Manual de Proteção de Dados Pessoais

LGPD Pernambuco

Secretaria da Controladoria Geral do Estado

GOVERNO DO ESTADO
PERNAMBUCO
MAIS TRABALHO, MAIS FUTURO.

Expediente

GOVERNO DO ESTADO DE PERNAMBUCO

PAULO HENRIQUE SARAIVA CÂMARA
Governador do Estado

LUCIANA BARBOSA DE OLIVEIRA SANTOS
Vice-Governadora do Estado

MARCONI MUZZIO PIRES DE PAIVA FILHO
Secretário da Controladoria-Geral do Estado
Ouvidor-Geral do Estado

FILIPE CAMELO DE CASTRO
Secretário-Executivo da Controladoria-Geral do Estado

CARMEN RAQUEL NUNES SILVA
Diretora de Tecnologia da Informação do Controle Interno – DTCI

RENATO BARBOSA
Coordenador de Proteção de Dados

ELABORAÇÃO:

RENATO BARBOSA CIRNE
Gestor Governamental - Controle Interno

KARLOS GUSTAVO ARAGÃO BUNGENSTAB
Gestor Governamental - Controle Interno

REVISÃO:

CARMEN RAQUEL NUNES SILVA
Gestora Governamental - Controle Interno

ÉRIKA GOMES LACET
Procuradora do Estado

www.scge.pe.gov.br | www.transparencia.pe.gov.br
www.ouvidoria.pe.gov.br | www.lai.pe.gov.br

Instagram: @scge_pe

SECRETARIA DA CONTROLADORIA-GERAL DO ESTADO
Rua Santo Elias, 535 - Espinheiro - Recife - PE - CEP: 52020-095
Telefone: 81.3183-0800

Sumário

Introdução

Em um cenário de forte demanda por serviços públicos de qualidade, eficientes, éticos e transparentes, é essencial promover a orientação dos servidores públicos. Dessa forma, será possível agregar valor ao atendimento das demandas da sociedade.

Nesse contexto, a Lei Geral de Proteção de Dados Pessoais - LGPD, Lei Federal no 13.709, de 14 de agosto de 2018, impôs um novo desafio ao regulamentar o tratamento dos dados pessoais por parte de entidades públicas e privadas. Ciente das implicações nos serviços públicos estaduais, o estado de Pernambuco editou o Decreto Estadual no 49.265, de 06 de agosto de 2020, instituindo a Política Estadual de Proteção de Dados Pessoais - PEPDP.

Nota-se, portanto, a necessidade de promover a sensibilização da gestão estadual quanto aos controles e aos atos de gestão necessários para adequação dos serviços públicos, com especial ênfase à proteção de dados pessoais.

Espera-se, assim, que a produção de materiais orientativos ajude no alcance desse objetivo, ao destacar conceitos, metodologias, controles, experiências, práticas e funcionamento dos normativos aplicados à proteção de dados.

Por ser um tema de relevância geral, uma vez que impactará todas as atividades da gestão pública estadual que tratam dados pessoais, o conteúdo desse material estará focado para a compreensão dos principais aspectos da Lei e visa alcançar todos os servidores públicos estaduais.

O Manual de Proteção de Dados Pessoais em Pernambuco tem por objetivo sensibilizar a gestão estadual, promover os controles e atos de gestão necessários para implantação da Política Estadual de Proteção de Dados Pessoais – PEPDP e produzir orientações práticas para a mudança cultural dos órgãos e entidades da Administração Pública Estadual direta, autárquica e fundacional no tratamento de dados pessoais.

A temática será abordada em quatro capítulos, seguindo uma estrutura lógica de aprendizado. Inicialmente, será apresentada a origem da Lei, o histórico e as influências que embasaram o texto atual, assim como, os principais conceitos relacionados ao tema que serão usados nos capítulos seguintes, uma vez que a Lei institui novos termos no ordenamento jurídico, como dado sensível, anonimização e tratamento. O documento também abordará os princípios norteadores da proteção de dados, com objetivo de facilitar a compreensão do conteúdo e suas repercussões.

Em seguida, o material elencará os principais requisitos no tratamento de dados, explicando as bases legais e relacionando-as a situações práticas de tratamento de dados. Assim como, serão mencionadas: as exigências estabelecidas para os dados sensíveis e dados de crianças e adolescentes; e as obrigações específicas para a gestão pública.

Na terceira parte desse material, os direitos dos titulares virão à tona e será abordado como o estado de Pernambuco está estruturado para atendê-los, com a indicação dos canais e os requisitos de atendimento. Nesse mesmo capítulo, será possível conhecer também o relacionamento da LGPD com a Lei de Acesso à Informação (LAI) na divulgação de dados pessoais, indicando situações práticas de como solucionar esse aparente "conflito", e as principais ressalvas no compartilhamento de dados pessoais.

Ainda, será apresentado como Pernambuco estruturou a Política Estadual de Proteção de Dados Pessoais – PEPDP. Por fim, o Manual abordará o modelo de governança, as principais responsabilidades de cada unidade estadual envolvida e as diretrizes e especificidades dadas pelo Decreto Estadual nº 49.265/2020.

Capítulo 1 – Origem, princípios, normas e conceitos advindos da LGPD

Em uma sociedade cada vez mais orientada a dados, cresce o número de uso abusivo de dados pessoais, como a comercialização ilegal e a sua exploração para outras finalidades. Em 2013, considerado um marco por expor a magnitude desse problema, vieram a público relatos de uso indevido das principais empresas de internet sediadas nos Estados Unidos da América, entre elas o Google e o Facebook, ao violarem a privacidade de seus usuários.

Como forma de inibir tais situações, surgem ações voltadas à proteção do titular do dado, como a promulgação de legislações garantidoras dos diversos direitos do indivíduo relacionados à privacidade e à criação de autoridades independentes fiscalizadoras.

Neste contexto, é promulgada a Lei Geral de Proteção de Dados Pessoais - LGPD, Lei Federal nº 13.709, de 14 de agosto de 2018, que regulamenta o tratamento dos dados pessoais por parte de entidades públicas e privadas, e se alinha às principais legislações sobre privacidade e tratamentos físicos e eletrônicos de dados pessoais em vigência em outros países.

Para implementar a proteção de dados pessoais, é necessário compreender, além da Lei e da sua origem, alguns conceitos básicos, como: "O que é um dado pessoal?", "O que o difere de um dado sensível?", "O que contempla as operações de tratamento de dados pessoais?" e "Como definir o titular do dado pessoal, controlador, operador e encarregado?".

1.1. A proteção de dados no mundo

Conforme Comissão Especial de Análise do Projeto da LGPD (CÂMARA FEDERAL, 2018), a fonte de inspiração da Lei advém do arcabouço europeu, dada a sua experiência no tema. O primeiro instrumento daquele bloco na temática é a Convenção do Conselho da Europa nº 108, de 1981, "Convenção para a Proteção de Indivíduos com Respeito ao Processamento Automático de Dados Pessoais", seguida da Diretiva Europeia nº 46, de 1995, conhecida como Diretiva de Proteção de Dados. Em terceiro lugar, cita-se a Diretiva nº 58, de 2002, focada na proteção da privacidade no âmbito das comunicações eletrônicas.

Em 2016, o sistema regulatório europeu foi finalmente revisado com a aprovação do **Regulamento Geral sobre a Proteção de Dados (RGPD)**, Regulamento nº 679, ou "General Data Protection Regulation (GDPR)". O regulamento trata da proteção das pessoas naturais com respeito ao processamento de dados pessoais e ao livre movimento desses dados. Por fim, em 25 de maio de 2018, o RGPD entra em vigor na União Europeia (UE), revogando a Diretiva nº 46/95 e unificando o quadro regulamentar europeu.

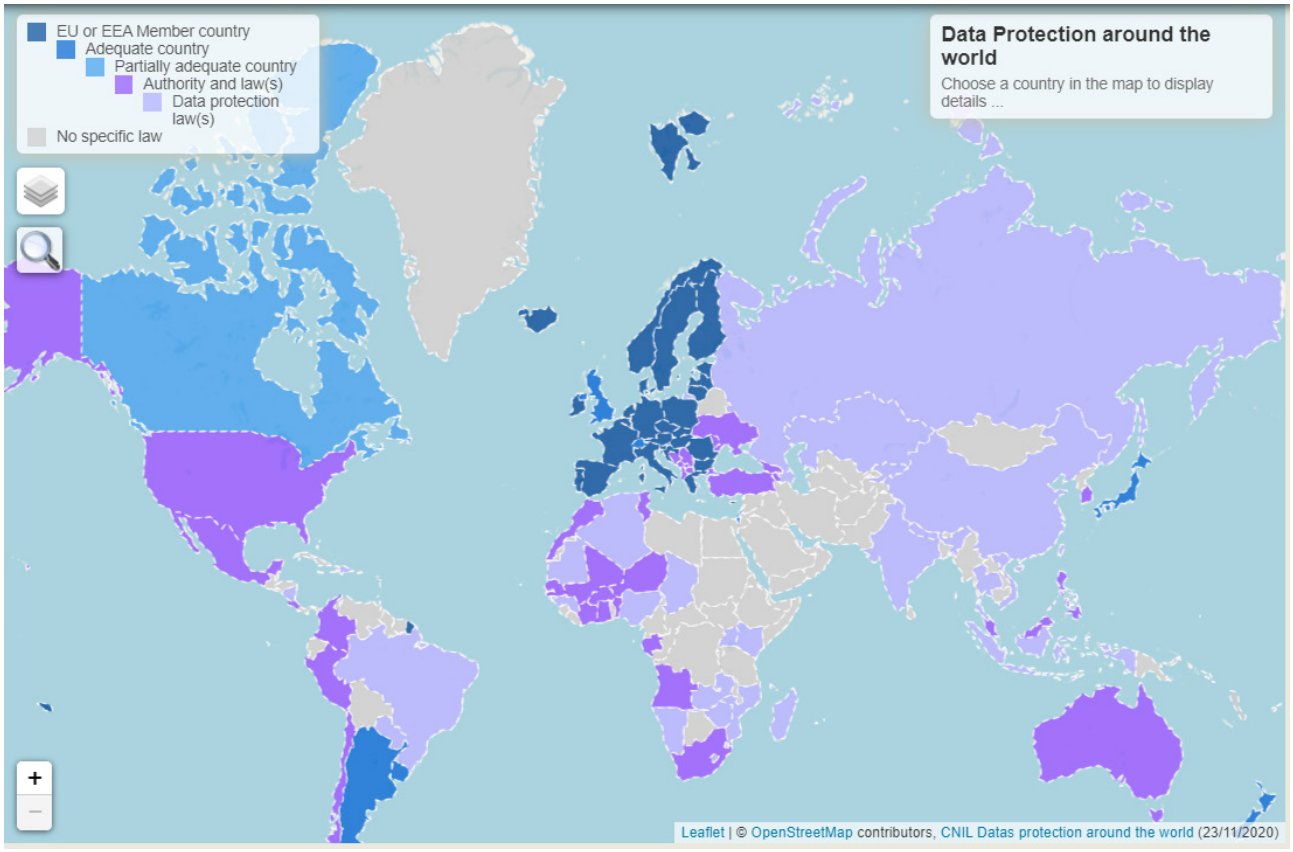

Figura 1. Mapa de Regulamentação de Proteção de Dados

Fonte: *Commission Nationale de l'Informatique et des Libertés (CNIL),* https://www.cnil.fr/en/data-protection-around-the-world

Descrição: A imagem apresenta o mapa-múndi com a indicação de intensidade de regulamentação por cor e por país.

Tal conjunto histórico de normas europeias demonstra que o tema "privacidade" já se encontrava devidamente internalizado nos países que compõem o bloco europeu há anos. Nesta contextualização internacional, é importante observar que o Regulamento não permite a transferência internacional de dados para países que não possuam legislação que garanta a mesma proteção dada pela Lei Europeia.

Além de reconhecer a relevância da informação pessoal para o indivíduo e a sociedade, proporcionando a esses, ferramentas e estruturas para que o titular

possa controlar o uso de seus dados, a Lei brasileira também foi concebida considerando a atratividade comercial do setor de TIC (Tecnologia da Informação e das Comunicações) dos países. Em tempos de computação em nuvem, um país que atenda à legislação europeia possui condições de atrair processamento de dados daquele bloco, além de estreitar suas relações comerciais. E atrair o tratamento de dados implica não só a possibilidade de instalação de centros de processamento de dados no território nacional, mas de investimento internacional das próprias empresas de TIC. Por isso, surgiu a necessidade de o Brasil possuir, sem renunciar as suas especificidades e soberania, uma legislação harmônica com o mundo e com os principais blocos organizados, como a União Europeia.

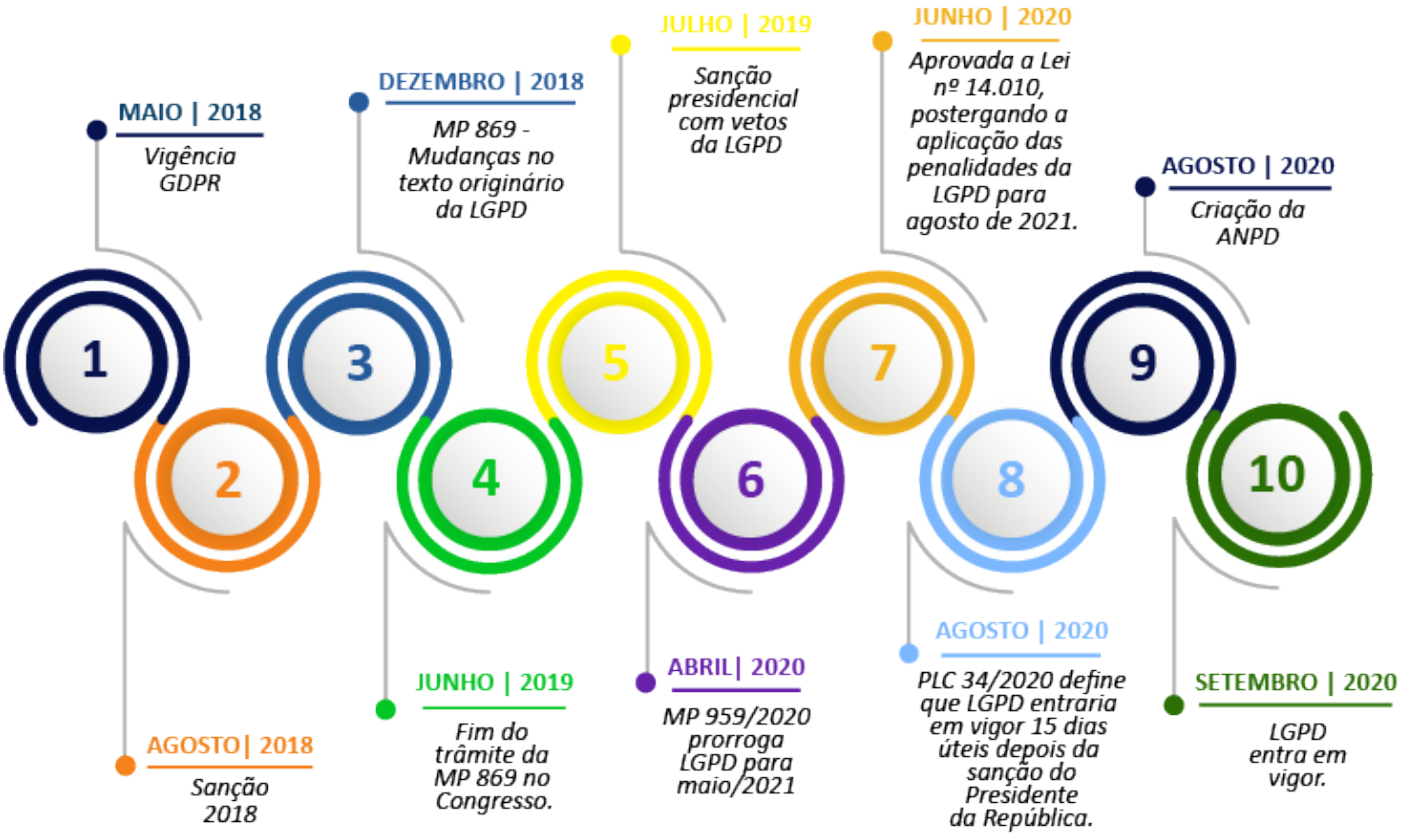

Figura 2. Linha do Tempo da LGPD

Fonte: Secretaria da Controladoria Geral do Estado de Pernambuco (SCGE-PE)

Descrição: A imagem apresenta linha do tempo em 10 etapas desde a vigência do GDPR em maio de 2018, até a vigência da LGPD em setembro de 2020.

A LGPD foi aprovada em 2018, e estava prevista para entrar em vigor no dia 14 de agosto de 2020. Cumpre lembrar que, após inúmeras alterações e postergações, conforme Figura 2, mesmo com o pedido de adiamento da vigência da Lei para maio de 2021, a proposta foi rejeitada por unanimidade pelo Congresso Brasileiro.

Por fim, depois de diversas sugestões de modificações, especialmente devido à pandemia da Covid-19, o Projeto de Lei (PL) nº 1179/2020 foi sancionado e convertido na Lei nº 14.010/2020 que **manteve a vigência da LGPD para setembro de 2020, mas com a condição de que as multas e sanções só começariam a valer a partir de 1º de agosto de 2021.**

1.2 – LGPD - Fundamentos legais

A LGPD tem por objetivo dar resposta apropriada aos rápidos avanços tecnológicos e à globalização, que trouxeram novos níveis de coleta e de compartilhamento de dados pessoais, inclusive transferidos internacionalmente. O normativo estabelece novos controles, bem como entrega às pessoas naturais o poder efetivo sobre seus próprios dados, detalhando os conceitos de transparência e de consentimento destacado, assim como, dados sensíveis, genéticos, anonimização, legítimo interesse e tratamento global (transferência internacional) dos dados pessoais.

Conforme ensina DA MOTA ALVES (2021), entre os elementos essenciais da lei brasileira, está o reconhecimento expresso do direito à privacidade e à autodeterminação informativa, permitindo a organização do marco legal em quatro ambientes de regulação: (I) fundamentos, princípios, aplicabilidade e conceitos; (II) direitos do titular; (III) obrigações regulatórias; e (IV) fiscalização, penalidades e regras de transição.

Assim, a LGPD institui um regime geral de proteção de dados no ordenamento brasileiro e disciplina as condições e os termos de compartilhamento de dados pessoais entre entidades que fazem uso de bancos de dados com informações dessa natureza, sejam eles físicos ou digitais. Além disso, estabelece a tutela fiscalizatória e sancionatória e obriga os responsáveis pelo tratamento dos dados a se ajustarem às diretrizes de defesa ao consumidor e cria a **Autoridade Nacional de Proteção de Dados Pessoais (ANPD)**, entidade responsável por fiscalizar o cumprimento da Lei.

Segundo a Autoridade Nacional de Proteção de Dados Pessoais (ANPD) (2021), a LGPD tem por objetivo proteger os direitos fundamentais relacionados à esfera informacional do cidadão. Assim, a Lei introduz uma série de novos direitos que asseguram maior transparência quanto ao tratamento dos dados e conferem protagonismo ao titular quanto ao seu uso. Além disso, a ANPD assume que a constituição de um ambiente jurídico voltado à proteção de dados pessoais corresponde também ao alinhamento com diretrizes da Organização

para a Cooperação e Desenvolvimento Econômico – OCDE, que há décadas vem desempenhando um relevante papel na promoção do respeito à privacidade como um valor fundamental e como um pressuposto para o livre fluxo de dados.

É possível acessar a LGPD através do seguinte link: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Lei/L13709.html

Figura 3. Conteúdos impactados pela LGPD

Fonte: Secretaria da Controladoria Geral do Estado de Pernambuco (SCGE-PE)

Descrição: A imagem apresenta uma lista de conteúdos impactados pela LGPD como: tutela da saúde, execução de contratos, proteção ao crédito, proteção da vida, exercício regular do direito, pesquisa.

Isto posto, todos os setores, seja público ou privado, devem operar de forma harmônica, internalizando os conceitos e princípios e instituindo procedimentos que irão uniformizar o tratamento de dados pessoais para o benefício do cidadão e com um potencial e expressivo ganho em termos de confiança e qualidade dos serviços.

Como já exposto acima, a ANPD, cuja estrutura restou regulamentada pelo Decreto Federal nº 10.474/2020, é o órgão responsável pela supervisão da Lei, por elaborar as diretrizes para a Política Nacional de Proteção de Dados Pessoais e Privacidade e promover a regulamentação dos setores que tratam dados pessoais. Entre as atribuições da ANPD está a de coordenar as ações com os órgãos e entidades responsáveis por setores específicos da atividade econômica para promover o seu adequado funcionamento, conforme as disposições regulamentares e a legislação.

Atualmente, a ANPD é órgão da administração pública federal integrante da Presidência da República e, a despeito de ser órgão, os membros de seu Conselho, embora designados pelo Presidente da República, têm mandato e somente o perderão em virtude de renúncia, condenação judicial transitada em julgado ou pena de demissão decorrente de processo administrativo disciplinar, o que reforça a autonomia técnica da autoridade (ANPD, 2021).

