CARTILHA DE GOVERNANÇA EM

PROTEÇÃO DE DADOS

PARA MUNICÍPIOS

MENTE ABERTA

RGB
DA GOVERNANÇA À ESPERANÇA

CARTILHA DE GOVERNANÇA EM

PROTEÇÃO DE DADOS

PARA MUNICÍPIOS

Lucas Paglia
Bruno Ferola
Fábio Correa Xavier

MENTE ABERTA
IGCP
INSTITUTO LATINO-AMERICANO DE GOVERNANÇA E COMPLIANCE PÚBLICO
RGB
DA GOVERNANÇA À ESPERANÇA
Enap

© 2021 Rede Governança Brasil (RGB) e Instituto Latino-Americano de Governança e Compliance Público (IGCP).

Qualquer parte desta publicação pode ser reproduzida, desde que citada a fonte. Todavia, a reprodução não autorizada para fins comerciais desta publicação, no todo ou em parte, constitui violação dos direitos autorais, conforme Lei nº 9.610/1998.

Distribuição gratuita - Venda proibida

DIRETORIA EXECUTIVA REDE GOVERNANÇA BRASIL
Presidente – Petrus Elesbão Lima da Silva
Vice–presidente – Flávio Feitosa Costa

DIRETOR ADMINISTRATIVO
Luís Fernando Pires Machado

DIRETOR FINANCEIRO
Henrique Farinon

DIRETOR DE ASSUNTOS ESTRATÉGICOS
Douglas Avedikian

DIRETOR JURÍDICO
Leonardo Andreotti Paulo de Oliveira

DIRETOR DE RELAÇÕES INTERNACIONAIS
Macleuler Costa Lima

DIRETORA DE RELAÇÕES INSTITUCIONAIS
Elise Eleonore de Brites

CONSELHO DE ADMINISTRAÇÃO
Presidente – Prof. Luiz Antonio Peixoto Valle
Vice–presidente – Cristiane Geiss Nardes Farinon
Conselheiro – Petrus Elesbão Lima da Silva
Conselheira – Vera Raquel Lopes Linhares da Silva
Conselheiro – Paulo Renato Menzel
Conselheiro – João Felipe Cunha Pereira
Conselheiro – Francisco Alexandre Colares Melo Carlos
Conselheira – Carla Simone Viana Lage
Conselheira – Rosimar da Silva Suzano

CONSELHO DE ÉTICA
Presidente – Roberta Muniz Codignoto
Conselheiro Titular – Bruno Galvão Ferola
Conselheira Titular – Marcella Blok
Conselheira Suplente – Clarissa Freitas Rodrigues de Lima Carvalho

CONSELHO FISCAL
Presidente – Renata Andrade Santos
Conselheiro Titular – Lucas Barbosa Paglia
Conselheiro Titular – Renato Lauri Breunig
Conselheiro Suplente – Walter Marinho

OUVIDORIA
Ouvidor – Pedro Henrique Andrade Souza

Coordenação do E–book

Comitê de Governança em LGPD
Lucas Paglia
Bruno Ferola
Fábio Correa Xavier

Comitê de Capacitação RGB
Cristiane Nardes Farinon
Robson Loureiro

Comitê de Governança em Educação
Ana Paula Arbache
Elise Brites

Comitê Cartilha de Governança RGB
Cristiane Nardes Farinon
Douglas Avedikian
Claudio Sarian
Ariene Rezende do Carmo Castro
Pryscilla Pereira de Araújo
Isabel Cristiane Loureiro
Elena Pacita Lois Garrido

Grupo de Estudos Rede Governança Brasil e Escola Nacional de Administração Pública
Regina Luna
Mariana Montenegro

Instituto Latino – Americano de Governança e Compliance Público – IGCP

Presidente
Marcelo Becker

Conselho Fiscal
Presidente do Conselho Fiscal – João Benício Aguiar
Conselheira – Izabela Zanotelli Collares
Conselheiro – Luiz Gustavo Wiechoreki

Rede Governança Brasil -
Cartilha de Governança em Proteção de Dados para Municípios / Lucas Paglia, Bruno Ferola, Fábio Xavier. Salvador, BA; Brasíllia, DF: Editora Mente Aberta; Rede Governança Brasil, 27 de outubro de 2021. [E-book].

42.553 Kb
65 p.
ISBN: 978-65-86483-65-9

1. Governança. 2. Proteção de dados. 3. Municípios. I. Paglia, Lucas. II. Ferola, Bruno. III. Xavier, Fábio. IV. Título.

CDD 025.1

PALAVRAS DO EMBAIXADOR DA REDE GOVERNANÇA BRASIL

Caros,

Esta cartilha sobre a Lei Geral de Proteção de Dados (LGPD) tem, como objetivo, esclarecer os pontos relevantes sobre o tema e trazer orientações quanto à sua aplicabilidade, além de estabelecer conceitos e princípios aplicados e sugerir algumas ações básicas para o programa de implementação.

A cartilha, ademais, traz importantes aspectos sobre a importância da governança através da implantação e integração entre liderança, estratégia e controle, com os chamados, mecanismos de governança em privacidade, como forma de compreensão de como a direção está presente nas formas de avaliação, direção e monitoramentos contínuos da gestão.

A Lei Geral de Proteção de Dados surge em um momento crucial devido ao alto nível de informações existentes e de inovações tecnológicas que permitem que o tratamento de dados seja realizado de diversas maneiras, e, por isso, é de suma importância a preocupação com as mudanças que a referida lei vai gerar em toda a sociedade, empresas, fundações, cooperativas, órgãos públicos e secretarias públicas, bem como para o próprio cidadão, titular de dados pessoais.

Essa transformação envolve considerar a privacidade e a proteção de dados pessoais em todas as etapas das atividades desenvolvidas na sociedade, desde o seu momento inicial, em que são colhidas as informações pertinentes, até à exclusão dos dados pessoais tratados.

O impacto de uma lei sobre proteção de dados pessoais é o equilíbrio das assimetrias de poder sobre os dados pessoais existentes entre o titular dos dados pessoais e aqueles que os utilizam e compartilham.

Agradeço, de forma especial, aos membros e aos coordenadores do Comitê Governança na Prática da Rede Governança Brasil (RGB), que estão trabalhando arduamente na disseminação das boas práticas de privacidade e proteção de dados.

Estimo que esta cartilha sobre governança em proteção de dados para municípios seja o caminho para avançar na transparência no uso dos dados pessoais das pessoas naturais e como forma de

harmonizar o controle que cada titular tem sobre os seus dados, em atenção ao direito fundamental de proteção à privacidade.

Desejo que, como relator da Lei Geral de Proteção de Dados (LGPD) no Tribunal de Contas da União (TCU), possa auxiliá-los a dar esse grande passo na educação sobre privacidade e proteção de dados, e que seja exemplo para todas as instituições o uso das boas práticas para transformar a nossa sociedade em um ambiente mais seguro para o tratamento de dados pessoais.

Fraterno abraço!

Augusto Nardes

(Ministro do Tribunal de Contas da União e Embaixador da Rede Governança Brasil)

APRESENTAÇÃO

Esta cartilha tem, como objetivo, fornecer orientações sobre a governança na aplicação da Lei Geral de Proteção de Dados Pessoais (LGPD), Lei n. 13.0709/2018, aos(às) prefeitos(as) brasileiros(as). Em vigor desde setembro de 2020, a lei traz diversas exigências e, para que os municípios consigam cumpri-las, é necessário definir estratégias, metas e objetivos, com ferramentas de controle e monitoramento capazes de identificar previamente os riscos no tratamento de dados pessoais e a melhor forma de inibi-los.

Para que os municípios consigam atingir um nível adequado de proteção de dados, precisaram realizar a implementação de uma cultura de proteção de dados pessoais que atinja todos os funcionários da Administração Pública e a sociedade.

O objetivo desta cartilha é contribuir com a implementação da cultura de proteção de dados nos dos municípios e garantir a conformidade com a lei a partir das diretrizes da governança.

Esta cartilha deverá ser atualizada, aperfeiçoada e ampliada permanentemente, uma vez que foi elaborada durante os meses de abril e maio de 2021. Neste momento, a LGPD vigora apenas em parte, pois as suas sanções serão aplicáveis apenas a partir de agosto de 2021 e a Autoridade Nacional de Proteção de Dados (ANPD), órgão responsável pela aplicação e por emitir diretrizes sobre a lei, ainda não está em funcionamento.

SUMÁRIO

1 O QUE É GOVERNANÇA? 13

2 GOVERNANÇA PÚBLICA E SUA IMPORTÂNCIA 15

2.1 Programa de Liderança para Desenvolvimento Regional (LIDER) 15

3 O QUE É PRIVACIDADE E POR QUE DEVEMOS PROTEGÊ-LA? 18

4 DO QUE TRATA A LEI GERAL DE PROTEÇÃO DE DADOS? 20

5 GLOSSÁRIO SOBRE A LGPD 22

6 O TRATAMENTO DE DADOS PESSOAIS 26

6.1 Estrutura normativo da Proteção de Dados 26

6.2 Princípios da Lei Geral de Proteção de Dados 28

6.3 Bases Legais para o Tratamento de Dados Pessoais 29

6.4 Compartilhamento de Dados Pessoais 32

6.5 Direitos dos Titulares 32

6.6 Comunicação com a ANPD e com os titulares de dados pessoais 33

6.7 O término do tratamento dos dados pessoais 34

6.8 A eliminação dos dados pessoais 34

7 AGENTES DE TRATAMENTO 36

7.1 Definição 36

7.2 Obrigações e responsabilidades 36

7.3 Encarregado pelo tratamento de dados pessoais/*data protection officer* (DPO) 37

7.4 Comitê de Privacidade e Proteção de Dados Pessoais 37

8 MUNICÍPIO COMO CONTROLADOR 39

9 DEFINIÇÃO DE UM MODELO DE GOVERNANÇA DO MUNICÍPIO 42

10 A GOVERNANÇA EM PROTEÇÃO DE DADOS E SEUS BENEFÍCIOS 44

11 COMO IMPLEMENTAR UMA GOVERNANÇA EM PROTEÇÃO DE DADOS NA PRÁTICA? 48

11.1 Diagnóstico 48

11.2 Execução das prioridades 49

11.3 Execução dos pontos complementares 49

11.2 Monitoramento 49

12 SEGURANÇA DA INFORMAÇÃO 52

12.1 Políticas de segurança da informação 52

12.2 Incidentes 53

12.2.1 Plano de resposta a incidente de segurança da informação envolvendo dados pessoais e dados pessoais sensíveis 54

12.2.2 Fluxo de medidas necessárias em caso de incidentes com dados pessoais 55

12.2.3 Fluxo de medidas necessárias em caso de incidentes com dados pessoais sensíveis 56

12.3 Supervisão 57

12.3.1 Medidas para a mitigação de riscos 57

13 A IMPORTÂNCIA DA PROTEÇÃO DE DADOS NO SISTEMA EDUCACIONAL - GOVERNANÇA DE DADOS PESSOAIS: UMA QUESTÃO VOLTADA PARA O SISTEMA EDUCACIONAL BRASILEIRO 59

REFERÊNCIAS 64

1 O QUE É GOVERNANÇA?

Etimologicamente, a palavra governança significa o ato de governar-se, entretanto restringir a palavra apenas ao seu significado oficial, sem contar as suas origens e as atuais interpretações, não seria o mais correto a se fazer.

