve incluir o respeito (a conduta de não-interferência ou, se necessário, de mínima interferência) e a promoção (a conduta proativa de incentivo) da proteção de dados pessoais e da privacidade.

Certo! Mas...

"Por que tanta importância a esses direitos?" Vivemos, hoje, em uma sociedade baseada em dados. Quanto mais e quão mais exatos os dados relacionados à sua pessoa estão nas mãos de outros, mais conhecimento e controle terão sobre você. Se isso não lhe parece, à primeira vista, muito impactante, tenha em mente que a evolução tecnológica já permite, inclusive, o tratamento de dados neurais – ou seja, de atividades cerebrais, de modo a já ser possível, por exemplo, a interpretação de pensamentos, memórias e sentimentos.

Quanto mais dados pessoais, mais cada um de nós se torna um livro aberto. A chave desse livro cabe, é claro, ao respeito e à promoção da proteção à privacidade e aos dados pessoais.

A fim de esclarecer a você, servidor, o que é, então, a privacidade e o que é a proteção de dados pessoais, assim como lhe informar como deve conduzir, em sua atuação, o respeito e a promoção desses direitos, a Controladoria Geral do Município de São Paulo (CGM/SP) elaborou este "*Guia Orientativo sobre a Privacidade e a Proteção de Dados Pessoais para a Administração Pública do Município de São Paulo*".

Para tanto, serão apresentados os conceitos elementares relacionados ao tema – segurança da informação, privacidade, proteção de dados pessoais e gestão de riscos à segurança da informação, à privacidade e à proteção de dados pessoais.

Capítulo 1

Privacidade e Proteção de Dados Pessoais

Capítulo I – Privacidade e Proteção de Dados Pessoais

1. O que é a privacidade e a proteção de dados pessoais?

A privacidade e a proteção de dados pessoais são ideias e conceitos distintos, mas convergentes. A ideia de privacidade existe há muito e foi construída ao decorrer da evolução da sociedade. Refere-se à ideia detida por cada indivíduo sobre os atributos entendidos como pertencentes à sua vida privada, que perdura indeterminadamente no tempo e desenvolve-se em espaços jamais pré-definidos.

Modernamente, no entanto, a sua construção conceitual se inicia, historicamente, no final do século XIX, em 1890, com a publicação, nos EUA, do artigo *"O Direito à Privacidade"* (*"The Right to Privacy"*), de Louis Brandeis e Samuel Warren[1].

A discussão sobre a sua definição evoluiu no decorrer do século XX, especialmente diante da crescente importância do tema frente à evolução das tecnologias, que se introduziram em quase todos os aspectos da vida e das atividades humanas – o que potencializou, em consequência, a redução da privacidade.

"Mas o que é a privacidade?"

A *privacidade* pode ser entendida como a expectativa de uma pessoa, em determinado contexto[2] (seja em sua casa, seja no transporte público), de ter respeitada, pelo outro, a sua *vida privada* (de uma conduta alheia pautada na não-interferência sobre a sua própria vida privada, ou, se necessária, de uma conduta alheia pautada na mínima interferência sobre a sua própria vida privada) e de poder exercê-la, ativamente, de forma autodeterminada (de uma conduta própria pautada no autocontrole e na autodeterminação).

"E o direito à privacidade?"

A fim de que essas expectativas possam ser protegidas e promovidas em sociedade, o Direito deve ter o condão de, efetivamente, protegê-las e de promovê-las. Por essa razão é que há, no mundo

[1] WARREN, Samuel; BRANDEIS, Louis. The Right to Privacy. *Harvard Law Review*, v. IV, n. 05, dez. 1890. Disponível em: <http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html>. Acesso em: 04 out. 2022.

[2] NISSENBAUM, Helen. *Privacy in Context*. Technology, Policy, and the Integrity of Social Life. Stanford, EUA: Stanford University Press, 2010.

de hoje, o *direito à privacidade*, que objetiva a proteção e a promoção das razoáveis expectativas dos indivíduos sobre a sua vida privada.

Privacidade e *vida privada* enquadram-se, nesse retrato, como aspectos da mesma expectativa[3]: a *privacidade* pode ser vista como um atributo da *vida*, que a torna, então, *privada*. Esse atributo, por fim, apenas pode ser preenchido por cada um de nós, contextualmente, em nossa própria vivência[4].

A essa altura, *vivendo* esta leitura, pode você se perguntar: *"Onde estão os dados pessoais?"*

"E os dados pessoais?"

É justamente a depender da vivência (do viver a vida) que os dados pessoais são gerados, tratados e eliminados. Não à toa, muito se fala em ciclo de vida de tratamento de dados pessoais: os dados pessoais são tratados a depender do contexto da vida de um indivíduo ao qual um outro requer acesso.

Nesse sentido, todo contexto da *vida privada* ou da *vida pública* do indivíduo é capaz de gerar dados pessoais. Um *dado pessoal*, por esse raciocínio, é um dado relativo a um indivíduo, seja este relativo à sua vida privada ou não, apto a torná-lo identificável aos olhos da sociedade.

O *direito à proteção de dados pessoais*, nesse sentido, não pode ser confundido com o *direito à privacidade*, porque a este, tão somente, não se resume, tendo-se em vista que a vivência de cada um de nós está atrelada a contextos nos quais temos ou não expectativa de privacidade.

Explicamo-nos: no metrô, você possui expectativa de privacidade? Possui a expectativa de manter privados os pertences de sua bolsa? Certamente, seria uma quebra de expectativa de privacidade se alguém, sem avisá-lo, abrisse a sua bolsa no intuito de conhecê-los. Mas, ainda no metrô, você possui a expectativa de manter privado o seu rosto? A cor de sua íris? Dificilmente haveria uma quebra de expectativa do gênero, em um contexto tão público como este.

É justamente na diferença entre esses contextos que está a existência ou inexistência da *privacidade*. Os *dados pessoais*, no entanto, permanecem em todos eles.

Apesar de objetivamente ser possível delinear essas diferenças, na prática, o Direito não tem a capacidade de captar qual é a expectativa de cada um de nós sobre o que entendemos como de nossa vida privada ou de nossa vida pública, em cada um dos contextos de nossas vidas. Além disso, muitas das vezes, a expectativa de privacidade de um indivíduo interfere na expectativa de

[3] FALCÃO, Daniel; PEROLI, Kelvin. As novas abordagens da privacidade: contextos, tipos e dimensões. *Migalhas de Proteção de Dados*, 30 dez. 2021. Disponível em: <https://www.migalhas.com.br/coluna/migalhas-de-protecao-de-dados/357252/as-novas-abordagens-da-privacidade-contextos-tipos-e-dimensoes>. Acesso em: 04 out. 2022.

[4] É nesse contexto que temos, por exemplo, a *intimidade*.

privacidade de outro. Disto origina-se a necessidade de um *direito à privacidade* que não seja apenas dependente da expectativa dos próprios indivíduos.

Por essas razões, essas expectativas, no melhor dos mundos, devem ser vistas à luz do princípio da razoabilidade, isto a fim de que o Direito proteja as razoáveis expectativas de privacidade dos indivíduos nos distintos contextos nos quais os próprios vivem as suas vidas.

"E o direito à proteção de dados pessoais?"

Apesar de não se confundir com o direito à privacidade, o direito à proteção de dados pessoais requer a sua observância conjunta.

Novamente, explicamo-nos: apesar de ser razoável o entendimento de que não há expectativa de privacidade, no contexto específico do metrô, sobre o seu rosto e sobre a cor de sua íris, a verdade é que a captura desses dados pessoais, neste contexto, sem uma necessidade específica e uma finalidade específica, poderá torná-los públicos em outros contextos nos quais entende-se ser razoável a sua expectativa de privacidade – ou seja, a expectativa em manter, em determinados outros contextos, privados o seu rosto e a cor de sua íris.

É por essa razão que os mesmos vetores aplicados à expectativa de privacidade podem ser aplicados à expectativa pela *proteção de dados pessoais*.

Traduzindo-se esse argumento ao *direito à proteção de dados pessoais*, pode se dizer que esse direito objetiva a proteção e a promoção das razoáveis expectativas dos indivíduos sobre a proteção de seus dados pessoais. Nesse sentido, a conduta alheia deve ser pautada pela não-interferência sobre os seus dados pessoais, ou, se necessário, de uma conduta alheia pautada pela mínima interferência sobre os seus dados pessoais. Além disso, deve-se ser promovida de modo a poder o indivíduo, titular de dados pessoais, razoavelmente exercer a sua expectativa de forma autodeterminada (uma conduta própria pautada no autocontrole e na autodeterminação).

Como bem pontuou o art. 1º da Lei Geral de Proteção de Dados Pessoais – LGPD (Lei Federal nº 13.708/2018, com redação dada pela Lei Federal nº 13.853/2019), a proteção de dados pessoais objetiva proteger os direitos fundamentais de privacidade e de liberdade da pessoa natural, além do livre desenvolvimento de sua personalidade.

2. Fundamentos da privacidade e da proteção de dados pessoais no Brasil

No Brasil, o direito fundamental à privacidade é extraído da previsão dos direitos fundamentais à vida privada e à intimidade, previstos no artigo 5º, inciso X, da Constituição Federal (CRFB/88).

A partir de 10 de fevereiro de 2022, com a promulgação da Emenda Constitucional nº 115/2022, de forma inequívoca, o Brasil também passou a deter a previsão do direito fundamental à proteção de dados pessoais, disposto no artigo 5º, inciso LXXIX, da CRFB/88.

De modo infraconstitucional, o direito à privacidade é protegido pelo Código Civil (Lei Federal nº 10.406/2002), especialmente por seu artigo 21, que afirma: *"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."*

O direito à proteção de dados pessoais, por sua vez, está garantido, sobretudo, pela Lei Geral de Proteção de Dados – LGPD (Lei Federal nº 13.708/2018, com redação dada pela Lei Federal nº 13.853/2019). No âmbito do Poder Executivo do Município de São Paulo, foi editado o Decreto Municipal nº 59.767/2020, que regulamenta a aplicação da LGPD[5].

Outros atos normativos, no entanto, também devem ser observados e interpretados harmonicamente quando da aplicação, na prática, das normas citadas, como a Lei do *Habeas Data* (Lei Federal nº 9.784/1997) e a Lei de Acesso à Informação – LAI (Lei Federal nº 12.527/2011), desafio que será trazido adiante, neste Guia.

3. Conceitos elementares e princípios da proteção de dados pessoais

Os conceitos e os princípios da proteção de dados pessoais estão elencados, sobretudo, pela LGPD. Em seu art. 5º, traz as suas definições para inúmeras palavras-chave sobre o tema, como "*dado pessoal*", "*dado pessoal sensível*", "*dado anonimizado*", "*anonimização*", "*titular*", "*controlador*", "*operador*", "*agentes de tratamento*", "*encarregado*" e "*tratamento*".

Nesse sentido, define "*dado pessoal*" como sendo uma "*informação relacionada a pessoa natural identificada ou identificável*" e "*dado pessoal sensível*" como "*dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural*" (art. 5º, incs. I e II, LGPD).

A interpretação desses dois conceitos traz importantes considerações: a proteção dada pela LGPD se restringe aos dados pessoais de pessoas naturais – não incluindo, portanto, dados pessoais de pessoas jurídicas. Mas isso não é óbvio? Não! Em muitos outros países, como os vizinhos Argentina e Uruguai, a proteção é estendida, igualmente, aos dados pessoais de pessoas jurídicas.

[5] FALCÃO, Daniel; PEROLI, Kelvin. São Paulo, 22 de julho de 2022: as novas abordagens da proteção de dados pessoais no âmbito da Administração Pública Municipal. *Migalhas de Proteção de Dados Pessoais*, 22 jul. 2022. Disponível em: <https://www.migalhas.com.br/coluna/migalhas-de-protecao-de-dados/370310/protecao-de-dados-pessoais-na-administracao-publica-municipal>. Acesso em: 04 out. 2022.

Isso significa que a LGPD protege os dados pessoais de todas as pessoas naturais? Juridicamente, a existência da pessoa natural termina com a sua morte (art. 6º, Código Civil), motivo pelo qual, ao tratar de "*pessoal natural*", a LGPD restringiu-se a proteger os dados pessoais de pessoas vivas. Estas são, então, o que designa o seu art. 5º, inc. V, como "*titular*": *"pessoa natural a quem se referem os dados pessoais que são objeto de tratamento"*.

A Lei, como se interpreta, protege os dados pessoais e os dados pessoais sensíveis. *"Dado pessoal sensível"* é uma categoria de *"dado pessoal"* que a Lei tutela de modo diferenciado, isto em razão da importância dada, socialmente, aos seus tipos (*"origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico"*).

"Dado anonimizado", por sua vez, é o dado resultante de um processo de anonimização de um *"dado pessoal"* ou de um *"dado pessoal sensível"*. A "*anonimização*", nesse sentido, é a *"utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo"* (art. 5º, inc. XI, LGPD).

E quem são aqueles que tratam dados pessoais? Os "*agentes de tratamento*". Um *"agente de tratamento"*, como entende a própria LGPD, pode ser classificado entre "*controlador*" e "*operador*". Um "*controlador*", nesse sentido, é uma "*pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais*" (art. 5º, inc. VI). Um "*operador*", por outro lado, é uma "*pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador*" (art. 5º, inc. VII).

Por fim, temos, também, o "*encarregado*", que é a *"pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD)"* (art. 5ª, inc. VIII).

Mas o que é, afinal, um "*tratamento*" de dados pessoais? É qualquer ação, orientada por um objetivo, que se utilize de dados pessoais. O art. 5º, inc. X, da LGPD, elenca, exemplificativamente, as ações relativas à *"coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração"* de dados pessoais.

Além de explicar-se por suas definições de conceitos elementares, a LGPD também se fundamenta nas definições de seus princípios, elencados por seu art. 6º, que são valores que devem ser observados em toda e qualquer atividade de tratamento de dados pessoais. Nesse sentido, dispõe de onze princípios:

(i) da boa-fé;

(ii) da finalidade, que é a realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;

(iii) da adequação, que é a compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;

(iv) da necessidade, que é a limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com a abrangência de dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;

(v) do livre acesso, ou seja, da garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;

(vi) da qualidade dos dados, que é a garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;

(vii) da transparência, que é garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;

(viii) da segurança, que é a utilização de medidas 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 difusão;

(ix) da prevenção, ou seja, da adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;

(x) da não discriminação, que é a impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos; e

(xi) da responsabilização e prestação de contas, ou seja, a demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

4. Agentes de Tratamento de Dados Pessoais e o Encarregado pela Proteção de Dados Pessoais

Como mencionado, os agentes de tratamento podem ser classificados do seguinte modo:

(i) controlador, que é a pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais; e

(ii) operador, que é a pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.

No tratamento de dados pessoais, nem sempre existem a figura de um operador. Entretanto, necessariamente, haverá a figura de um controlador, que pode, nesse sentido, tomar decisões e realizar, ele próprio, o tratamento de dados pessoais.

No âmbito do Poder Público, a Autoridade Nacional de Proteção de Dados (ANPD), órgão da Administração Pública Federal responsável por zelar, implementar e fiscalizar o cumprimento da LGPD[6], possui o entendimento de que são "*controladores*" os entes federativos (União, Estados,

[6] As atribuições da Autoridade Nacional de Proteção de Dados (ANPD) estão dispostas pelo art. 55-J da LGPD, a saber:
"Art. 55-J. Compete à ANPD:
I - zelar pela proteção dos dados pessoais, nos termos da legislação;
II - zelar pela observância dos segredos comercial e industrial, observada a proteção de dados pessoais e do sigilo das informações quando protegido por lei ou quando a quebra do sigilo violar os fundamentos do art. 2º desta Lei;
III - elaborar diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade;
IV - 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;
V - apreciar petições de titular contra controlador após comprovada pelo titular a apresentação de reclamação ao controlador não solucionada no prazo estabelecido em regulamentação;
VI - promover na população o conhecimento das normas e das políticas públicas sobre proteção de dados pessoais e das medidas de segurança;
VII - promover e elaborar estudos sobre as práticas nacionais e internacionais de proteção de dados pessoais e privacidade;
VIII - estimular a adoção de padrões para serviços e produtos que facilitem o exercício de controle dos titulares sobre seus dados pessoais, os quais deverão levar em consideração as especificidades das atividades e o porte dos responsáveis;
IX - promover ações de cooperação com autoridades de proteção de dados pessoais de outros países, de natureza internacional ou transnacional;
X - dispor sobre as formas de publicidade das operações de tratamento de dados pessoais, respeitados os segredos comercial e industrial;
XI - solicitar, a qualquer momento, às entidades do poder público que realizem operações de tratamento de dados pessoais informe específico sobre o âmbito, a natureza dos dados e os demais detalhes do tratamento realizado, com a possibilidade de emitir parecer técnico complementar para garantir o cumprimento desta Lei;
XII - elaborar relatórios de gestão anuais acerca de suas atividades;
XIII - editar regulamentos e procedimentos sobre proteção de dados pessoais e privacidade, bem como sobre relatórios de impacto à proteção de dados pessoais para os casos em que o tratamento representar alto risco à garantia dos princípios gerais de proteção de dados pessoais previstos nesta Lei;
XIV - ouvir os agentes de tratamento e a sociedade em matérias de interesse relevante e prestar contas sobre suas atividades e planejamento;
XV - arrecadar e aplicar suas receitas e publicar, no relatório de gestão a que se refere o inciso XII do caput deste artigo, o detalhamento de suas receitas e despesas;
XVI - realizar auditorias, ou determinar sua realização, no âmbito da atividade de fiscalização de que trata o inciso IV e com a devida observância do disposto no inciso II do caput deste artigo, sobre o tratamento de dados pessoais efetuado pelos agentes de tratamento, incluído o poder público;
XVII - celebrar, a qualquer momento, compromisso com agentes de tratamento para eliminar irregularidade, incerteza jurídica ou situação contenciosa no âmbito de processos administrativos, de acordo com o previsto no Decreto-Lei nº 4.657, de 4 de setembro de 1942;
XVIII - editar normas, orientações e procedimentos simplificados e diferenciados, inclusive quanto aos prazos, para que microempresas e empresas de pequeno porte, bem como iniciativas empresariais de caráter incremental ou disruptivo que se autodeclarem *startups* ou empresas de inovação, possam adequar-se a esta Lei;

Distrito Federal e Municípios), em seus diferentes Poderes (Executivo, Legislativo e Judiciário), enquanto pessoas jurídicas de direito público.