1.2.1 – Aplicação Territorial

As regras relativas à **aplicação territorial da Lei** encontram-se dispostas no seu art. 3º. Em síntese, a LGPD define que são **irrelevantes o meio, país da sede ou país onde estejam localizados os dados** desde que ocorra uma das três hipóteses:

> *Art. 3º Esta Lei aplica-se a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que:Art. 31. O tratamento das informações pessoais deve ser feito de forma transparente e com respeito à intimidade, vida privada, honra e imagem das pessoas, bem como às liberdades e garantias individuais.*
>
> *I - a operação de tratamento seja realizada no território nacional;*
>
> *II - a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; ou*
>
> *III - os dados pessoais objeto do tratamento tenham sido coletados no território nacional.*

Segundo MALDONADO et al. (2019), a primeira hipótese delas concerne à aplicação territorial clássica, que se impõe à sede da entidade e à hipótese em que ocorra operação de tratamento dentro do território nacional. Ou seja, trata-se de **agente de tratamento sediado no Brasil ou de operação realizada no País, impondo-se a aplicação da LGPD.** A terceira hipótese concerne à situação em

que os dados pessoais tenham sido **coletados no território nacional**, sendo dessa forma, de certa medida, redundante à primeira hipótese, uma vez que a coleta é considerada operação de tratamento, conforme será citado no tópico 1.5 – Tratamento de Dados deste Manual.

A segunda hipótese refere-se à oferta ou fornecimento de bens ou serviços ou ao tratamento de dados de indivíduos localizados no território nacional. É importante destacar que as hipóteses não são cumulativas. Assim, é a segunda hipótese a que traz a aplicação extraterritorial. Ou seja, independentemente de onde esteja localizado o agente de tratamento, estará abrangido pela legislação brasileira se atuar em **oferta ou fornecimento de bens ou serviços a quem esteja no território nacional** ou se tratar os seus dados. Isto porque os negócios digitais são passíveis de, potencialmente, ser acessados de qualquer lugar do mundo (MALDONADO et. al, 2019).

1.2.2 – Legislações Correlatas

Por óbvio, é importante reconhecer as legislações correlatas que estão diretamente ou indiretamente relacionadas com a proteção de dados pessoais, tais como: Código Civil; Marco Civil da Internet; Código de Defesa do Consumidor – CDC; Lei do Cadastro Positivo; Lei Carolina Dieckmann; e na esfera pública, a Lei de Acesso à Informação.

Código Civil – Lei Federal nº 10.406, de 10 de janeiro de 2002

Busca determinar como as pessoas naturais e jurídicas devem se relacionar e agir em sociedade, como por exemplo: direitos da personalidade, o casamento, a sucessão familiar, entre outros aspectos legais comuns às relações de uma sociedade.

Código de Defesa do Consumidor (CDC) – Lei Federal nº 8.078, de 11 de setembro de 1990

Objetiva regulamentar a proteção e defesa aos direitos do consumidor, bem como as responsabilidades de fornecedores, sendo “consumidor”, toda pessoa física ou jurídica que adquire ou utiliza um produto ou serviço e “fornecedor”, toda pessoa física ou jurídica, pública ou privada, nacional ou estrangeira que desenvolve atividades de produção, montagem, criação, construção, transformação, importação, exportação, distribuição ou comercialização de produtos ou prestação de serviços.

Marco Civil da Internet – Lei Federal nº 12.965, de 23 de abril de 2014

Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Reconhece para o ambiente virtual princípios constitucionais como a liberdade de expressão, a privacidade e os direitos humanos, além de definir responsabilidades dos provedores de serviços e orientar a atuação do Estado no desenvolvimento e uso da rede.

Lei do Cadastro Positivo – Lei Federal nº 12.414, de 9 de junho de 2011

Objetiva, através do banco de dados, definir score de crédito e, eventualmente, conceder taxas menores às pessoas físicas e jurídicas. Acaba repercutindo em bancos, comércio, concessionárias de água, energia e telefonia que são responsáveis por enviar dados de pessoas físicas e jurídicas às agências de crédito, que, por sua vez, criam pontuação sobre a pessoa que será consultada ao tentar linhas de crédito.

Lei Carolina Dieckmann – Lei nº 12.737, de 30 de novembro de 2012

Contempla a proteção de dados ao tipificar crimes relacionados à invasão de dispositivo informático para obtenção, adulteração e destruição de dados ou informações sem a autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita.

Lei de Acesso à Informação (LAI) – Lei Federal nº 12.527, de 18 de novembro de 2011

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. A Lei cria mecanismos que possibilitam a qualquer pessoa, física ou jurídica, sem necessidade de apresentar motivo, o recebimento de informações públicas dos órgãos e entidades. A LAI prevê como exceções à regra de acesso os dados pessoais, as informações classificadas por autoridades como sigilosas e as informações sigilosas com base em outras leis. Para a Lei, as informações pessoais não são públicas e terão seu acesso restrito, isto é, podem ser acessadas pelos próprios indivíduos e, por terceiros, apenas em casos excepcionais previstos na Lei.

1.3 - Dados Pessoais

Considera-se "**dado**", qualquer informação em potencial, porque os dados, em si, não possuem um significado próprio relevante. Eles se encontram no estado pré-informação e para ganharem o status informacional, requerem interpretação para posteriormente adquirirem sentido e poderem, assim, ser compreendidos por alguém. A informação, por sua vez, alude a algo além da representação contida no dado, chegando ao limiar da cognição e, mesmo nos efeitos que esta pode apresentar para o seu receptor. Sem aludir ao conteúdo em si, na informação já se pressupõe uma fase inicial de depuração de seu conteúdo – daí que a informação carrega em si também um sentido instrumental, no sentido de uma redução de um estado de incerteza. A doutrina, não raro, trata estes dois termos indistintamente (DONEDA, 2019).

Neste contexto, cumpre destacar algumas importantes definições trazidas pela LGPD:

Dado pessoal: *informação relacionada à pessoa natural identificada ou identificável;*

Dados pessoais são aquelas informações relacionadas a uma determinada pessoa. Para a ANPD, a LGPD adota um conceito aberto de dado pessoal, definido como a informação relacionada a uma pessoa natural identificada ou identificável.

Além das informações básicas relativas ao nome, número de inscrição no Registro Geral (RG) ou no Cadastro Nacional de Pessoas Físicas (CPF) e endereço residencial, são também considerados dados pessoais outras informações que estejam relacionadas com uma pessoa natural, tais como seus hábitos de consumo, sua aparência e aspectos de sua personalidade. Dentre as diversas categorias de dados pessoais, podemos destacar os seguintes:

1. Estado civil, identidade, dados de identificação, imagens;
2. Vida pessoal (estilo de vida, situação familiar etc.);
3. Informações econômico-financeiras (receita, situação financeira, situação tributária etc.);
4. Dados de conexão (endereço IP, logs etc.);
5. Dados de localização (movimentos, dados de GPS, GSM etc.);
6. Dados relacionados à Segurança Social (PIS, PASEP etc.);

7. Dados revelando origem racial ou étnica;
8. Dados revelando opiniões políticas;
9. Dados revelando crenças religiosas ou filosóficas;
10. Dados revelando associação sindical;
11. Dados genéticos;
12. Dados biométricos com o objetivo de identificar exclusivamente uma pessoa singular;
13. Dados relativos à saúde;
14. Dados relativos à vida sexual ou orientação sexual de uma pessoa singular;
15. Dados relativos a condenações e infrações cíveis, administrativas e penais.

Figura 4. Dados Pessoais

Fonte: Secretaria da Controladoria Geral do Estado de Pernambuco (SCGE-PE)

Descrição: A imagem apresenta um avatar com o link de imagens que estão associadas a informações como localização, informações financeiras, imagem e biometria.

Ademais, segundo a LGPD, poderão ser igualmente considerados como dados pessoais aqueles utilizados para formação do perfil comportamental de determinada pessoa natural, se identificada.

Dado pessoal sensível: *dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou à 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*

Os dados pessoais sensíveis são aqueles aos quais a LGPD conferiu uma proteção ainda maior, por estarem diretamente relacionados aos aspectos mais íntimos da personalidade de um indivíduo.

Dado anonimizado: *dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento.*

Segundo VAINZOF (2018), a anonimização é um mecanismo que busca garantir proteção à personalidade humana por meio do desfazimento de qualquer tipo de vínculo capaz de associar, direta ou indiretamente, um dado ao seu respectivo titular, valendo-se, para isso, da utilização de meios técnicos razoáveis e disponíveis no momento do tratamento dos dados pessoais.

O dado anonimizado pode ser obtido por meio do emprego de técnicas, como:

- **randomização:** em que se busca alterar a veracidade dos dados para remover a forte ligação entre eles e o titular por meio da aplicação de ruído ou permutação, por exemplo.
- **generalização:** busca substituir os dados precisos por categorias mais amplas e genéricas. Assim, ao invés de atrelar o dado tratado à cidade dele proveniente, correlaciona-o à região, dando, portanto, uma localização menos detalhada a fim de quebrar o vínculo de identificação.

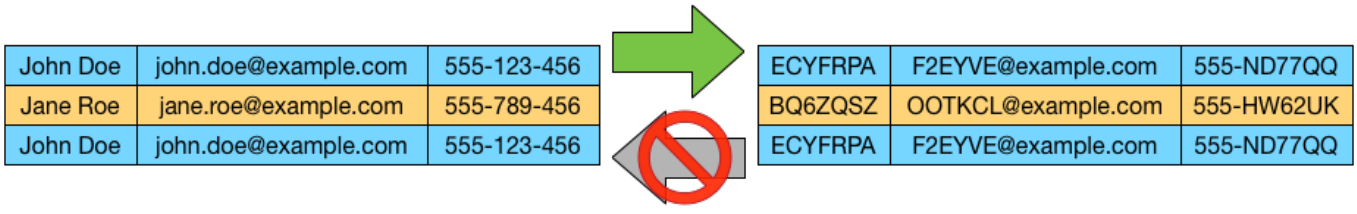

Figura 5. Processo de pseudonimização

Fonte: Pseudonimização e anonimização de dados para se adequar à LGPD (celsocestaro.com.br)

Descrição: A imagem tabela de dados pessoais que são anonimizadas pela técnica de randomização. Apesar de repetir o mesmo indivíduo na tabela, os dados anonimizados são diferentes.

1.4 - Titular do Dado Pessoal

Titular: *pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;*

O art. 1º da LGPD dispõe que a Lei versa sobre o tratamento de dados pessoais por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. Ou seja, a Lei concretiza, no plano infraconstitucional, a tutela da inviolável intimidade, vida privada, honra e imagem dos cidadãos, direitos já previstos na Constituição Federal (CF, art. 5º, X).

Há, dessa forma, de se destacar que somente dados pessoais acham-se abrangidos por seu escopo. Consequentemente, **dados relacionados a pessoas jurídicas não devem ser considerados para efeito da Lei, isto é, a LGPD não considera dados sigilosos organizacionais, segredos industriais, patentes, entre outras informações que não estão relacionadas a pessoa natural identificada ou identificável.**

1.5 - Tratamento de Dados

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

O Guia de Boas Práticas – Lei Geral de Proteção de Dados Pessoais (LGPD) (UNIÃO, 2020) detalha as operações de tratamento da seguinte forma:

- **ACESSO -** ato de ingressar, transitar, conhecer ou consultar a informação, bem como possibilidade de usar os ativos de informação de um órgão ou entidade, observada eventual restrição que se aplique;
- **ARMAZENAMENTO -** ação ou resultado de manter ou conservar em repositório um dado;

• **ARQUIVAMENTO -** ato ou efeito de manter registrado um dado em qualquer das fases do ciclo da informação, compreendendo os arquivos corrente, intermediário e permanente, ainda que tal informação já tenha perdido a validade ou esgotado a sua vigência;

• **AVALIAÇÃO -** analisar o dado com o objetivo de produzir informação;

• **CLASSIFICAÇÃO -** maneira de ordenar os dados conforme algum critério estabelecido;

• **COLETA -** recolhimento de dados com finalidade específica;

• **COMUNICAÇÃO -** transmitir informações pertinentes a políticas de ação sobre os dados;

• **CONTROLE -** ação ou poder de regular, determinar ou monitorar as ações sobre o dado;

• **DIFUSÃO -** ato ou efeito de divulgação, propagação, multiplicação dos dados;

• **DISTRIBUIÇÃO -** ato ou efeito de dispor de dados de acordo com algum critério estabelecido;

• **ELIMINAÇÃO -** ato ou efeito de excluir ou destruir dado do repositório;

• **EXTRAÇÃO -** ato de copiar ou retirar dados do repositório em que se encontrava;

• **MODIFICAÇÃO -** ato ou efeito de alteração do dado;

• **PROCESSAMENTO -** ato ou efeito de processar dados visando organizá-los para obtenção de um resultado determinado;

• **PRODUÇÃO -** criação de bens e de serviços a partir do tratamento de dados;

• **RECEPÇÃO -** ato de receber os dados ao final da transmissão;

• **REPRODUÇÃO -** cópia de dado preexistente obtido por meio de qualquer processo;

• **TRANSFERÊNCIA -** mudança de dados de uma área de armazenamento para outra, ou para terceiro;

• **TRANSMISSÃO -** movimentação de dados entre dois pontos por meio de dispositivos elétricos, eletrônicos, telegráficos, telefônicos, radioelétricos, pneumáticos etc.;

• **UTILIZAÇÃO -** ato ou efeito do aproveitamento dos dados.

Nesse contexto, resta claro que o tratamento de dados pessoais abrange um rol extenso de atividades e tem por objetivo reconhecer a responsabilidade de cada processamento do dado pessoal. Assim, a LGPD não adota qualquer tipo de segregação, considerando como tratamento, por exemplo, tanto a coleta quanto o armazenamento de dados pessoais, mesmo essas operações tratando de propósitos diferentes.

Além disso, a LGPD exige, de cada entidade – pública ou privada, uma estrutura de controle para gerenciar e auditar quem, e como é feito o acesso e a manipulação das suas bases de dados, a fim de garantir a sua integridade, ao prever a manutenção do registro das operações de tratamento de dados pessoais que realizarem (art. 37).

Vale ressaltar que não há uma definição de como será realizado esse registro. No entanto, conforme citado anteriormente, a referência do modelo europeu dá base de como poderia ser realizado. O RGPD (art. 30) não só previu a obrigação de manter o registro das atividades de tratamento de dados, como também o detalhou. Para noção do tipo de registro de um tratamento de dados pessoais, o dispositivo do RGPD apresenta o seguinte rol de informações:

1. a finalidade do tratamento;
2. descrição das categorias dos dados e dos titulares;
3. o fluxo dos dados para fora da organização;
4. as medidas de segurança;
5. informações de identificação e contato do controlador;
6. os períodos para a exclusão das diferentes categorias de dados.

Por fim, vale lembrar que a Lei destaca a aplicação de seus efeitos tanto nos meios digitais quanto nos meios físicos. Apesar de a existência majoritária de dados pessoais encontrarem-se, atualmente, em meios digitais, dada a transformação digital em curso, **os dados pessoais coletados e estruturados em formato físico também devem estar sujeitos aos mesmos mandamentos da Lei.**

1.6 - Ciclo de Vida do Dado

Como verificado no tópico anterior, o tratamento de dados contempla ao menos 20 exemplos de operações, algumas dessas manipulações são correlacionadas ao ciclo de vida do dado, que nada mais é do que uma sequência com início, desenvolvimento e fim ao qual o tratamento de dados perpassa. Em uma analogia simplificada temos o início do ciclo de vida do dado com a sua coleta, o desenvolvimento do dado com o seu processamento e, por fim, a eliminação encerra o ciclo de vida do dado pessoal.

O Guia de Boas Práticas da União (UNIÃO, 2020) determina que o ciclo de vida do tratamento de dados detém 5 fases, vide a seguir:

Figura 6. Fases do Ciclo de Tratamento

Fonte: Adaptado de Guia de Boas Práticas da União (UNIÃO, 2020)

Observa-se que recursos, documentos e sistemas estão envolvidos durante as fases do ciclo de tratamento. Além desses itens, as pessoas participam de diversas maneiras para viabilizar as operações nas fases que compõem o ciclo de vida do tratamento de dados. Denominam-se **ativos organizacionais** os indivíduos, documentos (digitais ou físicos), sistemas, base de dados e locais físicos que estão relacionados e se integram a uma das etapas do ciclo de vida do tratamento de dados (UNIÃO,2021).

O conhecimento de quais dados pessoais são tratados pela organização, os ciclos de vida dos mesmos e a correlação com os ativos organizacionais são requisitos que permitem uma elaboração adequada da implementação da política de proteção de dados e **é tema recomendado para o encarregado de dados**, que entre as competências mais relevantes **tem o dever de orientar a organização em que atua sobre as boas práticas de segurança de dados**. A figura a seguir apresenta cuidados básicos de cada fase:

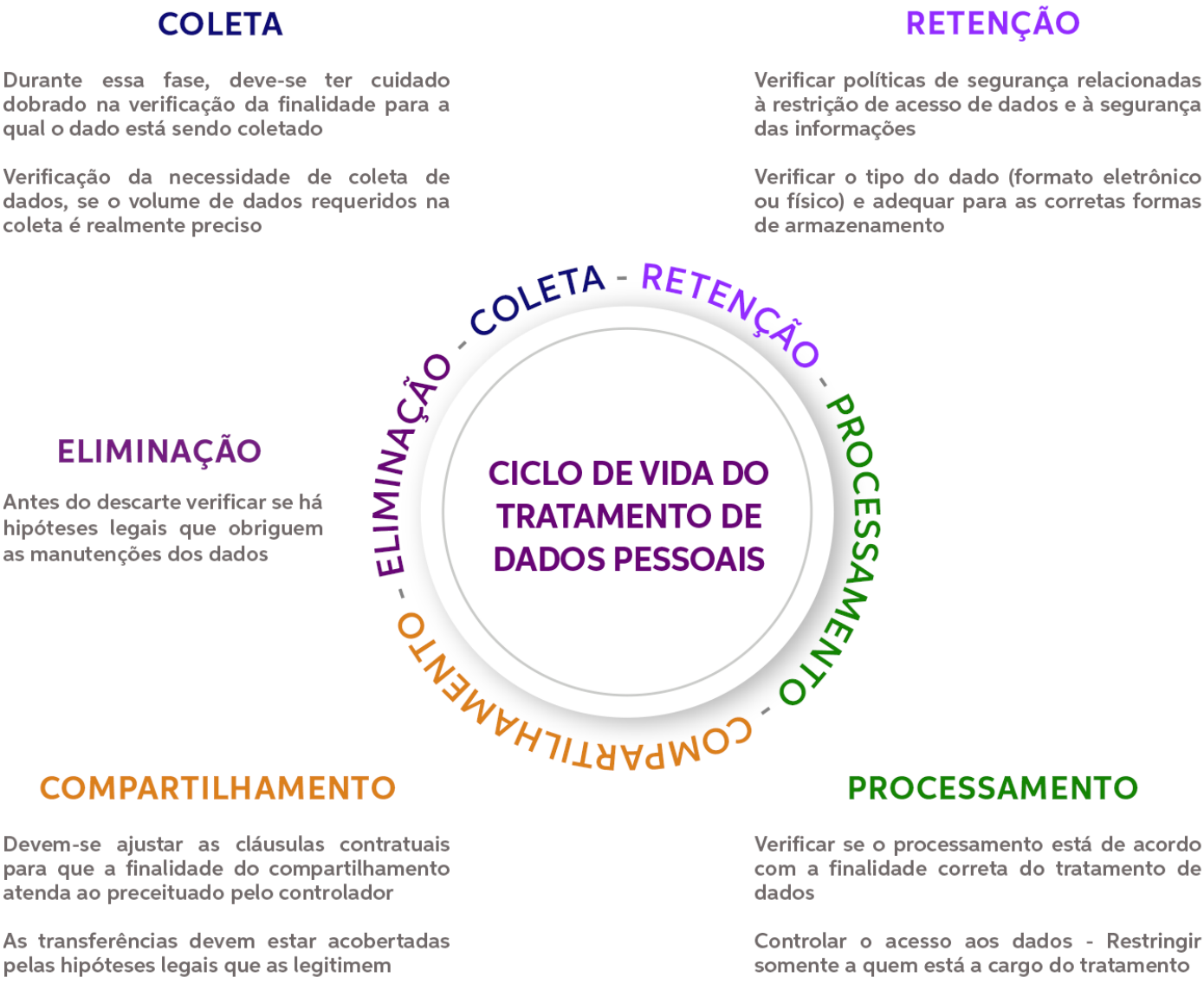

Figura 7. Especificidades das Etapas do Ciclo de Tratamento

Fonte: Adaptado de Guia de Boas Práticas da União (UNIÃO, 2021) e LGPD – Manual de Implementação (Maldonado, 2021).

1.7 - Princípios

É de se esperar que o tratamento de dados pessoais deve ser sempre pautado na boa-fé. Outro ponto importante, já destacado anteriormente, é definir bem o objetivo das operações de tratamento de dados pessoais. E mesmo com tais objetivos em mãos, será que sua entidade precisa dessa quantidade de dados

pessoais? Além disso, os dados pessoais podem gerar algum viés discriminatório? Será que todo o tratamento pode ser realizado sem que o titular tenha conhecimento do fato? Tais pontos e questões devem ser sempre considerados quando houver tratamento de dado pessoal. Nesse contexto, a LGPD listou em seu texto 10 (dez) princípios que devem ser considerados e observados nas atividades de tratamento de dados pessoais, que são:

1	**FINALIDADE**	Realização do tratamento para **propósitos legítimos**, **específicos**, **explícitos** e **informados** ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
2	**ADEQUAÇÃO**	**Compatibilidade** do tratamento com as **finalidades informadas** ao titular, de acordo com o **contexto** do tratamento;
3	**NECESSIDADE**	**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;
4	**ACESSO LIVRE**	**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;
5	**QUALIDADE DOS DADOS**	**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;
6	**TRANSPARÊNCIA**	**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;
7	**SEGURANÇA**	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**;
8	**PREVENÇÃO**	Adoção de **medidas** para **prevenir** a **ocorrência de danos** em virtude do tratamento de dados pessoais;
9	**NÃO DISCRIMINAÇÃO**	**Impossibilidade** de realização do tratamento para **fins discriminatórios ilícitos** ou **abusivos**;
10	**ACCOUNTABILITY**	**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**.