A palavra governança deriva do verbo grego *kubernaein* [*kubernáo*] que, metaforicamente, significa dirigir e, nos últimos anos, vem cada vez mais sendo atribuída à gestão pública e ao meio corporativo.

Na gestão pública, conforme o Decreto n. 9.203, de 22 de novembro de 2017, em seu art. 2.º, I, é definida como:

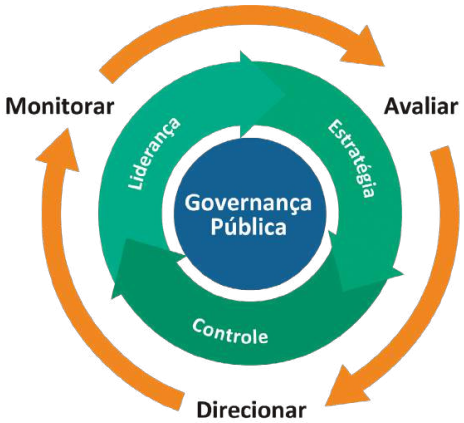
> Governança pública – conjunto de mecanismos de liderança, estratégia e controle postos em prática para avaliar, direcionar e monitorar a gestão, com vistas à condução de políticas públicas e à prestação de serviços de interesse da sociedade; [...]

Dessa forma, é possível compreender que a governança está presente nas formas de avaliação, direção e monitoramentos contínuos da gestão, com o intuito de potencializar suas estruturas e atender aos objetivos da instituição.

No meio corporativo, a definição apresentada no site do Instituto Brasileiro de Governança Corporativa (IBGC) sobre sovernança corporativa é: "o sistema pelo qual as empresas e demais organizações são dirigidas, monitoradas e incentivadas, envolvendo os relacionamentos entre sócios, conselho de administração, diretoria, órgãos de fiscalização e controle e demais partes interessadas".

Em resumo, pode-se dizer que a governança, em ambiente público, ou privado, refere-se ao conjunto de práticas que uma empresa ou órgão público adota para consolidar as suas estruturas e sua gestão, indicando a direção a ser seguida, demonstrando claramente quais as estratégias admitidas a partir da liderança e monitorando os resultados.

Em outras palavras, a governança auxilia o(a) prefeito(a) a organizar a gestão.



2 GOVERNANÇA PÚBLICA E SUA IMPORTÂNCIA

Conforme mencionamos anteriormente, a governança pública atua junto aos órgãos públicos consolidando as estruturas com objetivo de elevar sua capacidade de gestão, aumentando seu poder de resposta à sociedade.

Os municípios atendem às demandas da sociedade por meio de políticas públicas, que são as ações, metas e planos definidos pelo governo municipal, visando ao bem-estar da sociedade e seus interesses, sendo, a política pública, a base de sustentação de uma sociedade desenvolvida.

Os órgãos públicos possuem objetivos que, por vezes, são frustrados por conta de atitudes de seus integrantes ou dirigentes. Isso acontece quando estes utilizam a entidade pública para satisfazer seus próprios interesses em desfavor da instituição dirigida, por meio de ações corruptas, ilícitas ou até mesmo por incompetência.

As ações de governança visam à diminuição do risco dessas situações, pois com a definição de uma direção, a estratégia definida e controle contínuo dos processos e atividades, a instituição conseguirá mapear, de forma mais rápida e assertiva, quaisquer desvios ocasionados em seu interior, bem como inibi-los.

2.1 PROGRAMA DE LIDERANÇA PARA DESENVOLVIMENTO REGIONAL (LIDER)

O Sebrae desenvolveu um projeto com o objetivo de sanar a ausência de uma atuação integrada entre o poder público, instituições privadas e do terceiro setor para a promoção do desenvolvimento sustentável dos territórios brasileiros. O programa utiliza um método aplicado em mais de 600 municípios brasileiros, mobilizando pessoas e instituições regionais, fortalecendo as identidades dos municípios participantes.

Durante um ano, o programa reúne mensalmente as principais lideranças locais com o objetivo de criar uma visão de futuro compartilhada, sendo representada em uma agenda de desenvolvimento para a região, fortalecendo a governança regional de forma representativa, articuladora e institucionalizada para a implantação dessa agenda com a comunidade.

Conforme o Guia do Prefeito Empreendedor, disponível no site do Sebrae, os principais resultados do Programa LIDER, são:

- engajamento dos empresários e sociedade civil nos desafios da região;

• mudança de paradigma com os atores locais: de “cobrar” para “cooperar”;

• melhoria do diálogo de cada prefeitura com outras lideranças do seu município e de municípios vizinhos;

• início de um ciclo positivo de cooperação entre municípios, envolvendo os setores público, privado e terceiro setor;

• uma agenda de desenvolvimento da região para ser apresentada e “abraçada” pelas lideranças locais nas esferas municipais, regionais, estaduais e nacional;

• incentivo à atração de parceiros e recursos.


PRIVACY

3 O QUE É PRIVACIDADE E POR QUE DEVEMOS PROTEGÊ-LA?

O termo privacidade é recente e surge entre os séculos XVII e XVIII, em resposta aos regimes absolutistas da época. Entretanto, a privacidade se tornou uma questão passível de proteção pelo Estado somente ao final do século XIX, quando foram inventadas as câmeras de fotografia instantâneas e se iniciou a ampla circulação de jornais.

O termo privacidade foi associado, por um bom tempo, com isolamento, o chamado “direito de estar só”, em um artigo publicado por Samuel D. Warren e Louis D. Brandeis, nos EUA, no final do século XIX.

Não obstante, ao passar do tempo e com a crescente revolução tecnológica, assim como a palavra governança, o termo privacidade foi ganhando novos significados, como o dos indivíduos serem livres para tomar suas próprias decisões, a garantia do direito de não revelar seus pensamentos, o direito de não ter seu espaço violado (tanto o físico quanto o digital).

Apesar de o Brasil garantir, na Constituição do Império, em 1824, o direito à inviolabilidade do domicílio e suas correspondências, foi apenas na Constituição Federal de 1988 que a proteção à intimidade e a garantia à inviolabilidade do sigilo das comunicações, da vida privada, da honra e da imagem das pessoas foi mencionado, assegurando a privacidade dos brasileiros.

Com os avanços tecnológicos surgiram novas soluções que facilitaram o nosso dia a dia, todavia também surgiram novos problemas que ameaçam cada vez mais a nossa privacidade.

4 DO QUE TRATA A LEI GERAL DE PROTEÇÃO DE DADOS?

A Lei n. 13.709, de agosto de 2018, amplamente conhecida como Lei Geral de Proteção de Dados Pessoais (LGPD), baseou-se no Regulamento Geral sobre a Proteção de Dados (GDPR) que, apesar de ser idealizado desde 2012, devido ao aumento exponencial da utilização de dados pessoais com a internet e a utilização das redes sociais, acabou tornando-se uma resposta dos países aos escândalos envolvendo a empresa Cambridge Analytica, o Facebook e diversas campanhas políticas ao redor do planeta, incluindo as campanhas de Donald Trump à presidência dos EUA, em 2016, e a campanha a favor do Brexit, em 2019.

Desse modo, a lei visa a proteger as pessoas físicas em relação a suas informações pessoais, impondo regras em seu tratamento, definindo hipóteses para cada atividade de tratamento.

A LGPD, em seu art. 1.º, já informa que a lei dispõe sobre o tratamento de dados pessoais, tanto por pessoa jurídica de direito público quanto privado. Desse modo, existe a necessidade de adequação por parte dos municípios.

5 GLOSSÁRIO SOBRE A LGPD

LGPD: Lei Geral de Proteção de Dados – Lei n. 13.709/2018 – A LGPD possui, como objetivo, regulamentar as atividades que se utilizam de dados pessoais em território nacional, por pessoa natural ou jurídica de direito público ou privado, em ambientes físicos ou digitais. Dessa forma, a LGPD poderá compreender uma relação com estrangeiro, caso parte do processo seja realizado no Brasil. Importante mencionar que a LGPD foi elaborada para proteção de dados que identifiquem uma pessoa natural, e não informações sigilosas de empresas ou negócios.

Pessoa natural – Todos os seres humanos, independentemente de sexo, etnia, idade, orientação sexual, religião, nacionalidade, filiação partidária ou quaisquer outras características, possuindo direitos e obrigações.

Titular de dados pessoais – A pessoa natural a quem pertence o dado pessoal.

Documento físico e documento digital – Os documentos físicos são aqueles elaborados em suportes físicos, por exemplo, em papel. Já os documentos digitais são informações registradas, codificadas em forma analógica ou em dígitos binários, acessíveis e interpretáveis por meio de um equipamento eletrônico.

Dado pessoal – é qualquer informação que identifique ou possa identificar uma pessoa natural, de acordo com a LGPD.

Dados que identificam uma pessoa natural – São as informações que identificam uma pessoa por si só (nome completo, caso não exista homônimo; número do CPF, do RG, do passaporte, entre outros).

Dados que possam identificar pessoa natural – São as informações que, somadas, passam a identificar alguém (primeiro nome, endereço, características físicas, entre outros).

Dado pessoal sensível – A LGPD definiu, em seu art. 5, II, 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". Importante mencionar que se trata de um rol taxativo; portanto, apenas esses dados pessoais são considerados sensíveis.

Dado anonimizado – É o dado pessoal que, apesar de estar relacionado a uma pessoa natural, passou por um processo de anonimização e não pode mais ser identificado.

Anonimização – É o processo técnico que retira a possibilidade de o dado pessoal identificar uma pessoa natural de forma irreversível.

Pseudonimização – É a substituição de informação encontrável por identificadores artificiais, cifragem, codificação de mensagens e outros, sendo que o controlador mantém a informação em local separado.

Banco de dados – Conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico

Data center – É um ambiente projetado para concentrar servidores, equipamentos de processamento e armazenamento de dados e sistemas de ativos de rede.

Agente de tratamento – Pessoa natural ou jurídica de direito público ou privado que realize yratamento de dado pessoal, podendo ser controlador ou operador.

Controlador – Responsável por determinar as decisões tomadas sobre o tratamento dos dados.

Operador – Segue as orientações do controlador e realiza as ações conforme suas decisões.

Encarregado/*data protection officer* (DPO) – É o responsável pela comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados, bem como deve disseminar a cultura da proteção dos dados pessoais dentro de uma organização e avaliar as atividades de tratamento que a organização realiza.

Tratamento – Toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração

Consentimento – A LGPD definiu algumas hipóteses para tratamento dos dados pessoais, sendo uma delas o consentimento. Entretanto, para a coleta desse consentimento, foram impostos alguns requisitos, devendo, a manifestação do consentimento, ser livre, informada e inequívoca.