Os órgãos públicos, integrantes desses entes federativos, em razão da desconcentração administrativa, exercem atribuições específicas em nome daqueles. Por essa razão, a ANPD também entende que, apesar de possuírem atribuições específicas de um "controlador", esses órgãos as exercem em nome dos entes dos quais são integrantes.

Tratando-se especificamente dos Poderes Executivos da União, dos Estados, do Distrito Federal e dos Municípios, entende-se que suas entidades podem ou não ser caracterizadas como "*controladoras*" a depender da natureza de sua relação com o respectivo ente.

Nesse sentido, entidades que exercem as suas atribuições em regime de direito público não são vistas como "*controladoras*", em razão de as exercerem em nome do ente ao qual são integrantes. São exemplos as autarquias e também as fundações e as empresas estatais que atuam em regime de direito público.

Por outro lado, podem ser consideradas "*controladoras*" as entidades que exercem as suas atribuições em regime de concorrência, como fundações e empresas estatais. Excetuam-se do regime de "*controladoras*", no entanto, quando, por vezes, operacionalizam políticas públicas executadas pelos entes – hipótese em que são consideradas, justamente, como "*operadoras*".

Um "*operador*", por outro lado, é uma *"pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador"* (art. 5º, inc. VII).

Trazendo essas diferentes hipóteses à Cidade de São Paulo, o *"Poder Executivo do Município de São Paulo"* pode ser entendido como "*controlador*". Esse termo, no entanto, necessita ser interpretado no sentido de abarcar toda a Administração Pública direta e também uma parcela da Administração Pública indireta – justamente aquela que atua em regime de direito público, como suas autarquias

XIX - garantir que o tratamento de dados de idosos seja efetuado de maneira simples, clara, acessível e adequada ao seu entendimento, nos termos desta Lei e da Lei nº 10.741, de 1º de outubro de 2003 (Estatuto do Idoso);
XX - deliberar, na esfera administrativa, em caráter terminativo, sobre a interpretação desta Lei, as suas competências e os casos omissos;
XXI - comunicar às autoridades competentes as infrações penais das quais tiver conhecimento;
XXII - comunicar aos órgãos de controle interno o descumprimento do disposto nesta Lei por órgãos e entidades da administração pública federal;
XXIII - articular-se com as autoridades reguladoras públicas para exercer suas competências em setores específicos de atividades econômicas e governamentais sujeitas à regulação; e
XXIV - implementar mecanismos simplificados, inclusive por meio eletrônico, para o registro de reclamações sobre o tratamento de dados pessoais em desconformidade com esta Lei."

(AMLURB[7], HSPM[8], IPREM[9], SFMSP[10] e SP Regula[11]) e fundações (TMSP[12] e Fundação Paulistana de Educação, Tecnologia e Cultura). Suas empresas estatais (CET[13], COHAB/SP[14], PRODAM[15], SP Negócios[16], SP Parcerias[17], SPCine[18], SPDA[19], SPOBRAS[20], SPSEC[21], SPTrans[22], SPTuris[23] e SPUrbanismo[24]), a princípio, podem ser entendidas, cada uma, como "*controladoras*", isto por atuarem em regime de direito privado. No entanto, por vezes, ao operacionalizarem políticas públicas executadas pelo Poder Executivo do Município, contextualmente podem ser entendidas como "*operadoras*" – tendo em vista atuarem, nesses casos, em nome do Poder Executivo do Município de São Paulo.

Seguindo-se orientação da ANPD, os agentes públicos, atuantes em caráter subordinado ao Poder Público, não são considerados nem "*controladores*" nem "*operadores*". Isto importa a fim de esclarecer que não possuem as obrigações e as responsabilidades atribuídas a esses "*agentes de tratamento*" ("*controlador*" e "*operador*").

No entanto, não caracterizar os agentes públicos como "*agentes de tratamento*" não significa isentá-los de quaisquer obrigações e responsabilidades perante as atividades de tratamento de dados pessoais. Na Cidade de São Paulo, por exemplo, permanecem valendo as obrigações instituídas pelo Estatuto do Servidor Público (Lei Municipal nº 8.989/1979)[25], assim como a

[7] Autoridade Municipal de Limpeza Urbana.
[8] Hospital do Servidor Público Municipal.
[9] Instituto de Previdência Municipal de São Paulo.
[10] Serviço Funerário do Município de São Paulo.
[11] Agência Reguladora de Serviços Públicos.
[12] Fundação Theatro Municipal de São Paulo.
[13] Companhia de Engenharia de Tráfego.
[14] Companhia Metropolitana de Habitação de São Paulo.
[15] Empresa de Tecnologia da Informação e Comunicação do Município de São Paulo.
[16] São Paulo Negócios.
[17] São Paulo Parcerias.
[18] Empresa de Cinema e Audiovisual de São Paulo.
[19] Companhia São Paulo de Desenvolvimento e Mobilização de Ativos.
[20] São Paulo Obras.
[21] Companhia Paulistana de Securitização.
[22] São Paulo Transporte.
[23] São Paulo Turismo.
[24] São Paulo Urbanismo.
[25] Conforme os arts. 180, 181, e 182 do Estatuto do Servidor Público do Município de São Paulo: "Art. 180 - O funcionário responde civil, penal e administrativamente pelo exercício irregular de suas atribuições, sendo responsável por todos os prejuízos que, nesta qualidade, causar à Fazenda Municipal, por dolo ou culpa, devidamente apurados.
Parágrafo único. Caracteriza-se especialmente a responsabilidade:
I - pela sonegação de valores ou objetos confiados à sua guarda ou responsabilidade;
II - por não prestar contas ou por não as tomar, na forma e nos prazos estabelecidos em leis, regulamentos, regimentos, instruções e ordens de serviço;
III - pelas faltas, danos, avarias, e quaisquer outros prejuízos que sofrerem os bens e os materiais sob sua guarda ou sujeitos a seu exame e fiscalização;
IV - pela falta ou inexatidão das necessárias averbações nas notas de despacho, guias e outros documentos da receita ou que tenham com eles relação;

responsabilização administrativa em decorrência de ato contrário às suas disposições. Nesse mesmo contexto, recentemente, o Supremo Tribunal Federal assentou o entendimento de que o descumprimento das disposições da LGPD é apto a gerar responsabilização civil aos agentes públicos por improbidade administrativa[26].

Trazidas as figuras dos "*agentes de tratamento de dados pessoais*", resta a menção ao sujeito que articula as relações entre os titulares de dados pessoais, esses agentes de tratamento e a Autoridade Nacional de Proteção de Dados (ANPD): o "*encarregado*".

Como já mencionado, o "*encarregado*" é a "*pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD)*" (art. 5ª, inc. VIII, LGPD). Como se percebe da redação da Lei, o "*encarregado*" pode ser uma pessoa natural ou jurídica. Conforme estabelece o art. 41, § 2º, da LGPD, são suas atribuições:

(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.

A LGPD também traz, por seu art. 41, § 1º, a obrigação de que a identidade e as informações de contato do "*encarregado*" devem ser divulgadas publicamente, de forma clara e objetiva, preferencialmente nos endereços eletrônicos do "*controlador*".

Na Cidade de São Paulo, o Decreto Municipal nº 59.767/2020, que regulamenta a LGPD no âmbito do Poder Executivo do Município, instituiu o Controlador Geral do Município como

---

V - por qualquer erro de cálculo ou redução contra a Fazenda Municipal.
Art. 181 - Nos casos de indenização à Fazenda Municipal, o funcionário será obrigado à repor, de uma só vez e com os acréscimos de lei e correção monetária, a importância do prejuízo causado em virtude de alcance, desfalque, remissão ou omissão em efetuar recolhimentos ou entradas nos prazos legais.
Art. 182 - Excetuados os casos previstos no artigo anterior, será admitido o pagamento parcelado, na forma do artigo 96.
Art. 183 - A responsabilidade administrativa não exime o funcionário da responsabilidade civil ou criminal que no caso couber, nem o pagamento da indenização a que ficar obrigado o exime da pena disciplinar em que incorrer." SÃO PAULO (Cidade). Lei Municipal nº 8.989, de 29 de outubro de 1979. Dispõe sobre o estatuto dos funcionários públicos do município de São Paulo, e dá providências correlatas. São Paulo, *Diário Oficial da Cidade de São Paulo*, 29 de outubro de 1979. Disponível em: < http://legislacao.prefeitura.sp.gov.br/leis/lei-8989-de-29-de-outubro-de-1979>. Acesso em: 04 out. 2022.

[26] BRASIL. Supremo Tribunal Federal. ADI nº 6.649/DF e ADPF nº 695/DF. Julgamento Conjunto. Data de Julgamento: 15 set. 2022. Data de Publicação: 15 set. 2022. Brasília, *Diário Oficial da Justiça Eletrônico*, 15 set. 2022.

Encarregado pela Proteção de Dados Pessoais da Prefeitura do Município[27]. Isso significa que este "*encarregado*" o é apenas da Administração Pública direta do Município – diante, portanto, de seus órgãos, como Secretarias e Subprefeituras. As entidades que formam a Administração Pública indireta, por outro lado, devem ter instituídos os seus próprios encarregados.

Nesse sentido, dispôs o art. 6º do Decreto Municipal nº 59.767/2020 das atribuições do Encarregado pela Proteção de Dados Pessoais da Prefeitura do Município, que são:

(i) aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;

(ii) receber comunicações da ANPD e adotar providências;

(iii) orientar os funcionários e os contratados da Administração Pública Municipal direta a respeito das práticas a serem tomadas em relação à proteção de dados pessoais;

(iv) editar diretrizes para a elaboração dos Planos de Adequação;

(v) determinar a órgãos da Administração Pública Municipal direta a realização de estudos técnicos para elaboração dessas diretrizes;

(vi) submeter à Comissão Municipal de Acesso à Informação (CMAI), sempre que julgar necessário, matérias atinentes ao Decreto Municipal;

(vii) decidir sobre as sugestões formuladas pela ANPD a respeito da adoção de padrões e de boas práticas para o tratamento de dados pessoais;

(viii) providenciar a publicação dos Relatórios de Impacto à Proteção de Dados Pessoais previstos pelo art. 32 da LGPD;

(ix) recomendar a elaboração de Planos de Adequação relativos à proteção de dados pessoais aos encarregados das entidades integrantes da Administração Pública Municipal indireta, informando eventual ausência ao responsável pelo controle da entidade, para as providências pertinentes;

(x) providenciar, em caso de recebimento de informe da ANPD com medidas cabíveis para fazer cessar uma afirmada violação à LGPD, o encaminhamento ao órgão, fixando prazo para atendimento à solicitação ou apresentação das justificativas pertinentes;

[27] "Art. 5º Fica designado o Controlador Geral do Município como o encarregado da proteção de dados pessoais, para os fins do art. 41 da Lei Federal nº 13.709, de 2018.
Parágrafo único. A identidade e as informações de contato do encarregado devem ser divulgadas publicamente, de forma clara e objetiva, no Portal da Transparência, em seção específica sobre tratamento de dados pessoais."
SÃO PAULO (Cidade). Decreto Municipal nº 59.767/2020. Regulamenta a aplicação da Lei Federal nº 13.709, de 14 de agosto de 2018 – Lei de Proteção de Dados Pessoais (LGPD) - no âmbito da Administração Municipal direta e indireta. São Paulo, *Diário Oficial da Cidade de São Paulo*, 15 de setembro de 2020. Disponível em: <https://legislacao.prefeitura.sp.gov.br/leis/decreto-59767-de-15-de-setembro-de-2020>. Acesso em: 04 out. 2022.

(xi) avaliar a justificativa apresentada pelo órgão com relação aos informes da ANPD com medidas cabíveis para fazer cessar uma afirmada violação à LGPD, a fim de que:

a. caso avalie ter havido a violação, determinar a adoção das medidas solicitadas pela ANPD;

b. caso avalie não ter havido a violação, apresentar as justificativas pertinentes à ANPD, segundo o procedimento cabível;

(xii) requisitar dos órgãos da Administração Pública Municipal direta as informações pertinentes, para a sua compilação em Relatório de Impacto à Proteção de Dados Pessoais único, caso solicitada pela ANPD a sua publicação, nos termos do art. 32 da LGPD; e

(xiii) executar as demais atribuições estabelecidas em normas complementares.

5. Direitos dos titulares de dados pessoais

Os direitos dos titulares de dados pessoais, ou seja, das pessoas naturais a quem os dados pessoais dizem respeito, estão dispostos ao longo da LGPD, mas são explicitados, sobretudo, pelos arts. 9º e 17 a 22 da Lei.

Em primeiro lugar, traz o art. 17, ao iniciar o Capítulo da Lei sobre os direitos do titular, a máxima de que *"toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade, nos termos desta Lei."* Assim sendo, os dados pessoais jamais são de titularidade de outras pessoas que não das próprias que digam respeito.

O art. 18 da Lei, em seguida, traz os direitos que podem ser exercidos pelos titulares mediante requisição ao "*controlador*", a qualquer momento:

(i) direito à confirmação sobre a existência de tratamento de dados, observadas as disposições do art. 19 da Lei;

(ii) direito de acesso aos dados, observadas as disposições do art. 19 da Lei;

(iii) direito de correção de dados incompletos, inexatos ou desatualizados;

(iv) direito à anonimização, bloqueio ou eliminação de dados tratados em desconformidade à Lei;

(v) direito à portabilidade dos dados a outro fornecedor de serviço ou produto, observados os segredos comercial e industrial e futura regulamentação da Autoridade Nacional de Proteção de Dados (ANPD);

(vi) direito à revogação do consentimento e eliminação de dados tratados com o seu consentimento, exceto nas hipóteses elencadas pelo art. 16, da LGPD, que autorizam a conservação dos dados pelo controlador;

(vii) direito à informação sobre a possibilidade da recusa de consentimento e sobre as consequências dessa negativa; e

(viii) direito à informação sobre eventual uso compartilhado de seus dados entre Poder Público e entidades privadas.

Estreitamente relacionado ao direito de acesso aos dados pessoais, está o direito de acesso às informações sobre o tratamento de dados pessoais, conforme elencado pelo art. 9º da LGPD. Essas informações devem ser disponibilizadas de forma clara, adequada e ostensiva ao titular de dados, contendo, ao menos:

(i) os seus direitos, com menção explícita àqueles contidos no referido art. 18 da Lei;

(ii) a finalidade específica do tratamento;

(iii) a forma e a duração do tratamento, observados os segredos comercial e industrial;

(iv) a identificação do controlador;

(v) as informações de contato do controlador;

(vi) as informações acerca do uso compartilhado de dados pelo controlador e a finalidade; e

(vii) as responsabilidades dos agentes de tratamento.

Vale ressaltar que o direito de acesso aos dados pessoais (art. 18, inc. II) e o direito de acesso às informações sobre o tratamento de dados pessoais (art. 9º) devem ser interpretados, sempre que possível, em favor do princípio do livre acesso – mencionado anteriormente.

6. Hipóteses de tratamento de dados pessoais e de dados pessoais sensíveis

Ao tratarmos sobre o tratamento de dados pessoais, muito se fala sobre o consentimento do titular ao tratamento de seus dados. Entretanto, o consentimento não é a regra a ser sempre seguida e sim apenas uma das diversas hipóteses legais que autorizam o tratamento de dados pessoais.

O Poder Público, nesse sentido, dificilmente se utiliza do consentimento dos titulares a fim de realizar as suas atividades de tratamento de dados pessoais. Em muitos dos casos, por exemplo, o tratamento é justificado diante da necessidade do cumprimento de obrigações legalmente pré-

estabelecidas e à realização de políticas públicas previstas em atos normativos ou respaldadas em contratos administrativos, convênios e instrumentos congêneres.

A LGPD diferencia as hipóteses em que é possível haver o tratamento de "*dados pessoais*" (art. 7º) e as hipóteses em que é possível haver o tratamento de "*dados pessoais sensíveis*" (art. 11). Essa diferenciação é importante a fim de restringir o tratamento de "*dados pessoais sensíveis*", que são atributos que, quando relacionados à pessoa natural, tornam-na sensivelmente mais identificada que na hipótese do tratamento apenas de "*dados pessoais*" .