1.8 - Agentes de Tratamento

Agentes de tratamento: *o controlador e o operador.*

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

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

De acordo com a Comissão Europeia do RGPD (COMISSÃO EUROPEIA, 2010), no documento "Opinion 1/2010 on the concepts of "controller" and "processor", o controlador de dados determina as finalidades e os meios pelos quais os dados pessoais são tratados. Portanto, se uma dada empresa/organização decidir "por que" e "como" os dados pessoais devem ser processados, ela é a controladora dos dados. Já o operador de dados trata dados pessoais apenas em nome do controlador, isto é, o operador de dados geralmente é um terceiro externo à empresa. Dentre esses elementos decisórios principais para distinção entre controlador e operador, destaca-se a definição da finalidade do tratamento, que será sempre estabelecida pelo controlador, a quem compete, em conformidade com as disposições da LGPD, estipular os objetivos que justificam a realização do tratamento, bem como a sua respectiva base legal (ANPD, 2021)

Nesse mesmo sentido, o Guia de Boas Práticas da União (UNIÃO, 2020) reafirma a importância de estar atento às particularidades dos conceitos de controlador e operador em cada caso concreto, a fim de evitar confusões que ponham em risco a correta delimitação de responsabilidades entre os agentes envolvidos no tratamento de dados.

1.8.1 – Agentes de Tratamento - Controlador

De acordo com o art. 5º, VI, da LGPD, o controlador é pessoa natural ou jurídica, de direito público ou privado, a quem compete as decisões referentes ao tratamento de dados pessoais. Abaixo segue definição de controlador pela ANPD (2021):

O controlador é o agente responsável por tomar as principais decisões referentes ao tratamento de dados pessoais e por definir a finalidade deste tratamento. Entre essas decisões, incluem-se as instruções fornecidas a operadores contratados para a realização de um determinado tratamento de dados pessoais.

A ANPD (2021) ressalta que o papel de controlador pode decorrer expressamente de obrigações estipuladas em instrumentos legais e regulamentares ou em contrato firmado entre as partes. Não obstante, a efetiva atividade desempenhada por uma organização pode se distanciar do que estabelecem as disposições jurídicas formais, razão pela qual é de suma importância avaliar se o suposto controlador é, de fato, o responsável pelas principais decisões relativas ao tratamento.

A principal forma de identificação do controlador é o seu poder de decisão sobre o tratamento de dados. É o controlador que inicia o tratamento de dados pois é ele quem determina quais os dados serão tratados, compete ao controlador definir os aspectos relativos à finalidade para os quais os dados serão utilizados e os elementos essenciais dos meios de tratamento. Para consolidar o entendimento vide as definições abaixo (LAPIN, 2021):

- **Finalidade:** é a justificativa para a realização do tratamento de dados, o propósito para qual os dados serão utilizados, bem como a determinação da respectiva base legal (vide Capítulo 2 sobre as bases legais da LGPD) que dará suporte ao tratamento de dados. Em um órgão público, assim como em uma empresa privada, há vários motivos para o tratamento de dados.

- **Elementos essenciais dos meios de tratamento:** os meios de tratamento se dividem em essenciais e não essenciais, cabe ao controlador o poder de decisão sobre os elementos essenciais, o operador se limita a decidir sobre os elementos não essenciais. Os elementos essenciais correspondem à determinação dos dados que serão tratados e a duração do tratamento de dados (a definição por quanto tempo os dados serão armazenados e utilizados dentro da organização). De acordo com a ANPD (2021), outros elementos podem ser considerados para determinação de elementos essenciais conforme o contexto e as peculiaridades do caso concreto.

Além de decidir sobre a finalidade e os elementos essenciais, existem outras características que identificam o controlador: **garantir os direitos dos titulares através do fornecimento de informações, da correção, da portabilidade e da eliminação de dados do titular.**

Considerada referência internacional no tema, a autoridade de proteção de dados do Reino Unido, *Information Commissioner's Office* (ICO) (ICO, 2021), assim sintetizou as características do controlador:

Tabela 1 - Características de um controlador

CONTROLADOR
Decisão de coleta ou de tratamento dos dados pessoais.
Decisão de qual seria a finalidade do tratamento.
Decisão de quais dados pessoais devem ser coletados.
Decisão sobre quais indivíduos terão dados pessoais coletados.
Obtém um ganho comercial ou outro benefício do tratamento, exceto por qualquer pagamento por serviços de outro controlador.
Está tratando os dados pessoais como resultado de um contrato entre a entidade e o titular dos dados.
Os titulares dos dados são os funcionários da organização.
Toma decisões sobre os indivíduos envolvidos como parte ou como resultado do tratamento.
Exerce julgamento profissional no tratamento dos dados pessoais.
Tem uma relação direta com os titulares dos dados.
Tem total autonomia no tratamento dos dados pessoais.
Nomeia os operadores para tratar os dados pessoais em nome da entidade.

Fonte - *Adaptado da Information Commissioner's Office (ICO)*

?

O controlador pode ser uma pessoa física?

A ANPD (2021) ressalta que na maioria das vezes, o controlador será uma pessoa jurídica, seja de direito privado ou de direito público. A Autoridade reforça que uma pessoa natural poderá ser controladora nas situações em que é a responsável pelas principais decisões referentes ao tratamento de dados pessoais. Nessa hipótese, a pessoa natural age de forma independente e em nome próprio – e não de forma subordinada a uma pessoa jurídica ou como membro de um órgão desta. É o que ocorre, por exemplo, com os empresários individuais, os profissionais liberais (como advogados, contadores e médicos) e os responsáveis pelas serventias extrajudiciais

1.8.1.1 – Agentes de Tratamento - Controladoria Conjunta e Singular

Quando a decisão sobre a finalidade e os meios de tratamento essenciais é tomada por dois ou mais controladores é o caso de uma controladoria conjunta. A LGPD apresentou a controladoria conjunta de maneira simplificada e para retratar aspectos de responsabilização solidária, vide:

> *Art. 46, §1º,II - os controladores que estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados respondem solidariamente, salvo nos casos de exclusão previstos no art. 43 desta Lei.*

Abaixo segue a definição da ANPD (2021) para a controladoria conjunta:

> *A determinação conjunta, comum ou convergente, por dois ou mais controladores, das finalidades e dos elementos essenciais para a realização do tratamento de dados pessoais, por meio de acordo que estabeleça as respectivas responsabilidades quanto ao cumprimento da LGPD.*

Para complementar o entendimento é necessário definir o que é uma determinação conjunta comum e convergente (LAPIN, 2021):

- **Decisões comuns:** dois ou mais controladores possuem uma intenção comum sobre a finalidade e os meios de tratamento.
- **Decisões convergentes:** dois ou mais controladores decidem sobre aspectos distintos a respeito da finalidade e dos meios de tratamento, porém essas decisões se complementam e o tratamento de dados não seria possível sem tais controladores, a participação de cada entidade é essencial para ocorrer o tratamento de dados.

Ressalta-se que não será o caso de controladoria conjunta quando dois ou mais controladores utilizarem o mesmo conjunto de dados, mas com finalidades específicas e que o tratamento ocorra independentemente da participação de cada um, uma vez que as decisões não são convergentes ou complementares para o tratamento de dados. A exemplo de uma mesma base de dados governamental utilizada por mais de um controlador para execução de diferentes políticas públicas (ANPD, 2021).

1.8.1.2 – Agentes de Tratamento - Controlador pessoa jurídica de direito público

A ANPD, através da publicação do Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado, discorreu sobre a identificação dos agentes de tratamento das pessoas jurídicas de direito público. No documento, a ANPD (2021) assume que tal definição é uma situação peculiar, uma vez que na Administração Pública Direta as competências decisórias são distribuídas internamente entre diferentes órgãos públicos. É o que ocorre, por exemplo, com o Governo de Pernambuco (pessoa jurídica de direito público) e as Secretarias (órgãos públicos despersonalizados que integram o Poder Executivo Estadual e realizam tratamento de dados pessoais conforme o previsto na legislação).

De acordo com a ANPD (2021), há dois aspectos centrais:

1. Conforme o art. 5º, VI, da LGPD, o controlador é o Governo do Estado, pessoa jurídica de direito público que, em última análise, é responsável pelas obrigações decorrentes da lei, de instrumentos contratuais ou de atos ilícitos praticados pelos seus órgãos e servidores.

2. A LGPD atribui aos órgãos públicos obrigações típicas de controlador, indicando que, no setor público, essas obrigações devem ser distribuídas entre as principais unidades administrativas despersonalizadas que integram a pessoa jurídica de direito público e realizam tratamento de dados pessoais.

Dessa forma, **o Governo de Pernambuco, como controlador, é responsável perante a LGPD, mas as atribuições de controlador, por força da desconcentração administrativa, são exercidas pelos órgãos públicos que desempenham funções em nome da pessoa jurídica da qual fazem parte, fenômeno que caracteriza a distribuição interna das competências.**

Nesse contexto, a partir do Decreto Estadual nº 49.265/2020, o Governo de Pernambuco concretizou tal distribuição interna de atribuições típicas de controlador, a partir do art. 12, a cada órgão do Poder Executivo Estadual.

Sendo assim, cabe a cada Secretaria designar um encarregado, bem como realizar notificações à ANPD em casos de incidentes de segurança, dentre outras obrigações previstas na LGPD. No entanto, caso um titular de dados decida ajuizar uma ação judicial, questionando o tratamento realizado, deverá ingressar contra o controlador, que é o Governo de Pernambuco.

?

O agente de tratamento (controlador ou operador) pode ser uma pessoa física interna da organização?

A interpretação de que os agentes de tratamento são pessoas individualizadas dentro da entidade, ou seja, funcionários internos identificados como operadores ou controladores, não é sustentável à luz da própria LGPD. Tal entendimento é concretizado, seja quanto à responsabilidade dos agentes instituída pelo art. 42, seja no que se refere às inúmeras obrigações descritas no corpo do texto da Lei. Portanto, ainda que em tese seja possível desconsiderar a origem da Lei e da concepção consolidada na UE, há impossibilidade lógico-formal dentro da nossa própria legislação pátria (MALDONADO, 2021).

A ANPD (2021) pacificou esse entendimento ao afirmar que os agentes de **tratamento não são pessoas naturais que atuam como profissionais subordinados a uma pessoa jurídica ou como membros de seus órgãos.**

Por fim, **ressalta que cada entidade da Administração Indireta (autarquias, fundações, empresas públicas e afins) desempenhará a função de agente de tratamento (controlador e operador), conforme o regramento de pessoa jurídica estabelecido pela LGPD.**

1.8.2 – Agentes de Tratamento - Operador

De acordo com o art. 5º, VII, da LGPD, o operador é pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.

A ANPD (2021) complementa a definição da Lei ao acrescentar que o operador também atua de acordo com a finalidade delimitada pelo controlador e destaca

a principal diferença entre o controlador e o operador: o poder de decisão, o operador só poderá agir no limite das finalidades definidas pelo controlador. Outra característica é a de que o operador não detém o poder de decisão sobre os meios de tratamentos essenciais (poder de escolha sobre os dados, finalidade do tratamento, base legal que justifique o tratamento, período de armazenamento) seu nível de atuação se limita aos elementos não essenciais dos meios de tratamento (meios técnicos para o tratamento de dados).

Vale rememorar que na maioria dos casos o operador será uma pessoa jurídica. O operador é pessoa distinta do controlador, ou seja, não se deve confundi-lo com os servidores, funcionários, o departamento de TI de um órgão, esses estão sob o comando do controlador, fazem parte de sua estrutura e estão subordinados a ele. Para firmar o entendimento sobre a identificação do operador, vide o item 58 do Guia da ANPD (2021) sobre os agentes de tratamento:

> *Nesse cenário, empregados, administradores, sócios, servidores e outras pessoas naturais que integram a pessoa jurídica e cujos atos expressam a atuação desta não devem ser considerados operadores, tendo em vista que o operador será sempre uma pessoa distinta do controlador, isto é, que não atua como profissional subordinado a este ou como membro de seus órgãos.*

A ANPD (2021) também destaca algumas obrigações do operador:

- Seguir as instruções do controlador;
- Firmar contratos que estabeleçam, dentre outros assuntos, o regime de atividades e responsabilidades com o controlador;
- Dar ciência ao controlador em caso de contrato com suboperador.

O Guia de Boas Práticas da União (2020) assume que serão considerados controladores, por exemplo, os órgãos públicos que contratarem empresa privada para processar dados pessoais, na medida em que tal empresa agirá sob as ordens do órgão contratante. Nessa ilustração, o órgão contratante (controlador) não apenas estabelecerá a finalidade do tratamento, mas também exigirá da empresa contratada (operador) a adoção dos meios técnicos necessários para garantir a observância dos princípios que regem o tratamento dos dados pessoais, destacados anteriormente. Portanto, para distinguir entre controlador e operador, é fundamental reconhecer qual ente possui autonomia decisória quanto aos fins e meios de tratamento (controlador), e qual possui escopo eminentemente executório (operador), submetido aos desígnios de outrem.

Então **os deveres do operador para com o controlador devem ser especificados em um contrato ou outro ato jurídico.** Por exemplo, o contrato deve indicar o que acontece com os dados pessoais quando o contrato é rescindido. É possível assumir que uma atividade típica dos operadores é oferecer soluções de TIC, incluindo armazenamento em nuvem e manutenção de sistemas. Outra exigência comum em instrumentos jurídicos desse tipo é que o operador de dados só pode subcontratar uma parte de sua tarefa a outro operador ou nomear um operador conjunto quando tiver recebido autorização prévia por escrito do controlador de dados.

Considerada referência internacional no tema, a autoridade de proteção de dados do Reino Unido, *Information Commissioner's Office* (ICO) (ICO, 2021), assim sintetizou as características do operador:

Tabela 2 - Características de um operador

OPERADOR
Está seguindo instruções de outra pessoa em relação ao tratamento de dados pessoais.
Os dados pessoais foram fornecidos à entidade por um cliente ou terceiro semelhante, ou informados sobre quais dados coletar.
Não decide coletar dados pessoais de indivíduos.
Não decide quais dados pessoais devem ser coletados.
Não decide a base legal para o uso desses dados.
Não decide para que finalidades os dados serão usados.
Não decide se divulga os dados ou a quem.
Não decide por quanto tempo reter os dados.
Pode tomar algumas decisões sobre como os dados são tratados, mas implementa essas decisões sob um contrato com outra pessoa.
Não está interessada no resultado do tratamento.

Fonte - *Adaptado da Information Commissioner's Office (ICO)*

1.8.2.1 – Agentes de Tratamento - Suboperador

Segundo a ANPD (2021): o suboperador é aquele contratado pelo operador para auxiliá-lo a realizar o tratamento de dados pessoais em nome do controlador. A figura do suboperador foi apresentada pela ANPD (2021) e busca sinergia com a legislação equivalente da União Europeia, a RGPD[1], com a compreensão sobre a possibilidade de subcontratação pelo operador de um terceiro para a realização de parte do tratamento de dados.

1.8.3 – Exemplos de Agentes de Tratamento

Para esclarecer essa distinção de conceitos, serão apresentados alguns exemplos de situações em que uma entidade pode ser: controladora, controladora-conjunta, operadora de dados e suboperadora.

EXEMPLO 1

Uma cervejaria tem muitos funcionários. Assina contrato com uma empresa de folha de pagamento para pagar os salários. A cervejaria informa à empresa que trabalha com a folha de pagamento quando o salário deve ser pago, quando o funcionário sai ou tem aumento salarial, e fornece todos os demais detalhes do boleto e do pagamento do salário. A empresa de folha de pagamento fornece o sistema de TI e armazena os dados dos funcionários. Nesse caso, a cervejaria é a controladora dos dados e a empresa da folha de pagamento é a operadora dos dados.

EXEMPLO 2

Um banco contrata uma empresa de serviços de TI para armazenar dados arquivados em seu nome - garantindo que a empresa de TI tenha dado garantias suficientes sobre a segurança de seus sistemas e processos. O banco ainda controlará como e por que os dados são usados e determinará seu período de retenção. Na realidade, a empresa de serviços de TI usará grande parte de sua própria experiência técnica e julgamento profissional para decidir a melhor forma de armazenar os dados de maneira segura e acessível

No entanto, apesar dessa liberdade para tomar decisões técnicas, a empresa de TI ainda não é uma controladora de dados no que diz respeito aos dados fornecidos pelo banco - ela é uma operadora. Isso ocorre porque o banco detém controle exclusivo sobre a finalidade para a qual os dados são coletados.

[1] RGPD - Artigo 28º – Subcontratante.

EXEMPLO 3

A empresa ABC deseja entender quais tipos de consumidores têm maior probabilidade de se interessar por seus produtos e contrata um provedor de serviços, a XYZ, para obter as informações relevantes. Para tanto, ABC instrui XYZ sobre o tipo de informação em que está interessada e fornece uma lista de perguntas a serem feitas aos participantes da pesquisa de mercado.

A empresa ABC demandou apenas informações estatísticas (por exemplo, identificando tendências de consumo por região) de XYZ e não tem acesso aos dados pessoais em si. No entanto, a empresa ABC decidiu que o processamento deve ser realizado, e nesse caso, o processamento é realizado para o seu propósito e sua atividade e definiu à empresa XYZ instruções detalhadas sobre quais informações coletar. Portanto, a empresa ABC ainda deve ser considerada uma controladora no que diz respeito ao processamento de dados pessoais, apesar de serem coletadas por terceiros. Isto porque XYZ só pode processar os dados para os fins fornecidos por ABC e de acordo com suas instruções detalhadas e, portanto, deve ser considerada como operadora.

EXEMPLO 4

A Empresa X contrata uma terceirizada para instalação e manutenção de equipamentos de biometria para dar mais segurança ao acesso de suas dependências. A decisão de coletar a biometria para controle de acesso foi da Empresa X (controladora), o operador (empresa terceirizada) irá atuar conforme interesses do controlador. O operador se trata de outra pessoa jurídica (não faz parte dos quadros da Empresa X) e realizará o tratamento de dados (instalação de equipamentos de coleta das digitais e suportes ao sistema) com a finalidade de gerar relatórios das informações requeridas pelo controlador. A empresa terceirizada definirá a tecnologia que será aplicada de acordo com o tamanho e as necessidades da Empresa X, tais decisões são de carácter técnico e consideradas como meios de tratamento não essenciais, o que está dentro do escopo do tratamento de dados realizado por um operador. Nos próximos tópicos serão abordados outros exemplos sobre controlador e operador de dados.

EXEMPLO 5

Uma escola decide colocar um sistema de controle de acesso ao refeitório para contabilizar corretamente o número de comensais, neste caso o próprio departamento de informática da escola cria um sistema simples em que uma carteira com código de barras é cadastrada por aluno, sendo necessário para elaboração da identificação dos comensais as informações de nome e CPF. Neste exemplo a escola (identificada por sua pessoa jurídica) é a controladora dos dados. O setor de informática está sob comando diretivo da escola, portanto não é o operador de dados, apenas parte integrante da estrutura da escola. Neste exemplo não há operador de dados.

EXEMPLO 6

Um hospital decide contratar uma empresa especializada em biometria para fornecimento de catraca com captura biométrica para controlar o acesso de comensais ao seu refeitório. A empresa fornece o equipamento e detém o acesso ao sistema para verificação do funcionamento correto da catraca. O hospital é o controlador dos dados dos comensais e a empresa é a operadora. Foi firmado contrato de confidencialidade das informações e a empresa terceirizada somente utilizará os dados dos comensais para verificar a funcionalidade do sistema.

EXEMPLO 7

Dois hospitais decidem contratar o mesmo fornecedor para o desenvolvimento de um sistema de gestão integrada para controle de plantões extras. O objetivo do sistema é de otimizar os controles de plantões e evitar fraudes em casos de colaboradores que deveriam prestar atendimento no Hospital A, mas que abandonaram o posto para atender no Hospital B. A empresa C desenvolvedora do sistema terá acesso aos dados para verificação de erros e para realizar treinamento a equipe de tecnologia dos hospitais. Como o sistema é robusto a empresa subcontrata outra (empresa D) para ajudar na elaboração do sistema. Para este caso como ambos os hospitais possuem informações complementares e detém mesma finalidade que é o controle de plantões extras de seus colaboradores, é o caso de controladoria conjunta (decisão comum). A empresa C é operadora e a empresa D suboperadora.

1.8.4 – Responsabilidade e Formalização de Contrato entre os Agentes de Tratamento como Boa Prática

Após a compreensão de quem são os agentes de tratamento e suas principais características constata-se que o controlador detém a maior parte das responsabilidades sobre o tratamento de dados. Como foi apresentado nos tópicos anteriores as atribuições do controlador são as que produzem os efeitos iniciais do tratamento de dados, como a escolha dos dados que serão tratados, a determinação da finalidade para o qual serão utilizados e a de que caso utilize terceiro (operador) para o tratamento de dados ele deverá seguir conforme suas instruções.

A LGPD define objetivamente as responsabilidades dos agentes pelo tratamento do dado. **A Lei prevê que o agente que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, é obrigado a repará-lo, podendo, inclusive, a reparação ser exercida coletivamente em juízo, observado o disposto na legislação pertinente**, conforme destaca o art. 42.