Manifestação livre – A manifestação do consentimento deve partir do titular sem que haja qualquer tipo de pressão ou direcionamento.

Manifestação informada – Antes de dar o consentimento, o titular deverá ter acesso prévio, completo e detalhado sobre o tratamento de seus dados pessoais, incluindo sua natureza, objetivos, métodos, duração, justificativa, finalidades, risco, responsabilidades dos agentes de tratamento e benefícios antes de proferir o Consentimento.

Manifestação inequívoca – Não pode haver dúvidas sobre a manifestação do consentimento do titular, ou seja, deve existir a certeza de que o titular consentiu com o tratamento dos seus dados pessoais.

Transferência internacional – Transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro.

Órgão de pesquisa – Órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no país, que inclua, em sua missão institucional ou em seu objetivo social ou estatutário, a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico.

Relatório de impacto à proteção de dados pessoais (RIPD) – Quando o tratamento de dados puder gerar riscos à liberdade civil e aos direitos fundamentais do titular, o controlador deverá elaborar uma documentação contendo a descrição dos processos de tratamento de dados pessoais.

Autoridade Nacional de Proteção de Dados (ANPD) – Órgão criado para implementar e fiscalizar o cumprimento da LGPD em todo o território nacional, emitindo diretrizes e promovendo ações educativas à sociedade. Também será responsável pela aplicação de multas e sanções.

Bases legais – A LGPD definiu, em seu art. 7.º, dez hipóteses para tratamento dos dados pessoais e, em seu art. 11, sete hipóteses para tratamento de dados pessoais sensíveis, deveando, o agente de tratamento, escolher a mais adequada para cada atividade.

Privacy by design (privacidade desde a concepção) – Significa levar o risco de privacidade em conta em todo o processo de concepção de um novo produto ou serviço.

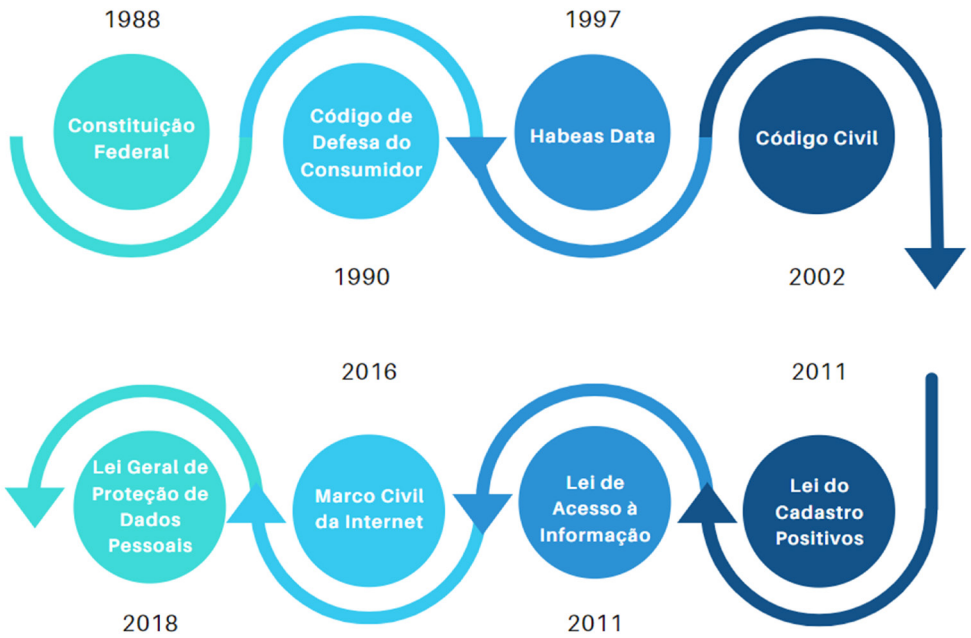
Privacy by default (privacidade por padrão) – Significa assegurar que são colocados em prática, dentro de uma organização, mecanismos para garantir que, por padrão, apenas será recolhida/coletada, utilizada e conservada, para cada atividade, a quantidade necessária de dados pessoais.

6 O TRATAMENTO DE DADOS PESSOAIS

6.1 ESTRUTURA NORMATIVA DA PROTEÇÃO DE DADOS

A Proteção de dados pessoais, há bastante tempo, é discutida e regulamentada ao redor do mundo. Desde os anos de 1970, por exemplo, há um debate em evolução na Europa. Como já mencionamos nesta cartilha, a proteção de dados pessoais faz parte do conceito de privacidade e é de grande importância, atualmente.

Nesta cartilha, apresentaremos as leis brasileiras que antecederam a LGPD e demonstraremos como os assuntos de privacidade e proteção de dados pessoais já estavam difundidos na legislação antes do advento da respectiva lei.



(i) **Constituição da República Federativa do Brasil de 1988** – A atual Constituição Federal possui a previsão legal de inviolabilidade da intimidade, vida privada, honra e imagem das pessoas, assegurando o direito à indenização pelo dano material ou moral decorrente de sua violação. Também possui a previsão legal da inviolabilidade das correspondências e das comunicações telegráficas, de dados e das comunicações telefônicas. Por fim, prevê o direito ao *habeas data*, que explicaremos mais adiante.

(ii) **Código de Defesa do Consumidor, Lei n. 8.078/1990** – O Código de Defesa do Consumidor assegura aos consumidores que tenham acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados que versem sobre ele próprio.

(iii) **Lei do *Habeas Data*, Lei n. 9.507/1997** – O *habeas data* é um instrumento constitucional que busca assegurar, aos cidadãos, o conhecimento de informações sobre si que constam em registros e bancos de dados de entidades governamentais ou de caráter público.

(iv) **Código Civil, Lei n. 10.406/2002** – O Código Civil contém, em seu capítulo II, disposições sobre os direitos da personalidade, que são intransferíveis e irrenunciáveis. Dentre tais direitos, estão o direito ao nome e à inviolabilidade da vida privada.

(v) **Lei do Cadastro Positivo, Lei n. 12.414/2011** – A Lei do Cadastro Positivo versa, em relação aos dados pessoais, sobre como devem ser tratados, sobre a revisão de informações incorretas e sobre a finalidade para a qual são coletados.

(vi) **Lei de Acesso à Informação, Lei n. 12.527/2011** – É a primeira legislação a estabelecer o que são dados pessoais, com a definição que temos hoje na LGPD, e a primeira legislação a proteger os dados pessoais como uma exceção à transparência intrínseca às democracias. Ainda, tal legislação responsabiliza o Poder Público caso haja dano em decorrência da divulgação não autorizada ou utilização indevida de informações sigilosas ou informações pessoais.

(vii) **Marco Civil da Internet, Lei n. 12.965/2014, e Decreto n. 8.771/2016** – O Marco Civil da Internet assegura, como princípio orientador do uso da internet, a proteção aos dados pessoais, e, como direito dos cidadãos, o não fornecimento de seus dados pessoais (exceto se houver ordem judicial em específico para tanto). Ainda instrui como empresas provedoras de conexão à internet e provedoras de conteúdo devem agir quanto à guarda e fornecimento de dados pessoais. O Marco Civil da Internet também prevê a figura do consentimento, porém de uma forma diferente do quanto disposto na LGPD (devendo ser livre, expresso e informado). Por sua vez, o seu decreto regulamentador possui todo um capítulo que versa sobre a proteção aos dados pessoais e às comunicações privadas que ocorrem em ambiente virtual, além de ser a primeira legislação nacional a prever o princípio da minimização de dados pessoais (previsto na LGPD como o princípio da necessidade, como veremos adiante).

(viii) **Lei Geral de Proteção de Dados, Lei n. 13.709/2018** – A LGPD visa a assegurar uma uniformidade nas atividades de tratamento de dados pessoais no Brasil. Assegura direitos e obrigações aos agentes de tratamento e aos titulares de dados pessoais. A vigência da LGPD foi iniciada em 03 de maio o ano de 2021, e as suas sanções passaram a ser aplicáveis a partir de 01 de agosto de 2021.

6.2 PRINCÍPIOS DA LEI GERAL DE PROTEÇÃO DE DADOS

A LGPD possui 10 princípios que devem ser observados por todos que tratem dados pessoais, além da boa-fé. Assim, todas as atividades de tratamento de dados pessoais devem observar os seguintes princípios:

(i) Finalidade: simboliza que as finalidades para ao tratamento de dados pessoais devem ser legítimas, específicas, explícitas e informadas ao titular.

(ii) Adequação: significa que as atividades devem ser compatíveis com as finalidades informadas ao titular.

(iii) Necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com a utilização de dados pessoais pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento.

(iv) Livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento de seus dados pessoais, bem como sobre a integralidade de seus dados pessoais.

(v) Qualidade dos dados pessoais: assegura aos titulares o direito de que os dados pessoais estejam exatos, claros, relevantes e atualizados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento.

(vi) Transparência: garante aos titulares informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial. A transparência pode ser passiva, atendendo ao titular sempre que este solicitar informações sobre o tratamento de seus dados pessoais, e a transparência pode ser ativa, feita de ofício, de maneira a deixar clara a finalidade do tratamento e seus aspectos legais.

(vii) Segurança: obriga os agentes de tratamento de dados pessoais a utilizarem medidas técnicas (como o uso de antivírus, firewall e controles de rede) e administrativas (como políticas de segurança da informação e a documentação de processos que ocorrem dentro da organização) aptas a proteger os dados pessoais.

(viii) Prevenção: obriga os agentes de tratamento de dados pessoais a adotarem medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais, ou seja, devem ser adotadas medidas antes que incidentes ocorram.

(ix) Não-discriminação: impossibilita o tratamento de dados pessoais para fins discriminatórios, ilícitos ou abusivos, o que já é intrínseco à própria ordem jurídica.

(x) Responsabilização e prestação de contas: os agentes de tratamento de dados pessoais devem adotar medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, atestar a eficácia dessas medidas.

6.3 BASES LEGAIS PARA O TRATAMENTO DE DADOS PESSOAIS

Para que uma atividade de tratamento de dados pessoais seja realizada, é necessário saber sob qual fundamento de legalidade estará baseada. A Lei de Acesso à Informação estabelece que, em regra, há necessidade de previsão legal ou consentimento do titular de dados pessoais para que tais atividades ocorram. O princípio constitucional da legalidade assegura que todas as ações que envolvem o Poder Público devem estar amparadas em disposições legais, incluindo a atribuição de tratar dados pessoais.

A LGPD afirma que todo tratamento de dados pessoais pelo Poder Público deverá ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público. Assim, sempre deve haver uma norma legal que fundamente, em algum nível, o tratamento de dados pessoais. A LGPD estabelece as seguintes bases legais para o tratamento de dados pessoais, conforme abaixo:

(i) **Consentimento**: o consentimento alinha-se à ideia da autodeterminação informacional do indivíduo, que signifca que a pessoa pode escolher fornecer as suas informações para alguém ou não. Ainda exige uma participação ativa e, consequentemente, um maior controle sobre o fluxo de suas informações pessoais. O consentimento tem algumas características que lhes são peculiares, e, para ser considerado válido, deverá ser livre, informado e inequívoco, bem como fornecido para uma determinada finalidade. Essa base legal deve ser utilizada com muita cautela, uma vez que um dos direitos do titular de dados pessoais é, exatamente, o direito à revogação do consentimento, como veremos mais adiante no tópico sobre os direitos do titular. Na hipótese de o Poder Público comunicar ou compartilhar dados pessoais, será necessário colher o consentimento do titular, exceto nas hipóteses de dispensa de consentimento, que são tratadas abaixo.