Assim conforme o art. 7º, é autorizado o tratamento de "*dados pessoais*":

(i) mediante o fornecimento de consentimento pelo titular (art. 7º, inc. I);

(ii) para o cumprimento de obrigação legal ou regulatória pelo controlador (art. 7º, inc. II);

(iii) pela Administração Pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em atos normativos ou respaldadas em contratos, convênios ou instrumentos congêneres (art. 7º, inc. III);

(iv) para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais (art. 7º, inc. IV);

(v) quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do próprio (art. 7º, inc. V);

(vi) para o exercício regular de direitos em processos judicial, administrativo ou arbitral, esse último nos termos da Lei de Arbitragem (art. 7º, inc. VI);

(vii) para a proteção da vida ou da incolumidade física do titular ou de terceiro (art. 7º, inc. VII);

(viii) para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária (art. 7º, inc. VIII);

(ix) quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais (art. 7º, inc. IX); e

(x) para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente (art. 7º, inc. X).

O art. 11, por sua vez, traz as hipóteses em que é possível haver o tratamento de "*dados pessoais sensíveis*":

(i) mediante o fornecimento de consentimento pelo titular (art. 11, inc. I);

(ii) para o cumprimento de obrigação legal ou regulatória pelo controlador (art. 11, inc. II, alínea "a");

(iii) pela Administração Pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em atos normativos (art. 11, inc. II, alínea "b");

(iv) para a realização de estudos por órgãos de pesquisa, garantia, sempre que possível, a anonimização dos dados pessoais sensíveis (art. 11, inc. II, alínea "c");

(v) para o exercício regular de direitos em contratos e em processos judicial, administrativo ou arbitral, esse último nos termos da Lei de Arbitragem (art. 11, inc. II, alínea "d");

(vi) para a proteção da vida ou da incolumidade física do titular ou de terceiro (art. 11, inc. II, alínea "e");

(vii) para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária (art. 11, inc. II, alínea "f"); e

(viii) para a 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 sensíveis (art. 11, inc. II, alínea "g").

Como se pode perceber, muitas das hipóteses são comuns ao tratamento de "*dados pessoais*" e de "*dados pessoais sensíveis*". Nesse sentido, porém, destaca-se que:

(i) a hipótese de tratamento relativa ao consentimento do titular, apesar de ser comum a ambas as categorias de dados (art. 7º, inc. I, e art. 11, inc. II), quando da hipótese relativa aos "*dados pessoais sensíveis*", requer a sua coleta de forma específica e destacada, para finalidades específicas;

(ii) a hipótese relativa ao tratamento e uso compartilhado de dados pela Administração Pública, apesar de ser comum a ambas as categorias de dados (art. 7º, inc. III, e art. 11, inc. II, alínea "b"), é mais restritiva quando da hipótese relativa aos "*dados pessoais sensíveis*", porque pode ser utilizada à execução de políticas públicas previstas apenas em atos normativos (leis ou regulamentos), frente à sua utilização à execução de políticas públicas previstas em atos normativos (leis ou regulamentos) ou também respaldadas em contratos, convênios ou instrumentos congêneres, quando da hipótese referente aos "*dados pessoais*".

Outras hipóteses, no entanto, são exclusivas ao tratamento de "*dados pessoais*", quais sejam:

(i) a hipótese relativa ao tratamento quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e

liberdades fundamentais do titular que exijam a proteção dos dados pessoais (art. 7º, inc. IX); e

(ii) para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente (art. 7º, inc. X).

Por fim, destaca-se que também há hipótese exclusiva de tratamento de "*dados pessoais sensíveis*", que é a hipótese de tratamento de dados pessoais sensíveis para a 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 sensíveis (art. 11, inc. II, alínea "g").

Além das hipóteses de tratamento de dados pessoais e de dados pessoais sensíveis, a LGPD traz, em seu art. 14, requisitos legais que devem ser observados quando do tratamento de dados pessoais de crianças e adolescentes. Nesse sentido, o art. 14, *caput*, traz que o tratamento de dados pessoais de crianças e adolescentes *"deverá ser realizado em seu melhor interesse, nos termos deste artigo e da legislação pertinente."*

O art. 14, § 1º, por sua vez, dispõe que o tratamento de dados pessoais de crianças (que são aquelas com até doze anos de idade incompletos, conforme o art. 2º do Estatuto da Criança e do Adolescente – Lei Federal nº 8.069/1990) *"deverá ser realizado com o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal."*

Apesar de essa definição do § 1º e a dos parágrafos subsequentes[28] poder, à primeira vista, levar a compreensão de que o tratamento de dados pessoais de crianças deve ser realizado exclusivamente

[28] "Art. 14. O tratamento de dados pessoais de crianças e de adolescentes deverá ser realizado em seu melhor interesse, nos termos deste artigo e da legislação pertinente.
§ 1º O tratamento de dados pessoais de crianças deverá ser realizado com o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal.
§ 2º No tratamento de dados de que trata o § 1º deste artigo, os controladores deverão manter pública a informação sobre os tipos de dados coletados, a forma de sua utilização e os procedimentos para o exercício dos direitos a que se refere o art. 18 desta Lei.
§ 3º Poderão ser coletados dados pessoais de crianças sem o consentimento a que se refere o § 1º deste artigo quando a coleta for necessária para contatar os pais ou o responsável legal, utilizados uma única vez e sem armazenamento, ou para sua proteção, e em nenhum caso poderão ser repassados a terceiro sem o consentimento de que trata o § 1º deste artigo.
§ 4º Os controladores não deverão condicionar a participação dos titulares de que trata o § 1º deste artigo em jogos, aplicações de internet ou outras atividades ao fornecimento de informações pessoais além das estritamente necessárias à atividade.
§ 5º O controlador deve realizar todos os esforços razoáveis para verificar que o consentimento a que se refere o § 1º deste artigo foi dado pelo responsável pela criança, consideradas as tecnologias disponíveis.
§ 6º As informações sobre o tratamento de dados referidas neste artigo deverão ser fornecidas de maneira simples, clara e acessível, consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, com uso de recursos audiovisuais quando adequado, de forma a proporcionar a informação necessária aos pais ou ao responsável legal e adequada ao entendimento da criança."

a partir da hipótese de consentimento específico e em destaque de seus pais ou responsáveis legais, a Autoridade Nacional de Proteção de Dados (ANPD), em seu Estudo Preliminar[29] sobre as hipóteses legais aplicáveis ao tratamento de dados pessoais de crianças e adolescentes, está inclinada a entender que o tratamento de dados pessoais de crianças e adolescentes pode ser realizado a partir de qualquer das hipóteses legais previstas no art. 7º, relativas aos "*dados pessoais*", e no art. 11, relativas aos "*dados pessoais sensíveis*", desde que observado o princípio do melhor interesse, conforme a previsão do art. 14, *caput*, da LGPD. Nesse raciocínio, quando da utilização das hipóteses legais de consentimento (art. 7º, inc. I, e art. 11, inc. I) ao tratamento de dados pessoais de crianças, necessário o cumprimento das condições previstas pelo art. 14, § 1º, da LGPD, ou seja, de ser um consentimento específico e em destaque não das crianças, mas sim de seus pais ou responsáveis legais.

7. A aplicação da privacidade e da proteção de dados pessoais no tempo e no espaço

Os direitos fundamentais, como o direito à privacidade e à proteção de dados pessoais, são imprescritíveis, o que significa que podem ser exercidos, nos termos das normas que a regulam, a qualquer tempo[30], inclusive o relativo à proteção de dados pessoais relacionado a contextos anteriores à existência da LGPD, de 14 de agosto de 2018, e da Emenda Constitucional nº 115, de 10 de fevereiro de 2022.

Apesar disso, a LGPD possuiu diferentes marcos de entrada em vigor de seus dispositivos:

(i) os relativos à criação da Autoridade Nacional de Proteção de Dados (ANPD), em vigor desde o dia 28 de dezembro de 2018;

(ii) os demais artigos, exceto os relativos às sanções administrativas decorrentes de infrações à norma, em vigor desde o dia 16 de agosto de 2020; e

(iii) os relativos, justamente, às sanções administrativas decorrentes de infrações à norma, em vigor desde o dia 1º de agosto de 2021.

BRASIL. Lei Federal nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, *Diário Oficial da União*, 15 de agosto de 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: 04 out. 2022.

[29] BRASIL. Autoridade Nacional de Proteção de Dados. Estudo Preliminar. *Hipóteses legais aplicáveis ao tratamento de dados pessoais de crianças e adolescentes.* Brasília, Autoridade Nacional de Proteção de Dados, 2022. Disponível em: <https://www.gov.br/participamaisbrasil/blob/baixar/17636>. Acesso em: 04 out. 2022.

[30] LIMA, Cíntia Rosa Pereira de; PEROLI, Kelvin A aplicação da Lei Geral de Proteção de Dados Pessoais do Brasil no tempo e no espaço. *In:* LIMA, Cíntia Rosa Pereira de (org.*). Comentários à Lei Geral de Proteção de Dados.* São Paulo: Almedina, 2021, pp. 69-100, *passim*.

Destaca-se, nesse sentido, que, embora os dispositivos legais da LGPD tenham, em sua maior parte, entrado em vigor até o dia 16 de agosto de 2020, as sanções administrativas decorrentes de infrações à norma apenas entraram em vigor quase um ano após, em 1º de agosto de 2021. Isto se deveu à publicação da Lei Federal nº 14.010/2020, que tratou sobre o *"Regime Jurídico Emergencial e Transitório das Relações Jurídicas de Direito Privado"*, criado diante do período pandêmico da COVID-19, que postergou o início da vigência das sanções – no intuito de conceder um maior prazo à sociedade brasileira em sua adequação ao respeito e a promoção da privacidade e da proteção de dados pessoais.

Os direitos à privacidade e à proteção de dados pessoais, como previstos constitucionalmente, valem, nos termos das normas que a regulam, para todos os contextos. A LGPD, porém, não é uma norma que regula o direito à proteção de dados pessoais em todos os contextos, ou seja, possui âmbito de aplicação limitado, determinado a partir de seus arts. 3º e 4º.

Nesse sentido, estabelece o art. 3º que as disposições da LGPD se aplicam:

(i) para qualquer tratamento de dados pessoais realizado por pessoa natural ou por pessoa jurídica, de direito público ou de direito privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados pessoais, desde que uma das seguintes condições seja atendida:

   a. o tratamento de dados pessoais seja realizado em território brasileiro;
   b. os dados pessoais objeto do tratamento de dados pessoais, realizado em território estrangeiro, tenham sido coletados em território brasileiro; ou
   c. o tratamento de dados pessoais tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados pessoais de pessoas naturais localizadas em território brasileiro.

A aplicação da Lei conforme o art. 3º é limitada, porém, aos termos do art. 4º, que dispõe não se aplicar a Lei quando o tratamento de dados pessoais:

(i) é realizado por pessoa natural para fins exclusivamente particulares e não econômicos;

(ii) é realizado para fins exclusivamente:

   a. jornalísticos;
   b. artísticos;
   c. acadêmicos, observados tão somente os arts. 7º e 11 da LGPD;
   d. de segurança pública;
   e. de segurança do Estado;
   f. de defesa nacional; ou

g. de atividades de investigação e repressão de infrações penais; ou

(iii) é proveniente de fora do território brasileiro e:

a. sobre o qual não tenha havido transferência internacional de dados pessoais a agentes de tratamento brasileiros; ou

b. sobre o qual não tenha havido transferência internacional de dados pessoais com outro país que não o Brasil, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto pela LGPD.

8. Tratamento de dados pessoais pelo Poder Público

A LGPD traz disposições específicas ao tratamento de dados pessoais pelo Poder Público. O primeiro questionamento que pode ser feito sobre esse tema é, justamente: *"quem é o Poder Público?"* Conforme esclareceu o Guia Orientativo[31] sobre tratamento de dados pessoais pelo Poder Público, da ANPD, o conceito abrange os órgãos dos entes federativos (União, Estados, Distrito Federal e Município) dos três Poderes (Executivo, Legislativo e Judiciário), inclusive os Tribunais de Contas e o Ministério Público. Além disso, conforme interpretação sistemática da LGPD, o conceito também inclui:

(i) os serviços notariais e de registro[32]; e

(ii) as entidades dos entes federativos dos três Poderes, inclusive as fundações e as empresas estatais (empresas públicas e sociedades de economia mista) que:

a. não estejam atuando em regime de concorrência; ou

b. estejam a operacionalizar políticas públicas.

---

[31] BRASIL. Autoridade Nacional de Proteção de Dados. Guia Orientativo. *Tratamento de dados pessoais pelo Poder Público.* Brasília, Autoridade Nacional de Proteção de Dados, 2022. Disponível em: <https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-poder-publico-anpd-versao-final.pdf>. Acesso em: 04 out. 2022.

[32] "Art 5º: Os titulares de serviços notariais e de registro são os:
I - tabeliães de notas;
II - tabeliães e oficiais de registro de contratos marítimos;
III - tabeliães de protestos e títulos;
IV - oficiais de registro de imóveis;
V - oficiais de registro de títulos e documentos e civis das pessoas jurídicas;
VI - oficiais de registro civis das pessoas naturais e de interdições e tutelas;
VII - oficiais de registro de distribuição."
BRASIL. Lei Federal nº 8.935, de 18 de novembro de 1994. Regulamenta o art. 236 da Constituição Federal, dispondo sobre serviços notariais e de registro. Brasília, *Diário Oficial da União*, 21 de novembro de 1994. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l8935.htm>. Acesso em: 17 nov. 2022.

Como dispõe o art. 23 da LGPD, o tratamento de dados pessoais pelo Poder Público deve ser realizado para o atendimento de finalidade pública, na consecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público. Nesse mesmo raciocínio, o art. 23, inc. I, da Lei, em respeito ao princípio da transparência, estabelece a necessidade de que o tratamento de dados pessoais pelo Poder Público seja guiado pela publicidade das informações sobre as hipóteses em que, no exercício de suas competências, realiza o tratamento de dados pessoais, fornecendo informações claras e atualizadas sobre a previsão legal, a finalidade e as práticas utilizadas para a execução dessas atividades, em veículos de fácil acesso, preferencialmente em seus *sites*.

Necessário, também, o destaque ao art. 23, § 3º, da Lei, que estabelece que os prazos e os procedimentos para o exercício dos direitos pelos titulares de dados pessoais perante o Poder Público devem observar as normas específicas a este relacionadas, especialmente as disposições constantes na Lei do *Habeas Data* (Lei Federal nº 9.507/1997), na Lei Geral do Processo Administrativo Federal (Lei Federal nº 9.784/1999) e na Lei de Acesso à Informação (Lei Federal nº 12.527/2011).

9. Uso compartilhado de dados pessoais

Conforme a definição do art. 5º, inc. XVI, da LGPD, o uso compartilhado de dados é um tratamento de dados pessoais caracterizado pela *"comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados"*.

Especificamente sobre o uso compartilhado de dados pelo Poder Público, o art. 25 da LGPD trata da necessidade da interoperabilidade entre os sistemas a fim de que os entes públicos possam utilizar-se do uso compartilhado de dados pessoais com vistas à execução de políticas públicas, à prestação de serviços públicos, à descentralização da atividade pública e à disseminação e ao acesso das informações pelo público em geral. Esse uso compartilhado, como estabelece o art. 26 da Lei, deve atender às finalidades específicas de execução de políticas públicas ou de atribuições legais do Poder Público.

Para além do uso compartilhado de dados pessoais entre os entes públicos, os arts. 26 e 27 da LGPD disciplinam o uso compartilhado entre estes e os entes privados, estabelecendo o consentimento do titular como hipótese legal matriz, porém também tornando-o possível a partir das hipóteses em que há a dispensa do consentimento do titular, enquanto previstas pela LGPD.

Conforme o art. 27, parágrafo único, da Lei, esse uso compartilhado de dados deverá ser informado à ANPD, de acordo com regulamentação ainda a ser elaborada pela Autoridade.

Nesse sentido, na Cidade de São Paulo, o art. 14 do Decreto Municipal nº 57.767/2020 dispôs que o uso compartilhado de dados pessoais entre a Administração Pública Municipal e os entes privados deverá ser informado ao Controlador Geral do Município, enquanto Encarregado pela Proteção de Dados Pessoais da Prefeitura do Município, a fim de que o informe à ANPD, na forma da citada regulamentação que ainda será elaborada.

Por fim, importante o destaque dos pressupostos de observância obrigatória à realização de uso compartilhado de dados pessoais entre os entes públicos, dispostos a partir do julgamento conjunto, pelo Supremo Tribunal Federal, da Ação Direta de Inconstitucionalidade (ADI) nº 6.649/DF e da Arguição de Descumprimento de Preceito Fundamental (ADPF) nº 695/DF, em que os Ministros, por maioria, a seguir o voto do Ministro-Relator Gilmar Mendes, explicitaram-nos do seguinte modo à Administração Pública[33]:

(i) eleição de propósitos legítimos, específicos e explícitos para o tratamento de dados pessoais (art. 6º, inc. I, da LGPD);

(ii) compatibilidade do tratamento com as finalidades informadas (art. 6º, inc. II);

(iii) limitação do uso compartilhado ao mínimo necessário para o atendimento da finalidade informada (art. 6º, inc. III);

(iv) rigorosa observância da transparência sobre as hipóteses em que os entes públicos compartilham ou têm acesso a bancos de dados pessoais (art. 23, inc. I); e

(v) cumprimento integral dos requisitos, garantias e procedimentos estabelecidos pela LGPD, no que for compatível com os entes públicos.

10. Transferência internacional de dados pessoais

A transferência internacional de dados pessoais é uma espécie de uso compartilhado de dados, conforme a definição supracitada (art. 5º, inc. XVI, da LGPD). Constitui-se pela transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o Brasil seja membro.