Desse modo, é relevante destacar as repercussões administrativas e cíveis desse novo direito. A Lei, inclusive, estabelece, conforme §2º do art. 42, que o juiz, no processo civil, poderá inverter o ônus da prova a favor do titular dos dados quando, a seu juízo, for verossímil a alegação, houver hipossuficiência para fins de produção de prova ou quando a produção de prova pelo titular resultar-lhe excessivamente onerosa.

Por garantir novos direitos, é relevante citar que, em caso de omissão pela LGPD, no caso concreto, o juiz ou a autoridade decidirá o caso de acordo com a analogia, os costumes e os princípios gerais de direito. No ordenamento jurídico, o juiz não é obrigado a observar o critério de legalidade estrita, podendo adotar em cada caso a solução que considerar mais conveniente ou oportuna (art. 723 do Código de Processo Civil) (LIMA, 2019).

Ainda de acordo com art. 42 da LGPD, **o operador responde solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da legislação de proteção de dados ou quando não seguir as instruções lícitas do controlador**, hipótese em que o operador se equipara ao controlador (de acordo com a ANPD essa é a única possibilidade em que essa paridade ocorre). Portanto a formalização através de um contrato das respectivas obrigações pertinentes

a cada agente de tratamento (controlador e operador) é defendida como boa prática pela ANPD (2021), vide:

> *O conceito e o escopo de atuação do operador indicam, também, a importância das definições contratuais para a relação entre controlador e operador. Ainda que a LGPD não determine expressamente que o controlador e o operador devam firmar um contrato sobre o tratamento de dados, tal ajuste se mostra como uma boa prática de tratamento de dados, uma vez que as cláusulas contratuais impõem limites à atuação do operador, fixam parâmetros objetivos para a alocação de responsabilidades entre as partes e reduzem os riscos e as incertezas decorrentes da operação.*

A RGPD (legislação europeia que inspirou a LGPD) deixa claro a necessidade de realizar um contrato entre o controlador e o operador, adicionalmente reafirma a importância de contrato ao tratar do suboperador e deixa claro que o controlador dê ciência por escrito da possibilidade de subcontratação, vide trechos do artigo 28:

> *O subcontratante não contrata outro subcontratante sem que o responsável pelo tratamento tenha dado, previamente e por escrito, autorização específica ou geral. Em caso de autorização geral por escrito, o subcontratante informa o responsável pelo tratamento de quaisquer alterações pretendidas quanto ao aumento do número ou à substituição de outros subcontratantes, dando assim ao responsável pelo tratamento a oportunidade de se opor a tais alterações.*

Portanto, prestadores de serviços de um órgão ou entidade que vierem a tratar dado pessoal em nome desta, são considerados operadores e desse modo, deverão cumprir os deveres legais da Lei, além das exigências contratuais ou instrumento congênere.

A procuradoria Geral do Estado já se pronunciou preliminarmente sobre o assunto através do http://www.pge.pe.gov.br/app_themes/doc_consultiva_boletim_02_2021.pdf

Outro aspecto importante na responsabilidade do agente de tratamento, conforme art.42, §4º, da LGPD, é o direito de regresso. Ou seja, aquele que reparar o dano ao titular tem direito de regresso contra os demais responsáveis, na medida de sua participação no evento danoso.

Por fim, a LGPD, no art.43, incisos I, II e III, da LGPD, prevê algumas hipóteses de exclusão de responsabilidade dos agentes de tratamento. Isto ocorrerá quando os agentes provarem:

(i) que não realizaram o tratamento de dados que lhes foi atribuído;

(ii) que mesmo tendo realizado o tratamento dos dados pessoais, não violaram a legislação de proteção de dados; ou

(iii) que o dano ao titular dos dados foi decorrente de culpa exclusiva do titular dos dados ou de terceiro.

1.9 - Encarregado

Encarregado: *pessoa indicada pelo controlador e operador corporativo para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD).*

O encarregado, no Brasil, é a pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares e a ANPD (art. 5º, VIII, da LGPD), conforme esquema disposto na Figura.

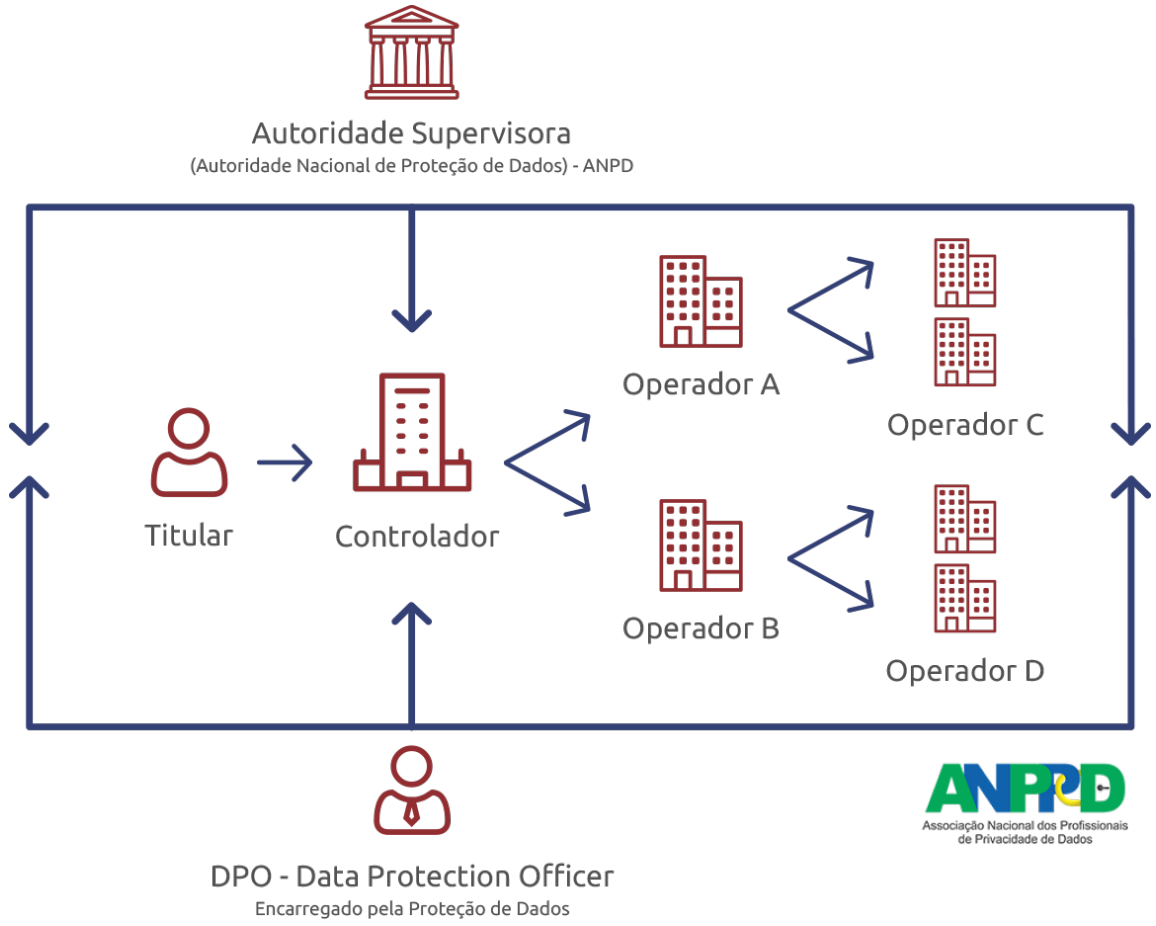

Figura 8. O Papel do encarregado e os agentes de tratamento

Fonte: Lei Geral de Proteção de Dados - LGPD - CIAware

Descrição: A imagem apresenta o relacionamento do encarregado enquanto pilar de conformidade do controlador com a LGPD, considerando os relacionamentos do controlador com os operadores e o tratamento de dados pessoais dos titulares. Além disso, inclui a ação da ANPD no papel de fiscalizador de todo esse sistema de atuação do encarregado.

Segundo BLUM et al. (2020), o conceito de encarregado, como ocorre em boa parte da LGPD, é oriundo do RGPD, conhecido por "Data Protection Officer (DPO)". Diferentemente da Lei nacional, que o encarregado está focado em servir de meio de comunicação e divulgação, o DPO ganhou mais relevância na União Europeia, contando com uma seção inteira dedicada ao assunto. Para os autores, o DPO no RGPD poderia ser compreendido como: **o responsável por monitorar a conformidade com as normas de proteção de dados e com as políticas do controlador ou do operador relativas à proteção de dados pessoais, incluindo a repartição de responsabilidades, a sensibilização e formação das pessoas que tratarão dos dados pessoais das auditorias correspondentes.**

BLUM et al. (2020) acrescentam que apesar de o encarregado não ser diretamente responsável por eventual descumprimento das normas de proteção de dados, mas sim os agentes de tratamento, uma das mais importantes medidas de governança das organizações é justamente avaliar a sua nomeação, posição e atribuições. Esse conteúdo será mais bem detalhado no tópico "4 – O Encarregado e equipe de apoio na PEPDP" da Capítulo 4.

Por último, vale lembrar que **a LGPD não definiu requisitos objetivos à nomeação do encarregado, mas deixou para a ANPD regulamentar o assunto, inclusive com a possibilidade de dispensa de nomeação do encarregado para certos controladores e operadores.**

Capítulo 2 – Hipóteses e requisitos para tratamento de dados pessoais

O Capítulo 1 abordou a origem da Lei e seus propósitos, assim como, alguns conceitos básicos, como: “dado pessoal”, “dado sensível”, “operações de tratamento de dados pessoais”. Também tratou da definição das principais figuras instituídas pela Lei como: titular do dado pessoal, controlador, operador e encarregado.

Por ser uma Lei de proteção de dados pessoais, a LGPD é garantidora de diversos direitos do indivíduo relacionados à privacidade. Ou seja, o tratamento de dados pessoais só deve ocorrer em certas condições e quando cumprir alguns requisitos.

2.1 – Hipóteses de Permissão de Tratamento de Dados

De acordo com a LGPD, todo tratamento de dados pessoais deve estar suportado por uma das bases legais presentes no art. 7º e art. 11, dentre as quais destacam-se: o consentimento do titular, obrigação legal ou regulatória, a tutela da saúde e o legítimo interesse. Tem-se que as hipóteses de tratamento estão divididas, a depender do tipo de dado pessoal, da seguinte forma:

I. Dados pessoais em geral (art. 7º);
II. Dados pessoais sensíveis (art. 11)

Dentre as diversas hipóteses, é relevante destacar que não há hierarquia entre os dispositivos, ou seja, todas as opções que autorizam o tratamento desses dados podem ser utilizadas, desde que sejam adequadas ao caso concreto.

Caso um dado órgão público esteja tratando dados pessoais, será preciso avaliar, além do tipo de dado, a finalidade do tratamento para, enfim, definir a hipótese aplicável. Lembrando que, **para que o tratamento seja considerado legítimo e lícito, não basta fundamentá-lo, é preciso considerar todos os princípios elencados anteriormente.**

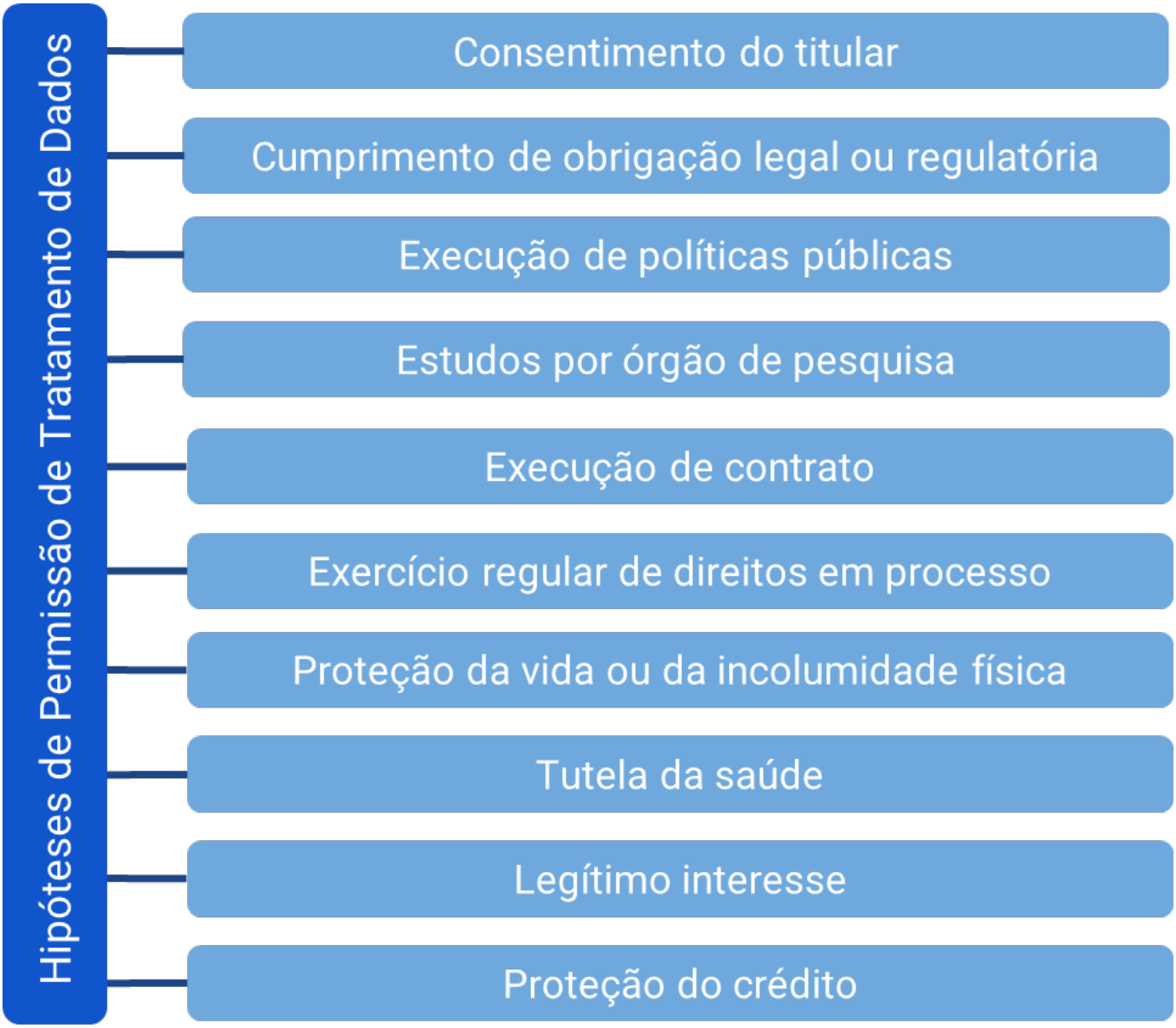

Figura 9. Hipóteses de Permissão de Tratamento de Dados Pessoais

Fonte: Autor

Descrição: A imagem apresenta a lista de hipóteses de tratamento de dados pessoais (Consentimento do titular, Cumprimento de obrigação legal ou regulatória, Execução de políticas públicas, Estudos por órgão de pesquisa, Execução de contrato, Exercício regular de direitos em processo, Proteção da vida ou da incolumidade física, Tutela da saúde, Legítimo interesse, Proteção do crédito)

A UNIÃO (2020) adverte que o princípio da responsabilização e prestação de contas requer que o órgão ou entidade que realiza o tratamento de dados pessoais possa demonstrar que está plenamente aderente à LGPD com a indicação da hipótese, comprovando a observância e o cumprimento das normas de proteção de dados pessoais estabelecidas, inclusive quanto a sua eficácia. Assim o titular estará ciente da hipótese utilizada no processamento de seus dados pessoais e poderá resguardar seus direitos.

?

Um tratamento de dados pessoais pode ocorrer sustentado por mais de uma hipótese?

Tal entendimento é, no caso do RGPD, para servir de referência, o enquadramento pode ser realizado considerando mais de uma das hipóteses, porém, tal conteúdo está sujeito a novas interpretações por parte da ANPD.

Vale ressaltar que a LGPD, no seu art. 4º, prevê casos que a Lei não deve ser aplicada ao tratamento de dados pessoais, que são:

- Tratamento realizado por pessoa natural para fins exclusivamente particulares e não econômicos;
- Tratamento realizado para fins exclusivamente jornalístico e artísticos;
- Tratamento realizado para fins exclusivamente acadêmicos, aplicando-se a esta hipótese os art. 7º e 11 desta Lei;
- Tratamento realizado para fins exclusivos de segurança pública, defesa nacional, segurança do estado, ou atividades de investigação e repressão de infrações penais;
- Tratamentos provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto nesta Lei.

Isto posto, não sendo uma das situações de exclusão citadas anteriormente, o tratamento de dados pessoais deverá estar enquadrado em pelo menos uma das hipóteses legais.

Por fim, apesar de interpretações e exemplos práticos apresentados neste Manual, cumpre destacar que ainda não há definição nacional sobre as lacunas deixadas sobre a LGPD, assim como não há orientações, decisões administrativas da Autoridade Nacional de Proteção de Dados (ANPD) sobre o conteúdo.

2.1.1 – Consentimento do titular

I - mediante o fornecimento de consentimento pelo titular;

A primeira base legal indicada na LGPD para tratamento de dados pessoais é o consentimento do titular. A LGPD elevou o nível de exigência do consentimento, ao considerá-lo uma manifestação **livre, informada e inequívoca** pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada. Neste sentido, vale frisar que um consentimento genérico, sem uma finalidade específica, não seria considerado válido para a LGPD (MAIA et al., 2020).

Quanto às condições impostas citadas para o consentimento, têm-se as seguintes definições (MENDES et al., 2019):

- **Livre:** o titular pode escolher entre aceitar ou recusar a utilização de seu dado, sem intervenções ou situações que viciem o seu consentimento.
- **Informada:** o titular do dado tem de ter ao seu dispor as informações necessárias e suficientes para avaliar corretamente a situação e a forma como seus dados serão tratados.
- **Inequívoca:** a manifestação de vontade deve ser não ambígua, evidente e ocorrer de forma clara.

O tratamento de dados pessoais com base no consentimento deverá ser precedido por um ato positivo e claro do titular de dados. Assim, **o silêncio ou situações com opções marcadas previamente em sites ou aplicativos e a omissão não são suficientes para caracterizar o consentimento válido.** O pedido de consentimento precisa ser destacado, apresentado de forma inteligível, de fácil acesso e com uma linguagem clara e simples, além de ser demonstrável (MAIA et al., 2020).

Para MENDES et al. (2019), o consentimento do titular dos dados pessoais recebeu tutela destacada na LGPD. Aliás, em determinados casos, os autores alertam que a obtenção do consentimento poderá ser até mesmo inadequada, tendo em vista a existência de outra base legal mais precisa para o tratamento em questão. Nesses casos, parece ser mais adequado e seguro usar outra base legal ao invés do consentimento do titular dos dados, ainda que seja possível obtê-lo.

Nessa esteira, MENDES et al. (2019) alertam para que as organizações tenham um maior cuidado com o consentimento do titular no atual cenário tecnológico. Atualmente, há fatos que corroboram com este receio, como: a coleta em massa de dados pessoais, a mercantilização desses dados e a pouca transparência dos

tratamentos. Nesse sentido, defendem que **a interpretação do consentimento deverá ocorrer de forma restritiva, não podendo o agente estender a autorização concedida a ele para o tratamento de dados visando outros meios além daqueles pactuados, para momento posterior ou para finalidade diversa.**

Para ilustrar tal base legal, serão apresentados alguns exemplos de situações em que uma organização se utiliza do consentimento como hipótese para tratamento de dados pessoais.

EXEMPLO 1

Uma produtora de jogos mobile XYZ dispõe a opção de coleta dados de geolocalização para que o usuário receba anúncios de jogadores disponíveis na região em que se encontra (MAIA et al., 2020).

EXEMPLO 2

Uma cafeteria decide fornecer wi-fi gratuito aos seus clientes. Para acessar o serviço, o cliente deve fornecer seu nome e número de celular e, em seguida, concordar com os termos e condições da cafeteria, consentindo com o tratamento dos dados pessoais para tal finalidade (MAIA et al., 2020).

Conforme disposto no § 5º do art. 8º, o consentimento poderá ser revogado a qualquer momento, mediante manifestação expressa do titular, por procedimento gratuito e facilitado. Logo, o consentimento deve ser compreendido como temporário. Entretanto, não parece razoável que quem recebeu a autorização para o tratamento dos dados tenha que sofrer risco ilimitado nem que a revogação se dê em flagrante prejuízo ao interesse público (MENDES et al., 2019).

O controlador que obteve o consentimento e necessita comunicar ou compartilhar dados pessoais com outros controladores deverá obter consentimento específico do titular para esse fim, ressalvadas as hipóteses de dispensa do consentimento previstas na Lei. A partir dessa disposição, afirma-se que existiria dever que não se restringiria apenas ao controlador originário, devendo ser observado por todos aqueles que tenham acesso aos dados, dos quais se exigiria o dever de verificar a licitude do procedimento de acesso ou compartilhamento, inclusive no que tange ao consentimento específico do titular (MENDES et al, 2020).

2.1.2 – Cumprimento de obrigação legal ou regulatória

II - para o cumprimento de obrigação legal ou regulatória pelo controlador;

O inciso II do art. 7º afirma que o tratamento de dados pessoais poderá ser realizado para o cumprimento de obrigação legal ou regulatória pelo controlador. Ou seja, em circunstâncias em que, para cumprir uma lei ou regulamento específico, o controlador precisa realizar o tratamento dos dados pessoais.