(ii) **Para o cumprimento de uma obrigação legal ou regulatória**: quando há necessidade de tratamento de dados pessoais por conta do ordenamento jurídico ou, até, perante o próprio regulador de determinado segmento econômico.

(iii) **Pela Administração Pública**: para o tratamento e uso compartilhado de dados pessoais necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres. A LGPD possui um capítulo inteiro sobre o tratamento de dados pessoais pela Administração Pública. A grande questão no desenvolvimento de políticas públicas estruturadas em dados pessoais é equilibrar a relação entre o Poder Público e os direitos dos cidadãos. O tratamento de dados pessoais pelo Poder Público deve se orientar por meio

dos princípios gerais de proteção de dados pessoais, que vimos acima, e, além disso, buscar equacioná-los com os princípios norteadores da própria Administração Pública. A ratificação de políticas públicas deve sempre buscar diminuir a assimetria que há entre o Estado e os cidadãos.

(iv) **Realização de estudos por órgão de pesquisa, desde que garantida, se possível, a anonimização ou pseudonimização dos dados pessoais**: para compreender perfeitamente esta base legal, é necessário observar a conceituação de órgão de pesquisa situada no glossário desta cartilha.

(v) **Execução de contratos em que o titular seja parte**: esta base legal poderá ser utilizada quando (a) o tratamento seja estritamente necessário para a execução de contrato do qual o titular é parte ou (b) quando o tratamento for necessário no contexto contratual. Isso ocorre, por exemplo, em atividades de tratamento de dados pessoais que decorrem de um contrato de prestação de serviço.

(vi) **Exercício regular de direitos em processo judicial, administrativo ou arbitral**: trata-se de uma base legal bastante ampla e autoriza o tratamento de dados pessoais em processos de qualquer tipo. Portanto, dados pessoais que constam em bases de dados relacionadas aos processos devem sempre respeitar as finalidades para as quais foram disponibilizadas.

(vii) **Proteção da vida ou da incolumidade física do titular ou de terceiros**: esta é uma base legal muito importante, pois permite o tratamento de dados pessoais quando um titular estiver em risco de vida, como, por exemplo, quando um cidadão é levado a um hospital após sofrer um grave acidente.

(viii) **Para a tutela da saúde, em procedimento realizado por profissionais da saúde**: é utilizada quando, por exemplo, um cidadão se dirige a uma farmácia para obter remédios.

(ix) **Para atender aos interesses legítimos do controlador ou de terceiros**: pode ser utilizada para fundamentar atividades de tratamento de dados pessoais que tenham finalidades legítimas, consideradas a partir de situações concretas, como apoio e promoção de atividades do Poder Público, e para proteger os titulares de dados pessoais do exercício regular de seus direitos ou prestação de serviços que o beneficiem. Esta é uma base legal complexa, uma vez que, ao tratar dados pessoais sob tal hipótese, há necessidade de elaboração de um relatório de impacto que pode ser exigido pela ANPD, o chamado *Legitimate Interest Assessment* (ou, LIA). Trata-se de um teste de proporcionalidade em quatro passos e que deverá avaliar: (a) a legitimidade do interesse, isto é, verificar se a finalidade para a qual se busca o tratamento é, efetivamente, legítima, e, além disso, se a situação é concreta; (b) a necessidade do referido tratamento, ou seja, se o tratamento será realizado de forma menos intrusiva possível, em conformidade com o princípio da minimização, e, ainda, se existem outras bases legais que podem estruturar tal tratamento de forma menos onerosa; (c) o balanceamento entre o tratamento que se pretende realizar e a legítima expectativa do titular, assim como a não infringência de direitos e liberdades fundamentais; e, por fim, (d) estabelecer salvaguardas e garantias que assegurem ao titular transparência, mecanismos de oposição e mitigação de riscos.

(x) **Para a proteção do crédito**: a proteção do crédito como base legal para o tratamento de dados pessoais criou um microssistema de proteção de dados pessoas em que, para esses casos, há

o convívio pleno e integrado entre diversas normas consumeristas; por exemplo, o Código de Defesa do Consumidor, a Lei do Cadastro Positivo e a própria LGPD. Portanto, a referida base legal estrutura efetivamente um sistema em que se busca a proteção do crédito.

É importante informar que, para o caso de tratamento de dados pessoais sensíveis, não poderá ser utilizada a base legal de interesses legítimos do controlador ou de terceiros.

Por sua vez, o consentimento, no caso de dados pessoais sensíveis, deverá ser específico, destacado e para finalidades específicas. Ou seja, esse consentimento é diferente do consentimento necessário para o tratamento dos dados pessoais comuns. Para que sejam tratados dados pessoais sensíveis sob a base legal do consentimento, o titular precisará ser informado exatamente para quais finalidades os seus dados pessoais serão tratados, devendo expressar o seu consentimento em uma cláusula em separado e em destaque do contrato original, como, por exemplo, assinando um anexo.

Há, ainda, outra base legal para o tratamento de dados pessoais sensíveis, que é para a garantia de prevenção à fraude e à segurança do titular, em processos de identificação e autenticação de cadastro em sistemas eletrônicos, ou seja, quando, por exemplo, utiliza-se a biometria para acessar uma conta em um caixa eletrônico.

Por fim, para o tratamento de dados pessoais sensíveis, sem o fornecimento do consentimento pelo titular, será possível utilizar as outras bases legais explicadas acima, como: (i) o cumprimento de obrigação legal ou regulatória pelo controlador; (ii) pela Administração Pública, para a execução de políticas públicas previstas em leis ou regulamentos; (iii) a realização de estudos por órgão de pesquisa; (iv) o exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral; (v) a proteção da vida ou da incolumidade física do titular ou de terceiro; e, por fim, (vi) a tutela da saúde, exclusivamente em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária.

No que tange ao tratamento de dados pessoais de menores de idade, a LGPD informa que deverá ser realizado em seu melhor interesse. Para tratar dados pessoais de crianças (a pessoa até doze anos de idade incompletos), é necessário o consentimento específico e em destaque dado por, pelo menos,um dos pais ou responsáveis legais. Quando houver o tratamento de dados pessoais de crianças, os controladores deverão manter informações públicas sobre quais são os dados coletados, como ocorre o tratamento e quais os procedimentos para o exercício dos direitos do titular.

Há exceção para o tratamento de dados pessoais de crianças. Tais dados pessoais poderão ser tratados sem o consentimento de um dos pais ou responsáveis legais quando a coleta for necessária para contatá-los. Esses dados pessoais deverão ser utilizados apenas uma única vez, sem a possibilidade de armazenamento e em nenhum caso poderão ser repassados a terceiros sem o consentimento de um dos pais ou responsáveis legais.

Ainda em relação ao tratamento de dados pessoais de crianças, os controladores não poderão condicionar a participação em jogos ou em aplicações de internet, ou outras atividades, ao fornecimento de dados pessoais, além das informações estritamente necessárias à atividade.

Por fim, o controlador deve envidar esforços para verificar se o consentimento foi dado por um dos pais ou responsáveia legais pela criança. As informações sobre o tratamento de tais dados pessoais deverão ser fornecidas de maneira simples, clara e acessível, para que as próprias crianças possam compreender o que ocorrerá com seus dados pessoais. Poderão ser utilizadas cartilhas, vídeos, desenhos animados e quaisquer outros formatos que sejam interessantes para as crianças.

Por sua vez, no que se refere ao tratamento de dados pessoais de adolescentes (a pessoa entre doze e dezoito anos de idade incompletos), a LGPD não faz distinção.

6.4 COMPARTILHAMENTO DE DADOS PESSOAIS

A LGPD estabelece que os dados pessoais tratados pelo Poder Público deverão ser mantidos em formato interoperável e estruturado para o uso compartilhado com seus diversos órgãos e esferas, com vistas à execução de políticas públicas, para a prestação de serviços públicos, para a descentralização da atividade pública e para a disseminação e acesso das informações pelos cidadãos em geral.

O Poder Público só poderá compartilhar dados pessoais se tal atividade atender a finalidades específicas de execução de políticas públicas e atribuição legal pelos órgãos e entidades públicas, sempre respeitando aos princípios da lei, expostos no item 6.2.

O Poder Público poderá compartilhar dados pessoais constantes de bases de dados a que tenha acesso nas seguintes situações: (i) em casos de execução descentralizada da atividade pública que exija a transferência, exclusivamente para esse fim específico e determinado, observado o disposto na Lei de Acesso à Informação; (b) nos casos em que os dados pessoais forem acessíveis publicamente; (c) quando houver previsão legal ou a transferência for respaldada em contratos, convênios ou instrumentos congêneres, que deverão ser comunicados à ANPD; ou (d) na hipótese de a transferência dos dados pessoais objetivar exclusivamente a prevenção de fraudes e irregularidades, ou proteger e resguardar a segurança e a integridade do titular dos dados pessoais, desde que vedado o tratamento para outras finalidades.

6.5 DIREITOS DOS TITULARES

Conforme vimos acima, a LGPD unifica uma série de leis que já existiam anteriormente e unifica a forma como os dados pessoais devem ser tratados. Diversas legislações já proporcionavam direitos aos

Titulares de dados pessoais, como o Código de Defesa do Consumidor. Porém, a LGPD inovou ao trazer diversos direitos aos titulares de dados pessoais.

Inicialmente, a LGPD informa que toda pessoa natural tem assegurados e garantidos os seus direitos fundamentais de liberdade, intimidade e privacidade, o que é essencial, pois, como vimos no início desta cartilha, a proteção de dados é um dos direitos que visam a complementar tais direitos. Os demais direitos garantidos ao titular de dados pessoais são:

(i) confirmação da existência de tratamento;

(ii) acesso aos dados;

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

(iv) anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com a lei;

(v) portabilidade dos dados pessoais, ou seja, a transferência dos dados pessoais de um controlador a outro, desde que assegurados o segredo industrial e comercial;

(vi) eliminação dos dados pessoais tratados sob a base legal do consentimento;

(vii) informações sobre o compartilhamento de dados pessoais;

(viii) informações sobre a possibilidade de não fornecer o consentimento e sobre as consequências de tal negativa;

(ix) revogação do consentimento.

6.6 COMUNICAÇÃO COM A ANPD E COM OS TITULARES DE DADOS PESSOAIS

As pessoas jurídicas de direito público deverão indicar um encarregado pelo tratamento de dados pessoais, que terá, como função, comunicar-se com a ANPD e com os titulares de dados pessoais, prestando informações, quando solicitadas, ou informações a respeito das atividades de tratamento de dados pessoais realizadas.