O art. 33 da LGPD traz as hipóteses legais que permitem a realização de uma transferência internacional de dados pessoais. Nesse sentido, é possível a transferência:

[33] BRASIL. Supremo Tribunal Federal. ADI nº 6.649/DF e ADPF nº 695/DF. Julgamento Conjunto. Data de Julgamento: 15 set. 2022. Data de Publicação: 15 set. 2022. Brasília, *Diário Oficial da Justiça Eletrônico*, 15 set. 2022.

(i) para países ou organismos internacionais que proporcionem grau de proteção de dados pessoais adequado ao previsto na Lei (art. 33, inc. I);

(ii) quando o controlador oferecer e comprovar garantias de cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados previstos na LGPD, na forma de (art. 33, inc. II):

   a. cláusulas contratuais específicas para determinada transferência (art. 33, inc. II, alínea "a");
   b. cláusulas-padrão contratuais (art. 33, inc. II, alínea "b");
   c. normas corporativas globais (art. 33, inc. II, alínea "c"); e
   d. selos, certificados e códigos de conduta regularmente emitidos (art. 33, inc. II, alínea "d");

(iii) quando a transferência for necessária para a cooperação jurídica internacional entre órgãos públicos de inteligência, de investigação e de persecução, de acordo com os instrumentos de direito internacional (art. 33, inc. III);

(iv) quando a transferência for necessária para a proteção da vida ou da incolumidade física do titular ou de terceiro (art. 33, inc. IV);

(v) quando a ANPD autorizar a transferência (art. 33, inc. V);

(vi) quando a transferência resultar em compromisso assumido em acordo de cooperação internacional (art. 33, inc. VI);

(vii) quando a transferência for necessária para a execução de política pública ou atribuição legal do serviço público, desde que seja dada a publicidade nos termos do art. 23, inc. I, da LGPD (art. 33, inc. VII);

(viii) quando o titular tiver fornecido o seu consentimento específico e em destaque para a transferência, com informação prévia sobre o caráter internacional da operação, distinguindo claramente esta de outras finalidades (art. 33, inc. VIII); ou

(ix) quando necessário para atender as hipóteses de (art. 33, inc. IX):

   a. cumprimento de obrigação legal ou regulatória pelo controlador (art. 7º, inc. II);
   b. execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados (art. 7º, inc. V); e
   c. exercício regular de direitos em processo judicial, administrativo ou arbitral (art. 7º, inc. VI).

Com relação à específica hipótese legal de transferência internacional para países ou organismos internacionais que proporcionem grau de proteção de dados pessoais adequado ao previsto na

LGPD (art. 33, inc. I), dispõe o art. 34 da Lei que será a ANPD quem avaliará os níveis de adequação, levando, necessariamente, em consideração:

(i) as normas gerais e setoriais da legislação em vigor no país de destino ou no organismo internacional (art. 34, inc. I);
(ii) a natureza dos dados (art. 34, inc. II);
(iii) a observância dos princípios gerais de proteção de dados pessoais e direitos dos titulares previstos na LGPD (art. 34, inc. III);
(iv) a adoção de medidas de segurança previstas em regulamentos (art. 34, inc. IV);
(v) a existência de garantias judiciais e institucionais para o respeito aos direitos de proteção de dados pessoais (art. 34, inc. V); e
(vi) outras circunstâncias específicas relativas à transferência (art. 34, inc. VI).

Por fim, estabelece o art. 34 da LGPD que a ANPD é também quem determinará a definição do conteúdo das cláusulas contratuais específicas, cláusulas-padrão contratuais, normas corporativas globais, selos, certificados e códigos de conduta regularmente emitidos, quando da específica hipótese legal de transferência internacional por meio desses instrumentos (art. 33, inc. II).

11. Abrindo a caixa de ferramentas: a efetivação dos direitos do titular de dados pessoais pela Administração Pública

"Como efetivar os direitos do titular de dados pessoais?"

Como informa o art. 46 da LGPD, 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. Nesse sentido, a resposta a este questionamento está, justamente, na prática.

O art. 46, § 2º, da Lei, traz a necessidade da observância, pelos agentes de tratamento, das medidas de segurança, técnicas e administrativas, desde a etapa de concepção de um produto ou de um serviço até a etapa de sua execução. Trata-se, em outros termos, dos princípios conhecidos como "*Privacy By Design*" e "*Privacy by Default*".

Esses princípios, que serão melhor explorados adiante, trazem a noção de que os valores da privacidade e da proteção de dados pessoais devem ser observados, por todos os agentes envolvidos em tomadas de decisão, em todo o "*ciclo de vida*" de um "*processo*" – referimo-nos a

"*processo*" como qualquer ação de um agente orientada por um objetivo e a "*ciclo de vida de um processo*" como o conjunto de etapas de uma ação de uma agente orientada por um objetivo. Essa observância é necessária, justamente, para efetivar os direitos dos titulares de dados pessoais em todo o "*ciclo de vida*" do tratamento de dados pessoais existente em cada "*processo*" realizado.

"Mas como proceder com a observância da privacidade e da proteção de dados pessoais em todas as etapas de um processo"?

Este é um questionamento cuja resposta depende do tipo de estrutura de uma organização. No entanto, é possível traçar boas práticas e ações comuns a todas as organizações à efetividade dos direitos do titular de dados pessoais.

Essas ações comuns podem ser dirigidas a partir do que é entendido como um Programa de Governança em Privacidade e Proteção de Dados Pessoais[34], que nada mais é que a organização desse conjunto de ações. Nesse sentido, o art. 50 da LGPD dispõe da faculdade de sua implementação[35].

---

[34] PEROLI, Kelvin; FALEIROS JÚNIOR, José Luiz de Moura. Comentários aos arts. 50 e 51 da LGPD. *In:* MARTINS, Guilherme Magalhães; LONGHI, João Victor Rozatti; FALEIROS JÚNIOR, José Luiz de Moura (orgs.). *Comentários à Lei Geral de Proteção de Dados Pessoais.* Indaiatuba: Foco, 2022, pp. 461-479, *passim*.

[35] Conforme o art. 50 da LGPD: "Art. 50. Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais.

§ 1º Ao estabelecer regras de boas práticas, o controlador e o operador levarão em consideração, em relação ao tratamento e aos dados, a natureza, o escopo, a finalidade e a probabilidade e a gravidade dos riscos e dos benefícios decorrentes de tratamento de dados do titular.

§ 2º Na aplicação dos princípios indicados nos incisos VII e VIII do caput do art. 6º desta Lei, o controlador, observados a estrutura, a escala e o volume de suas operações, bem como a sensibilidade dos dados tratados e a probabilidade e a gravidade dos danos para os titulares dos dados, poderá:

I - implementar programa de governança em privacidade que, no mínimo:

a) demonstre o comprometimento do controlador em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais;

b) seja aplicável a todo o conjunto de dados pessoais que estejam sob seu controle, independentemente do modo como se realizou sua coleta;

c) seja adaptado à estrutura, à escala e ao volume de suas operações, bem como à sensibilidade dos dados tratados;

d) estabeleça políticas e salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade;

e) tenha o objetivo de estabelecer relação de confiança com o titular, por meio de atuação transparente e que assegure mecanismos de participação do titular;

f) esteja integrado a sua estrutura geral de governança e estabeleça e aplique mecanismos de supervisão internos e externos;

g) conte com planos de resposta a incidentes e remediação; e

h) seja atualizado constantemente com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas;

Na Cidade de São Paulo, o Decreto Municipal nº 59.767/2020 dispõe do que é denominado de um "*Plano de Adequação*", que é conjunto entre as boas práticas e o Programa de Governança em Privacidade e Proteção de Dados Pessoais adotado pela Prefeitura do Município de São Paulo. Conforme o seu art. 2º, inc. XIII, é o *"conjunto das regras de boas práticas e de governança de dados pessoais que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos agentes envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos, o plano de respostas a incidentes de segurança e outros aspectos relacionados ao tratamento de dados pessoais."* O art. 4º, inc. III, e o art. 10, inc. II, do Decreto Municipal, por sua vez, dispuseram da obrigação do Poder Executivo, por meio da Administração Pública Municipal direta e indireta, de realizá-lo e de mantê-lo atualizado.

O Decreto Municipal, em seu art. 15, também estabeleceu os requisitos mínimos a serem observados nos Planos de Adequação da Administração Pública Municipal direta e indireta:

(i) publicidade das informações relativas ao tratamento de dados pessoais em veículos de fácil acesso, preferencialmente nas páginas dos órgãos e entidades na Internet, bem como no Portal da Transparência, em seção específica (art. 15, inc. I);

(ii) atendimento das exigências que vierem a ser estabelecidas pela ANPD (art. 15, inc. II); e

(iii) manutenção de dados pessoais em formato interoperável e estruturado para o uso compartilhado de dados com vistas à execução de políticas públicas, à prestação de serviços públicos, à descentralização da atividade pública e à disseminação e ao acesso das informações pelo público em geral (art. 15, inc. III).

Com relação à Administração Pública Municipal direta, dispôs o art. 4º, *caput*, do Decreto Municipal, que cada Secretaria e cada Subprefeitura devem realizá-lo e mantê-lo atualizado, observadas as diretrizes editadas pelo Controlador Geral do Município, enquanto Encarregado pela Proteção de Dados Pessoais da Prefeitura do Município, após deliberação favorável da Comissão Municipal de Acesso à Informação (CMAI).

II - demonstrar a efetividade de seu programa de governança em privacidade quando apropriado e, em especial, a pedido da autoridade nacional ou de outra entidade responsável por promover o cumprimento de boas práticas ou códigos de conduta, os quais, de forma independente, promovam o cumprimento desta Lei.

§ 3º As regras de boas práticas e de governança deverão ser publicadas e atualizadas periodicamente e poderão ser reconhecidas e divulgadas pela autoridade nacional."

BRASIL. Lei Federal nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, *Diário Oficial da União*, 15 de agosto de 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: 04 out. 2022.

Com relação à Administração Pública Municipal indireta, apesar de possuírem os seus próprios encarregados, conforme o art. 10, *caput*, do Decreto Municipal, também devem realizar e manter atualizados os seus Planos de Adequação, observadas as diretrizes do Controlador Geral do Município, nos termos do art. 10, inc. II.

A partir de sua atribuição de emissão de diretrizes, o Controlador Geral do Município, após deliberação favorável da CMAI, editou a Instrução Normativa CGM/SP nº 01, de 21 de julho de 2022[36], que estabelece disposições às ações relativas aos Planos de Adequação dos órgãos e entidades da Administração Pública Municipal, como:

(i) elaboração de programas de capacitação dos servidores que objetive a conscientização sobre os processos ou atividades que se utilizam do tratamento de dados pessoais e das 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 outra forma de tratamento inadequado ou ilícito (art. 14, inc. VI);

(ii) realização de "*Registros das Operações de Tratamento de Dados Pessoais*" – também conhecido como "*Inventários de Dados Pessoais*" e "*Mapeamentos de Dados Pessoais*" (art. 14, inc. IV); e

(iii) realização de "*Relatórios de Impacto à Proteção de Dados Pessoais"* (art. 14, inc. V).

A Instrução Normativa CGM/SP nº 01/2022 é o primeiro passo à padronização das ações da Administração Pública Municipal com relação aos Planos de Adequação de cada órgão e entidade. Nesse sentido, outras ações, que dependam ou não das disposições desta Instrução, poderão ser ainda propostas pelo Controlador Geral do Município, enquanto Encarregado pela Proteção de Dados Pessoais da Prefeitura do Município, no uso da atribuição que lhe conferiu o art. 6º, inc. IV, do Decreto Municipal nº 59.767/2020. Vale o destaque que o cumprimento dessa Instrução Normativa, emitida pelo Encarregado pela Proteção de Dados Pessoais da Prefeitura do Município, é de caráter obrigatório para a Administração Pública Municipal direta e de caráter orientativo para a Administração Pública Municipal indireta, conforme dispõe o seu art. 1º, parágrafo único.

Ao fim de dar cumprimento às ações constantes na Instrução Normativa e subsidiar a elaboração dos Planos de Adequação dos demais órgãos e entidades da Administração Pública Municipal, a Controladoria Geral do Município promoveu a elaboração deste Guia e do "*Guia Orientativo sobre a*

[36] SÃO PAULO (Cidade). Instrução Normativa CGM/SP nº 01, de 21 de julho de 2022. Estabelece disposições referentes ao tratamento de dados pessoais no âmbito da Administração Pública Municipal de São Paulo. São Paulo, *Diário Oficial da Cidade*, 22 de julho de 2022. Disponível em: <https://legislacao.prefeitura.sp.gov.br/leis/instrucao-normativa-controladoria-geral-do-municipio-cgm-1-de-21-de-julho-de-2022>. Acesso em: 04 out. 2022.

Instrução Normativa CGM/SP nº 01/2022 para a Administração Pública do Município de São Paulo", assim como está a elaborar o seu próprio Plano de Adequação à Instrução Normativa CGM/SP nº 01/2022.

12. Abrindo a caixa de ferramentas: o Mapeamento de Processos e o Mapeamento de Dados Pessoais

No âmbito da elaboração de um Programa de Governança em Privacidade e Proteção de Dados Pessoais, elementar é a elaboração de um "*Mapeamento de Processos*"[37], que pode ser entendido como a identificação categorial de todas as ações existentes em uma organização.

O "*Mapeamento de Processos*" precede a realização de um "*Registro das Operações de Tratamento de Dados Pessoais*" (*"Inventário de Dados Pessoais"* ou *"Mapeamento de Dados Pessoais"*, conforme a terminologia do Decreto Municipal nº 59.767/2020 e da Instrução Normativa CGM/SP nº 01/2022), isto porque é necessária, justamente, a identificação categorial de todas as ações existentes ("*Mapeamento de Processos*") a fim de que possa haver a identificação das operações de tratamento de dados pessoais havidas em cada processo ("*Registro das Operações de Tratamento de Dados Pessoais*").

"Mas como realizar um Mapeamento de Processos adequado à realização de um Registro das Operações de Tratamento de Dados Pessoais?"

A Controladoria Geral do Município de São Paulo, por meio de seu Encarregado pela Proteção de Dados Pessoais, desenvolveu metodologia que objetiva padronizar a realização de um "*Mapeamento de Processos*" que possibilita a realização de um "*Registro das Operações de Tratamento de Dados Pessoais*" em conformidade ao que dispõe a Instrução Normativa CGM/SP nº 01/2022.

Esse "*Mapeamento de Processos*" dispõe da necessidade da identificação dos processos e das etapas de cada um dos processos, com a descrição, para cada etapa:

(i) de seu objetivo;

(ii) dos recursos humanos utilizados[38];

(iii) dos recursos físicos e tecnológicos utilizados[39];

[37] Por "*processo*", como já referido, entende-se qualquer ação de um agente orientada por um objetivo.

[38] Por "*recursos humanos*", entende-se o quantitativo de agentes públicos envolvidos em cada etapa de um processo.

[39] Por "*recursos físicos e tecnológicos*", entende-se a infraestrutura física e tecnológica utilizada em cada etapa de um processo.

(iv) do modo de comunicação entre os recursos humanos utilizados e o modo de compartilhamento das informações entre as etapas; e

(v) dos recursos informacionais utilizados[40].

Orientações específicas à realização do "*Mapeamento de Processos*" podem ser encontradas no "*Guia Orientativo sobre a Instrução Normativa CGM/SP nº 01/2022 para a Administração Pública do Município de São Paulo*".

"*E como realizar um Registro das Operações de Tratamento de Dados Pessoais?"*

O art. 14, inc. IV, da Instrução Normativa CGM/SP nº 01/2022, dispôs dos requisitos necessários à elaboração de um "*Registro das Operações de Tratamento de Dados Pessoais"* (*"Inventário de Dados Pessoais"* ou *"Mapeamento de Dados Pessoais"*), observado, materialmente, o Anexo II da Instrução Normativa, "*Mapeamento de Dados Pessoais*":

(i) data de sua criação e de sua atualização, quando aplicável;

(ii) descrição sobre os processos do órgão ou entidade nos quais há o tratamento de dados pessoais;

(iii) identificação dos agentes de tratamento e do Encarregado;

(iv) descrição do ciclo de vida do tratamento de dados pessoais;

(v) descrição da natureza e do escopo do tratamento de dados pessoais;

(vi) descrição da finalidade do tratamento de dados pessoais;

(vii) categorias de dados pessoais tratados, inclusive com a descrição das categorias de dados pessoais sensíveis;

(viii) descrição do volume das operações de tratamento de dados pessoais e das categorias de dados pessoais tratados, inclusive o volume das categorias de dados pessoais sensíveis tratados;

(ix) descrição das categorias de titulares de dados pessoais;

(x) descrição do compartilhamento de dados pessoais, inclusive com a descrição dos agentes de tratamento com os quais os dados pessoais são compartilhados;

(xi) descrição dos contratos de serviços e de soluções de tecnologia da informação que tratam os dados pessoais do processo mapeado;

(xii) descrição das transferências internacionais de dados pessoais; e

[40] Por "*recursos informacionais*", entende-se o rol de "*documentos*" gerados ou compartilhados em cada etapa de um processo somado ao rol de "*informações*" geradas ou compartilhadas em cada etapa de um processo.

(xiii) gestão de riscos à segurança da informação, à privacidade e à proteção de dados pessoais.