Cumpre destacar que, conforme disposto no art. 7º, **a obrigação do cumprimento da lei ou regulamento deverá ser do controlador para a aplicação dessa base legal.** Além disso, tal hipótese não excepcionaliza o dever do controlador em conduzir o tratamento de dados pessoais em respeito aos princípios elencados na Lei, especialmente o Princípio da Transparência. Nesse contexto, a organização deve promover conteúdos claros e transparentes, a fim de que o titular esteja ciente que o tratamento de seus dados pessoais é realizado a partir de um dispositivo normativo específico para tal.

Para enquadramento nessa hipótese, deve-se avaliar (UNIÃO, 2020):

1. É possível identificar a obrigação legal ou regulatória específica que requer o processamento do dado?
2. É possível identificar a competência legal do órgão que dará cumprimento à obrigação legal ou regulatória?
3. O titular do dado será informado sobre a norma que determina a obrigação legal ou regulatória que exige o tratamento do dado?
4. Em se tratando de dados pessoais sensíveis, será dada publicidade à referida dispensa de consentimento, nos termos do inciso I do caput do art. 23 da Lei?

Para ilustrar essa hipótese, serão apresentados alguns exemplos de situações em que uma organização se utiliza da obrigação legal como hipótese para tratamento de dados pessoais.

EXEMPLO 1

A empresa ABC realiza exame médico do seu funcionário para comprovar o estado de saúde física e psíquica, conforme Consolidação das Leis Trabalhistas (art. 168) e Normas Regulamentadoras nº 4 e nº 7 (MAIA et al., 2020).

EXEMPLO 2

Hospital XYZ guarda prontuários médicos por 20 anos em atendimento às exigências do Conselho Federal de Medicina (CFM) (Resolução nº 1639/2002, art. 4º) (MAIA et al., 2020).

2.1.3 – Execução de políticas públicas previstas em leis e regulamentos

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

Ao mesmo tempo que é a hipótese mais importante para o setor público, é também a de maior desafio de quem se propõe a entender a sua abrangência. Na doutrina, não há um consenso da definição exata do que se enquadraria com o termo "política pública". Uma definição que pode ser utilizada seria "política pública é uma diretriz elaborada para enfrentar um problema público", onde "a razão para o estabelecimento de uma política pública é o tratamento ou solução de um problema entendido como coletivamente relevante". Cumpre destacar que **para que os dados sejam tratados pelo Poder Público, ou por quem lhe fizer às vezes, é preciso que exista um instrumento legal que minimamente institua a política pública e que crie suas diretrizes.** Devem estar contemplados no documento, por exemplo, quem serão os entes públicos ou as organizações privadas que serão responsáveis por sua gestão ou execução, e que o fim exclusivo da política prevista seja o atingimento do interesse público (União, 2020). A organização deve promover conteúdos claros e transparentes, a fim de que o titular esteja ciente que o tratamento de seus dados pessoais é realizado a partir de um dispositivo normativo específico para tal.

Tem-se, dessa forma, duas hipóteses que estão diretamente ligadas ao serviço público: cumprimento de obrigação legal ou regulatória (art. 7º, II); e execução

de políticas públicas (art. 7º, III). Ou seja, em ambos os casos, resta dispensada a hipótese de tratamento de dados pessoais com base no consentimento do titular.

Então, considerando o dever do Poder Público de oferecer à população serviços públicos a partir do tratamento de dados pessoais, o controlador no setor público deve assumir, salvo melhor juízo, que tal política pública decorre da obrigação imposta ao seu órgão ou entidade. Tal fato, enseja uma avaliação interna se a ação governamental resta respaldada por normativo, a fim de garantir a proteção de dados pessoais e afastar a necessidade de consentimento.

Para enquadramento nessa hipótese, deve-se avaliar (UNIÃO, 2020):

1. O controlador é pessoa jurídica de direito público?

2. Não sendo pessoa jurídica de direito público, o controlador é empresa pública ou sociedade de economia mista que realizará o tratamento de dados para execução de políticas públicas, e não para atividades inerentes ao regime de concorrência?

3. O tratamento do dado será realizado para a execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres?

4. É possível identificar claramente a lei, regulamento ou outro instrumento legal que especifique a política pública que exige o tratamento de dados pessoais?

5. É possível identificar a competência legal que autoriza o órgão à execução da política pública?

6. O titular do dado será informado sobre a lei, regulamento ou outro instrumento legal que especifique a política pública que exige o tratamento do dado?

7. Em se tratando de dados pessoais sensíveis, será dada publicidade à referida dispensa de consentimento, nos termos do inciso I do caput do art. 23 da Lei, inclusive quando da necessidade de compartilhamento de dados?

8. Será indicado um encarregado (art. 5º, inciso VIII) para garantir a comunicação do órgão ou entidade pública com o titular do dado e com a Autoridade Nacional de Proteção de Dados, que verificará a observância das instruções e normas sobre a política pública em questão?

Para esclarecer essa base legal, serão oferecidas algumas situações em que uma entidade se utiliza da execução de políticas públicas como hipótese para tratamento de dados pessoais.

EXEMPLO 1

As empresas privadas de água provavelmente podem considerar a hipótese de execução de políticas públicas, mesmo que não se enquadrem na definição de uma autoridade pública na LGPD. Isso ocorre porque são consideradas como "desempenhando funções de administração pública" e tais exercem poderes legais especiais para a prestação de serviços de utilidade pública.

EXEMPLO 2

Gestão descentralizada do Bolsa Família: União, Estados, Distrito Federal e Municípios compartilham entre si processos e tomadas de decisão, com tratamento dos dados pessoais presentes no cadastro único para programas sociais do governo federal (acesso aos dados regulamentado pela Portaria nº 502 de 2017) (MAIA et al., 2020).

EXEMPLO 3

Política pública de prevenção ao HIV - Programa Nacional de DST/Aids: Programa de execução descentralizada inclusive com participação da sociedade civil, conforme preceitua a Constituição Federal, Lei nº 8080/90 e 8.142/90, entre outras, com tratamento de dados cadastrais e dados de saúde (MAIA et al., 2020).

EXEMPLO 4

Programa Chapéu de Palha: programa estadual criado para combater os efeitos do desemprego decorrentes da entressafra da cana-de-açúcar e da fruticultura irrigada e das condições adversas para a pesca artesanal. Para ter direito ao benefício, a família deverá apresentar informações que atendam os requisitos de acesso ao auxílio (Lei Estadual nº 13.244, de 11 de junho de 2007).

2.1.4 – Estudos por órgão de pesquisa, desde que mantido o anonimato

IV - para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;

A LGPD também prevê o tratamento de dados pessoais para a realização de estudos por órgãos de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais. Conforme a Lei, em seu inciso XVII do art. 5º, órgão de pesquisa é *"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".*

Destaca-se que a atividade científica, em grande parte, sustenta-se a partir da coleta e análise de dados e, não raro, torna imprescindível o tratamento de dados pessoais. Além disso, os estudos realizados por tais órgãos têm um papel relevante no desenvolvimento econômico, tecnológico e na inovação, questões que são verdadeiros fundamentos da disciplina da proteção de dados pessoais, conforme art. 2º da Lei (MAIA et al., 2020).

Diferentemente das outras, essa hipótese reforça a importância da anonimização. Não é por menos que as técnicas de anonimização são amplamente conhecidas por órgãos de pesquisa. Sendo assim, o tratamento pelo órgão de pesquisa deve ser considerado, sempre que possível, com a anonimização dos dados pessoais.

De acordo com o art. 13, os órgãos de pesquisa poderão ter acesso a bases de dados pessoais de saúde pública. No entanto, tais tratamentos serão realizados exclusivamente dentro do órgão e estritamente para a finalidade de realização de estudos e pesquisas em regulamento específico e que incluam, sempre que possível, a anonimização ou pseudoanonimização dos dados (MENDES et al., 2019).

Não menos importante, acrescenta-se que a divulgação dos resultados ou de qualquer excerto do estudo ou da pesquisa de que trata o caput do art. 13 (bases de dados pessoais de saúde pública), em nenhuma hipótese, poderá revelar dados pessoais. Além disso, os órgãos serão responsáveis pela guarda e não poderão transferir os dados pessoais para terceiros em circunstância alguma (MENDES et al., 2019).

A seguir serão apresentados exemplos de órgãos de pesquisa que se utilizam de dados pessoais da execução de sua função institucional:

EXEMPLO 1

Prática utilizada pelos órgãos de pesquisa com o intuito de anonimizar os dados é quando em uma pesquisa para apuração de intenção de votos em uma eleição as informações são alocadas levando em conta sexo, escolaridade, região geográfica e classe social dos indivíduos de maneira agregada (MENDES et al., 2019).

EXEMPLO 2

O Condepe/Fidem, autarquia estadual e identificada como Órgão de Estatística do Estado de Pernambuco, realizou pesquisa para determinar o Índice de Desenvolvimento Humano Municipal em Pernambuco. O município do Manari, localizado no Sertão do Moxotó, apresentou IDH abaixo da média, o que requisitou investimento públicos. A pesquisa foi realizada mediante questionário aplicado aos cidadãos da região e pela análise de dados sócio-econômicos; as informações foram demonstradas em formato agregado, o que impede a identificação dos titulares de dados. Por fim, o Condepe/Fidem está dentro dos parâmetros definidos pela LGPD como órgão de pesquisa (Art. 5º, XVIII).

2.1.5 – Execução de contrato do qual é parte o titular dos dados

V - quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;

Nesse caso, o tratamento de dados se dará a pedido do próprio titular dos dados para garantir a execução de um contrato ou de seus procedimentos preliminares. Essa hipótese se assemelha um pouco com o tratamento de dados via consentimento, com a diferença de que o titular dos dados não poderá revogar o seu fornecimento a qualquer momento, uma vez que a outra parte estará resguardada pela LGPD para poder manter os dados fornecidos pelo titular enquanto durar a vigência do contrato (MAIA et al, 2020).

A título de exemplo, seguem alguns exemplos de tratamento de dados pessoais para execução de um contrato do qual o titular é parte:

EXEMPLO 1

Contratação por parte de um titular de dados de um serviço cujo objeto principal é o tratamento de dados pessoais, tal como acontece com a inserção de dados em um serviço de armazenamento em nuvem.

EXEMPLO 2

Empresa que comercializa, via internet, e antes de celebrar o contrato com o titular coleta o nome, o endereço de entrega, o número de cartão de crédito.

EXEMPLO 3

Levantamentos realizados por instituições financeiras, a pedido do titular, anteriormente à concessão de crédito dele.

2.1.6 – Exercício regular de direitos em processo judicial, administrativo ou arbitral

VI - para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);

O inciso VI do art. 7º dá o permissivo legal para que o controlador trate dados pessoais quando tiver por finalidade subsidiar o exercício regular de direitos em processo judicial, administrativo ou arbitral, seja existente ou a ser movido no futuro. Os direitos podem ser tanto do controlador quanto de terceiros ou do próprio titular (MAIA et al, 2020).

A partir desse dispositivo, MAIA et al. (2020) assumem que ficaria resguardado o direito de o controlador produzir provas, mesmo que estas incluam dados pessoais da outra parte ou de terceiros (não precisando, portanto, de consentimento para tal), sempre levando-se em consideração a finalidade, a adequação e a necessidade do uso dos dados pessoais, bem como os demais princípios previstos no art. 6º da LGPD.

EXEMPLO 1

A ação de acostar aos autos de processo administrativo, judicial ou arbitral um documento ou fotografia que contenha dados pessoais.

EXEMPLO 2

Retenção de dados pessoais por período adicional ao término do tratamento, uma vez que pode haver a necessidade de utilização dos dados em processo judicial e, para isso, pode-se considerar como parâmetro de prazo de retenção o prazo prescricional aplicável.

2.1.7 – Proteção da vida ou da incolumidade física do titular ou de terceiro

VII - para a proteção da vida ou da incolumidade física do titular ou de terceiro;

Essa hipótese é aplicável para o tratamento de dados para a proteção da vida ou da incolumidade física do titular ou de terceiros.

Para enquadramento nessa hipótese, deve-se avaliar (UNIÃO, 2020):

1. O tratamento de dados pessoais se faz necessário para proteger a vida ou a incolumidade física do titular ou de terceiros?

2. O titular está impossibilitado de oferecer o consentimento para o tratamento do dado pessoal?

Cumpre destacar que os tratamentos de dados pessoais com base nessa hipótese ainda encontram-se sujeitos aos princípios previstos no art. 6º da norma. Assim sendo, não basta que o tratamento tenha sido realizado com tal base, mas também que ele deve ter uma finalidade e necessidade definidas, ser adequado, utilizar medidas técnicas necessárias para garantir a segurança do dado contra incidentes e estar pronto para, ao final, ser descartado.

EXEMPLO 1

Eventuais situações de internação em que for necessário priorizar a integridade psicofísica do titular ou do terceiro, sobrepondo-se ao exercício de sua autonomia, seja por incapacidade ou pela urgência da situação (MAIA et al., 2020).

EXEMPLO 2

Situação de acidentes em que o titular sofre um acidente e é levado inconsciente ao hospital. Neste caso, para poder atendê-lo da maneira adequada, os médicos deverão acessar seu histórico de saúde e ter acesso a dados pessoais e dados sensíveis, no entanto, respeitando os demais princípios da LGPD e, levando-se em consideração restrição de acesso, ou seja, apenas deve ter acesso aos dados aquele que efetivamente necessitar (MAIA et al., 2020).

2.1.8 – Tutela da saúde, com procedimento realizado por profissionais da área da saúde ou por entidades sanitárias

VIII - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;

A base legal da tutela da saúde autoriza o tratamento tanto de dados sensíveis, como de dados não sensíveis. Segundo o CNS (2021), para utilização dessa base é necessário cautela, tendo em vista que seu conceito não se aplica indiscriminadamente a todas as etapas da prestação de serviços de saúde. Assim, sugere-se que a sua utilização seja realizada à luz do conceito de tutela da saúde presente no Artigo 9(2)(h) e Artigo 9(3) do Regulamento Geral sobre a Proteção de Dados da União Europeia (RGPD):

> *"Se o tratamento for necessário para efeitos de medicina preventiva ou do trabalho, para a avaliação da capacidade de trabalho do empregado, o diagnóstico médico, a prestação de cuidados ou tratamentos de saúde ou de ação social ou a gestão de sistemas e serviços de saúde ou de ação social com base no direito da União ou dos Estados-Membros ou por força de um contrato com um profissional de saúde, sob reserva das condições e garantias previstas no nº 3;*
>
> *(...)*
>
> *3. Os dados pessoais referidos no nº 1 podem ser tratados para os fins referidos no nº 2, alínea h), se os dados forem tratados por ou sob a*

responsabilidade de um profissional sujeito à obrigação de sigilo profissional, nos termos do direito da União ou dos Estados-Membros ou de regulamentação estabelecida pelas autoridades nacionais competentes, ou por outra pessoa igualmente sujeita a uma obrigação de confidencialidade ao abrigo do direito da União ou dos Estados-Membros ou de regulamentação estabelecida pelas autoridades nacionais competentes."

Sendo assim, ainda que a uma primeira vista a tutela da saúde pareça ser a base legal aplicável à maioria dos processos de tratamento do setor de saúde, é necessário distinguir quais tratamentos são realizados no âmbito das atividades-fim dos prestadores (medicina preventiva ou do trabalho, para a avaliação da capacidade de trabalho do empregado, o diagnóstico médico, a prestação de cuidados ou tratamentos de saúde) e por profissionais de saúde sujeitos à obrigação de sigilo. Caso contrário, a base legal "tutela da saúde" pode não ser a mais adequada (CNS, 2021).

2.1.9 – Legítimo interesse do controlador ou de terceiros

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;

O legítimo interesse é a hipótese legal que visa possibilitar tratamentos de dados importantes, vinculados ao escopo de atividades praticadas pelo controlador, e que encontrem justificativas legítimas. Diante da flexibilidade dessa base legal, as expectativas do titular dos dados têm peso especialmente relevante para sua aplicação, devendo ser consideradas também a finalidade, a necessidade e a proporcionalidade da utilização dos dados. Quanto mais invasivo, inesperado ou genérico for o tratamento, menor será a probabilidade de que seja reconhecido o legítimo interesse (MENDES et al., 2019).

Diante do amplo espectro de interpretação do que viria a ser "legítimo interesse", a LGPD delimitou a sua aplicabilidade, conforme disposto no seu art.10:

"Art. 10. O legítimo interesse do controlador somente poderá fundamentar tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas, que incluem, mas não se limitam a:

I - apoio e promoção de atividades do controlador; e

II - proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas as legítimas

expectativas dele e os direitos e liberdades fundamentais, nos termos desta Lei.

§ 1º Quando o tratamento for baseado no legítimo interesse do controlador, somente os dados pessoais estritamente necessários para a finalidade pretendida poderão ser tratados.

§ 2º O controlador deverá adotar medidas para garantir a transparência do tratamento de dados baseado em seu legítimo interesse.

§ 3º A autoridade nacional poderá solicitar ao controlador relatório de impacto à proteção de dados pessoais, quando o tratamento tiver como fundamento seu interesse legítimo, observados os segredos comercial e industrial."

Por ser um tema de difícil aplicação prática, e até que a ANPD estabeleça critérios objetivos para o tratamento de dados pessoais por tal hipótese de permissão, é possível utilizar o modelo proposto pela autoridade de proteção de dados do Reino Unido, Information Commissioner's Office (ICO). A ICO propõe a realização de três questionários (Legitimate Interests Assessment (LIA)) para avaliar a aplicabilidade do legítimo interesse como hipótese de tratamento de dados pessoais: identificação da finalidade, teste de necessidade e teste de proporcionalidade, conforme quadros adaptados a seguir.

Teste de finalidade:

1. Por que você deseja tratar os dados - o que você está tentando alcançar?
2. Quem se beneficia com o processamento?
3. De que maneira?
4. Há algum benefício público mais amplo para o tratamento?
5. Qual a importância desses benefícios?
6. Qual seria o impacto se você não pudesse ir em frente com o tratamento?
7. O uso dos dados seria antiético ou ilegal de alguma forma?

Teste de necessidade:

1. Esse tratamento realmente ajuda a promover esse interesse?
2. É uma maneira razoável de fazer isso?
3. Existe outra maneira menos invasiva de obter o mesmo resultado?

Teste de proporcionalidade:

Considere o impacto do seu tratamento e se isso substitui o interesse que você identificou:

1. Qual é a natureza do seu relacionamento com o titular?
2. Algum dos dados é sensível?
3. As pessoas esperariam que você usasse seus dados dessa maneira?
4. Você está feliz em explicar isso a eles?
5. Algumas pessoas podem objetar ou considerá-lo intrusivo?
6. Qual é o possível impacto no indivíduo?
7. Que impacto isso pode ter sobre eles?
8. Você está tratando dados de crianças ou adolescentes?
9. Algum dos indivíduos é vulnerável de alguma outra forma?
10. Você pode adotar alguma proteção para minimizar o impacto?
11. Você pode oferecer uma opção de saída?

Com base nas respostas dos questionários anteriores, o controlador precisa tomar uma decisão sobre se ainda acha que a base legal do legítimo interesse é apropriada. A ICO (2021) relata que não existe uma fórmula infalível para o resultado do teste de proporcionalidade - mas o controlador deve ter certeza de que seus interesses legítimos não são substituídos pelos riscos identificados.

A seguir serão apresentados exemplos de tratamento de dados pessoais que se utilizam da hipótese de legítimo interesse:

EXEMPLO 1

Tratamento de dados pessoais estritamente necessário aos objetivos de prevenção e controle de fraudes ou para garantir a segurança da rede e da informação nos sistemas informáticos de determinada instituição (MENDES et al., 2019).

EXEMPLO 2

No caso de uso de dados por uma empresa para fazer ofertas mais adequadas e personalizadas a seus clientes, usando apenas os dados estritamente necessários para tal (MENDES et al., 2019).

EXEMPLO 3

Tratamento de dados de empregados para programas de retenção de talentos e iniciativas de bem-estar (MENDES et al., 2019).

EXEMPLO 4

Envio de e-mail com descontos específicos para os produtos buscados por determinado usuário ou com indicações de compras, tomando como base seu histórico de compras (MENDES et al., 2019).

EXEMPLO 5

Coleta de dados para lembrar o usuário que ele deixou itens no carrinho online, mas não finalizou a compra (MENDES et al., 2019).

2.1.10 – Proteção do crédito, nos termos do Código de Defesa do Consumidor

X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

A base legal de proteção de crédito tem por finalidade garantir que instituições financeiras busquem ampliar e facilitar a concessão de crédito, melhorar as análises de riscos e impulsionar o mercado. Este dispositivo, conforme previsto na Lei, deverá estar em constante sinergia com o Código de Defesa do Consumidor (CDC) e a Lei do Cadastro Positivo (MENDES et al., 2019).

EXEMPLO 1

Criação de banco de dados de cadastros de inadimplentes e adimplentes; e Compartilhamento de dados pessoais constantes em banco de dados de cadastros de inadimplentes e adimplentes para avaliação do risco de crédito quando o Titular solicita um empréstimo ou financiamento (MAIA et al., 2020).

Cumpre destacar que MAIA et al. (2020) ressalvam que ainda pairam dúvidas sobre como a ANPD, o Judiciário e a doutrina irão interpretar a amplitude do tratamento de dados pessoais subsidiado por tal base legal, bem como se haverá algum tipo de restrição sobre quais dados pessoais poderiam eventualmente ser tratados neste escopo.