A ANPD deverá regulamentar diversos pontos sobre a LGPD e fiscalizará o cumprimento da legislação. Com relação ao Poder Público, a ANPD poderá dispor sobre as formas de que o Poder Público poderá se utilizar para dar publicidade às operações de tratamento de dados pessoais.

6.7 O TÉRMINO DO TRATAMENTO DOS DADOS PESSOAIS

O tratamento de dados pessoais não pode ser eterno. Por essa razão, a LGPD preocupou-se com especificar sob quais hipóteses poderá ocorrer o término do tratamento. Vejamos abaixo:

(i) quando a finalidade do tratamento for alcançada, ou quando os dados pessoais deixarem de ser necessários para o alcance da finalidade almejada;

(ii) o fim do período para o qual o dado pessoal foi coletado;

(iii) a pedido do titular, inclusive no exercício de seu direito de revogação do consentimento, resguardado o interesse público;

(iv) por determinação da ANPD ou quando houver violação ao disposto na LGPD.

6.8 A ELIMINAÇÃO DOS DADOS PESSOAIS

Os dados pessoais poderão ser eliminados após o término de seu tratamento, observados os limites técnicos empregados, ou seja, nem sempre será possível eliminar os dados pessoais de uma organização, principalmente quando pensamos em dados pessoais armazenados em arquivos antigos ou arquivos físicos.

Poderão ser armazenados os dados pessoais para as seguintes finalidades:

(i) cumprimento de obrigação legal ou regulatória pelo controlador, ou seja, quando um dispositivo legal determinar que o dado pessoal seja armazenado por maior período de tempo;

(ii) estudo por órgão de pesquisa, garantida, quando possível, a anonimização de tais dados pessoais;

(iii) quando o dado pessoal for transferido a terceiro, como, por exemplo, quando um dado pessoal for compartilhado com um prestador de serviço, o que tornará impossível, ao agente de tratamento original, solicitar a exclusão de tal dado;

(iv) quando o controlador fizer uso exclusivo de tais dados pessoais, desde que sejam anonimizados.

7 AGENTES DE TRATAMENTO

7.1 DEFINIÇÃO

A LGPD define a figura dos agentes de tratamento de dados pessoais como os indivíduos que controlam ou tratam informações que contenham dados pessoais. A lei elenca expressamente, no artigo 5.º, inciso IX, que os agentes de tratamento são definidos como controlador e o operador.

A diferença entre o controlador e o operador está no escopo da função: o controlador coleta os dados pessoais dos titulares de dados e a ele compete as decisões quanto ao tratamento dos dados pessoais obtidos.

O operador tratará os dados pessoais em nome do controlador, isto é, realizará o tratamento de dados pessoais em virtude de contrato, respeitando as instruções do controlador.

7.2 OBRIGAÇÕES E RESPONSABILIDADES

A LGPD diferencia os agentes de tratamento e dispõe sobre as obrigações e responsabilidades no caso de ressarcimento de danos decorrentes do tratamento inadequado de dados pessoais, bem como no caso de incidentes de segurança da informação.

A principal obrigação que a lei atribui aos agentes acima citados é a de manterem um registro das operações de tratamento que realizarem, especialmente quando esse tratamento de dados pessoais for realizado segundo a base legal do legítimo interesse.

Por sua vez, é dever do operador realizar o tratamento de dados pessoais conforme as instruções fornecidas pelo controlador, que verificará a observância das próprias instruções e das normas sobre a matéria. É necessário que todas as instruções a serem cumpridas sejam claras e, preferencialmente, formais, para que não haja incerteza ou falha no processo de tratamento de dados pessoais.

O agente de tratamento que, em razão do tratamento inadequado de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo. Nesse sentido, o operador, apesar de tratar os dados conforme as instruções fornecidas pelo controlador, também poderá ser responsabilizado a reparar o dano causado.

7.3 ENCARREGADO PELO TRATAMENTO DE DADOS PESSOAIS / *DATA PROTECTION OFFICER* (DPO)

A LGPD, em seu artigo 5.º, inciso VIII, designa a criação do cargo de encarregado de proteção de dados pessoais, figura também conhecida como *data protection officer* (DPO). Esse profissional será o responsável por acompanhar todas as atividades que dizem respeito à proteção de dados pessoais, bem como será o ponto focal para a comunicação interna do município, para a comunicação com os titulares de dados pessoais e para a comunicação com a ANPD.

A imputação de uma necessidade de um encarregado busca garantir que as informações sobre proteção de dados pessoais sejam centralizadas dentro da organização. O cargo poderá ser ocupado por uma pessoa física ou jurídica, que poderá ser interna ou externa, ou até mesmo em um modelo híbrido, com contratados internos e externos, ao mesmo tempo. Poderá, ainda, ser um departamento com pessoas de diversas áreas, a fim de que possam cumprir com as diversas funções que o encarregado possui.

O encarregado tem, também, a atribuição de fazer a gestão das reclamações e comunicações dos titulares de dados pessoais, receber comunicações da ANPD, orientar os funcionários e contratados do município sobre boas práticas a serem adotadas em relação à proteção de dados, o que compreende elaborar treinamentos, revisar políticas e procedimentos internos, educar os funcionários sobre a importância da LGPD e mitigar riscos de incidentes de segurança da informação, e, por fim, executar as demais atribuições que o município lhe atribuir.

O profissional deverá ter autonomia para auditar e fiscalizar as possíveis irregularidades, a fim de serem corrigidas e notificadas conforme rege a lei, não podendo, portanto, haver conflito de interesses entre suas funções, caso as acumule.

7.4 COMITÊ DE PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS

O Comitê de Privacidade e Proteção de dados pessoais deve atuar em conjunto com o DPO, para auxiliar no desenvolvimento de algumas atividades ligadas à organização, como, por exemplo:

(i) facilitar a promoção de uma cultura de proteção aos dados pessoais dentro da organização;

(ii) propor políticas de segurança da informação;

(iii) gerenciar atividades relacionadas ao tratamento de dados pessoais, bem como avaliar se estão de acordo com as normas de proteção aos dados pessoais;

(iv) fiscalizar processos que envolvam o tratamento de dados pessoais;

(v) realizar treinamentos para os funcionários da organização, fornecedores e terceiros sobre a importância da proteção aos dados pessoais.

8 MUNICÍPIO COMO CONTROLADOR

Os municípios, assim como as empresas e demais instituições, em regra, são controladores de dados pessoais; afinal, realizam o cadastro dos seus habitantes para questões relacionadas a moradia, saúde, emprego, transporte e diversas outras atividades. Além disso, realizam o cadastro e utilizam os dados pessoais para realizar a cobrança de impostos, promover demandas judiciais e implementar políticas públicas. Outra forma de tratamento de dados pessoais realizado pelo município é o cadastro dos seus funcionários.

Desse modo, resta claro que o município figura como agente de tratamento, devendo ser considerado como controlador.

Mas quais as principais implicações a partir disso? O município deverá:

• **nomear encarregado/***data protection officer* **(DPO):** cada município deverá nomear um responsável pela comunicação entre os titulares, o próprio município e a ANPD, expondo o contato do DPO, de preferência em seu website;

• **responder aos titulares de dados pessoais:** a LGPD elencou um rol de direito ao titular, sendo possível solicitar o acesso, a retificação e a confirmação de tratamento, entre outros direitos. A LGPD estabeleceu o prazo de quinze dias para resposta dos agentes de tratamento, sob pena de multa por descumprimento;

• **manter um registro das atividades:** conforme mencionado anteriormente, o município deve passar por um projeto de adequação, tendo que mapear as atividades de tratamento de dados e deixar os fluxos registrados, bem como suas alterações;

• **comunicar incidente:** caso ocorra um incidente de segurança que possa acarretar risco ou dano relevante aos titulares, o município deverá informar à ANPD em prazo razoável;

• **elaborar um RIPD:** conforme mencionamos acima, caso o município realize o tratamento de dados pessoais que possa gerar riscos às liberdades civis e aos direitos fundamentais dos titulares, deverá elaborar um relatório de impacto (RIPD). Caso o tratamento seja realizado a partir da base legal do legítimo interesse, a ANPD também poderá solicitar um relatório de impacto ao município;

• **ônus da prova no consentimento:** caso o município realize o tratamento de dados pessoais com suporte na base legal do consentimento, deverá provar que o titular manifestou claramente esse consentimento;

• **transparência sobre os tipos de dados coletados de crianças:** quando o município realizar o tratamento de dados pessoais de crianças, além de ter que solicitar o consentimento de um dos pais ou representantes legais, deverá manter pública a informação sobre os tipos de dados coletados, a forma de sua utilização e os procedimentos utilizados.

Ao estabelecer as boas práticas adotadas internacionalmente, as instituições serão reconhecidas perante a população, elevando seu patamar de confiabilidade e transparência.

9 DEFINIÇÃO DE UM MODELO DE GOVERNANÇA DO MUNICÍPIO

Para que o município obtenha êxito na transformação, sobretudo na implementação de uma cultura de proteção de dados, deverá possuir iniciativa para estruturar o próprio modelo de governança, sempre adequado à sua realidade, pois no Brasil existem municípios com milhões, milhares e outros com menos de mil habitantes, com territórios diferentes, orçamentos diferentes e problemas diferentes.

Entretanto, o que todos os municípios têm em comum ao implementar o programa de governança é que deve ser feito em conjunto e de forma articulada, para que possam usufruir do que há de melhor na gestão do município.

Dessa forma, o gestor deverá compreender que a governança é um meio para se atingir os objetivos da administração pública e, para tanto, precisa-se ter conhecimento com relação ao:

• **ambiente interno de sua gestão:** é compreendido pelas forças e fraquezas da sua gestão. Desse modo, o gestor deverá conhecer as competências da sua equipe, as normas, a infraestrutura, os *gaps* e riscos existentes na gestão etc. O ambiente interno afeta diretamente a imagem do gestor perante a sociedade e, por isso, é de extrema importância controlá-lo;

• **ambiente externo de sua gestão:** é compreendido pelos anseios da população, pela situação do município, oportunidades de crescimento e ameaças aos objetivos. O(a) prefeito(a) poderá ter ciência do ambiente externo através de pesquisa e diagnósticos aplicados no município por uma equipe multidisciplinar, que forneça os dados e as informações necessárias para o planejamento e tomada de decisões.

Importante lembrar que o(a) prefeito(a) pode formar uma rede com entidades, organizações e conselhos que lhe permita a articulação e implantação de iniciativas.

10 A GOVERNANÇA EM PROTEÇÃO DE DADOS E SEUS BENEFÍCIOS

A proteção dos dados pessoais era vista apenas como boa prática, e agora, com a LGPD, torna-se uma obrigação às instituições. A própria LGPD traz uma seção voltada para boas práticas e governança, em seus artigos 50 e 51, definindo os requisitos e as diretrizes de um programa de governança.

O art. 50 da LGPD menciona que as regras de boas práticas e de governança devem estabelecer:

> [...] 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.