13. Abrindo a caixa de ferramentas: o Relatório de Impacto à Proteção de Dados Pessoais

Conforme o art. 5º, inc. XVII, da LGPD, o "*Relatório de Impacto à Proteção de Dados Pessoais*" é a documentação do controlador que contém a descrição dos *"Registros das Operações de Tratamento de Dados Pessoais"* que possam gerar riscos às liberdades civis e aos direitos fundamentais dos titulares de dados pessoais, bem como medidas, salvaguardas e mecanismos de mitigação de riscos já adotados ou que serão adotados por uma organização.

Como dispõe o art. 32 da LGPD, a ANPD, a qualquer momento, pode solicitar ao Poder Público a publicação de Relatório e sugerir a adoção de boas práticas para o tratamento de dados pessoais. Visando a padronizá-lo no âmbito do Poder Executivo Municipal, a Controladoria Geral do Município, por meio de sua Instrução Normativa CGM/SP nº 01/2022, também estabeleceu requisitos para a sua elaboração e disponibilizou, em seu Anexo II, *layout* à realização do "*Relatório de Impacto à Proteção de Dados Pessoais*".

Como aduziu o art. 14, inc. V, da Instrução Normativa CGM/SP nº 01/2022, o Relatório de Impacto à Proteção de Dados Pessoais deve contemplar:

(i) data de sua criação e de sua atualização, quando aplicável;

(ii) identificação dos agentes de tratamento e do encarregado;

(iii) descrição sobre a necessidade de sua elaboração ou de sua atualização;

(iv) descrição do tratamento de dados pessoais, com base no "*Mapeamento de Dados Pessoais*";

(v) descrição sobre a natureza e sobre o escopo do tratamento de dados pessoais;

(vi) descrição sobre o contexto e sobre a necessidade do tratamento de dados pessoais;

descrição sobre a finalidade do tratamento de dados pessoais;

(vii) descrição sobre a "*Gestão de Riscos à Segurança da Informação, à Privacidade e à Proteção de Dados Pessoais*"; e

(viii) descrição sobre as partes consultadas durante a sua elaboração.

No intuito da consecução de "*Relatório de Impacto à Proteção de Dados Pessoais*" por cada órgão ou entidade, a Controladoria Geral do Município também desenvolveu metodologia que busca a padronização da realização de Gestão de Riscos à Segurança da informação, à Privacidade e à Proteção de Dados Pessoais, que podem ser encontradas neste Guia e, especialmente, no "*Guia*

Orientativo sobre a Instrução Normativa CGM/SP nº 01/2022 para a Administração Pública do Município de São Paulo".

Conforme atribuição conferida pelo art. 6º, inc. VIII, do Decreto Municipal nº 59.767/2020, o Encarregado pela Proteção de Dados Pessoais da Prefeitura do Município deverá publicar os Relatórios de Impacto à Proteção de Dados Pessoais de cada órgão da Administração Pública Municipal, isto quando assim solicitado pela ANPD, nos termos do art. 32 da LGPD: *"A autoridade nacional poderá solicitar a agentes do Poder Público a publicação de relatórios de impacto à proteção de dados pessoais e sugerir a adoção de padrões e de boas práticas para os tratamentos de dados pessoais pelo Poder Público."*

14. Abrindo a caixa de ferramentas: a transparência e a proteção de dados pessoais. Descrição das ações práticas necessárias ao diálogo entre a transparência e a proteção de dados pessoais

A transparência e a proteção de dados pessoais não são antagônicas, inclusive no Poder Público. A LGPD, nesse sentido, traz a transparência como um de seus princípios (art. 6º, inc. VI), dispondo-a como a *"garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial".*

Como se interpreta da definição legal, a transparência, neste caso, está relacionada à disponibilização de informações do titular de dados pessoais ao próprio titular, isto de modo claro, preciso e facilmente acessível. Por outro lado, a transparência, enquanto relacionada à disponibilização de informações do titular de dados pessoais a terceiros, não está incluída nessa definição. É justamente a partir desse contexto que a proteção de dados pessoais, especialmente a partir da LGPD, e a transparência, especialmente a partir da Lei de Acesso à Informação (LAI), se harmonizam.

Nesse sentido, traz o art. 31 da LAI disposições sobre o tratamento de dados pessoais, principalmente relativas à divulgação desses dados a terceiros. Conforme o art. 31, § 1º, incs. I e II, os dados pessoais terão seu acesso restrito, independentemente de classificação de sigilo e pelo prazo máximo de 100 anos a contar da data de seu tratamento, ao próprio titular de dados pessoais e a agentes públicos legalmente autorizados, podendo ser autorizada a sua divulgação a terceiros diante do consentimento do titular a que os dados se refiram ou por outras hipóteses legais.

Como verificado, a LGPD traz tanto a hipótese legal do consentimento do titular quanto outras a justificar o tratamento de dados pessoais (art. 7º) e de dados pessoais sensíveis (art. 11). Nesse sentido, é possível a divulgação de dados pessoais de um titular a terceiros, independentemente do consentimento, se essa divulgação é justificada diante de outras hipóteses legais.

Vale ressaltar que a Lei de Acesso à Informação (LAI), por seu art. 1º, dispõe de seu âmbito de aplicação ao Poder Público. O art. 23 da LGPD, por sua vez, remete-se, justamente, ao art. 1º da LAI[41], isto para delimitar, também, a sua aplicação para todo o Poder Público, enquanto assim caracterizado pelo referido dispositivo da LAI.

Nesse sentido, entre as ações práticas, necessárias ao diálogo entre a transparência e a proteção de dados pessoais, estão: (i) a definição sobre a possível ocultação de categorias de dados pessoais, inclusive de categorias de dados pessoais sensíveis, quando da divulgação de documentos públicos que possuam dados pessoais – isto a fim de que os dados pessoais sejam tratados, apenas, quando da existência de(as) hipótese(s) legal(is) apta(s) a ser(em) concretizada(s); e (ii) a definição de procedimento de atendimento aos direitos dos titulares de dados pessoais que se adeque, conjuntamente, aos termos da LGPD, da LAI e, também, da Lei do *Habeas Data* (Lei Federal nº 9.507/1997)[42].

[41] "Art. 1º Esta Lei dispõe sobre os procedimentos a serem observados pela União, Estados, Distrito Federal e Municípios, com o fim de garantir o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal.
Parágrafo único. Subordinam-se ao regime desta Lei:
I - os órgãos públicos integrantes da administração direta dos Poderes Executivo, Legislativo, incluindo as Cortes de Contas, e Judiciário e do Ministério Público;
II - as autarquias, as fundações públicas, as empresas públicas, as sociedades de economia mista e demais entidades controladas direta ou indiretamente pela União, Estados, Distrito Federal e Municípios."
BRASIL. Lei Federal nº 12.527, de 18 de novembro de 2011. Regula o acesso a informações previsto no inciso XXXIII do art. 5º , no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. Brasília, *Diário Oficial da União*, 18 de novembro de 2011. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm>. Acesso em: 17 nov. 2022.

[42] A Lei do *Habeas Data* traz ao cidadão a possibilidade de impetrar esse remédio constitucional, contra órgão ou entidade do Poder Público, a partir: (i) da recusa ou da omissão, por mais de 10 dias sem decisão, do Poder Público, em disponibilizar o conhecimento de informações relativas à pessoa do impetrante, constantes de registro ou banco de dados de entidades governamentais ou de caráter público; (ii) da recusa ou da omissão, por mais de 15 dias sem decisão, do Poder Público, em retificar dados relativos à pessoa do impetrante, também constantes de registro ou banco de dados de entidades governamentais ou de caráter público; e (iii) da recusa ou da omissão, por mais de 15 dias sem decisão, do Poder Público, em promover a contextualização de dados relativos à pessoa do impetrante, também constantes de registro ou banco de dados de entidades governamentais ou de caráter público.
BRASIL. Lei Federal nº 9.507, de 12 de novembro de 1997. Regula o direito de acesso a informações e disciplina o rito processual do habeas data. Brasília, *Diário Oficial da União*, 13 de novembro de 1997. Disponível em: <https://www.planalto.gov.br/ccivil_03/leis/l9507.htm>. Acesso em: 17 nov. 2022.

Capítulo 2

Segurança da Informação

Capítulo II – Segurança da Informação

15. Sociedade Informacional e Segurança da Informação

Globalmente, durante o século XX, a sociedade, em seu contínuo processo de alterações, transformou-se, estruturalmente, de uma "*sociedade industrial*" a uma "s*ociedade informacional*". Essa noção de "*sociedade informacional*" foi, essencialmente, introduzida pelo sociólogo Daniel Bell[43], que entendeu haver o surgimento desse novo desenho social a partir, entre outras características elementares, de uma relação mais próxima da sociedade com a tecnologia e com uma economia mais atrelada à prestação de serviços, em contraposição a uma economia mais atrelada à produção de bens – característica elementar da anterior "*sociedade industrial*".

Em um contexto de maior proximidade da sociedade com a tecnologia, essa "*sociedade informacional*" pode ser ilustrada a partir da ascensão do espaço digital ("*cyberspace*"), no qual a Internet[44] e o grande potencial de tratamento de dados e de dados pessoais ("*Big Data*") são partes componentes de uma rearticulação das relações sociais que levaram, então, ao desenvolvimento de uma economia direcionada à prestação de serviços cujos objetos recaem, principalmente, sobre dados e informações.

"*Mas toda sociedade se constrói a partir de informação!*". Como pontuou o filósofo espanhol Manuel Castells, apesar de todos os modos de desenvolvimento da sociedade possuírem a informação como atributo elementar, o uso do termo "*informacional*", para esta nova sociedade, indica "*uma forma específica de organização social na qual a geração, o processamento e a transmissão de informação se convertem nas fontes fundamentais da produtividade e do poder por conta das novas condições tecnológicas surgidas neste período histórico*"[45].

No contexto dessa "*sociedade informacional*", vive-se a necessidade de que essas informações, a fim de que continuem a mover este modo de desenvolvimento, encontrem-se "*seguras*". Para tanto, a sociedade desenvolveu e desenvolve o que é entendido como "*segurança da informação*".

---

[43] BELL, Daniel. The Coming of Post-Industrial Society. *The Educational Forum*, EUA, vol. 40, n. 04, 1976, pp. 574-579.

[44] "O acesso à Internet tornou-se um direito básico, de que também depende desenvolvimento humano e, em última instância, a realização de Direitos Humanos e liberdades fundamentais."
BACCIOTTI, Karina Joelma. *Direitos Humanos e novas Tecnologias da Informação e Comunicação*: o acesso à Internet como Direito Humano. Dissertação de Mestrado. Pontifícia Universidade Católica de São Paulo, São Paulo, 2014, p. 111.

[45] CASTELLS, Manuel. *The Information Age.* Economy, Society, and Culture. The Rise of The Network Society. Chichester, Reino Unido: Wiley-Blackwell, 2010, p. 21.

"E o que é, então, a segurança da informação?"

Entre os diversos conceitos a este termo, é possível defini-lo, nos dizeres de Marcos Sêmola, como "*uma área do conhecimento dedicada à proteção de ativos da informação contra acessos não autorizados, alterações indevidas ou sua indisponibilidade*"[46]. Gustavo Alberto Alves, por sua vez, entende-o como uma área que "*visa a proteger a informação de forma a garantir a continuidade dos negócios, minimizando os danos e maximizando o retorno dos investimentos e as oportunidades de negócios*"[47].

A fim de padronizar o conceito deste termo, a Norma Técnica ISO/IEC nº 17799, publicada, originalmente, em 2005, entendeu a segurança da informação a partir de seus atributos de *"preservação da confidencialidade, integridade e disponibilidade da informação"*, entendendo, ainda, que, *"adicionalmente, outras propriedades, como autenticidade, responsabilidade, não repúdio e confiabilidade, podem também estar envolvidas"*.

Esse conceito se refere, como é possível notar, à segurança de qualquer tipo de informação – seja em meio analógico, sejam em meio digital. Porém, com o avanço da sociedade informacional, viu-se a necessidade de uma especificação da segurança da informação, justamente, ao meio digital, isto porque, em um cenário de circulação transfronteiriça de dados e de dados pessoais, não há mais distâncias físicas que não possam ser vencidas à obtenção de informações – o que gera, então, a necessidade de controles específicos aptos a viabilizá-las de forma segura.

Para tanto, para além da citada Norma Técnica ISO/IEC nº 17799:2005, revisada e renumerada, em 2007, como a Norma Técnica nº 27002:2007, a Norma Técnica ISO/IEC nº 27001, publicada, inicialmente, em 2005, por sua vez, promoveu a adoção de uma abordagem de processo para a gestão da segurança da informação ambientada, inclusive, no meio digital, isto de modo a orientar o estabelecimento, a implementação, a operação, o monitoramento, a análise, a manutenção e a melhoria contínua de um Sistema de Gerenciamento da Segurança da Informação (SGSI) em uma organização.

Partindo-se da premissa de que a informação é um ativo de uma organização, possui valor e deve, portanto, ser assegurada. Os recursos tecnológicos, porém, não são suficientes a essa segurança: é necessária, nesse contexto, a utilização de recursos humanos, dedicados a lidar com a segurança da informação, isto de modo a adotar metodologias específicas para a estruturação de ações, inclusive relacionadas à conscientização e orientação de todos os agentes integrantes de uma organização e a esta relacionados.

---

[46] SÊMOLA, Marcos. *Gestão de Segurança da Informação*: uma visão executiva. São Paulo: Editora Campus, 2003, p. 09.

[47] ALVES, Gustavo Alberto. *Segurança da Informação*: uma visão inovadora da gestão. Rio de Janeiro: Ciência Moderna, 2006, p. 15.

Essa estruturação, no entanto, não ocorre de uma vez: é preciso que haja um constante aprimoramento, tendo-se em vista que as alterações contextuais do amanhã – como alterações sociais, econômicas, políticas, culturais e tecnológicas – podem, sempre, trazer novas incertezas sobre os controles ontem adotados.

Conforme Pedro Tenório Mascarenhas Neto e Wagner Junqueira Araújo[48], vive-se uma onda, em organizações, do crescente uso de diversos recursos tecnológicos, isto a partir da justificativa dos ganhos em benefícios às próprias organizações, como o aumento da produtividade. Ainda segundo os autores, essa justificativa, porém, em muitos casos, não é acompanhada da reflexão sobre os prejuízos que os diferentes tipos de vulnerabilidades e de ameaças, introduzidos nas organizações a partir do uso desses recursos tecnológicos, são capazes de, às próprias, proporcionar.

Assim, diante de um cenário ascendente do uso de recursos tecnológicos que objetivam inserir as organizações em uma economia informacional, surge-se o seguinte questionamento: *"como gerenciar o uso desses recursos tecnológicos, isto de modo a assegurar as informações sem limitar o desenvolvimento de uma organização?"*

16. Confidencialidade, integridade e disponibilidade da Segurança da Informação

Como indicado na Norma Técnica ISO/IEC nº 27001:2013, a ISO/IEC nº 27002:2022 estabelece um código de práticas para a gestão da segurança da informação, e lhe apresenta atributos elementares – que são, essencialmente: (i) a confidencialidade da informação; (ii) a integridade da informação; e (iii) a disponibilidade da informação.

A confidencialidade é a propriedade de que a informação não seja revelada a indivíduos não autorizados a acessá-la. Nesse sentido, garante que somente os remetentes e os destinatários tenham o devido acesso à informação.

No caso de informações relacionadas ao meio digital, é necessária a criação de medidas aptas a protegê-las contra ameaças à confidencialidade, justamente, relacionadas ao "*cyberspace*". Veja-se o exemplo de um *website* de um banco, no qual todos os dados bancários de seus clientes são, pela rede, compartilhados de forma criptografada. Para que haja acesso a esses dados bancários, são necessários dados de "*senha*" ("*password*") e, por vezes, de "*token*", a depender do nível da informação a qual deseja-se obter acesso ou do serviço o qual deseja-se utilizar. Nesse contexto, a segurança da informação é garantia a partir de três medidas: (i) uma "*senha*" traz a garantia de que o indivíduo conhece a palavra-passe necessária ao acesso dos dados bancários; (ii) um "*token*", por

[48] MASCARENHAS NETO, Pedro Tenório; ARAÚJO, Wagner Junqueira. *Segurança da Informação:* uma visão sistêmica para implantação em organizações. João Pessoa: Editora UFPB, 2019.

sua vez, traz a segurança de que o indivíduo possui o dispositivo de acesso; e (iii) a criptografia, em seu turno, garante que não haja nenhum outro indivíduo com acesso aos dados bancários que não aqueles que estejam como remetentes e destinatários dessa comunicação.

A integridade, por sua vez, diz respeito à propriedade de salvaguarda da completude e da exatidão da informação. No exemplo citado acima, é possível dizer que há a confidencialidade da informação, mas, para que haja a integridade, é necessário que haja a salvaguarda de sua própria existência e de sua própria exatidão. Ao tratar-se de integridade, nesse sentido, trata-se da confiabilidade da informação – tanto relacionada ao seu conteúdo, tanto relacionada à sua origem.

A disponibilidade, por fim, garante que a informação esteja acessível no instante desejado. A fim de que isso ocorra, todas as partes componentes do sistema que disponibiliza essa informação devem estar em funcionamento. Ordinariamente, a disponibilidade é definida em termos de "*qualidade do serviço*". Assim, na hipótese de estar acordada a disponibilidade de um serviço no período entre às 08h e às 18h, em dias úteis, qualquer indisponibilidade desse serviço, nesse período, é uma violação à disponibilidade. *A contrario sensu*, qualquer indisponibilidade desse serviço, fora desse período, não é uma violação à disponibilidade.