2.2 – Tratamento de Dados Sensíveis

Segundo a ANPD, os dados pessoais sensíveis são aqueles aos quais a LGPD conferiu uma proteção ainda maior, por estarem diretamente relacionados aos aspectos mais íntimos da personalidade de um indivíduo.

O art. 11 da LGPD apresenta uma lista de hipóteses que autorizam o tratamento de dados pessoais sensíveis, destacando o consentimento como a principal. Neste caso, o consentimento deve ocorrer de **forma específica** e **destacada**, para **finalidades específicas**.

Portanto, o **tratamento de dados sensíveis somente poderá ocorrer quando houver o consentimento do titular de dados ou quando for indispensável para o cumprimento de uma das hipóteses previstas no inciso II**, que são:

> *a) cumprimento de obrigação legal ou regulatória pelo controlador;*
>
> *b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;*
>
> *c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;*
>
> *d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);*
>
> *e) proteção da vida ou da incolumidade física do titular ou de terceiro;*

f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou

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

Conforme é possível depreender, algumas bases são idênticas às previstas no art. 7º, especificamente, as alíneas de "a" a "f". Sendo assim, todas as considerações elencadas no tópico anterior são válidas para dados pessoais sensíveis. Como forma de sintetizar tal convergência, segue esquema comparativo de hipóteses de tratamento de dados pessoais gerais e sensíveis (Figura 10)

Dados Pessoais em Geral

1.1 - Consentimento do titular
1.2 - Cumprimento de obrigação legal ou regulatória
1.3 - Execução de políticas previstas em leis e regulamentos
1.4 - Estudos por órgão de pesquisa, desde que mantido o anonimato
1.5 - Execução de contrato do qual é parte o titular de dados
1.6 - Exercício regular de direitos em processo judicial, administrativo ou arbitral
1.7 - Proteção da vida ou da incolumidade física do titular ou de terceiro
1.8 - Tutela de saúde, com procedimento realizado por profissionais da área da saúde ou por entidades sanitárias
1.9 - Legítimo interesse do controlador ou de terceiros
1.10 - Proteção do crédito, nos termos do Código de Defesa do Consumidor

Dados Pessoais Sensíveis

1.1 - Consentimento do titular
1.2 - Cumprimento de obrigação legal ou regulatória
1.3 - Execução de políticas previstas em leis e regulamentos
1.4 - Estudos por órgão de pesquisa, desde que mantido o anonimato
1.6 - Exercício regular de direitos em processo judicial, administrativo ou arbitral
1.7 - Proteção da vida ou da incolumidade física do titular ou de terceiro
1.8 - Tutela de saúde, com procedimento realizado por profissionais da área da saúde ou por entidades sanitárias
1.11 - Garantia da prevenção à fraude e à segurança do titular

Figura 10. Bases Legais art. 7º e art. 11

Fonte: Conselho Nacional de Saúde (2021)

Descrição: A imagem é uma tabela a lista de hipóteses de tratamento de dados pessoais em geral e sensíveis

2.2.1 – Garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos

Como notado anteriormente, há uma hipótese que não possui correspondência com nenhuma das bases gerais para tratamento de dados dispostas no art. 7º, a alínea "g". Esta hipótese diz respeito à garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos previstos na LGPD (art. 6º) e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

Tal base legal específica para dados pessoais sensíveis se refere, portanto, aos dados que serão obtidos quando estes forem indispensáveis para cumprir a finalidade de prevenção à fraude e à segurança do titular nos processos de identificação e autenticação de cadastro em sistemas eletrônicos. Nesse sentido, dentre os tipos de dados sensíveis, envolve especialmente o tratamento de dados biométricos que servirão para autenticação e identificação do titular de dados em meios eletrônicos (MAIA et al., 2020).

MAIA et al. (2020) destacam que o princípio do livre acesso (art. 6º, IV) e da transparência (art. 6º, VI) ganham notoriedade nessa base legal, pois o titular de dados deve ter garantido o seu direito de obter informações, de forma facilitada, sobre a forma, a duração, os agentes de tratamento e todo o contexto envolvendo o tratamento de seus dados pessoais, como forma de resguardar e proteger seus direitos previstos no art. 9º.

EXEMPLO 1

Cumprimento de programas sociais; Lei Federal 16.758/2018 – tratamento de dados de origem racial para melhoria de políticas públicas (MAIA et al., 2020).

EXEMPLO 2

Coleta da biometria de funcionários para garantir o acesso seguro a uma dada empresa.

2.3 – Tratamento de Dados Pessoais de Crianças e de Adolescentes

A LGPD destacou uma seção (Seção III) específica para o tratamento de dados de crianças e adolescentes. A Lei, em seu art. 14, já estabelece que tal tratamento deverá ser realizado em seu melhor interesse, e em convergência com a legislação pertinente, em especial, com o Estatuto da Criança e Adolescente (ECA), Lei nº 8.069, de 13 de julho de 1990.

A Lei exige também que o consentimento seja específico e em destaque, dado por pelo menos um dos pais ou pelo responsável legal, conforme disposto no § 1º do art.14.

?

Os controladores deverão manter pública a informação sobre os tipos de dados pessoais coletados de criança e adolescente, a forma de sua utilização e os procedimentos para acesso às informações tratadas.

De acordo com a UNIÃO (2020), é também dever do controlador envidar todos os esforços razoáveis para verificar se o consentimento foi dado realmente pelo responsável da criança ou adolescente, consideradas as tecnologias disponíveis. Nesses casos, as hipóteses que dispensam o referido consentimento ocorrem quando:

a) A coleta for **necessária para contatar os pais, ou o responsável legal, ou, ainda, para a própria proteção da criança ou adolescente**. Nesses casos, os dados deverão ser utilizados uma única vez, vedados o armazenamento e o seu repasse a terceiros;

b) O **tratamento de dados for imprescindível para o exercício de direitos da criança ou adolescente ou para lavratura de registros públicos.**

Cumpre destacar que MENDES et al. (2019) afirmam que, **além do consentimento parental previsto, são hipóteses de permissão de tratamento de dados pessoais de crianças e adolescentes as bases legais elencadas no art. 11, II.** Porém, em todos esses casos, será sempre indispensável o balanceamento com o melhor interesse das crianças e dos adolescentes, de modo que seus

direitos fundamentais sejam plenamente garantidos.

Sendo assim, é preciso destacar os direitos da criança ou adolescentes previstos no art. 227 da Constituição Federal:

> *Art. 227. É dever da família, da sociedade e do Estado assegurar à criança, ao adolescente e ao jovem, com absoluta prioridade, o direito à vida, à saúde, à alimentação, à educação, ao lazer, à profissionalização, à cultura, à dignidade, ao respeito, à liberdade e à convivência familiar e comunitária, além de colocá-los a salvo de toda forma de negligência, discriminação, exploração, violência, crueldade e opressão.*

Ainda neste contexto e no melhor interesse das crianças e adolescentes, MAIA et al. (2020) ressaltam que a LGPD estabeleceu regras específicas a serem observadas na disponibilização de jogos, aplicações de internet ou outras atividades oferecidas, a participação dos vulneráveis não deve estar condicionada à coleta de seus dados pessoais, salvo quando estritamente necessário à atividade oferecida.

EXEMPLO 1

Caso os órgãos e entidades públicas desenvolvam jogos, aplicações de internet ou outras atividades semelhantes voltadas ao público infanto-juvenil, a coleta de dados pessoais dos jovens deverá restringir-se ao estritamente necessário à atividade proposta.

EXEMPLO 2

Tratamento pela Administração Pública de dados pessoais de crianças matriculadas na rede pública de ensino para a oferta concreta do serviço de transporte escolar àqueles alunos (fase de implementação).

2.4 – Tratamento Dados Pessoais pelo Poder Público

No âmbito público, a proteção ao dado pessoal deve ser destacada, especialmente em formato digital, considerando a expansão do governo digital, que busca a eficiência, economicidade e segurança dos serviços públicos e a prestação de serviços à sociedade 24 horas / 7 dias em qualquer território.

A LGPD estabelece uma série de medidas, do art. 23 ao 32, que devem ser adotadas pelos agentes de tratamento no setor público, dentre elas destacam-se:

1. a identificação das bases legais que justificam as atividades de tratamento de dados (art. 23, I);
2. a adoção de processos e políticas internas que assegurem o cumprimento das normas de proteção de dados pessoais (art. 23, I);
3. e o estabelecimento de um canal de contato com os titulares de dados pessoais com a indicação de um encarregado (art. 23, III).

Em determinadas circunstâncias, conforme a natureza e o porte da entidade ou o volume de operações de tratamento de dados, a ANPD poderá estabelecer hipóteses de dispensa da necessidade de sua indicação.

O art. 23 disciplina o tratamento de dados pessoais por pessoas jurídicas de direito público, estabelecendo que deverá ser realizado para "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". O dispositivo reforça a necessidade de que **o controlador, mesmo revestido de base legal ou para execução de políticas públicas, deve respeitar o princípio da finalidade pública do tratamento.**

Figura 11. Escopo de aplicação da LGPD no setor público

Fonte: Secretaria da Controladoria-Geral do Estado de Pernambuco (SCGE-PE)

Descrição: A imagem é uma arte de uma flor com "LGPD Setor Público" ao centro e cada pétala é uma estrutura organizacional do setor público

A UNIÃO[2] (2020) destaca que, com base no princípio da legalidade (art. 37, caput, da Constituição Federal), o administrador público está, em toda sua atividade funcional, sujeito aos mandamentos da lei e às exigências do bem comum, e deles não se pode afastar ou desviar, sob pena de praticar ato inválido e expor-se à responsabilidade disciplinar, civil e criminal, conforme o caso. Portanto, **sempre que a administração pública efetuar uma atividade de tratamento de dados pessoais, ela deverá informar de forma clara a previsão legal e a finalidade da política pública relacionada ao serviço prestado.**

Isto é, os órgãos ou entidades devem divulgar informações como leis e normativos de fácil consulta pelo titular para esclarecimento de dúvidas relacionadas ao serviço e que envolvam: tratamento dos dados; transparência na administração pública; direitos dos titulares; competências legais do órgão ou entidade para tratamento dos dados; direito do consumidor etc.

Cumpre destacar que tanto o rol do art. 7º, quanto o art. 11 são taxativos. Ou seja, cobrem todas as hipóteses de tratamento de dados. Há, entretanto, autores (MENDES e DONEDA, 2018) que defendem a existência de uma outra base legal para o tratamento de dados pessoais no art. 23 da LGPD, para exercício geral das competências ou o cumprimento de atribuições legais da Administração Pública. Contudo, MENDES et al. (2019) entendem que o tratamento de dados pessoais para tais atividades já estaria contemplado, em grande parte, nas hipóteses relativas ao cumprimento de uma obrigação legal (art. 7º, II, e art. 11, II, “a”).

Até que seja pacificado pela ANPD, será considerado neste Manual que o art. 23 não constitui mais uma base legal de tratamento, mas regras adicionais e específicas para o tratamento de dados pessoais pela Administração Pública, isto é, complementam o conteúdo dos art. 7º e art. 11.

[2] Guia de elaboração de Termo de Uso e Política de Privacidade para serviços públicos (2021)

?

As autoridades públicas podem usar interesses legítimos?

No regime jurídico nacional, esta resposta ainda não se encontra pacificada. Entretanto, para fins educativos, vale a pena conhecer a resposta para essa pergunta dada pela autoridade de proteção de dados do Reino Unido, *Information Commissioner's Office* (ICO) (ICO, 2021):

Sim, em alguns casos, as autoridades públicas podem considerar o uso de interesses legítimos como base legal. No entanto, se você for uma autoridade pública, não poderá usar os interesses legítimos como base legal se o tratamento for no desempenho de suas tarefas como autoridade pública. O RGPD do Reino Unido explica que o motivo dessa exclusão é porque cabe ao legislador dar às autoridades públicas autoridade legal para processar dados pessoais; ou seja, se for uma autoridade pública, só deverá poder processar dados pessoais no desempenho das suas tarefas se a lei o autorizar.
Outras bases legais estão disponíveis se você for uma autoridade pública e elas provavelmente serão mais apropriadas para alguns tipos de tratamento; por exemplo, se estiver executando suas atribuições, deve considerar a base 'política pública'.
Embora não possa usar interesses legítimos como base ao processar suas atribuições como autoridade pública, isso não significa que isso nunca possa ser aplicado. Essa restrição ao uso do legítimo interesse diz respeito à natureza da atribuição, não à natureza da organização. Isso significa que, se você for uma autoridade pública, o legítimo interesse pode estar potencialmente disponível se puder demonstrar que o tratamento não faz parte do desempenho de suas atribuições como autoridade pública.

Capítulo 3 – Direitos dos titulares de dados pessoais e os impactos na gestão pública

A LGPD introduz uma nova visão, onde o foco está nas ameaças aos direitos e liberdades dos titulares. Assim, o agente de tratamento deve refletir sobre as implicações que o processamento de dados de natureza pessoal tem sobre os titulares, adequar suas atividades e prover novos serviços, desde a instituição de canais de atendimento ao fornecimento de informações úteis.

Assim, este capítulo visa estabelecer a compreensão dos direitos dos titulares e as respectivas convergências com os princípios previstos no art. 6º. Além de explicar o funcionamento do atendimento ao titular no Poder Executivo Estadual, considerando suas particularidades, serão abordados os impactos na transparência e no compartilhamento de informações pessoais no setor público.

3.1 – Os Direitos do Titular

A LGPD deve ser considerada, essencialmente, focada no combate às possíveis transgressões ao direito de personalidade. Sendo assim, propõe uma nova cultura organizacional, baseada no respeito à privacidade e na mitigação de riscos, a partir da adequação de suas atividades.

No julgamento sobre a Lei do Censo alemã, sob a alegação de violação de direitos fundamentais, entre eles o direito ao livre desenvolvimento da personalidade, o tribunal alemão reconheceu que a pessoa humana tem um direito de personalidade que abrange, especialmente, a proteção contra o processamento sem limites de seus dados pessoais. Ou seja, esse direito fundamental deve assegurar o poder de o cidadão decidir, ele mesmo, sobre como seus dados devem ser tratados (direito à autodeterminação informacional) (DA MOTA ALVES, 2021).

Direito à autodeterminação informativa

Direito com status de direito fundamental enquanto direito de personalidade, garantindo ao indivíduo o poder de controlar as suas próprias informações. Ou seja, seria uma afirmação do personalíssimo no âmbito das interações entre indivíduo e sociedade (DONEDA, 2019).

Os direitos básicos atribuídos ao titular pelas diversas legislações nacionais e tratados internacionais para o controle do fluxo de seus dados, decorrentes do direito à autodeterminação informativa, são conhecidos pela sigla "ARCO", abreviação de: **acesso, retificação, cancelamento e oposição.** Além dos chamados direitos ARCO, a LGPD prevê uma série de outros direitos para o titular (MENDES, 2019).

Os direitos da LGPD estão previstos nos artigos 18, 19 e 20 e podem ser sintetizados da seguinte forma:

Figura 12. Direitos dos titulares de dados pessoais

Fonte: Quais são os seus direitos? — LGPD - Lei Geral de Proteção de Dados Pessoais | Serpro (adaptado)

Descrição: A imagem apresenta a relação de direitos dos titulares com ícones representativos

Em termos quantitativos, não é preciso muito esforço para compreender que a LGPD possui muito mais dispositivos e controles que repercutem em obrigações legais do que qualquer outro elemento que a compõe. Isso porque se trata de uma lei de regulação da atividade social, ou seja, seu propósito é, de fato, intervir

na atividade de tratamento praticada pelo particular ou pelo Estado impondo mecanismos e limitações que vão condicionar a maneira como se processarão os dados pessoais (DA MOTA ALVES, 2021).

Conforme ensina DONELA (2019), além da LGPD, outros diplomas normativos brasileiros contêm direitos para o cidadão sobre seus dados. Por exemplo, o Código de Defesa do Consumidor (CDC) procura proteger os direitos do consumidor sobre seus próprios dados pessoais, em particular quando presentes em bancos de dados de proteção ao crédito. O Marco Civil da Internet, por sua vez, estabelece uma série de prerrogativas e direitos aos usuários da Internet sobre seus próprios dados. Uma tutela de escopo mais amplo, porém igualmente voltada para a proteção de dados pessoais, pode ser observada no próprio Código Civil, incidindo a partir da proteção dos direitos de personalidade e da tutela dos direitos subjetivos.

3.1.1 – Direito de acesso facilitado às informações sobre o tratamento de dados pessoais

O direito de acesso (art. 18, II), comumente conhecido por "acesso do titular", dá aos indivíduos o direito de obter uma cópia de seus dados pessoais, bem como outras informações complementares. Ajuda o titular a entender como e porque o agente de tratamento está usando seus dados e a verificar se está em conformidade com a Lei.

Detalhado no art. 9º, o dispositivo determina que direito de acesso precisa ser facilitado e que as informações devam ser disponibilizadas de forma clara, adequada e ostensiva acerca de (entre outras):

1. finalidade específica do tratamento;
2. forma e duração do tratamento, observados os segredos comercial e industrial;
3. identificação do controlador;
4. informações de contato do controlador;
5. informações acerca do uso compartilhado de dados pelo controlador e a finalidade;
6. responsabilidades dos agentes que realizarão o tratamento; e
7. direitos do titular.

Portanto, o controlador deve fornecer informações de privacidade aos indivíduos quando coleta seus dados pessoais. Dentre os produtos mais importantes para o cumprimento desse direito, cita-se a Política de Privacidade, documento informativo pelo qual o prestador de serviço público transparece a forma como ele realiza o tratamento dos dados pessoais e como ele fornece privacidade ao usuário.

Tal direito está intimamente relacionado ao princípio da transparência: ter acesso às informações sobre o tratamento de dados pessoais é o início de um processo de autodeterminação informativa. Afinal, só é possível exercer qualquer outro direito quando se tem suficiente conhecimento sobre como, para que e por quem os dados estão sendo tratados (DA MOTA ALVES, 2021).

EXEMPLO 1

O produtor cultural, antes de fornecer os seus dados pessoais para o recebimento dos benefícios da Lei Aldir Blanc, toma conhecimento da Política de Privacidade do serviço público.

EXEMPLO 2

Um dado titular beneficiário do Bolsa Família requisita ao órgão gestor o acesso aos seus dados pessoais para confirmar sua integridade.

3.1.2 – Direito de confirmação da existência do tratamento

O direito de ser informado da existência do tratamento é um dos principais requisitos de transparência da LGPD. Trata-se de fornecer aos demandantes informações claras e concisas sobre a existência de tratamento de dados pessoais na organização.

Cumpre destacar que a confirmação de existência (art. 18, I) não se confunde com o acesso aos dados (art. 18, II). Entende-se que a requisição de acesso será atendida apenas pela completude dos dados enviados referentes ao titular. Por outro lado, a confirmação da existência limita-se à informação de que a organização processa tais dados, assumindo-se que seja atendida de forma célere pelas organizações.

EXEMPLO 1

Um dado titular beneficiário do Bolsa Família requisita ao órgão gestor a confirmação da existência dos seus dados pessoais.

3.1.3 – Direito de correção de dados incompletos, inexatos ou desatualizados

De acordo com o inciso III do art. 18 da LGPD, o titular tem o direito de retificar dados pessoais incorretos. O titular também pode ter dados pessoais inexatos, ou até desatualizados. Isso pode envolver, inclusive, o fornecimento de uma declaração complementar aos dados pessoais incompletos.

O procedimento de correção poderá ser realizado através da requisição formal no canal de atendimento ou, quando possível, através da própria ferramenta de coleta de dados que o titular tenha acesso.

Este direito está intrinsecamente relacionado com o princípio da qualidade dos dados (art. 6º, V). Assim, embora a organização já possa ter tomado medidas para garantir que os dados pessoais estivessem corretos quando coletados, este direito impõe a obrigação de reconsiderar a exatidão mediante solicitação.

EXEMPLO 1

O titular beneficiário do Bolsa Família tem acesso aos seus dados pessoais, identifica que estão desatualizados e requisita ao órgão gestor a sua atualização cadastral.

EXEMPLO 2

O produtor cultural, após fornecer os seus dados pessoais para o recebimento dos benefícios da Lei Aldir Blanc, identifica que há inconsistências e decide corrigi-los na própria ferramenta de coleta.

3.1.4 – Direito de anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade

O inciso IV do art.18 da LGPD concede aos titulares o direito de restringir o processamento de seus dados pessoais em determinadas circunstâncias. Isso significa que um indivíduo pode limitar a maneira como uma organização usa seus dados. No caso, a anonimização é uma alternativa à opção de solicitar a eliminação dos dados pessoais.

Tal direito decorre diretamente do direito fundamental da autodeterminação informacional citado anteriormente. Assim, os titulares têm o poder de restringir o tratamento dos seus dados pessoais sempre que tenham um motivo específico para tal. Isso pode ocorrer quando da ocorrência de problemas com o conteúdo das informações que a organização possui ou como ela processou os dados. Na maioria dos casos, o controlador não será obrigado a bloquear os dados pessoais de um indivíduo indefinidamente, mas precisará ter a restrição em vigor por um determinado período solicitado.

Assim, os titulares têm o direito de ter seus dados pessoais apagados se tais dados não são mais necessários para os fins aos quais o controlador os coletou ou processou originalmente. Isso também vale para tratamentos realizados a partir da hipótese de legítimo interesse, e tal interesse resta superado, assim como aqueles tratados ilicitamente.