Ainda no art. 50, § 2.º, I, a LGPD permite ao controlador a implementação de um programa de governança 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;

Dessa forma, é possível verificar que os requisitos para um programa de governança presentes na LGPD seguem as diretrizes adotadas por grandes empresas e órgãos públicos.

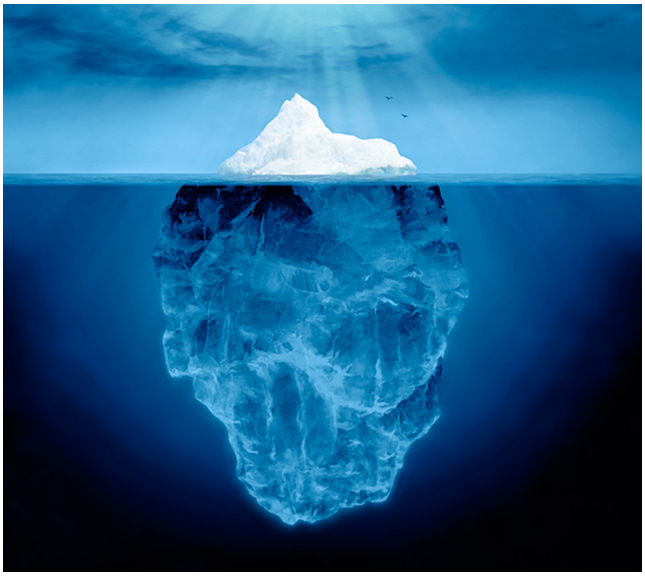
Cada política, norma e ação criada no município deve ser documentada para demonstrar a efetividade de seu programa de governança quando houver questionamento e, em especial, a pedido da ANPD. A adoção de políticas de boas práticas e governança não apenas auxilia o município a cumprir com as obrigações estabelecidas pela LGPD, como também demonstra os esforços nesse sentido, e todos os registros documentados das ações adotadas serão considerados em uma eventual aplicação de sanção por tratamento inadequado de dados pessoais.

Conforme já mencionamos, a governança irá possibilitar aos municípios um aumento em sua capacidade de gestão, aumento do controle e integridade das informações, servindo como base de sustentação dos seus processos internos.

Em proteção de dados, isso significa mapear as atividades que utilizam dados pessoais, em que eles ficam armazenados, quais os controles de segurança no armazenamento, quais pessoas possuem acesso aos dados, quem pode alterá-los, corrigi-los e excluí-los, por quanto tempo os dados permanecem com o município, se são compartilhados com terceiros e como são excluídos.

Tais ações irão garantir aos municípios um controle maior sobre os dados pessoais dos seus clientes, fornecedores, parceiros, funcionários, do público em geral e demais *stakeholders*, diminuindo o risco de vazamento e, consequentemente, afastando multas, mídia negativa e demandas judiciais.

Termo de Consentimento
Política de Privacidade
Cláusula Padrão
Cookies



Termo de Consentimento
Política de Privacidade
Cláusula Padrão
Cookies
Programa de Governança de Dados
Transparência
Minimização
Prestação de Contas
Responsabilidade
Bases legais
Processos e Políticas
Boa fé
Gestão de Riscos
Muitos outros

A imagem acima demonstra que grande parte das ações não está à vista, devendo o município realizar um projeto de adequação com a profundidade necessária para garantir o controle da sua gestão de privacidade e proteção de dados.

É comum vermos e ouvirmos, sobretudo atualmente, com as redes sociais, pessoas mencionando que, para estar em conformidade com a LGPD, basta possuir as políticas de privacidade e de *cookies* em seu sítio eletrônico, inserir cláusula padrão de proteção de dados nos seus contratos e elaborar um termo de consentimento para utilização dos dados pessoais de clientes, funcionários, fornecedores e demais *stakeholders*.

Entretanto, trata-se de um equívoco, pois, para que a instituição esteja em *compliance* com a LGPD, deve empreender diversas ações internas, realizando uma varredura dos dados pessoais utilizados, a verificação dos sistemas, o mapeamento do fluxo percorrido por parte dos dados pessoais, a revisão de contratos, processos e políticas, o percebimento dos princípios presentes na LGPD, a identificação, gestão e mitigação dos riscos etc.

11 COMO IMPLEMENTAR UMA GOVERNANÇA EM PROTEÇÃO DE DADOS NA PRÁTICA?

Cada município deverá passar por um processo de adequação à LGPD, que compreende algumas etapas, como veremos a seguir.

11.1 DIAGNÓSTICO

Nesta fase inicial, o município deve levantar todas as suas atividades que compreendem o tratamento de dados pessoais, verificando todo o caminho percorrido pelos dados pessoais e identificando os riscos em cada processo. A partir dessas informações, é possível identificar o nível de aderência do município à LGPD e recomendar as alterações necessárias.

Em um projeto de adequação à LGPD, o mapeamento de dados é dividido da seguinte forma:

Nesse momento, será possível detalhar cada dado pessoal tratado, entendendo as fases do seu ciclo de vida. Será possível entender como os dados são recebidos, como e onde estão armazenados, quem tem acesso, se os dados são compartilhados com terceiros, quais os riscos associados a cada operação e a base legal adequada. Dessa forma, será possível analisar a forma como o município lida com os dados pessoais de seus colaboradores, clientes e parceiros.

Após o mapeamento dos processos, será possível identificar diversas questões em desacordo com a LGPD ou com as melhores práticas de segurança da informação, ou, ainda, com as práticas setoriais aplicáveis. Nesse momento, deve-se definir as bases legais adequadas para cada atividade de tratamento de dados pessoais executada na companhia, bem como elaborar um relatório com os principais gaps, apontando quais as medidas necessárias para a mitigação de riscos envolvendo incidentes de segurança da informação.

11.2 EXECUÇÃO DAS PRIORIDADES

Após mapear os riscos e recomendar as ações necessárias para a sua mitigação, chega o momento de colocá-las em prática. Entretanto, nesse primeiro momento, o município deve separar as ações em prioritárias e complementares, iniciando por aquelas que trazem um risco maior.

Após analisados os gaps encontrados, será necessário verificar quais as prioridades do município e elaborar um cronograma para mitigar os riscos localizados nas etapas anteriores. Será necessária a indicação de responsáveis para cada atividade de tratamento com necessidade de alteração e a verificação dos diferentes níveis de criticidade de cada medida.

É chegada a hora de implementar as medidas encontradas em desconformidade com a legislação. Nesse momento, será necessário adequar plataformas, processos, contratos, práticas e documentos que versem sobre o tratamento de dados pessoais.

11.3 EXECUÇÃO DOS PONTOS COMPLEMENTARES

Após a realização da adequação e mitigação dos principais riscos, o município poderá dar ênfase à formação de uma cultura de dados, desenvolvendo e aplicando palestras, treinamentos e comunicações com o intuito de demonstrar a importância da privacidade e da proteção dos dados para cada indivíduo, para o próprio município e para a sociedade.

11.4 MONITORAMENTO

Após a realização do diagnóstico, da implementação das ações prioritárias e complementares, é necessário que haja um monitoramento do projeto de adequação à LGPD e seus resultados, sendo o monitoramento um dos principais pontos da governança.

Nesse momento, chegamos ao final do nosso projeto de adequação à LGPD, porém não seria correto dizer que o projeto chegou ao fim, pois sempre será necessário manter as informações em ordem, sendo monitoradas e avaliadas com frequência. Além disso, o município é um organismo vivo que sofre constantes mudanças, assim como as leis podem sofrer alterações; desse modo, a etapa de monitoramento acaba não tendo um fim.

Dessa maneira, é essencial que o município tenha funcionários (internos, externos ou mesmo uma equipe híbrida) que sejam capazes de monitorar todas as novidades que podem ocorrer, para nunca deixar a organização desatualizada, tendo a possibilidade de sofrer uma sanção pela ANPD.

Outro ponto fundamental do monitoramento é a necessidade de treinamentos com certa periodicidade, para que a cultura da proteção aos dados pessoais seja parte do dia a dia do município.

Além disso, para a correta adequação à LGPD pela Administração Pública, sugerimos a estruturação de um grupo de trabalho que seja responsável pelo projeto e pelo estudo do tema. É essencial que, nesse grupo, estejam presentes e engajadas pessoas da alta diretoria da administração, bem como pessoas de setores que tratam dados pessoais em seu dia a dia.


SECURITY

12 SEGURANÇA DA INFORMAÇÃO

Segurança da informação é um conjunto de mecanismos e ferramentas que uma instituição utiliza com a finalidade de proteger um conjunto de informações, para proteger o valor que tais informações geradas pela instituição possuem. É, assim, um conjunto de regras essencial às instituições, principalmente para aquelas que lidam com informações valiosas e sigilosas.

Sob a LGPD, os controladores e operadores devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acesso não autorizado, destruição, perda, modificação, comunicação ou outros tipos de tratamento não autorizados ou ilegais. Espera-se que a ANPD forneça diretrizes para padrões técnicos mínimos no futuro.

O Marco Civil da Internet e seu decreto regulamentador estabelecem as seguintes diretrizes sobre normas de segurança que devem ser observadas pelos provedores de conexão e de aplicação no tratamento de dados pessoais e de comunicações privadas que trafegam pela internet: (i) o estabelecimento de controles rígidos sobre o acesso a dados pessoais, estabelecendo responsabilidades para aqueles que terão acesso a dados pessoais; (ii) o fornecimento de mecanismos de autenticação para o acesso a registros, usando, por exemplo, sistemas de autenticação dupla para garantir a individualização dos responsáveis pelo tratamento de dados pessoais; (iii) a criação de inventários detalhados de *logs* referentes à conexão e ao acesso aos aplicativos, que devem conter data, hora, minuto, segundo e a duração do acesso, a identidade do indivíduo que acessou os arquivos e quais arquivos foram acessados; e (iv) o uso de soluções de gerenciamento de registros por meio de técnicas que garantam a inviolabilidade dos dados pessoais, como criptografia ou medidas de proteção equivalentes.

Além disso, cada setor possui regras específicas quanto a padrões mínimos ou esperados que garantam a segurança da informação das organizações.

Alguns princípios que podem nortear uma política de segurança da informação são: (i) confidencialidade, para que as informações sejam acessadas apenas por pessoas autorizadas; (ii) integridade, para que as informações apenas sejam alteradas por pessoas autorizadas; e (iii) disponibilidade, as informações devem sempre estar disponíveis para quem é autorizado, evitando interrupções no fluxo de trabalho.