Existem diversas medidas técnicas aptas a garantir a disponibilidade de sistemas tecnológicos. Nesse sentido, *e.g.*, é possível trazer a hipótese de serviços públicos, prestados pela Prefeitura do Município, que possam ser apenas solicitados pela Internet. Em caso de uma eventual paralização de um servidor que hospeda determinado serviço público, em razão de um ataque "*hacker*", o que ocorre, portanto, é um impacto na indisponibilidade desse serviço aos seus usuários. A fim de mitigar esse risco, é possível a manutenção de dois servidores distintos que ofereçam o mesmo serviço público. Desse modo, mesmo que um dos servidores se encontre, temporariamente, indisponível, os usuários continuarão a usufruir da disponibilidade do serviço.

Capítulo 3

Gestão de Riscos à Segurança da Informação, à Privacidade e à Proteção de Dados Pessoais

Capítulo III – Gestão de Riscos à Segurança da Informação, à Privacidade e à Proteção de Dados Pessoais

17. Identificação de Riscos à Segurança da Informação, à Privacidade e à Proteção de Dados Pessoais

O Dicionário Priberam da Língua Portuguesa[49] define "*risco*", entre outras definições, como perigo ou inconveniente. Quando se aborda o conceito de risco, está-se diante de uma possibilidade existente nos mais distintos contextos da vida, na qual, pelo risco, há um perigo ou um inconveniente.

Conforme define a norma ABNT NBR ISO nº 31000:2018, "*risco*" é o "*efeito da incerteza nos objetivos*"[50]. A "*gestão de riscos*", por sua vez, é o conjunto de "*atividades coordenadas para dirigir e controlar uma organização no que se refere aos riscos*"[51].

O objetivo da abordagem convergente entre os temas da segurança da informação, da privacidade e da proteção de dados pessoais, é, justamente, garantir a segurança das informações, inclusive relacionadas aos dados pessoais, que estão sob a guarda da organização.

Nesse contexto, quando da gestão de riscos, deve-se ter em mente a prevenção de "*elementos que, individualmente ou combinados, tenham o potencial para gerar um risco*", ou seja, um perigo e/ou um inconveniente à garantia da segurança da informação, da privacidade e da proteção dos dados pessoais.

No entanto, um evento que venha a ter "*consequências negativas*" nos objetivos não é improvável que ocorra, ainda que haja medidas de segurança, técnicas e administrativas, implementadas para tanto. É o que entendemos como *"likelihood"*, ou seja, a "*probabilidade*" da ocorrência de um risco.

É a partir desse contexto que temos como necessário o estabelecimento de "*controles*", ou seja, de "*medidas que mantenham e/ou modifiquem o risco*". Essas medidas podem incluir, por exemplo, processos e procedimentos.

"E como identificar os riscos que tragam perigo ou inconveniente no que se refere à segurança da informação, à privacidade e à proteção de dados pessoais?"

---

[49] PRIBERAM. *Dicionário Priberam da Língua Portuguesa.* Lisboa: Priberam, 2022. Disponível em: <https://dicionario.priberam.org/risco>. Acesso em: 03 jan. 2023.
[50] Item 3.1, "*risco*", da norma ABNT NBR ISO nº 31000:2018.
[51] Item 3.2, "*gestão de riscos*", da norma ABNT NBR ISO nº 31000:2018.

Nos termos previstos pela ABNT NBR ISO nº 31000:2018[52], na etapa de "*identificação de riscos*", os seguintes "*fatores*" devem ser considerados:

(i) *"Fontes tangíveis e intangíveis de risco"*: as "*fontes tangíveis*" são fontes palpáveis, físicas, como portões, catracas, cadeados, "*hardware*" e pessoas, enquanto as "*fontes intangíveis*" são fontes que não são alcançáveis pelo tato, como processos e tecnologias. Nesse sentido, imagine a hipótese de um portão ou catraca para impedir o acesso de pessoas não autorizadas a um determinado ambiente que contenha informações, porém o portão não está trancado ou a catraca está liberada. Trata-se, neste caso, de "*fontes tangíveis*". Ou, ainda, que a organização tenha adquirido certa tecnologia para proteger informações que estão armazenadas em um servidor, porém a tecnologia não foi configurada corretamente, por não ter havido a implementação de processos de verificação, ou mesmo porque os profissionais não foram treinados com o intuito da obtenção do máximo grau de usabilidade da tecnologia. Trata-se, neste caso, de "*fontes intangíveis*";

(ii) "*Causas*" e *"eventos"*: as "*causas*" ocasionam determinados "*eventos*", que, por sua vez, podem gerar um perigo e/ou um inconveniente. É neste contexto que há a importância da realização de um mapeamento dos "*eventos*" que geram "*riscos*" efetivos ou potenciais a um processo, assim como a importância do conhecimento de suas "*causas*". Nesse sentido, por exemplo, na hipótese de João ser responsável por uma catraca, necessitar se ausentar a fim de ir ao banheiro e decidir deixar a catraca liberada, no intuito de não impedir a entrada de algum funcionário, tem-se como "*evento*" a liberação da catraca, que possui como "*causa*", em seu turno, a ausência de designação de outro funcionário que substitua João em suas tarefas;

(iii) "*Ameaças*" e "*oportunidades*": uma *"ameaça"* é um "*evento*" que tem o potencial de comprometer "*ativos*", como as "*fatores temporais*", indicados pela ABNT NBR ISO nº 31000:2018. As "*oportunidades*", em seu turno, podem ser definidas como um hiato ("*gap*") entre um contexto presente e um contexto futuro em que é possível visualizar alguma vantagem;

(iv) "*Vulnerabilidades*" e *"capacidades"*: a "*vulnerabilidade"* representa uma fraqueza que pode ser explorada com consequências negativas, ou seja, é um ponto fraco

[52] Item 6.4.2, "*identificação de riscos*", da norma ABNT NBR ISO nº 31000:2018.

existente, por exemplo, em um recurso tecnológico ou mesmo em um recurso humano, como as "*limitações de conhecimento e de confiabilidade da informação"* e os "*vieses, hipóteses e crenças dos envolvidos*", descritas pela ABNT NBR ISO nº 31000:2018. A "*capacidade*", por sua vez, é a aptidão para a execução de uma determinada ação. Neste contexto, é a aptidão em proteger a privacidade e os dados pessoais; e

(v) *"Mudança nos contextos externos e internos":* o "*contexto externo*" diz respeito ao contexto em que uma determinada organização existe e atua, podendo estar relacionado, por exemplo, aos fatores sociais, culturais, políticos, jurídicos, tecnológicos, econômicos e ambientais que afetam os processos da organização. Um exemplo de "*mudança de contexto externo*" que afetou a todas as organizações é a própria LGPD, que alterou o trato de todos com a privacidade e com os dados pessoais. O "*contexto interno*", por sua vez, diz respeito ao contexto existente no interior da organização, como, entre outros, os elementos relacionados a sua estrutura e a sua cultura organizacional, além de seus recursos humanos, físicos, tecnológicos e informacionais. Nesse sentido, as "*mudanças*" nesses contextos podem ser "*causas*" de "*eventos*" que venham a gerar um risco efetivo ou potencial a um processo; e

(vi) "*Natureza e valor dos ativos*": um "*ativo*" é algo que possui valor para a organização e que, portanto, requer proteção. Identificar a natureza e o valor de determinado ativo significa classificá-lo a partir de um contexto pré-determinado ("*natureza*") e também classificá-lo a partir da valoração pré-determinada de um ativo para a organização ("*valor*").

É importante ressaltar, como o próprio termo anglófono "*likelihood"* indica, que não há como se dizer sobre um "*risco zero*", uma vez que sempre haverá riscos em qualquer ambiente. A função da gestão de riscos aplicada à segurança da informação é minimizar a probabilidade de ocorrência de eventos danosos – quer para a organização, quer para o usuário. Essa mitigação é possível com a alocação dos recursos necessários à organização – o que inclui, por exemplo, os recursos humanos, com as suas competências e experiências, assim como por boas práticas aplicadas aos processos, aos métodos e as ferramentas a serem empregadas.

Nesse sentido, as seguintes "*etapas"* podem ser aplicadas no processo de "*identificação de riscos*":

(i) Identificação dos "*ativos*": como mencionado, um "*ativo*" é algo que possui valor para a organização e que, portanto, requer proteção. No presente contexto, os

"*ativos*" são as "*informações*" havidas pela Administração Pública do Município, que necessitam de proteção. As informações possuem valor intrínseco, ou seja, não se resumem em sua representação em dados, enquanto representados pela linguagem. Assim, as ideias e os conceitos contidos nas informações são "*formas intangíveis*" do valor havido nas informações. A identificação das "*informações*" requer, nesse sentido, um "*mapeamento de processos*", como explicitado anteriormente, a fim de que haja a identificação das "*informações*" existentes nos processos que afetam a privacidade e que contenham dados pessoais;

(ii) Identificação das "*ameaças*": a identificação das "*ameaças*" pode ser realizada por uma análise sobre os "*eventos*" anteriores e sobre os processos realizados pela organização. Essas "*ameaças*" podem ser de natureza humana ou de ordem natural e se classificam de acordo com a sua natureza acidental ou intencional. As "*ameaças*" podem resultar na modificação, na perda ou no furto de "*informações*" e até mesmo na paralisação dos serviços que estão sendo executados;

(iii) Identificação das "*vulnerabilidades*": a identificação das "*vulnerabilidades*" depende da compreensão sobre as "*ameaças*" que afetam cada área da organização, como o uso não controlado de "*softwares"* e o uso de conexões de rede desprotegidas. Como já mencionado, a "*vulnerabilidade*" representa uma fraqueza que pode ser explorada e que possua "*consequências*" negativas, ou seja, é um ponto fraco existente em um processo de uma organização;

(iv) Identificação dos "*controles*" já existentes: a identificação dos "*controles*" existentes consiste na verificação sobre quais medidas estão sendo adotadas no tratamento dos "*ativos*" de modo a manter e/ou modificar o "*risco*". Concomitantemente à identificação dos "*controles*" existentes, é importante que a verificação de sua eficácia e de sua eficiência sejam realizadas, uma vez que um "*controle*" ineficaz ou ineficiente pode ser causa de "*vulnerabilidades*". Ademais, poderá ser preciso, como se verá, adiante, que "*controles*" suplementares sejam aplicados, caso os "*controles*" iniciais falhem ou sejam insuficientes; e

(v) Identificação das *"consequências*": uma "*consequência*" é o resultado de um "*evento*". As "*consequências*" podem ser negativas, positivas, ou indiferentes ao objetivo de proteção do "*ativo*" considerado – neste caso, as "*informações*". Uma "*consequência*" pode ser, por exemplo, a perda da eficácia e da efetividade da proteção. Assim, a identificação das "*consequências*" visa a apresentar os cenários decorrentes de um "*evento*" que resulte na ocorrência de um "*risco*", isto de modo a considerar, por

exemplo, os danos à privacidade e à proteção de dados pessoais e os eventuais reparos necessários ao retorno da prestação de um serviço, em caso da ocorrência do "*evento*".

Apresentados os principais "*fatores*" e as "*principais etapas*" a uma "*identificação de riscos*", exemplifica-se, a seguir, quadro de "*ameaças*" e de "*vulnerabilidades*" que podem estar presentes nos recursos humanos, físicos, tecnológicos e informacionais de uma organização:

Tabela I – Exemplos de ameaças e de vulnerabilidades aos recursos humanos

Ameaça	Vulnerabilidade
Indisponibilidade de recursos humanos	Ausência de recursos humanos
Erro durante o uso	Treinamento insuficiente
Destruição de equipamentos ou mídia	Procedimento de recrutamento inadequado

Tabela II – Exemplos de ameaças e vulnerabilidades aos recursos físicos, tecnológicos e informacionais

Ameaça	Vulnerabilidade
Inundação	Localização em área suscetível à inundação
Interrupção do suprimento de energia	Fornecimento de energia instável
Destruição de equipamento ou mídia	Uso inadequado
Erro durante o uso	Inexistência de política de uso de correspondência eletrônica
Repúdio de ações	Atribuição inadequada das responsabilidades pela segurança da informação
Furto de equipamentos	Inexistência de controle sobre ativos fora das dependências da organização
Furto de mídia ou documentos	Armazenamento não protegido
Destruição de equipamento ou mídia	Falta de uma rotina de substituição periódica
Poeira, corrosão e congelamento	Sensibilidade à umidade e sujeira
Erro durante o uso de *software*	Datas incorretas
Abuso de direitos	Atribuição errônea de direitos de acesso
Forjamento de direitos	Gestão de senhas incorreto

18. Análise de Riscos à Segurança da Informação, à Privacidade e à Proteção de Dados Pessoais

A partir do contexto da sociedade informacional e do "*Big Data*", o "*valor*" dos dados pessoais está a crescer dia-a-dia.

No âmbito da gestão de riscos, conforme se refere a ABNT NBR ISO/IEC nº 29100:2020, a salvaguarda da privacidade e da proteção de dados pessoais pode relacionar-se a muitas etapas distintas do tratamento de dados pessoais – como, por exemplo, as de coleta e de retenção de dados pessoais, de compartilhamento de dados pessoais com terceiros e de uso compartilhado de dados pessoais, por uma relação contratual, entre controladores e operadores.

Após a "*identificação*" dos riscos à segurança da informação, à privacidade e à proteção de dados pessoais existentes nos distintos processos da organização, é necessária uma "*análise*" sobre a "*natureza*" dos riscos e de suas respectivas "*características*".

Entre as "*características*" a serem analisadas, é possível a classificação dos riscos com base:

(i) no "*contexto*" de sua ocorrência, conforme o "*Manual de Gestão de Riscos*", da Controladoria Geral do Município de São Paulo (CGM/SP)[53], e o Anexo VI deste Guia, "*Gestão de Riscos à Segurança da Informação, à Privacidade e à Proteção de Dados Pessoais*";

(ii) na "*análise dos controles existentes*", conforme o "*Manual de Gestão de Riscos*", da Controladoria Geral do Município de São Paulo (CGM/SP)[54], e a norma ABNT NBR ISO nº 31000:2018[55];

Após a classificação dos riscos a partir dessas "*características*", é possível a diferenciação de sua "*natureza*" entre:

(i) "*risco inerente*", que é um risco intrínseco à natureza de um processo, conforme o "*Manual de Gestão de Riscos*", da Controladoria Geral do Município de São Paulo

[53] Por "*contexto*", é possível entender a classificação, realizada pelo "*Manual de Gestão de Riscos*" da Controladoria Geral do Município de São Paulo (CGM/SP), que objetiva a categorização dos riscos em: (i) operacionais; (ii) orçamentários; (iii) de imagem; (iv) de conformidade; (v) social; e (vi) de integridade.
Os conceitos relativos a cada categoria contextual de risco podem ser encontrados no próprio "*Manual de Gestão de Riscos*" e no Anexo VI deste Guia, "*Gestão de Riscos à Segurança da Informação, à Privacidade e à Proteção de Dados Pessoais*".

[54] O *"Manual de Gestão de Riscos"* da Controladoria Geral do Município de São Paulo (CGM/SP) dispõe dos seguintes critérios com relação ao nível de confiança sobre os controles existentes: (i) inexistente; (ii) fraco; (iii) mediano; (iv) satisfatório; e (v) forte. A descrição sobre cada nível pode ser encontrada no próprio "*Manual de Gestão de Riscos*" e no Anexo VI deste Guia, "*Gestão de Riscos à Segurança da Informação, à Privacidade e à Proteção de Dados Pessoais*".

(CGM/SP)[56], e o Anexo VI deste Guia, "*Gestão de Riscos à Segurança da Informação, à Privacidade e à Proteção de Dados Pessoais*"; e

(ii) "*risco residual*", que é um risco remanescente após a adoção dos controles existentes, conforme o "*Manual de Gestão de Riscos*", da Controladoria Geral do Município de São Paulo (CGM/SP)[57], e o Anexo VI deste Guia, "*Gestão de Riscos à Segurança da Informação, à Privacidade e à Proteção de Dados Pessoais*".

Posteriormente à distinção dos riscos entre "*riscos inerentes*" e "*riscos residuais*", é possível a classificação dos riscos com base nas seguintes "*características*":

(i) na "*probabilidade*" de sua ocorrência, conforme o "*Manual de Gestão de Riscos*", da Controladoria Geral do Município de São Paulo (CGM/SP)[58], e o Anexo VI deste Guia, "*Gestão de Riscos à Segurança da Informação, à Privacidade e à Proteção de Dados Pessoais*"; e

(ii) no "*impacto*" de sua ocorrência, conforme o "*Manual de Gestão de Riscos*", da Controladoria Geral do Município de São Paulo (CGM/SP)[59], e o Anexo VI deste Guia, "*Gestão de Riscos à Segurança da Informação, à Privacidade e à Proteção de Dados Pessoais*".

A fim de mensurar, objetivamente, a análise dos "*riscos inerentes*" e dos "*riscos residuais*", é possível o uso de uma "*matriz de riscos*", que considere a "*probabilidade*" e o "*impacto*" de suas respectivas ocorrências.

Para tanto, o "*Manual de Gestão de Riscos*", da Controladoria Geral do Município de São Paulo (CGM/SP), traz metodologia que pode ser utilizada e que se encontra já instrumentalizada e

---

[56] Item 6.4.3, "*análise de riscos*", da norma ABNT NBR ISO nº 31000:2018.