Mesmo existindo o direito de o titular solicitar a eliminação dos dados, é importante destacar o poder-dever dos agentes de tratamento em realizar a eliminação de tais dados com o término de seu tratamento, independente de petição do titular, conforme disposto no art. 16:

> *Art. 16. Os dados pessoais serão eliminados após o término de seu tratamento, no âmbito e nos limites técnicos das atividades, autorizada a conservação para as seguintes finalidades:*
>
> *I - cumprimento de obrigação legal ou regulatória pelo controlador;*
>
> *II - estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;*
>
> *III - transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos nesta Lei; ou*
>
> *IV - uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados.*

EXEMPLO 1

Uma empresa solicitou e armazena o telefone dos seus clientes nos seus cadastros, mas a sua operação comercial não possui necessidade de contato telefônico. Nesse caso, o cliente pode pedir para que tal dado seja eliminado da base de dados, por entender que o dado é desnecessário.

EXEMPLO 2

Um cidadão decidiu realizar viagem por tempo indeterminado a outro país e detém dados cadastrados em uma rede de supermercados que oferece descontos personalizados. O cidadão solicita o bloqueio do tratamento de dados e decidiu só reativar as operações de contato caso retorne da viagem. Essa demanda implica na suspensão do tratamento de dados pela rede de supermercados, que não poderá contatar o cliente, nem realizar outro tipo de tratamento de dados. Tal exemplo difere da eliminação de dados, uma vez que as informações do titular permanecerão cadastradas pela empresa, porém não poderão ser utilizadas.

3.1.5 – Direito de portabilidade de dados

O direito à portabilidade dos dados (art. 18, V) dá aos titulares o direito de receber os dados pessoais fornecidos a um agente de tratamento em um formato estruturado, comumente usados e legíveis por máquina. Assim como, dá o direito ao titular de solicitar que um controlador transfira esses dados diretamente para outro controlador.

A portabilidade dos dados pessoais, direito derivado do poder geral de controle do titular sobre seus dados (direito à autodeterminação informativa), implica na necessidade de o controlador implementar mecanismos que possibilitem o compartilhamento de dados pessoais para outros (MENDES et al., 2019).

Mas, quando esse direito se aplica? O direito à portabilidade de dados só se aplica mediante requisição expressa sem restrições na LGPD, desde que observados os segredos comercial e industrial.

Por fim, cumpre ressaltar que a Lei prevê que o conteúdo será objeto de regulamentação por parte da ANPD. Dessa forma, **assume-se que tal dispositivo possui eficácia limitada. Enquanto não existir tal regulamentação, salvo melhor juízo, o direito só poderá ser exercido de acordo com as previsões contratuais ou a partir da existência de uma política do controlador dispondo sobre tal.**

EXEMPLO 1

Qualquer pessoa no país pode manter o seu número de telefone (dado pessoal) se realizar a troca da operadora, conforme estabelecido pela Resolução nº 460/2007 da ANATEL.

3.1.6 – Direito de eliminação de dados pessoais tratados com o consentimento

De acordo com o inciso VI do art. 18 da LGPD, **os titulares têm o direito de que seus dados pessoais obtidos através do consentimento sejam eliminados.** Isso também é conhecido como o "direito de ser esquecido".

O referido direito também se aplica nos casos de tratamentos de dados pessoais de crianças e adolescentes coletados a partir do consentimento do responsável.

Cumpre destacar, igualmente citada no item 3.1.4, a obrigação da eliminação ou do apagamento dos dados após o término de seu tratamento por parte dos agentes de tratamento, no âmbito e nos limites técnicos das atividades, sendo autorizada a conservação somente nas exceções legais.

3.1.7 – Direito de informação sobre o compartilhamento de dados pessoais

Decorrente do Princípio da Transparência, o direito de informação sobre o compartilhamento de dados pessoais encontra-se previsto no inciso VII do art. 18 da LGPD. O controlador tem a obrigatoriedade de informar ao titular de dados pessoais as informações sobre o compartilhamento de seus dados.

Nesse contexto, conforme inciso V do art. 9º, o controlador deverá disponibilizar as informações de forma clara, adequada e ostensiva acerca do uso compartilhado de dados e a sua finalidade.

No caso da administração pública, em que o tratamento é embasado nas hipóteses de dispensa de consentimento original, o compartilhamento demandará uma nova justificativa de tratamento, conforme § 5º do art. 7º. Além disso, tal direito pressupõe a devida publicidade em relação ao tratamento

compartilhado de dados necessários à execução de políticas públicas previstas em leis ou regulamentos (art. 11, § 2º)

Lembrando que, segundo § 6º do art. 18, o responsável deverá informar, de maneira imediata, aos agentes de tratamento com os quais tenha realizado uso compartilhado de dados a correção, a eliminação, a anonimização ou o bloqueio dos dados, para que repitam idêntico procedimento, exceto nos casos em que esta comunicação seja comprovadamente impossível ou implique esforço desproporcional.

3.1.8 – Direito de informação sobre a possibilidade de não fornecimento de consentimento

O inciso VI do art.18 estabelece o direito de informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa. Este direito está diretamente relacionado ao ato de consentir com a coleta de dados pessoais através de instrumentos próprios.

Conforme já citado anteriormente nas hipóteses de permissão de tratamento de dados pessoais, o consentimento deve ser uma manifestação **livre, informada e inequívoca** pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada. Espera-se, no ato, que o agente de tratamento informe todas as condições e possibilidades sobre o consentimento para que não reste dúvida ao titular da sua manifestação e que esta esteja sendo realizada de livre opção.

3.1.9 – Direito de revogação do consentimento

Conforme citado anteriormente, o consentimento, como uma autorização expressa, de semelhante forma, pode ser objeto de revogação. O procedimento de revogação pode ser requisitado a qualquer tempo, de forma gratuita e facilitada.

O agente de tratamento deve ter cuidado: **a revogação do consentimento não acarreta a determinação para a eliminação automática dos dados coletados licitamente.** Sendo assim, sugere-se que na condição de uma revogação, seja dada a oportunidade ao titular de requisitar a eliminação conjuntamente.

Ademais, alterações quanto ao tratamento de dados, seja na finalidade, forma e duração do tratamento, alteração do controlador ou compartilhamento permitem a revogação do consentimento caso haja discordância por parte do titular.

3.1.10 – Direito de peticionar perante a Autoridade Nacional de Proteção de Dados (ANPD) e organismos de defesa do consumidor

Diante da negativa de parte do controlador em atendimento aos direitos antes citados, por requerimento expresso do titular, ou de representante legalmente constituído, a Lei prevê o direito do titular de dados de apresentar à ANPD petições contendo a comprovação do fato (art. 18, § 1º).

A ANPD já disponibiliza canal para registrar petições do titular contendo a comprovação da apresentação de reclamação ao controlador não solucionada através do link: https://www.gov.br/secretariageral/pt-br/sei-peticionamento-eletronico

3.1.11 – Direito à oposição

Segundo o § 2º do art. 18, o titular pode opor-se a tratamento realizado com fundamento em uma das hipóteses de dispensa de consentimento, em caso de descumprimento ao disposto nesta Lei.

O dispositivo dá aos titulares o direito de se opor ao tratamento de seus dados pessoais a qualquer momento quando da aparente ilicitude do processamento. Assim, o titular poderá efetivamente exercer controle sob uso indevido de seus dados por agentes de tratamento.

Cumpre destacar que a objeção pode estar relacionada a todos os dados pessoais tratados ou apenas em parte de tal conteúdo. Esta oposição pode considerar inclusive o desvio de finalidade, e o desrespeito ao Princípio da Necessidade, estabelecido no inciso III do art. 6º. Entretanto, apesar de ser um direito controverso, pela leitura do §2º do art. 18, é possível extrair a conclusão de que o uso de dados dispensados de consentimento, dentro dos limites legais,

não estaria sujeito à oposição de seu titular[3]. Ou seja, o direito à oposição não é absoluto e deve ser limitado nos casos do tratamento realizado para execução de políticas públicas ou no exercício legal ou regulatório.

3.1.12 – Direito de revisão de decisões tomadas unicamente com base em tratamento automatizado

A tomada de decisão individual automatizada é uma decisão feita por meios automatizados, sem qualquer envolvimento humano. Em certos casos, a tomada de decisão individual automatizada resulta na criação de perfis, a partir de informações pessoais sobre indivíduos de uma variedade de fontes diferentes.

Conteúdos como: pesquisas na Internet, hábitos de compra, estilo de vida e dados de comportamento coletados de telefones celulares, redes sociais e sistemas de videomonitoramento, são comumente usados pelas organizações para a tomada de decisão unicamente com base em tratamento automatizado.

Nesse contexto, o agente de tratamento deverá fornecer, mediante solicitação, informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, observados os segredos comercial e industrial (art. 20).

Apesar da tomada de decisão unicamente com base em tratamento automatizado poder levar a decisões mais rápidas e robustas, é importante que o titular exerça a tutela fiscalizatória do uso abusivo, dado os riscos ao titular de decisões enviesadas ou por base em dados sensíveis.

EXEMPLO 1

Cliente solicita revisão de uma decisão automatizada realizada em ferramenta online de concessão de empréstimo por uma instituição financeira.

EXEMPLO 2

Candidato solicita revisão de um teste de aptidão de recrutamento que usa algoritmos e critérios pré-programados.

[3] https://www.migalhas.com.br/depeso/293745/a-excecao-dos-dados-pessoais-tornados-manifestamente-publicos--pelo-titular-na-lgpd

3.2 – Demandas dos Titulares

A LGPD estabelece um conjunto de demandas que deverão ser atendidas pelos controladores a partir da positivação dos direitos dos titulares de dados pessoais no canal de atendimento, dentre as quais podem ser destacadas as seguintes:

Tabela 3 - Demandas dos titulares

	DEMANDAS DOS TITULARES A SEREM ATENDIDAS NO CANAL DE ATENDIMENTO	REFERÊNCIA LEGISLATIVA (LGPD)
1	Solicitação da confirmação da existência de tratamento	art. 18, I
2	Solicitação de acesso aos dados pessoais tratados pelo controlador	art. 18, II
3	Solicitação de correções de dados incompletos, inexatos ou desatualizados	art. 18, III
4	Requisição da anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com a LGPD	art. 18, IV
5	Solicitação da eliminação ou do apagamento dos dados, no âmbito e nos limites técnicos das atividades, sendo autorizada a conservação somente nas exceções legais	art.18, VI c/c art. 16
6	Solicitação de informações acerca do uso compartilhado de dados pelo controlador; finalidade, responsabilidades dos agentes que realizarão o tratamento e direitos do titular	art. 18, VII c/c art. 9º, § 3º
7	Solicitação de informações sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa	art. 18, VIII
8	Solicitação da revogação do consentimento a qualquer tempo, mediante manifestação expressa do titular, por procedimento gratuito e facilitado	art. 18, IX c/c art. 8º, § 5º
9	Oposição ao tratamento realizado com fundamento em uma das hipóteses de dispensa de consentimento, em caso de descumprimento ao disposto na LGPD	art. 18, § 2º
10	Solicitação de acesso às informações a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, observados os segredos comercial e industrial	art. 19, §3º

Ressalta-se que o direito à portabilidade não se encontra elencado na Tabela 3 dada a limitação da sua eficácia, conforme citado no item 3.1.5 – Direito de portabilidade de dados. Ademais, os serviços 5, 7 e 8 estão diretamente relacionados à hipótese de tratamento de dados pessoais com base no consentimento e, conforme citado anteriormente no Capítulo 2, tal base deve ser considerada em situações extraordinárias na administração pública.

A criação de um canal de atendimento aos titulares para que possam exercer seus direitos previstos na Lei é uma das principais obrigações para o poder público. Não por menos, em Pernambuco, conforme Decreto Estadual nº 49.265/2020, o atendimento do titular de dados pessoais será realizado através dos canais de atendimento eletrônicos – no www.ouvidoria.pe.gov.br - ou presenciais da ouvidoria. Dessa forma, será possível prover funções de registro e gerenciamento, com intuito de proporcionar o acompanhamento de cada demanda.

Registre-se, que o citado Decreto confere à OGE – Ouvidoria Geral do Estado - a incumbência de encaminhar o atendimento ao encarregado do órgão ou entidade responsável pelos dados e de acompanhar a sua resolutividade. Quando concluído o atendimento, as informações solicitadas deverão ser entregues ao titular ou seu representante legal, através de meio eletrônico protegido ou pessoalmente (art. 16, §2 º).

3.3 – Transparência e Proteção de Dados Pessoais

É importante destacar que a LGPD dispensa a exigência do consentimento, conforme § 4º do art. 7º, para os dados "tornados manifestamente públicos pelo titular". Porém, isto não isenta os agentes de tratamento a observar os direitos do titular e os princípios previstos na Lei. Assim como na hipótese dos dados de acesso público, aqui deve ser considerado o contexto em que a informação foi disponibilizada, bem como haver compatibilidade entre o seu uso e as circunstâncias pelas quais tal informação foi tornada pública, tendo em vista a ressalva disposta na Lei, que não autoriza o uso indiscriminado desses dados. Esses tipos de dados, ainda que sejam considerados públicos, não deixam de ser pessoais, sendo necessário considerar sempre a finalidade da circulação e o que justifica sua disponibilização (MENDES et al., 2020).

EXEMPLO 1

O fato de alguém ser proprietário de um imóvel, sócio de uma empresa ou casado, cuja divulgação pública é obrigatória (MENDES et al., 2020).

EXEMPLO 2

A consulta de CPFs no site da Receita Federal com o propósito de mera confirmação de titularidade para operações financeiras, cuja divulgação pública é obrigatória (MENDES et al., 2020).

No âmbito público, o princípio da publicidade é um dos pilares da Administração Pública, estando previsto no art. 37, da Constituição Federal. Tal princípio foi recentemente destacado de forma mais objetiva pela Emenda Constitucional nº 108/2020:

> *Art. 163-A. A União, os Estados, o Distrito Federal e os Municípios disponibilizarão suas informações e dados contábeis, orçamentários e fiscais, conforme periodicidade, formato e sistema estabelecidos pelo órgão central de contabilidade da União, de forma a garantir a rastreabilidade, a comparabilidade e a publicidade dos dados coletados, os quais deverão ser divulgados em meio eletrônico de amplo acesso público. (Incluído pela Emenda Constitucional nº 108, de 2020)*

A Lei de Acesso à Informação (LAI), Lei Federal nº 12.527, de 18 de novembro de 2011, segue nessa esteira e se destina à regulamentação da publicização dos dados tratados pelo Poder Público, pressupondo que seu domínio é público. Seu foco, portanto, é a forma e o meio em que as informações pessoais são acessadas por terceiros ou disponibilizadas ao público.

Segundo a Controladoria-Geral da União (CGU)[4], para garantir a efetividade do acesso à informação pública, uma legislação sobre direito à informação deve observar um conjunto de padrões estabelecidos com base nos melhores critérios e práticas internacionais. Dentre esses princípios, destacam-se:

- Acesso é a regra, o sigilo, a exceção (divulgação máxima)
- Requerente não precisa dizer por que e para que deseja a informação (não exigência de motivação)
- Hipóteses de sigilo são limitadas e legalmente estabelecidas (limitação de exceções)
- Fornecimento gratuito de informação, salvo custo de reprodução (gratuidade da informação)
- Divulgação proativa de informações de interesse coletivo e geral (transparência ativa)
- Criação de procedimentos e prazos que facilitam o acesso à informação (transparência passiva)

Considerando os direitos e garantias estabelecidos pela LGPD, em princípio, estar-se-ia diante de um suposto conflito entre a Lei de Acesso à Informação e as proteções conferidas aos dados pessoais pela Lei nº 13.709/2018. Sendo assim, é dever dos órgãos e entidades públicas promover, independentemente de requerimentos, a divulgação de informações de interesse coletivo ou geral por eles produzidas ou custodiadas.

[4] https://www.gov.br/acessoainformacao/pt-br/assuntos/conheca-seu-direito/principais-aspectos/principais-aspectos

A Procuradoria-Geral do Estado (PGE) destaca não haver hierarquia entre as leis em questão, de modo que não se pode falar em prevalência de uma sobre a outra, vez que ambas estão em condições de igualdade no ordenamento jurídico brasileiro. Trata-se de leis ordinárias, de abrangência nacional e que contêm normas gerais a respeito dos direitos fundamentais por elas garantidos (acesso à informação e proteção de dados individuais). Dessa forma, é preciso proceder a interpretação das normas de forma sistemática, em conjunto, buscando delas extrair seus conceitos fundamentais e obter a harmonização entre ambas.

Sobreleva destacar que a proteção conferida ao tratamento de dados pessoais pela LGPD incide desde a coleta de tais dados até sua divulgação e descarte. No entanto, é preciso avaliar, no âmbito público, se um dado pessoal deve ser, de fato, publicizado por força da Lei de Acesso à Informação - LAI.

Cumpre destacar que, no art. 6º da LAI, é assegurada a proteção da informação pessoal, observada a sua disponibilidade, autenticidade, integridade **e eventual restrição de acesso**. Ademais, conforme inciso II, do art. 31, da LAI, só poderão ter autorizada sua divulgação diante:

1. **de previsão legal**; ou
2. **consentimento expresso da pessoa a que elas se referirem.**

Sendo assim, tais condições encontram-se coerentes com a LGPD, uma vez que o art. 7º da Lei prevê as seguintes hipóteses de tratamento de dados:

1. mediante o fornecimento **de consentimento pelo titular**;
2. para o cumprimento de **obrigação legal ou regulatória** pelo controlador.

A LAI, ao prever a transparência dos registros das despesas, segundo inciso III do § 1º do art. 8º, também estabelece no § 2º do art. 7º que, quando não for autorizado acesso integral à informação, por ser ela parcialmente sigilosa, é assegurado o acesso à parte não sigilosa por meio de certidão, extrato ou cópia com ocultação da parte sob sigilo.

Dessa forma, apenas os dados estritamente necessários à transparência devem ser publicizados. Ou seja, o inteiro teor das informações pessoais não é essencial para o controle social, e dessa forma, deve ser ocultado ou anonimizado, salvo obrigação legal em contrário.

Quanto ao nível de informação a ser disponibilizada, que no caso assume-se que a dúvida paira sobre um suposto conflito entre a LGPD e a Lei de Acesso à Informação - LAI, é preciso fazer a análise do conteúdo duvidoso caso a caso. No entanto, orienta-se que se faça uma reflexão se há risco na divulgação de dados pessoais com base na interpretação da LAI, i.e., se pode ocasionar dano aos titulares dos dados.

Em contraponto, caso seja relevante para a entidade tornar tais informações pessoais públicas e não havendo base específica de tratamento na LGPD, orienta-se a aplicação dos mecanismos de obtenção de consentimento expresso dos titulares. E até que tal situação se concretize, recomenda-se a anonimização dos referidos dados.

Ademais, os dados pessoais já publicizados e que não atendem a finalidade devem ser revistos, uma vez que o tratamento de dados de divulgação é continuamente executado. Assim, a revisão do conteúdo e ocultação de tais informações minimizarão os potenciais danos aos titulares, reduzindo o risco de questionamentos futuros.

?

A publicação na íntegra dos instrumentos contratuais celebrados pelo estado com dados pessoais no seu conteúdo poderia conflitar com a proteção conferida aos dados pessoais pela LGPD?

Acesse o Boletim Informativo da PGE Consultiva nº 12/2020 – Orientações quanto à inserção dos dados pessoais das partes e seus representantes no preâmbulo dos instrumentos contratuais e congêneres e respectivos extratos, para fins de atendimento à Lei Geral de Proteção de Dados Pessoais (LGPD) no link: http://www.pge.pe.gov.br/app_themes/doc_consultiva_boletim_12_2020.pdf

?

As informações financeiras dos servidores devem ser consideradas como dados pessoais e, portanto, não podem ser divulgadas?

Os dados relacionados à remuneração e ao subsídio dos servidores devem ser considerados dados pessoais. No entanto, apesar de sujeitos à LGPD, devem ser publicizados por obrigação legal, conforme a Lei de Acesso à Informação - LAI.

O Decreto Estadual nº 38.787/2012 regulamentador da Lei Estadual de Acesso à Informação (Lei Estadual nº 14.804/2012) em seu inciso VI do art. 7º, ao definir o conteúdo de divulgação, previu a inclusão de informações financeiras dos servidores, ao citar as informações concernentes a "remuneração e subsídio" e outros adicionais financeiros, vide:

Art. 7º É dever dos órgãos e entidades promover, independentemente de requerimento, a divulgação, em seus sítios na internet, de informações de interesse coletivo ou geral por eles produzidas ou custodiadas, observado o disposto no artigo 4º da Lei no 14.804, de 2012.

(...)

VI - **remuneração e subsídio** recebidos por ocupante de cargo, posto, graduação, função e emprego público, incluindo **Auxílios, ajudas de custo, jetons e quaisquer outras vantagens pecuniárias, bem como os proventos de aposentadoria e pensões,** todos de maneira individualizada;

O fato de parte do conteúdo da folha de pagamento ser publicizada, não isenta a responsabilidade do órgão e entidade de promover a proteção dos dados pessoais dos servidores públicos, considerando os princípios previstos no art. 6º da LGPD em harmonia com o interesse público e o controle social.

3.4 – Compartilhamento de Dados Pessoais no Poder Público

Apesar da LGPD autorizar o compartilhamento de dados entre agentes de tratamento, é relevante diferenciar o compartilhamento entre agentes de tratamento do setor público e o compartilhamento com agentes do setor privado. Esta diferenciação é importante, pois produz situações distintas para a Lei e enseja consequências jurídicas diversas.