12.1 POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO

Parte fundamental no programa de governança são as políticas, normas e procedimentos de segurança da informação. Abaixo, listamos as principais políticas presentes em um programa de governança em proteção de dados pessoais e privacidade:

• Políticas de Privacidade, tanto para clientes quanto para empregados, para representantes comerciais e para candidatos a vagas;

• Política de Backup e Restore;

• Norma para acesso à Rede Remotamente;

• Norma para Uso de Recursos de Tecnologia da Informação e Comunicação;

• Norma de Gestão de Incidentes de Segurança da Informação;

• Norma para Classificação da Informação;

• Norma para Uso de Dispositivos Móveis;

• Norma para uso de Mídias Sociais;

• Norma de Uso de Wi-Fi;

• Norma para o Descarte de informações;

• Procedimento para Gestão de Segurança da Informação;

• Política sobre o uso de aplicativos de mensagens instantâneas;

• Procedimento de comunicação entre a instituição, a ANPD e os Titulares de dados pessoais;

• Procedimento sobre a Portabilidade de dados pessoais;

• Norma para Inventário de ativos

• Política ou Procedimento de Gestão de Riscos

• Plano de continuidade de negócios

• Norma de Controle de Acesso físico e lógico

• Norma de Desenvolvimento Seguro de Aplicações

• Política para uso de criptografia

12.2 INCIDENTES

De acordo com a página da ANPD no site do Governo Federal, um incidente de segurança com dados pessoais é "qualquer evento adverso, confirmado ou sob suspeita, relacionado à violação na segurança de dados pessoais, tais como acesso não autorizado, acidental ou ilícito que resulte na destruição, perda, alteração, vazamento ou, ainda, qualquer forma de tratamento de dados inadequada ou ilícita, os quais possam ocasionar risco para os direitos e liberdades do titular dos dados pessoais".

Como exemplos de incidentes de segurança da informação, podemos mencionar o acesso de terceiro não autorizado em redes de computadores, ou seja, quando algum agente externo, ou mesmo um funcionário da organização acessa (ou tenta acessar) uma parte do sistema que não deveria.

Os vírus e códigos maliciosos também são caracterizados como incidentes de segurança da informação e sua detecção requer o uso de ferramentas próprias, como antivírus.

Por fim, como último exemplo, podemos citar o uso impróprio de sistemas ou de informações, que ocorrem quando um funcionário da organização usa um e-mail corporativo para a promoção de negócios pessoais, ou quando instala uma ferramenta não autorizada no computador da organização, utiliza um *pen drive* de forma não autorizada ou, ainda, exemplificando com documentos físicos, imprime documentos sigilosos de forma não autorizada e os repassa para terceiros.

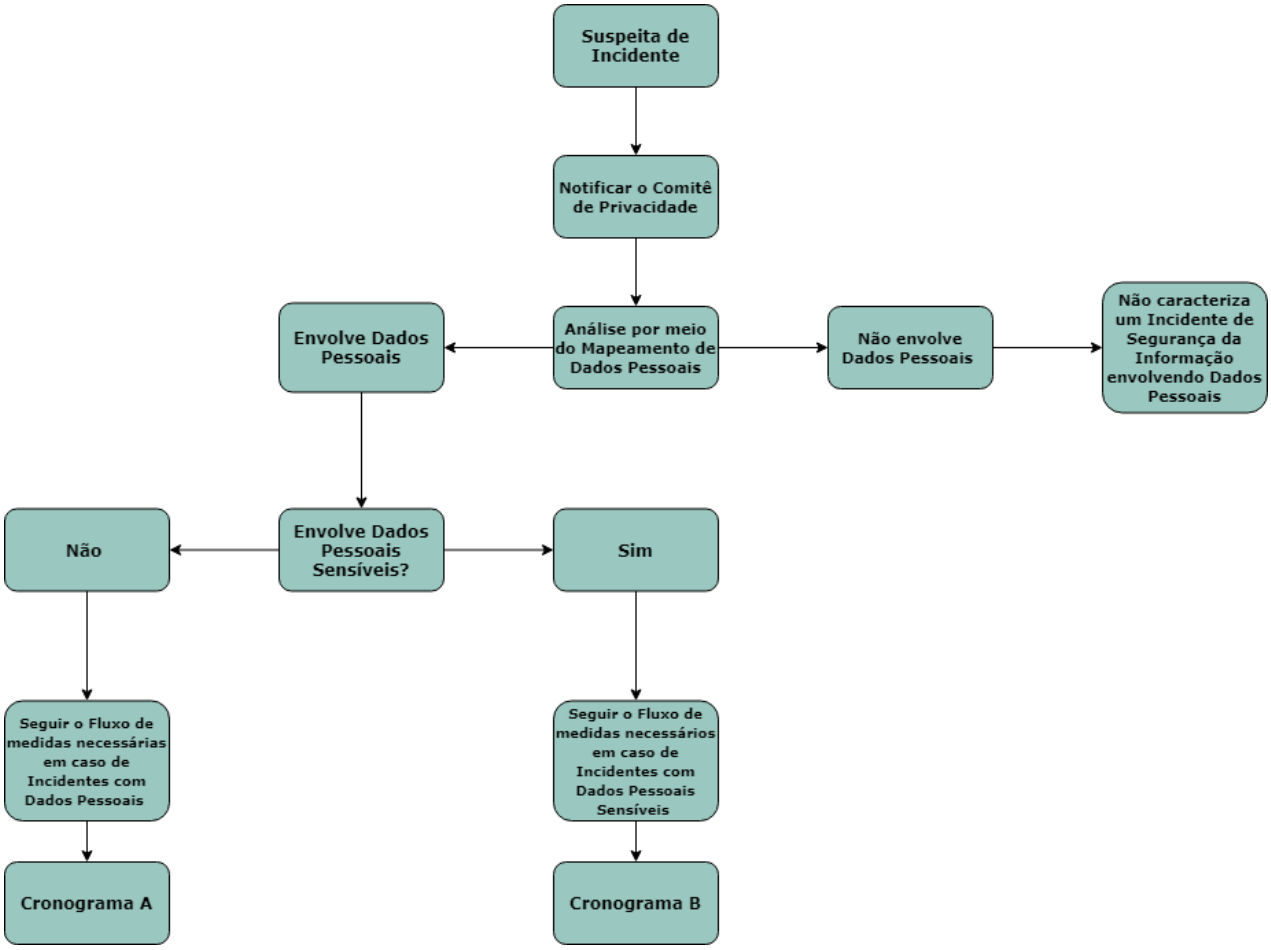
O art. 47 da LGPD diz que "Os agentes de tratamento ou qualquer outra pessoa que intervenha em uma das fases do tratamento obriga-se a garantir a segurança da informação prevista nesta Lei em relação aos dados pessoais, mesmo após o seu término". Dessa forma, é imprescindível que o município adote medidas técnicas e administrativas de segurança capazes de proteger os dados pessoais de acessos não autorizados e de situações acidentais ou maliciosas.

12.2.1 PLANO DE RESPOSTA A INCIDENTE DE SEGURANÇA DA INFORMAÇÃO ENVOLVENDO DADOS PESSOAIS E DADOS PESSOAIS SENSÍVEIS

O Plano de Respostas a Incidentes de Segurança envolvendo dados pessoais (Plano de Resposta a Incidente) tem, como objetivo, descrever como o município procederá a partir de situações que identifiquem a ocorrência ou suspeita de um incidente de segurança da informação. Por sua gravidade, o município tem o compromisso de elaborar e aplicar imediatamente as melhores medidas técnicas e jurídicas que visem à transparência, confiança e agilidade.

Os principais agentes responsáveis por lidar com os incidentes de segurança são:

- **Notificador:** pessoa física ou sistema de monitoramento que comunicará imediatamente a equipe responsável sobre a ocorrência ou a mera suspeita de um Incidente.
- **Comitê de Privacidade:** grupo formado por pessoas envolvidas diretamente com a execução de tratamento de dados pessoais dentro da corporação, responsável por receber as notificações de incidentes de forma imediata, estruturando medidas ágeis e adequadas sobre o ocorrido.



12.2.2 FLUXO DE MEDIDAS NECESSÁRIAS EM CASO DE INCIDENTES COM DADOS PESSOAIS

Em 24 horas:

1 - notificar o Comitê sobre o incidente;

2. analisar o mapeamento de dados pessoais.

Em 48 horas:

1 - elaboração de *Data Breach Score* e confecção de parecer técnico;

2 - elaborar um Relatório de Impacto à Proteção de Dados Pessoais (DPIA);

3 - elaborar um plano de notificação do incidente de segurança da informação;

4 - comunicação ao titular dos dados pessoais sobre o incidente de segurança da informação;

5 - comunicação à Autoridade Nacional de Proteção de Dados (ANPD).

Em 72 horas:

1 - Elaborar relatório de providências adotadas e revisão do programa de governança em privacidade e proteção de dados pessoais;

12.2.3 FLUXO DE MEDIDAS NECESSÁRIAS EM CASO DE INCIDENTES COM DADOS PESSOAIS SENSÍVEIS

Em 24 horas:

1 - notificar o Comitê sobre o incidente;

2 - analisar o mapeamento de dados pessoais;

3 - elaboração de *Data Breach Score* e confecção de parecer técnico;

4 - elaborar um Relatório de Impacto à Proteção de Dados Pessoais (DPIA);

5 - elaborar um plano de notificação do incidente de segurança da informação;

6 - comunicação ao titular dos dados pessoais sobre o incidente de segurança da informação;

7 - comunicação à Autoridade Nacional de Proteção de Dados (ANPD);

8 - Comunicação ao Banco Central do Brasil.

Em 48 horas:

1 - elaborar relatório de providências adotadas e revisão do programa de governança em privacidade e proteção de dados pessoais.

Além disso, a ANPD disponibilizou no site do governo,[1] o quê, como, quando e por quem devem ser feitas as comunicações de incidente de segurança da informação com dados pessoais.

12.3 SUPERVISÃO

O supervisor de tecnologia da informação (TI) é o profissional responsável por realizar o monitoramento das atividades que suportam a rede da área de informática de uma instituição, envolvendo a elaboração de projetos de implantação, desenvolvimento e integração de sistemas.

O supervisor de TI é responsável pela realização de planejamento de projetos, atendendo às necessidades e negócios da instituição, atuando na parte de dados informáticos, administrando e controlando o centro de processamento da instituição, realizando manutenções e instalações dos equipamentos informáticos, garantindo o cumprimento das políticas de segurança da informação, dentre muitas outras funções.

12.3.1 MEDIDAS PARA A MITIGAÇÃO DE RISCOS

Dentre as principais medidas que podemos apresentar para a mitigação de riscos envolvendo incidentes de segurança da informação, encontram-se desde pontos muito simples, que podem ser adotados no dia a dia das pessoas, como a instalação de um antivírus e a recomendação de não abertura de e-mails de endereços desconhecidos, até mesmo questões mais complexas, como a atualização de sistemas (principalmente os sistemas de proteção e operacionais).

Importante mencionar, ainda, a recomendação de estabelecer políticas de segurança da informação e treinamentos a serem ministrados a todos os funcionários de uma organização. É essencial que os funcionários sejam treinados para que saibam como agir diante de situações que podem configurar como uma tentativa de provocar um incidente e, mesmo, diante de um incidente de segurança da informação propriamente dito.

Por fim, as políticas são excelentes maneiras de formalizar como a organização trata os sistemas, informações e processos, e são essenciais para o dia a dia de uma organização.

1 Essas informaçõs podem ser encontradas no seguinte endereço eletrônico: https://www.gov.br/anpd/pt-br/assuntos/incidente-de-seguranca.