[56] Por "*contexto*", é possível entender a classificação, realizada pelo "*Manual de Gestão de Riscos*" da Controladoria Geral do Município de São Paulo (CGM/SP), que objetiva a categorização dos riscos em: (i) operacionais; (ii) orçamentários; (iii) de imagem; (iv) de conformidade; (v) social; e (vi) de integridade.
Os conceitos relativos a cada categoria contextual de risco podem ser encontrados no próprio "*Manual de Gestão de Riscos*" e no Anexo VI deste Guia, "*Gestão de Riscos à Segurança da Informação, à Privacidade e à Proteção de Dados Pessoais*".

[57] Por "*contexto*", é possível entender a classificação, realizada pelo "*Manual de Gestão de Riscos*" da Controladoria Geral do Município de São Paulo (CGM/SP), que objetiva a categorização dos riscos em: (i) operacionais; (ii) orçamentários; (iii) de imagem; (iv) de conformidade; (v) social; e (vi) de integridade.
Os conceitos relativos a cada categoria contextual de risco podem ser encontrados no próprio "*Manual de Gestão de Riscos*" e no Anexo VI deste Guia, "*Gestão de Riscos à Segurança da Informação, à Privacidade e à Proteção de Dados Pessoais*".

[58] O *"Manual de Gestão de Riscos"* da Controladoria Geral do Município de São Paulo (CGM/SP) dispõe dos seguintes critérios com relação à análise da probabilidade: (i) muito baixa; (ii) baixa; (iii) média; (iv) alta; e (v) muito alta. A descrição sobre cada nível pode ser encontrada no próprio "*Manual de Gestão de Riscos*" e no Anexo VI deste Guia, "*Gestão de Riscos à Segurança da Informação, à Privacidade e à Proteção de Dados Pessoais*".

[59] O *"Manual de Gestão de Riscos"* da Controladoria Geral do Município de São Paulo (CGM/SP) dispõe dos seguintes critérios com relação à análise de impacto: (i) muito baixo; (ii) baixo; (iii) médio; (iv) alto; e (v) muito alto. A descrição sobre cada nível pode ser encontrada no próprio "*Manual de Gestão de Riscos*" e no Anexo VI deste Guia, "*Gestão de Riscos à Segurança da Informação, à Privacidade e à Proteção de Dados Pessoais*".

adaptada ao contexto da segurança da informação, da privacidade e da proteção de dados pessoais, isto nos Anexos VI e VII do "Guia Orientativo sobre a Instrução Normativa CGM/SP nº 01/2022 para a Administração Pública do Município de São Paulo" – que são, respectivamente, "*Riscos à Segurança da Informação, à Privacidade e à Proteção de Dados Pessoais*", e "*Registro dos Riscos à Segurança da Informação, à Privacidade e à Proteção de Dados Pessoais*"

19. Avaliação de Riscos à Segurança da Informação, à Privacidade e à Proteção de Dados Pessoais

A "*mensuração*" é importante para tornar possível à organização a sua *"Avaliação de Riscos à Segurança da Informação, à Privacidade e à Proteção de Dados Pessoais"*, ou seja, a sua tomada de decisão frente aos riscos identificados. A norma ABNT NBR ISO nº 31000:2018 entende, por exemplo, ser possível as seguintes tomadas de decisão quanto aos riscos identificados:

(i) "*fazer mais nada*";
(ii) "*considerar as opções de tratamento de riscos*";
(iii) "*realizar análises adicionais para melhor compreender o risco*";
(iv) "*manter os controles existentes*"; e
(v) "*reconsiderar os objetivos*".

O "*Manual de Gestão de Riscos*", da Controladoria Geral do Município de São Paulo (CGM/SP), por sua vez, exemplificou as seguintes tomadas de decisão:

(i) *"evitar"*;
(ii) *"reduzir"*;
(iii) *"compartilhar"*;
(iv) *"aceitar"*; e
(v) *"potencializar"*.

Nesse sentido, a partir da "*análise de riscos*", é possível, então, diferentes "*avaliações*" com relação aos riscos identificados.

"Mas por que não fazer mais nada?"

Muitas vezes, apesar de ser possível, por "*controles*", manter ou tratar os riscos identificados e analisados, a organização pode avaliar não valer a pena implementá-los, tendo em vista, por exemplo, a possibilidade da incidência de novos riscos ou a expansão de aqueles já existentes.

20. Tratamento de Riscos à Segurança da Informação, à Privacidade e à Proteção de Dados Pessoais

Conforme a norma ABNT NBR ISO/IEC nº 27002:2022, um "*controle*" é uma medida apta a manter ou modificar um risco[60]. Assim, um "*controle*" pode reduzir ou eliminar a probabilidade e/ou o impacto de um risco identificado, analisado e avaliado.

Nesse sentido, pode um "*controle*" dizer respeito a todo o contexto de incidência da privacidade e da proteção de dados pessoais no âmbito da organização, ou mesmo ser aplicado a contextos específicos de incidência, a partir dos contextos internos e externos que influem nos distintos processos da organização.

Os "*controles*" devem estar todos em conformidade com os "*princípios*"[61] que devem orientar toda a organização diante da privacidade e da proteção de dados pessoais. Por "*princípios*", é possível entender as "*verdades ou juízos fundamentais, que servem de alicerce ou de garantia de certeza a um conjunto de juízos, ordenados em um sistema de conceitos relativos à dada porção da realidade*"[62].

Nesse sentido, a norma ABNT NBR ISO/IEC nº 29100:2020 lhes dispôs do seguinte modo:

(i) consentimento e escolha: o "*consentimento*" é a manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais, enquanto a "*escolha*" é o momento prévio em que o titular age em direção ao seu consentimento. No âmbito da LGPD, está especialmente relacionado ao seu art. 7º, inc. I, e ao seu art. 11, inc. I, que dispõem, respectivamente, das hipóteses de tratamento de dados pessoais e de dados pessoais sensíveis pelo consentimento;

(ii) legitimidade e especificação de objetivo: a "*legitimidade*" consiste na competência legal ou contratual para o tratamento de dados pessoais, enquanto a "*especificação do objetivo*" trata-se da determinação da finalidade do tratamento, inclusive ao titular. No âmbito da LGPD, está especificamente relacionado ao seu art. 6º, inc. I, relativo ao princípio da finalidade;

(iii) limitação da coleta: a "*limitação da coleta*" dispõe da necessidade da realização de um tratamento sempre pautado em propósitos legítimos, específicos, explícitos e informados ao titular, sem a possibilidade de tratamento posterior de forma incompatível com esses propósitos. No âmbito da LGPD, está também especificamente relacionado ao seu art. 6º, inc. I, relativo ao princípio da finalidade;

[60] Item 0.3, "*controles*", da norma ABNT NBR ISO/IEC nº 27002:2022.
[61] Item 5.1, "*visão geral dos princípios de privacidade*", da norma ABNT NBR ISO/IEC nº 29100:2020.
[62] REALE, Miguel. *Filosofia do Direito*. 11ª ed. São Paulo: Saraiva, 1986, p 60.

(iv) minimização de dados pessoais: a "*minimização de dados pessoais*", apesar de relacionado ao princípio da limitação da coleta, diz respeito à 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. No âmbito da LGPD, está especificamente relacionado ao seu art. 6º, inc. III, relativo ao princípio da necessidade;

(v) limitação do uso, da retenção e da divulgação: a "*limitação do uso, da retenção e da divulgação*", estreitamente relacionada ao princípio da "*limitação da coleta*", refere-se, pois, também à necessidade da realização de um tratamento sempre pautado em propósitos legítimos, específicos, explícitos e informados ao titular, sem a possibilidade de tratamento posterior de forma incompatível com esses propósitos. No mesmo sentido, no âmbito da LGPD, está também especificamente relacionado ao seu art. 6º, inc. I, relativo ao princípio da finalidade;

(vi) precisão e qualidade: a "*precisão e qualidade*" diz respeito à necessidade da garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento. No âmbito da LGPD, está relacionado ao seu art. 6º, inc. V, relativo ao princípio da qualidade dos dados;

(vii) abertura, transparência e notificação: a "*abertura, transparência e notificação*" traz a ideia da necessidade da garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento. No âmbito da LGPD, está relacionado ao seu art. 6º, inc. VI, relativo ao princípio da transparência;

(viii) participação individual e acesso: a "*participação individual e acesso*" diz respeito à necessidade da garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais. No âmbito da LGPD, está relacionado ao seu art. 6º, inc. IV, relativo ao princípio do livre acesso;

(ix) responsabilização: a "*responsabilização*" traz a necessidade da demonstração, pelos agentes de tratamento, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas relativas à segurança da informação, à privacidade e à proteção de dados pessoais e, inclusive, da eficácia dessas medidas. No âmbito da LGPD, está relacionado ao seu art. 6º, inc. X, relativo ao princípio da responsabilização e prestação de contas;

(x) segurança da informação: a "*segurança da informação*" é aqui trazida com a ideia da utilização de medidas 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 difusão. No âmbito da LGPD, está relacionado ao seu art. 6º, inc. VII, relativo ao princípio da segurança;

(xi) *compliance* com a privacidade: o "*compliance com a privacidade*" indica, de modo geral, a necessidade da conformidade e da demonstração da conformidade, pelo agente de tratamento, ao sistema normativo de salvaguarda à privacidade e à proteção de dados pessoais vigente. No âmbito da LGPD, para além dos princípios supracitados, é possível a abrangência, neste princípio da norma ABNT NBR ISO/IEC nº 29100:2020, de todos os demais – dos princípios da adequação, da prevenção e da não discriminação, respectivamente presentes no art. 6º, incs. II, VIII e IX.

"E como estruturar a implementação de controles?"

Como mencionado, a implementação de "*controles*" depende da especificidade dos riscos identificados, analisados e avaliados no contexto da salvaguarda à segurança da informação, da privacidade e da proteção de dados pessoais de uma organização.

Apesar disso, algumas normas técnicas e guias orientativos trazem exemplos que podem servir de parâmetro à análise dos controles existentes e como parâmetro à implementação de novos controles. Nesse sentido encontram-se os controles presentes na norma ABNT ISO/IEC nº 27001:2013, que trata de controles de segurança da informação, e na norma ABNT ISO/IEC nº 29151:2020, que trata de controles para a salvaguarda da privacidade e da proteção de dados pessoais.

No intuito de sistematizar os controles presentes na norma ABNT ISO/IEC nº 27001:2013 e na e na norma ABNT ISO/IEC nº 29151:2020, o Anexo VI do "*Guia Orientativo sobre a Instrução Normativa CGM/SP nº 01/2022 para a Administração Pública do Município de São Paulo*", "*Gestão de Riscos à Segurança da Informação, à Privacidade e à Proteção de Dados Pessoais*", os apresenta como rol exemplificativo de controles aptos ao tratamento dos riscos.

Capítulo 4

Boas Práticas em Segurança da Informação, Privacidade e Proteção de Dados Pessoais

Capítulo IV – Boas Práticas em Segurança da Informação, Privacidade e Proteção de Dados Pessoais

21. Utilizando a caixa de ferramentas: "*Privacy by Design*" e "*Privacy by Default*"

O objetivo de um Programa de Governança em Privacidade e Proteção de Dados Pessoais é, sem dúvidas, a efetividade da garantia dos direitos fundamentais da privacidade e da proteção de dados pessoais. Nesse sentido, esses "*valores*" devem estar imbuídos durante todo o ciclo de vida de um processo – enquanto conjunto de atividades orientadas por um objetivo. Assim, é preciso que a privacidade e a proteção de dados pessoais sejam vistas como o padrão de conduta ético a ser perseguido pelos "*recursos humanos*" e o padrão sociotécnico a ser adotado pelos "*recursos físicos*", "*recursos tecnológicos*" e "*recursos informacionais*" empregados em todos os processos. É a partir desse raciocínio que também é necessário, do mesmo modo, a observância da segurança da informação. Para tanto, é necessário que esses "*valores*" estejam acoplados em todas as etapas dos processos, assim desde o início ("*by design*") e como padrão de conduta ("*by default*"). É a partir deste prognóstico que Ann Cavoukian[63], ex *Privacy Commissioner* de Ontário, Canadá, entabulou sete "*princípios*" fundamentais para a construção da proteção à privacidade e à proteção de dados pessoais – que podem ser vistos, nesse sentido, como boas práticas:

(i) *"Proactive not reactive, preventive not remedial"*: o padrão de conduta a ser perseguido deve ser o de uma conduta sempre preventiva e não apenas reativa aos riscos à privacidade e à proteção de dados pessoais;

(ii) *"Privacy as the default setting"*: os valores da privacidade e da proteção de dados pessoais devem ser incorporados como o padrão de conduta;

(iii) *"Privacy embedded by design"*: os valores da privacidade e da proteção de dados pessoais devem ser incorporados desde o início ("*by design*") do ciclo de vida dos processos;

(iv) *"Full functionality – positive-sum, not zero-sum"*: os valores da privacidade e da proteção de dados pessoais, incorporados por todo o ciclo de vida dos processos, não podem ser obstáculos à funcionalidade integral dos produtos ou dos serviços, ou seja, não se pode reduzir as funcionalidades de um produto ou de um serviço em razão da adoção de um padrão de conduta pautado nos valores da privacidade e da proteção de dados pessoais;

(v) *"End-to-end security – full lifecycle protection"*: as medidas de segurança devem ser adotadas em todo o ciclo de vida dos processos;

[63] CAVOUKIAN, Ann. *Privacy by Design*. The 7 Foundational Principles. Toronto: Information and Privacy Commissioner of Ontario, 2011, pp. 01-02. Disponível em: <https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf>. Acesso em: 04 out. 2022.

(vi) "*Visibility and transparency – keep it open"*: a transparência, como princípio, deve ser adotada em todo o ciclo de vida dos processos; e

(vii) "*Respect for user privacy – keep it user-centric*": todo o ciclo de vida dos processos deve ser orientado a partir do respeito ao titular de dados pessoais.

Seguidos esses "*princípios*", é possível, assim, fortalecer um padrão de conduta ético de todos os agentes públicos e implementar os "*valores"* da privacidade, da proteção de dados pessoais e da segurança da informação em todo o ciclo de vida dos processos da Administração Pública Municipal – incluindo, nesse sentido, os padrões adotados a partir do uso dos recursos humanos, físicos, tecnológicos e informacionais[64].

Como boas práticas de "*controles*" a serem implementados, é possível, a partir dos "*controles*" exemplificados pela norma ABNT ISO/IEC nº 27001:2013 e pela ABNT ISO/IEC nº 29151:2020, a menção[65] às boas práticas:

(i) controles de segurança em recursos humanos[66]: a conscientização e a capacitação sobre os fundamentos da segurança da informação, da privacidade e da proteção de dados pessoais são a premissa à melhoria da conduta dos agentes públicos e podem ser concretizadas, por exemplo, por meio de campanhas informativas e por cursos de capacitação orientados a todos os agentes públicos;

(ii) controles de acesso físico e lógico[67]: a gestão do controle de acesso às informações é necessária ao fim de se ofertar o acesso aos dados pessoais exclusivamente àqueles que detenham propósitos legítimos, específicos e explícitos, e deve estar orientada a partir do tipo de espaço no qual encontram-se as informações – que podem encontrar-se, documentalmente, em espaços físicos, como salas e almoxarifados, e em espaços digitais, como em dispositivos eletrônicos e em nuvem. O controle de acesso físico, nesse sentido, diz respeito aos controles de segurança física e do ambiente relativas à manutenção de controles de acesso aos espaços físicos, como chaves de segurança – que podem ser físicas, como fechaduras manuais ou digitais, como fechaduras eletrônicas. O controle de acesso lógico, por sua vez, se refere à manutenção do

[64] Como "*hardware"* ("*recurso físico*") e "*software"* ("*recurso tecnológico*"), utilizados para o armazenamento de documentos em formatos digital.
[65] XAVIER, Fábio Correa. *Recomendações de Segurança da Informação para Municípios de Pequeno Porte na jornada de adequação à LGPD.* São Paulo: Tribunal de Contas do Estado de São Paulo, 21 out. 2021. Disponível em: <https://www.tce.sp.gov.br/6524-artigo-recomendacoes-seguranca-adequacao-lgpd-por-fabio-xavier>. Acesso em: 03 nov. 2022.
[66] Item 7, "*segurança em recursos humanos*", da norma ABNT ISO/IEC nº 29151:2020.
[67] Item 9, "*controle de acesso*", da norma ABNT ISO/IEC nº 29151:2020.

controle de acesso em espaços digitais, como aplicações utilizadas pela organização, e que podem ser concretizadas, por exemplo, a partir de política de senhas, que:

a. desabilite senhas padrão de fabricantes e que detenha requisitos à elaboração e duração de novas senhas;
b. adote o princípio do menor privilégio, ou seja, que atribua ao agente o nível de acesso estritamente necessário para a realização de suas atribuições;
c. recomende o não compartilhamento de senhas; e
d. recomende a utilização de autenticação com múltiplos fatores, ou seja, com o uso, para além das senhas, por exemplo, de biometria, de reconhecimento facial, de *tokens* ou de autorização superior para o acesso.

(iii) controles de segurança física e do ambiente[68]: a gestão da segurança física e do ambiente deve estar pautada pelo princípio da necessidade (art. 6º, inc. III, LGPD), a fim de que haja a limitação da retenção de dados pessoais 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 pessoais, com atenção para:

a. configuração segura das estações de trabalho, incluindo a configuração segura de dispositivos pessoais para o acesso aos sistemas da organização (política "*Bring Your Own Device*" – BYOD);
b. não utilização de dispositivos de armazenamento externo, como HDs ("*Hard Disks*") e "*pendrives*";
c. gestão de uma política de cópias de segurança ("*backup*"); e
d. utilização de controles criptográficos[69].