13 A IMPORTÂNCIA DA PROTEÇÃO DE DADOS NO SISTEMA EDUCACIONAL – GOVERNANÇA DE DADOS PESSOAIS: UMA QUESTÃO VOLTADA PARA O SISTEMA EDUCACIONAL BRASILEIRO

Desde as origens dos tempos, a humanidade vem buscando formas de otimizar suas atividades, trazendo celeridade, por meio do armazenamento de dado que, antes, era físico; porém, na atualidade, é quase que, em sua integralidade, virtual. Sabendo que os dados pessoais podem ser caracterizados como sensíveis, tendo seu acesso restrito ou reservado, ocorreu a necessidade de os países promulgarem regulamentos para a proteção dos dados pessoais. Essas normas de proteção, por exemplo, na União Europeia (UE), já são maduras e servem de modelo para as demais nações mundiais, por serem consideradas **padrão-ouro** em todo o mundo.

Nos últimos anos, os cidadãos do globo assistiram à veloz transformação tecnológica de suas vidas, a qual aconteceu de maneira inimaginável; por isso, esses regulamentos estão em constante revisão.

A União Europeia, por exemplo, em 2016, teve, como uma de suas maiores conquistas, o Regulamento Geral de Proteção de Dados (RGPD), substituindo a Diretiva de Proteção de Dados de 1995, a qual foi adotada no momento em que a internet estava em seu início. Esse regulamento (GDPR) é, agora, reconhecido como uma lei de referência, que vem servindo de inspiração para os outros países, assim como o Brasil. No mundo inteiro, há mais de 125 países com legislações de proteção de dados pessoais. Muitas nações já possuem legislação para regulamentar a coleta e o processamento de dados pessoais. Nesse sentido, a nação brasileira também teve que se adequar para se tornar mais competitiva e aderente, conforme os ditames internacionais.

A Lei Geral de Proteção de Dados (LGPD) foi desenhada para se "harmonizar" com as demais leis de privacidade de dados mundiais, primando por oferecer maior proteção e direitos aos indivíduos. A Lei n. 13.709/2018, LGPD, possui acepções humanitárias, uma vez que o dado pessoal pertence, pelo viés legal, ao seu titular, o qual deveria ter autonomia para decidir como deseja que suas informações pessoais sejam tratadas.

Nesse sentido, o sistema educacional brasileiro precisa estar voltado para a conscientização do indivíduo desde sua mais tenra idade, uma vez que o dado de cada indivíduo também configurar-se-á como elemento básico do ser humano, envolvendo princípios, valores, propósitos e até direitos civis e políticos, direitos econômicos, direitos sociais e culturais, direitos difusos e coletivos.

Na esfera educacional, a proteção de dados envolverá muito além do processo de facilitar o aprendizado e aquisição do conhecimento, de habilidades, de crenças e de hábitos. Inclui a conscientização

de que os dados pessoais de cada pessoa são direitos fundamentais, de liberdade e de privacidade, o que permite o desenvolvimento da personalidade da pessoa natural.

O sistema de ensino vem migrando, por exemplo, da modalidade presencial para a versão remota e à distância. Trabalha-se, em sala de aula, inclusive, componentes interligados aos conteúdos e às habilidades. Todas as escolas, universidades e ambientes educacionais precisarão se adaptar para evitar sanções que podem ir desde um mero bloqueio de banco de dados até à aplicação de severas multas.

Dessa maneira, não só o planejamento em sala de aula deverá ser alterado, como também a postura de todas as instituições de ensino em nosso país.

O anteparo para o tratamento de dados nas unidades de organização institucional no âmbito do ensino é imprescindível, pois promoverá: a privacidade; a autodeterminação informativa; a liberdade de expressão, de informação, de comunicação e de opinião; a inviolabilidade da intimidade, da honra e da imagem; o desenvolvimento econômico e tecnológico e a inovação; a livre iniciativa, a livre concorrência e a defesa do consumidor; os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

As escolas, academias, colégios, faculdades, universidades, institutos, *edutechs*, regionais de ensino trabalham com uma quantidade inimaginável de informações pessoais, o que inclui dados como nome completo do aluno, endereços, tipo sanguíneo, filiação, telefones de contato, informações médicas, imagens, CPF, número da identidade, gênero, data e local de nascimento, e-mail, estado de saúde, desempenho acadêmico e muito mais. Não só dados de estudantes são armazenados nas instituições de ensino. Há informações pessoais de professores, funcionários, colaboradores etc.

Em tempo, importante destacar que, além das instituições de ensino que contemplam Lei de Diretrizes e Bases da Educação Brasileira (LDB 9394/96), em nosso país, há o advento das Edtechs, as quais são empreendimentos com atividade empresarial focada na criação de soluções contemporâneas, revolucionárias e inovadoras para a educação. As Edtechs, englobando as startups, por sua finalidade e quando bem estimuladas pelo governo local, trabalham com tecnologia como sua principal ferramenta. Essas microempresas, starups e empresários que se transformam e empreendem em favor da educação brasileira oferecem, plataformas de ensino, cursos online, jogos educativos, sistemas de estímulo ao aprendizado, games pedagógicos, entre outras iniciativas. Assim, o gestor público precisará voltar sua atenção para as possíveis e variadas retenções de dados pessoais que são de fulcral relevância.

Os arquivos físicos e digitais do sistema educacional brasileiro estão repletos de nomes e datas de nascimento de funcionários e alunos. Existem fotos que confirmam sua identidade e podem ser vinculadas a informações pessoais adicionais; números da Previdência Social; informações de recrutamento; registros financeiros, como informações fiscais e dados bancários; informações relativas ao comportamento e à frequência; registros médicos; condições médicas; avaliações de desenvolvimento pessoal e outras. Além disso, há as informações relacionadas a candidatos a empregos, gestores, servidores públicos e privados, funcionários e voluntários que venham a ter relação com o ambiente educacional.

Por esse grande volume de dados, deverá ser impulsionada uma mudança imediata na operação e no tratamento realizado por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados esses e outros dados.

Salienta-se que a proteção de dados pessoais no universo educacional deverá contemplar mais que a esfera administrativa e de armazenamento. Ela estará consagrada quando fizer parte da mudança cultural com a aplicação de métodos educacionais que incluem o ensino, o treinamento, o debate, a discussão e a pesquisa direcionada com vistas ao estímulo e observância da boa-fé.

As instituições de ensino municipal, estadual e federal deverão 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. Essa proteção de dados refere-se à proteção de informações privadas e importantes contra comprometimento, corrupção e perda.

Assim, muito mais que a gestão da massa documental e de informações internas, o ambiente educacional necessitará ampliar os horizontes de uma sociedade orientada a dados físicos e virtuais, à medida que a quantidade de informações criadas e armazenadas se expanda, ano a ano.

Dessarte, o Brasil como um todo, diante da regulamentação de proteção de dados de cada indivíduo, precisará aderir às diretrizes rígidas publicadas, voltando-se a um esforço conjunto para destacar a importância da proteção de dados nos setores privado, público e terceiro.

O processamento de dados pessoais armazenados em sites de instituições de ensino, papéis, servidores e bancos de dados é coberto pela LGPD e por normas internacionais. De maneira crítica, a Administração Pública e privada terá que realizar avaliações rigorosas do impacto da proteção de dados ao atualizar softwares, alterar a infraestrutura de tecnologia da informação e comunicação (TIC) ou introduzir uma nova tecnologia que lida com dados pessoais.

O direito de proteção de dados configura um direito de personalidade do individuo, o que demanda esforço do aparato estatal para sua tutela legal. Devido à interdisplinaridade essencial ao tema de proteção de dados, exige-se que as instituições de ensino busquem entender o conceito e funcionamento, reservado na medida em que cabe ao sistema de ensino propagar a prática social e o desenvolvimento do ser humano. Dessa forma, apenas com a governança de dados será possível fomentar potencialidades, habilidades e competências, além de zelar pelo direito fundamental de todos, perpassando pelo desenvolvimento humano através do ensino e da aprendizagem para desenvolver e potencializar a capacidade intelectual de todos os indivíduo e partes interessadas, a fim de assegurar limites éticos.

A LGPD é uma legislação extremamente essencial para o setor de educação, pois, ao cumpri-la, a Administração Pública estará muito mais alinhada às políticas e procedimentos que poderão favorecer ao desenvolvimento nacional por meio da legalidade, da justiça, da transparência, da prestação de contas, da equidade e da responsabilidade corporativa.

Apenas com a junção de esforços, bem como com a intenção cooperativa, poderemos aliar a mudança de postura de cada indivíduo, de cada aluno e de cada instituição de ensino para efetivamente preservar os direitos dos titulares de dados pessoais.

REFERÊNCIAS

BRASIL. Presidência da República. **Comunicação de incidentes de segurança**. 21 jul. 2021. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/incidente-de-seguranca. Acesso em: 9 set. 2021.

BRASIL. **Lei n. 3.709, de 14 de agosto de 2018**. Dispõe sobre a proteção de dados pessoais e altera a Lei nº12.965, de 23 de abril de 2014 (Marco Civil da Internet). **Diário Oficial da República Federativa do Brasil**, 15 agosto de 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 9 set. 2021

BRITES, Elise. Os Desafios da Lei Geral de Proteção de Dados – LGPD: Medida Provisória Prorroga LGPD – Medida Provisória nº 959, de 3 de maio de 2020. **Jus Brasil**, 2020. Disponível em: https://elisebrites.jusbrasil.com.br/artigos/846573208/os-desafios-da-lei-geral-de-protecao-de-dados-lgpd?ref=serp. Acesso em: 9 set. 2021.

CAMPOS, A. **Sistemas de Segurança da Informação**. 2 .ed. Florianópolis: Visual Books, 2007.

IBGC. Instituto Brasileiro de Governança Corporativa. **Governança Corporativa**. [202-?]. Disponível em: https://www.ibgc.org.br/conhecimento/governanca-corporativa. Acesso em: 9 set. 2021.

INSTITUTO LATINO-AMERICANO DE GOVERNANÇA E COMPLIANCE PÚBLICO. **Governança pública municipal: Transformando sua administração**. Brasília: NT, 2020. [E-book]. Disponível em: https://www.rgb.org.br/cartilha-rgb-1. Acesso em: 9 set. 2021.

MACIEL, Rafael Fernandes. **Manual Prático sobre a Lei Geral de Proteção de Dados Pessoais** (Lei nº 13.709/18). 1. ed. Goiânia: RM Digital Education, 2019. MONTEIRO, Sheila de Góes. Gestão de riscos, Ameaças e Vulnerabilidades. Estácio de Sá, Rio de Janeiro, 2018.

SEBRAE. **Seja um prefeito empreendedor:** dicas e ações do Sebrae. Brasília: Sebrae, 2021. Disponível em: https://www.prefeitoempreendedor.sebrae.com.br/guia-do-prefeito/. Acesso em: 9 set. 2021.

IGCP

INSTITUTO LATINO-AMERICANO
DE GOVERNANÇA E COMPLIANCE PÚBLICO

RGB

DA GOVERNANÇA
À ESPERANÇA

Enap