(iv) controles de segurança nas comunicações[70]: a gestão da segurança do uso compartilhado e do compartilhamento de dados pessoais deve estar pautada pela:

a. utilização de protocolos de comunicação seguros, como TLS ("*Transport Layer Security*") e HTTPS ("*Hyper Text Transfer Protocol Secure*");
b. utilização de tecnologias de proteção de tráfego de pacotes de dados, como sistemas de "*firewall*", "*antivirus*", "*antispyware*" e "*antispam*";
c. gestão de uma política de cópias de segurança ("*backup*"); e
d. utilização de controles criptográficos[71].

[68] Item 11, "*segurança física e do ambiente*", da norma ABNT ISO/IEC nº 29151:2020.
[69] Item 10, "*criptografia*", da norma ABNT ISO/IEC nº 29151:2020.
[70] Item 13, "*segurança nas comunicações*", da norma ABNT ISO/IEC nº 29151:2020.

(v) controles de conformidade das licitações, contratos administrativos, convênios e instrumentos congêneres[72]: no âmbito dos controles, é necessário que todos as licitações, contratos administrativos, convênios e instrumentos congêneres em vigor, assim como os futuros, sejam e estejam adequados à segurança da informação e à salvaguarda à privacidade e à proteção de dados pessoais. Nesse sentido, quando do uso de serviços de pessoas físicas ou jurídicas contratadas ou parceiras da organização, como serviços de nuvem, é recomendável o uso de Acordo de Nível de Serviço – ANS ("*Service Level Agreement*" – SLA), ou seja, do compromisso do contratante ou parceiro – por meio, por exemplo, da aposição de cláusula específica no instrumento – da manutenção e da comprovação do mesmo nível de segurança da informação e de salvaguarda à privacidade e à proteção de dados pessoais havido no Poder Executivo do Município de São Paulo, quando da hipótese de tratar dados pessoais em nome daquele, ou mesmo quando da hipótese de uso compartilhado ou compartilhamento de dados pessoais com aquela.

[72] Item 10, "*criptografia*", da norma ABNT ISO/IEC nº 29151:2020.
[72] Item 18, "*compliance*", da norma ABNT ISO/IEC nº 29151:2020.

Referências bibliográficas

ABNT. Associação Brasileira de Normas Técnicas. ABNT ISO/TR nº 31004:2015. *Gestão de riscos* – guia para implementação da ABNT NBR ISO 31000. Rio de Janeiro: ABNT, 2015.

ABNT. Associação Brasileira de Normas Técnicas. ABNT NBR ISO nº 31000:2018. *Gestão de riscos* – diretrizes. Rio de Janeiro: ABNT, 2018.

ABNT. Associação Brasileira de Normas Técnicas. ABNT NBR ISO/IEC nº 27001:2013. *Tecnologia da informação* – técnicas de segurança – sistemas de gestão da segurança da informação – requisitos. Rio de Janeiro: ABNT, 2013.

ABNT. Associação Brasileira de Normas Técnicas. ABNT NBR ISO/IEC nº 27002:2022. *Segurança da informação, segurança cibernética e proteção à privacidade* – controles de segurança da informação. Rio de Janeiro: ABNT, 2022.

ABNT. Associação Brasileira de Normas Técnicas. ABNT NBR ISO/IEC nº 27701:2020. *Técnicas de segurança* – extensão da ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 para gestão da privacidade da informação – requisitos e diretrizes. Rio de Janeiro: ABNT, 2020.

ABNT. Associação Brasileira de Normas Técnicas. ABNT NBR ISO/IEC nº 29100:2020. *Tecnologia da informação* – técnicas de segurança – estrutura de privacidade. Rio de Janeiro: ABNT, 2020.

ABNT. Associação Brasileira de Normas Técnicas. ABNT NBR ISO/IEC nº 27018:2021. Tecnologia da informação – técnicas de segurança – código de prática para proteção de dados pessoais em nuvens públicas que atuam como operadores de dados pessoais. Rio de Janeiro: ABNT, 2021.

ABNT. Associação Brasileira de Normas Técnicas. ABNT NBR ISSO/IEC nº 29151/2020. *Tecnologia da informação* – técnicas de segurança – código de prática para proteção de dados pessoais. Rio de Janeiro: ABNT, 2020.

ABNT. Associação Brasileira de Normas Técnicas. ABNT NBR/IEC nº 31010:2021. *Gestão de riscos* – técnicas para o processo de avaliação de riscos. Rio de Janeiro: ABNT, 2021.

ALLEN, Anita. *Unpopular Privacy*: What Must We Hide? Oxford, UK: Oxford University Press, 2011.

ALVES, Gustavo Alberto. *Segurança da Informação*: uma visão inovadora da gestão. Rio de Janeiro: Ciência Moderna, 2006, p. 15.

BACCIOTTI, Karina Joelma. *Direitos Humanos e novas Tecnologias da Informação e Comunicação*: o acesso à Internet como Direito Humano. Dissertação de Mestrado. Pontifícia Universidade Católica de São Paulo, São Paulo, 2014. Disponível em: https://tede2.pucsp.br/handle/handle/6578

BELL, Daniel. The Coming of Post-Industrial Society. *The Educational Forum*, EUA, vol. 40, n. 04, 1976, pp. 574-579.

BRASIL. Autoridade Nacional de Proteção de Dados. Estudo Preliminar. *Hipóteses legais aplicáveis ao tratamento de dados pessoais de crianças e adolescentes*. Brasília, Autoridade Nacional de Proteção de Dados, 2022. Disponível em: <https://www.gov.br/participamaisbrasil/blob/baixar/17636>. Acesso em: 04 out. 2022.

BRASIL. Autoridade Nacional de Proteção de Dados. Guia Orientativo. *Tratamento de dados pessoais pelo Poder Público*. Brasília, Autoridade Nacional de Proteção de Dados, 2022. Disponível em: <https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-poder-publico-anpd-versao-final.pdf>. Acesso em: 04 out. 2022.

BRASIL. Constituição da República Federativa do Brasil de 1988. Brasília, *Diário Oficial da União*, Brasília, 05 out. 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em: 17 nov. 2022.

BRASIL. Lei Federal nº 10.406, de 10 de janeiro de 2002. Institui o Código Civil. Brasília, *Diário Oficial da União*, 11 de janeiro de 2002. Disponível em: <https://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm>. Acesso em: 17 nov. 2022.

BRASIL. Lei Federal nº 12.527, de 18 de novembro de 2011. Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. Brasília, *Diário Oficial da União*, 18 de novembro de 2011. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm>. Acesso em: 17 nov. 2022.

BRASIL. Lei Federal nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, *Diário Oficial da União*, 24 de abril de 2014. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 17 nov. 2022.

BRASIL. Lei Federal nº 13.146, de 06 de julho de 2015. Institui a Lei Brasileira de Inclusão da Pessoa com Deficiência (Estatuto da Pessoa com Deficiência). Brasília, *Diário Oficial da União*, 07 de julho de 2015. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/l13146.htm>.

BRASIL. Lei Federal nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, *Diário Oficial da União*, 15 de agosto de 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: 04 out. 2022.

BRASIL. Lei Federal nº 14.010, de 10 de junho de 2020. Dispõe sobre o Regime Jurídico Emergencial e Transitório das relações jurídicas de Direito Privado (RJET) no período da pandemia do coronavírus (COVID-19). Brasília, *Diário Oficial da União*, 10 de junho de 2020. Disponível em: < https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/lei/L14010.htm>. Acesso em: 17 nov. 2022.

BRASIL. Lei Federal nº 8.069, de 13 de julho de 1990. Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências. Brasília, *Diário Oficial da União*, 16 de julho de 1990.

Disponível em: <https://www.planalto.gov.br/ccivil_03/leis/l8069.htm>. Acesso em: 17 nov. 2022.

BRASIL. Lei Federal nº 8.935, de 18 de novembro de 1994. Regulamenta o art. 236 da Constituição Federal, dispondo sobre serviços notariais e de registro. Brasília, *Diário Oficial da União*, 21 de novembro de 1994. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l8935.htm>. Acesso em: 17 nov. 2022.

BRASIL. Lei Federal nº 9.307, de 23 de setembro de 1996. Dispõe sobre a arbitragem. Brasília, *Diário Oficial da União*, 24 de setembro de 1996. Disponível em: <https://www.planalto.gov.br/ccivil_03/leis/l9307.htm>. Acesso em: 17 nov. 2022.

BRASIL. Lei Federal nº 9.507, de 12 de novembro de 1997. Regula o direito de acesso a informações e disciplina o rito processual do *habeas data*. Brasília, *Diário Oficial da União*, 13 de novembro de 1997. Disponível em: <https://www.planalto.gov.br/ccivil_03/leis/l9507.htm>. Acesso em: 17 nov. 2022.

BRASIL. Lei Federal nº 9.784, de 29 de janeiro de 1999. Regula o processo administrativo no âmbito da Administração Pública Federal. Brasília, *Diário Oficial da União*, 1º de fevereiro de 1999. Disponível em: <https://www.planalto.gov.br/ccivil_03/leis/l9784.htm>. Acesso em: 17 nov. 2022.

BRASIL. Supremo Tribunal Federal. ADI nº 6.649/DF e ADPF nº 695/DF. Julgamento Conjunto. Data de Julgamento: 15 set. 2022. Data de Publicação: 15 set. 2022. Brasília, *Diário Oficial da Justiça Eletrônico*, 15 set. 2022.

CASTELLS, Manuel. *The Information Age*. Economy, Society, and Culture. The Rise of The Network Society. Chichester, Reino Unido: Wiley-Blackwell, 2010.

CAVOUKIAN, Ann. *Privacy by Design*. The 7 Foundational Principles. Toronto: Information and Privacy Commissioner of Ontario, 2011, pp. 01-02. Disponível em: <https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf>. Acesso em: 04 out. 2022.

PRIBERAM. *Dicionário Priberam da Língua Portuguesa*. Lisboa: Priberam, 2022. Disponível em: <https://dicionario.priberam.org/risco>. Acesso em: 03 jan. 2023.

FALCÃO, Daniel; PEROLI, Kelvin. As novas abordagens da privacidade: contextos, tipos e dimensões. *Migalhas*, Migalhas de Proteção de Dados Pessoais, 30 dez. 2021. Disponível em: <https://www.migalhas.com.br/coluna/migalhas-de-protecao-de-dados/357252/as-novas-abordagens-da-privacidade-contextos-tipos-e-dimensoes>. Acesso em: 04 out. 2022.

FALCÃO, Daniel; PEROLI, Kelvin. Imagem, dado pessoal sensível? *Consultor Jurídico*, Observatório Constitucional, 28 maio 2022. Disponível em: <https://www.conjur.com.br/2022-mai-28/observatorio-constitucional-imagem-dado-pessoal-sensivel>. Acesso em: 17 nov. 2022.

FALCÃO, Daniel; PEROLI, Kelvin. São Paulo, 22 de julho de 2022: as novas abordagens da proteção de dados pessoais no âmbito da Administração Pública Municipal. *Migalhas*, Migalhas de Proteção de Dados Pessoais, 22 jul. 2022. Disponível em: <https://www.migalhas.com.br/coluna/migalhas-de-protecao-de-dados/370310/protecao-de-dados-pessoais-na-administracao-publica-municipal>. Acesso em: 04 out. 2022.

KOOPS, Bert-Jaap; NEWELL, Bryce Clayton; TIMAN, Tjerk; ŠKORVÁNEK, Ivan; CHOKREVSKI, Tomislav; GALIČ, Maša. A Typology of Privacy. *University of Pennsylvania Journal of International Law*, vol. 38, n. 2, 2017, art. 4, pp. 483-575.

LIMA, Cíntia Rosa Pereira de. A responsabilidade civil dos provedores de aplicação de internet por conteúdo gerado por terceiro antes e depois do Marco Civil da Internet (Lei Federal nº 12.965/2014). *Revista da Faculdade de Direito*, Universidade de São Paulo, São Paulo, v. 110, jan./dez. 2015, pp. 155-176. Disponível em: <https://www.revistas.usp.br/rfdusp/article/view/115489>. Acesso em: 17 nov. 2022.

LIMA, Cíntia Rosa Pereira de; PEROLI, Kelvin A aplicação da Lei Geral de Proteção de Dados Pessoais do Brasil no tempo e no espaço. *In:* LIMA, Cíntia Rosa Pereira de (org.*). Comentários à Lei Geral de Proteção de Dados*. São Paulo: Almedina, 2020, pp. 69-100.

MASCARENHAS NETO, Pedro Tenório; ARAÚJO, Wagner Junqueira. *Segurança da Informação:* uma visão sistêmica para implantação em organizações. João Pessoa: Editora UFPB, 2019.

MENDES, Laura Schertel Ferreira. Habeas data e autodeterminação informativa: os dois lados de uma mesma moeda. *Direitos Fundamentais & Justiça*, Belo Horizonte, ano 12, n. 39, jul./dez. 2018, pp. 185-216. Disponível em: <https://doi.org/10.30899/dfj.v12i39.655>. Acesso em: 17 nov. 2022.

NISSENBAUM, Helen. *Privacy in Context*. Technology, Policy, and the Integrity of Social Life. Stanford, EUA: Stanford University Press, 2010.

PENTEADO, Luciano de Camargo. O direito à vida, o direito ao corpo e às partes do corpo, o direito ao nome, à imagem e outros relativos à identidade e à figura social, inclusive intimidade. *Revista de Direito Privado*, São Paulo, vol. 13, n. 49, jan./mar. 2012, pp. 73-109.

PEROLI, Kelvin; FALEIROS JÚNIOR, José Luiz de Moura. Comentários aos arts. 50 e 51 da LGPD. *In:* MARTINS, Guilherme Magalhães; LONGHI, João Victor Rozatti; FALEIROS JÚNIOR, José Luiz de Moura (orgs.). *Comentários à Lei Geral de Proteção de Dados Pessoais.* Indaiatuba: Foco, 2022, pp. 461-479.

REALE, Miguel. *Filosofia do Direito*. 11ª ed. São Paulo: Saraiva, 1986.

SÃO PAULO (Cidade). Decreto Municipal nº 53.623, de 12 de dezembro de 2012. Regulamenta a Lei Federal n° 12.527, de 18 de novembro de 2011, no âmbito do Poder Executivo, estabelecendo procedimentos e outras providências correlatas para garantir o direito de acesso à informação, conforme especifica. São Paulo, Diário Oficial da

SÃO PAULO (Cidade). Decreto Municipal nº 59.767, de 15 de setembro de 2020. Regulamenta a aplicação da Lei Federal nº 13.709, de 14 de agosto de 2018 – Lei Geral de Proteção de Dados Pessoais (LGPD) - no âmbito da Administração Municipal direta e indireta. São Paulo, *Diário Oficial da Cidade de São Paulo*, 15 de setembro de 2020. Disponível em: <https://legislacao.prefeitura.sp.gov.br/leis/decreto-59767-de-15-de-setembro-de-2020>. Acesso em: 04 out. 2022.

SÃO PAULO (Cidade). Instrução Normativa CGM/SP nº 01, de 21 de julho de 2022. Estabelece disposições referentes ao tratamento de dados pessoais no âmbito da Administração Pública Municipal de São Paulo. São Paulo, *Diário Oficial da Cidade*, 22 de julho de 2022. Disponível em:

<https://legislacao.prefeitura.sp.gov.br/leis/instrucao-normativa-controladoria-geral-do-municipio-cgm-1-de-21-de-julho-de-2022>. Acesso em: 04 out. 2022.

SÃO PAULO (Cidade). Lei Municipal nº 8.989, de 29 de outubro de 1979. Dispõe sobre o estatuto dos funcionários públicos do município de São Paulo, e dá providências correlatas. São Paulo*, Diário Oficial da Cidade de São Paulo*, 29 de outubro de 1979. Disponível em: < http://legislacao.prefeitura.sp.gov.br/leis/lei-8989-de-29-de-outubro-de-1979>. Acesso em: 04 out. 2022.

SÊMOLA, Marcos. *Gestão de Segurança da Informação*: uma visão executiva. São Paulo: Editora Campus, 2003, p. 09.

SOLOVE, Daniel J. A Taxonomy of Privacy. *University of Pennsylvania Law Review*, jan. 2006, vol. 154, n. 3, pp. 477–560. Disponível em: <https://scholarship.law.upenn.edu/penn_law_review/vol154/iss3/1/>. Acesso em: 17 nov. 2022.

UNIÃO EUROPEIA. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Bruxelas, *Jornal Oficial da União Europeia*, 27 abril 2016. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016R0679>. Acesso em: 17 nov. 2022.

WARREN, Samuel; BRANDEIS, Louis. The Right to Privacy. *Harvard Law Review*, v. IV, n. 05, dez. 1890. Disponível em: <http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html>. Acesso em: 04 out. 2022.

WESTIN, Alan Furman. *Privacy and Freedom*. New York, EUA: Atheneum, 1967.

XAVIER, Fábio Correa. *Recomendações de Segurança da Informação para Municípios de Pequeno Porte na jornada de adequação à LGPD*. São Paulo: Tribunal de Contas do Estado de São Paulo, 21 out. 2021. Disponível em: <https://www.tce.sp.gov.br/6524-artigo-recomendacoes-seguranca-adequacao-lgpd-por-fabio-xavier>. Acesso em: 03 nov. 2022.

CIDADE DE
SÃO PAULO
CONTROLADORIA
GERAL DO MUNICÍPIO