A LGPD, no seu art. 26, permite a transferência de dados pessoais entre os agentes de tratamento do setor público desde que tenha por objetivo:

1. finalidades específicas de execução de políticas públicas previstas em leis

e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres; e
2. cumprir atribuição legal pelos órgãos e pelas entidades públicas, respeitados os princípios de proteção de dados pessoais elencados no art. 6° da Lei.

Nessas condições, o controlador público deve manter o registro do compartilhamento dos dados pessoais para efeito de comprovação prevista no inciso VII do art. 18 da Lei Federal nº 13.709/18, o qual trata de informações das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados.

A LGPD condiciona a transferência de dados por determinado controlador que já obteve consentimento, a novo e específico consentimento, como apresentado no item 2.1.1 – Consentimento do titular. No caso do poder público, em que o tratamento é embasado nas hipóteses de dispensa de consentimento original, o compartilhamento demandará uma nova justificativa de tratamento, conforme § 5° do art. 7° da Lei.

A LGPD veda a transferência entre controladores do setor público quando se tratar de dados pessoais sensíveis referentes à saúde. Por outro lado, é possível quando envolver hipóteses relativas à prestação de serviços de saúde, de assistência farmacêutica e de assistência à saúde, desde que observado o § 5° do art. 11 da Lei, incluídos os serviços auxiliares de diagnose e terapia, em benefício dos interesses dos titulares de dados.

A Lei, no § 1° do art. 26, veda a transferência de dados pessoais pelos agentes de tratamento do setor público com entidades privadas, exceto quando:

1. os dados forem acessíveis publicamente;
2. houver previsão legal ou a transferência for respaldada em contratos, convênios ou instrumentos congêneres;
3. objetivar exclusivamente a prevenção de fraudes e irregularidades, ou proteger e resguardar a segurança e a integridade do titular dos dados, desde que vedado o tratamento para outras finalidades; ou
4. nos casos de execução descentralizada de atividade pública que exija a transferência, exclusivamente para esse fim específico e determinado, observado o disposto na Lei Federal nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação).

Ademais, caso o Poder Público vislumbre, no caso concreto, não se encaixar em nenhuma das hipóteses legais autorizadoras do compartilhamento de dados pessoais com entidades privadas, e, mesmo assim, pretenda efetuar o compartilhamento, deverá, obrigatoriamente, atender aos seguintes requisitos:

a) obter o consentimento expresso e destacado do titular do dado; e
b) comunicar à ANPD. Lembrando que tal obrigação de comunicação possui eficácia limitada, dada sua necessidade de regulamentação, conforme Parágrafo Único do art. 27.

Outro aspecto relevante da Lei no compartilhamento de dados pelo Poder Público com entidades privadas é o disposto no § 3º do art. 11, que estabelece: a comunicação ou o uso compartilhado de dados pessoais sensíveis entre controladores com objetivo de obter vantagem econômica poderá ser objeto de vedação ou de regulamentação por parte da ANDP, ouvidos os órgãos setoriais do Poder Público, no âmbito de suas competências.

Por fim, cumpre citar o Decreto Estadual nº 50.474, de 29 de março de 2021, que dispõe sobre a Política Estadual de Compartilhamento de Dados e cria a Plataforma de Compartilhamento e Análise de Dados dos órgãos e entidades da administração direta e indireta do Poder Executivo Estadual. Assim, o normativo visa fomentar o desenvolvimento de estruturas e regras essenciais para habilitar o compartilhamento de dados facilitado, colaborativo, seguro, acessível às atividades institucionais e para oportunizar apoio à formulação de políticas públicas orientadas a dados.

3.5 – Sanções

No Brasil, a legislação adotou a sistemática regulatória sustentada na criação de uma autoridade reguladora associada à competência de fiscalização e aplicação de multas, a oportunidade de adoção de boas práticas por parte dos agentes de tratamento.

A LGPD estabelece que poderão ser aplicadas pela Autoridade Nacional, **a partir de agosto de 2021** (art. 65, I-A), as seguintes **sanções administrativas** (art. 52):

1. **advertência,** com indicação de prazo para adoção de medidas corretivas;

2. **multa simples, de até 2% do faturamento da pessoa jurídica de direito privado,** grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, **limitada, no total, a R$ 50 milhões por infração,** exceto quando não dispuser ou for incompleto o valor de faturamento no ramo;
3. **multa diária,** observado o limite total de R$ 50 milhões por infração;
4. **publicização da infração** após devidamente apurada e confirmada a sua ocorrência;
5. **bloqueio dos dados pessoais** a que se refere à infração;
6. **eliminação dos dados pessoais** a que se refere à infração;
7. **suspensão parcial do funcionamento do banco de dados** a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização;
8. **suspensão do exercício da atividade** a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período; ou
9. **proibição parcial ou total do exercício de atividades** relacionadas a tratamento de dados.

Quanto à fiscalização e às sanções administrativas, é preciso observar a limitação prevista na Lei para controladores do setor público. Nesse aspecto, a LGPD, nos termos do §3º do art. 52, prevê que poderão ser aplicados **às entidades e órgãos públicos as seguintes sanções: advertência, publicização da infração, bloqueio ou eliminação dos dados pessoais, suspensão parcial do banco de dados, suspensão do exercício da atividade** e proibição parcial ou total de atividade. Tais sanções administrativas podem ser aplicadas **aos controladores,** sem prejuízo do disposto nos estatutos dos servidores de cada ente, na Lei Federal nº 8.429, de 2 de junho de 1992, Lei de Improbidade Administrativa, e na Lei nº 12.527, de 18 de novembro de 2011, Lei de Acesso à Informação (UNIÃO, 2021).

Resta evidente a preocupação do legislador com relação ao estabelecimento de mecanismos institucionais que asseguram transparência e participação dos interessados quanto à definição dos critérios de sancionamento. Por outro lado, interessa notar que, para além das tradicionais sanções administrativas (advertência), pecuniárias (multas) e restritivas de atividade (bloqueio ou eliminação dos dados pessoais a que se refere a infração), a lei introduz também sanção com impactos reputacionais, ao prever, no art. 52, IV, a possibilidade de "publicização da infração após devidamente apurada e confirmada a sua ocorrência" (MENDES et al., 2019).

?

Os órgãos e entidades da Administração Pública não estão sujeitos às penalidades de multa simples e multa diária de até 2% do faturamento da pessoa jurídica, limitada, no total, a R$ 50 milhões por infração.

A Autoridade Nacional de Proteção de Dados Pessoais, após procedimento administrativo que possibilite a oportunidade da ampla defesa, de forma gradativa, isolada ou cumulativa, aplicará a sanção de acordo com as peculiaridades do caso concreto e considerados os seguintes parâmetros e critérios previstos no §1º do art. 52, quais sejam:

a) a gravidade e a natureza das infrações e dos direitos pessoais afetados;
b) a boa-fé do infrator;
c) a vantagem auferida ou pretendida pelo infrator;
d) a condição econômica do infrator;
e) a reincidência;
f) o grau do dano;
g) a cooperação do infrator;
h) a adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano, voltados ao tratamento seguro e adequado de dados, em consonância com o disposto no inciso II do §2º do art. 48 da Lei;
i) a adoção de política de boas práticas e governança;
j) a pronta adoção de medidas corretivas; e,
k) a proporcionalidade entre a gravidade da falta e a intensidade da sanção.

É importante destacar que as penalidades elencadas na LGPD são aplicadas diretamente aos agentes de tratamento, que no caso da Administração Pública, referem-se aos órgãos ou às entidades, e não diretamente ao agente público autor da infração. Entretanto, conforme citado anteriormente, a Lei ressalta a possibilidade das sanções administrativas aplicáveis aos agentes públicos - quer seja pela Lei de Improbidade Administrativa, quer seja disciplinarmente pelos respectivos estatutos de cada ente.

Ademais, a Lei de Proteção de Dados Pessoais não substitui a aplicação das sanções administrativas, civis ou penais definidas na Lei nº 8.078, de 11 de setembro de 1990 (Código de Defesa do Consumidor), e em legislação específica.

Conforme já mencionado anteriormente, a LGPD prevê que o agente que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, é obrigado a repará-lo, podendo, inclusive, a reparação ser exercida coletivamente em juízo, observado o disposto na legislação pertinente, conforme destaca o art. 42. Sendo assim, o órgão ou entidade da Administração Pública pode ser, em juízo, obrigada a reparar dano patrimonial, moral, individual ou coletivo, independentemente de sanção administrativa pecuniária. Nesse caso, cumpre ressaltar o direito de regresso previsto no art. 37, § 6º da Constituição Federal, que estabelece que as pessoas jurídicas de direito público e as de direito privado prestadoras de serviços públicos responderão pelos danos que seus agentes, nessa qualidade, causarem a terceiros, assegurado o direito de regresso contra o responsável nos casos de dolo ou culpa.

Em especial, a Lei de Acesso à Informação define como conduta ilícita divulgar ou permitir a divulgação ou acessar ou permitir acesso indevido à informação pessoal. Nesses casos, conforme art. 34 da LAI, os órgãos e entidades públicas respondem diretamente pelos danos causados, cabendo a apuração de responsabilidade funcional nos casos de dolo ou culpa, assegurado o respectivo direito de regresso.

A ANPD, no caso do Poder Público, antes de aplicar as sanções de **suspensão** ou proibição, deverá ouvir os respectivos órgãos e entidades com competências sancionatórias, nos termos do art. 52, §6º, II. Além disso, tais penalidades **somente poderão ser aplicadas após já ter sido imposta ao menos uma das sanções para o mesmo caso concreto de: publicização da infração, bloqueio ou eliminação dos dados pessoais.**

Por fim, adotando mecanismos regulatórios baseados em regras de livre pactuação pelos interessados, a LGPD prevê, no caso de vazamento de dados ou acessos não autorizados, a possibilidade de conciliação entre o controlador e o titular dos dados, conforme autoriza o §7º do art. 52.

Capítulo 4 – Modelo de governança, responsabilidades e obrigações definidas pelo Decreto Estadual nº 49.265/2020

4.1 – Política Estadual de Proteção de Dados Pessoais – PEPDP

Diante das exigências nacionais de adequação dos serviços prestados, considerando o tratamento de dados pessoais, o Poder Executivo Estadual estabeleceu, através do Decreto Estadual no 49.265/2020, a Política Estadual de Proteção de Dados Pessoais (PEPDP).

Conforme art. 1º do Decreto, a PEPDP é um conjunto de princípios, diretrizes, normas e obrigações para o desenvolvimento e a adaptação da ação governamental à LGPD no âmbito da Administração Pública Estadual direta, autárquica e fundacional do Poder Executivo Estadual.

Figura 13. Logo da Política Estadual de Proteção de Dados Pessoais

Fonte: Secretaria da Controladoria-Geral do Estado (SCGE-PE)

Descrição: A imagem apresenta o logo da "LGPD Pernambuco" com um escudo com as cores de Pernambuco

A Política será implementada através do Plano Quadrienal Estratégico de Proteção de Dados Pessoais - PPDP que estabelecerá as prioridades estaduais quanto à adequação à LGPD, contribuindo para aumentar a efetividade, a integração das ações e a conformidade da ação governamental.

O Plano Quadrienal deverá trazer as ações prioritárias distribuídas em quatro anos, a fim de garantir a coerência dos órgãos e entidades do Poder Executivo Estadual. Nesse contexto, o Plano Quadrienal será elaborado pela Secretaria da Controladoria-Geral do Estado (SCGE) após ciclos de debates entre os envolvidos,

considerando propostas de adequação, as adaptações às realidades dos órgãos e entidades, assim como a gradação das medidas a depender da capacidade operativa de cada unidade.

Cumpre ressaltar que o Plano Quadrienal deve estar alinhado ao Planejamento Estratégico do Estado e deverá prever ações prioritárias concretas a serem executadas pelos órgãos e entidades da Administração Pública Estadual direta, autárquica e fundacional do Poder Executivo Estadual.

Para tanto, as ações prioritárias não devem condicionar sua execução à criação de novas despesas (custeio e pessoal) e/ou a uma estrutura orçamentária específica. Isto porque, as ações de mitigação dos riscos devem estar adequadas às condições orçamentárias, à estrutura disponível e à efetividade das políticas públicas.

Sendo assim, a Política Estadual de Proteção de Dados Pessoais deverá ser pautada a partir das seguintes diretrizes:

- Proporcionalidade de normas e procedimentos de segurança da informação;
- Controle de acesso aos sistemas e afins;
- Registro de acessos e alterações de dados;
- Acompanhamento permanente do cumprimento da Política Estadual de Segurança da Informação;
- Gestão de riscos de TIC (Tecnologia da Informação e Comunicação);
- Gestão da qualidade da segurança da informação;
- Gestão de incidentes da segurança da informação;
- Gestão de continuidade de serviços da TIC;
- Boas práticas e governança;
- Atendimento simplificado e eletrônico;
- Alinhamento com a promoção da transparência pública;
- Proporcionalidade das medidas de privacidade e segurança da informação;
- Nível de maturidade dos tratamentos dos dados;
- Manutenção da segurança jurídica dos instrumentos firmados;
- Economicidade das ações;
- Aderência ao planejamento estratégico do Estado; e,
- Aderência à Política de Tecnologia da Informação e Comunicação do Estado.

4.2 – Política de Proteção de Dados Pessoais Local – PPDPL

A Lei exige por parte do poder público a instituição de processos e políticas internas, visando a adequação dos serviços públicos à cultura de proteção de dados pessoais. Em especial, a LGPD prevê que os agentes de tratamento, no âmbito de suas competências, poderão formular regras de boas práticas e de governança que estabeleçam condições de organização, o regime de funcionamento, os procedimentos, 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.

Em especial, a LGPD prevê (art. 50, §2º) que o controlador deverá implementar programa de governança em privacidade que demonstre o seu comprometimento em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais sob seu controle. A Lei espera que o programa seja adaptado à estrutura, à escala e ao volume de suas operações, bem como à sensibilidade dos dados tratados, assim como, seja atualizado constantemente com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas.

Portanto, o programa de governança visa estabelecer o modelo de implantação, comunicação e de gerenciamento dos riscos associados à proteção de dados. Assim, todas as atividades poderão ser dirigidas, monitoradas e incentivadas, envolvendo as principais partes interessadas e promovendo a adoção das medidas mitigadoras dos riscos identificados.

O art. 6º do Decreto determina que os órgãos e as entidades da Administração Pública Estadual direta, autárquica e fundacional deverão estabelecer suas respectivas **Políticas de Proteção de Dados Pessoais Locais – PPDPL** a serem aprovadas pelo dirigente máximo e deverão estabelecer, no mínimo:

1. princípios, diretrizes e prioridades locais da proteção de dados pessoais;
2. responsabilidades e papéis pela proteção de dados pessoais;
3. processo de gerenciamento de riscos; e,
4. controles internos de proteção de dados pessoais.

Cumpre destacar que as Políticas de Proteção de Dados Pessoais Locais deverão considerar ações prioritárias do Plano Quadrienal no planejamento de suas atividades.

O Decreto Estadual no 49.265/20 pode ser acessado no seguinte link: https://legis.alepe.pe.gov.br/texto.aspx? id=51399&tipo=

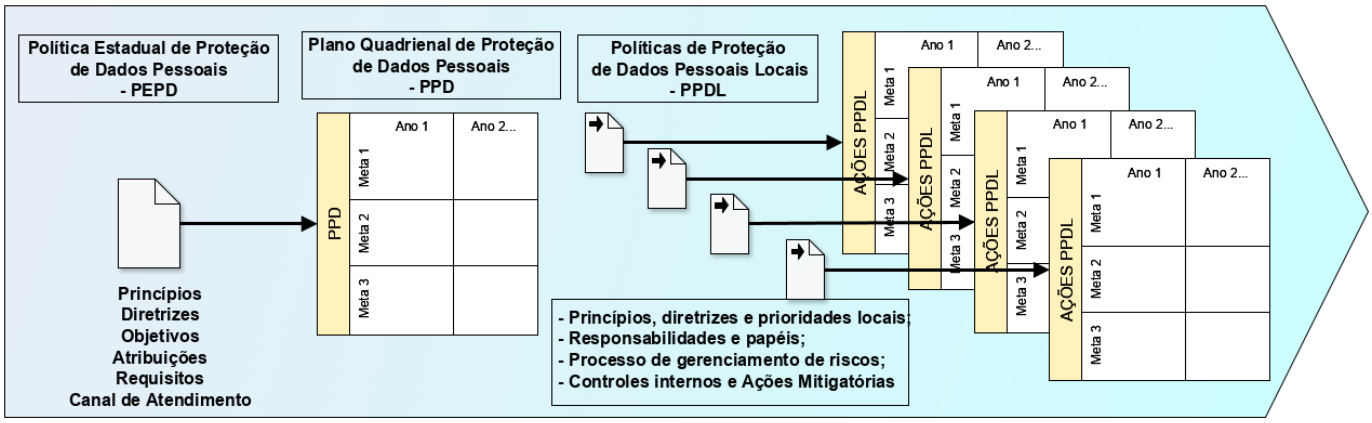

Figura 14. Processo esquematizado da Política Estadual de Proteção de Dados Pessoais.

Fonte: Secretaria da Controladoria-Geral do Estado (SCGE-PE)

Descrição: A imagem apresenta o processo esquematizado da Política Estadual de Proteção de Dados Pessoais, o Plano Quadrienal e as Políticas de Proteção de Dados Pessoais Locais.

Assim, espera-se que a entidade ou órgão com a adoção da PPDPL atenda tal exigência, esteja ciente dos processos e defina responsáveis pela governança de dados pessoais em sua estrutura e que o projeto de implementação das exigências da LGPD possa ter condições de execução.

Como orientação, encontra-se disponível o Modelo de Política de Proteção de Dados Pessoais Local no site da SCGE. Cumpre destacar que o conteúdo deve ser adaptado à realidade de cada órgão e entidade.

Como visto, a Política Local definirá o processo de gerenciamento de riscos, os controles internos de proteção de dados pessoais e as ações mitigadoras dos riscos. Portanto, apenas a partir do diagnóstico de conformidade com a Lei será possível avaliar quais medidas/correções deverão ser realizadas, inclusive, estabelecendo a priorização na sua implantação, de acordo com a maturidade e capacidade operacional de cada órgão ou entidade.

O órgão ou entidade, ao instituí-la, poderá conduzir o trabalho de adaptação dos seus processos de forma estruturada e alinhada às suas prioridades, uma vez que a proteção de dados pessoais depende do envolvimento de diversos setores, desde as áreas de negócio, como também os setores jurídicos, de tecnologia da informação e de controle interno.

O documento também atende aos princípios da transparência e de prevenção da LGPD, visto que, agora, os titulares de dados pessoais estarão cientes da forma de condução das ações de proteção de dados do órgão ou entidade e, de como a organização tem se movimentado para promover a mudança organizacional, em conformidade com o disposto no § 3º do art. 50.

4.3 – Gestão de Riscos

As organizações públicas enfrentam e enfrentarão uma série de riscos que podem afetar a continuidade dos serviços, desde a aplicabilidade de sanções administrativas, como a suspensão e a eliminação de dados pessoais, à obrigatoriedade de reparação de dano patrimonial, moral, individual ou coletivo, por conduta ilícita relacionada à proteção de dados pessoais.

Nesse contexto, o Governo de Pernambuco tem editado normativos com foco na promoção da gestão de riscos, a exemplo do Decreto Estadual nº 46.855/2018. Segundo o art. 17 do Decreto, a alta administração das organizações da administração pública estadual direta, autárquica e fundacional deverá estabelecer, manter, monitorar e aprimorar sistema de gestão de riscos e controles internos com vistas à identificação, à avaliação, ao tratamento, ao monitoramento e à análise crítica de riscos que possam impactar a implementação da estratégia e a consecução dos objetivos da organização no cumprimento da sua missão institucional.

Controle Interno

Processo conduzido pela estrutura de governança, administração e outros profissionais da entidade, e desenvolvido para proporcionar segurança razoável com respeito à realização dos objetivos relacionados a estratégia, operações, divulgação e conformidade (COSO, 2004).

Cumpre ressaltar que a LGPD está alinhada ao conteúdo de gestão de riscos, como exemplo, o art. 50 que prevê que, 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, bem como a gravidade dos riscos e dos benefícios decorrentes de tratamento de dados do titular.

Certo, mas o que é risco? E o que é gerenciamento de riscos? Usada como referência para implantação de diversos sistemas de gestão, a Organização Internacional de Normalização (ISO) produziu uma norma tratando especificamente do gerenciamento de risco, a ISO 31000:2018. No guia produzido pela entidade, na seção de "Conceitos Gerais", a ISO 31000:2018 define o gerenciamento de riscos como:

> *"processo para identificar, avaliar, administrar e controlar potenciais eventos ou situações e fornecer segurança razoável no alcance dos objetivos organizacionais. Ou seja, o gerenciamento de riscos inclui a aplicação de métodos lógicos e sistemáticos para comunicar e consultar durante todo esse processo; estabelecer o contexto para identificar, analisar, avaliar, tratar os riscos associados a qualquer atividade, processo, função ou produto; monitorar e revisar riscos; relatando e registrando os resultados adequadamente"*

Ou seja, o risco é a possibilidade de um evento ocorrer e afetar adversamente a consecução de objetivos organizacionais. No caso da LGPD, o risco está associado diretamente à desconformidade com a lei e os princípios de proteção de dados pessoais.

Dessa forma, o processo de gerenciamento de riscos ajudará a tomada de decisões com foco na proteção de dados pessoais, levando em consideração a incerteza e a possibilidade de eventos ou circunstâncias futuras (intencionais ou não) e seus efeitos na conformidade com a Lei.

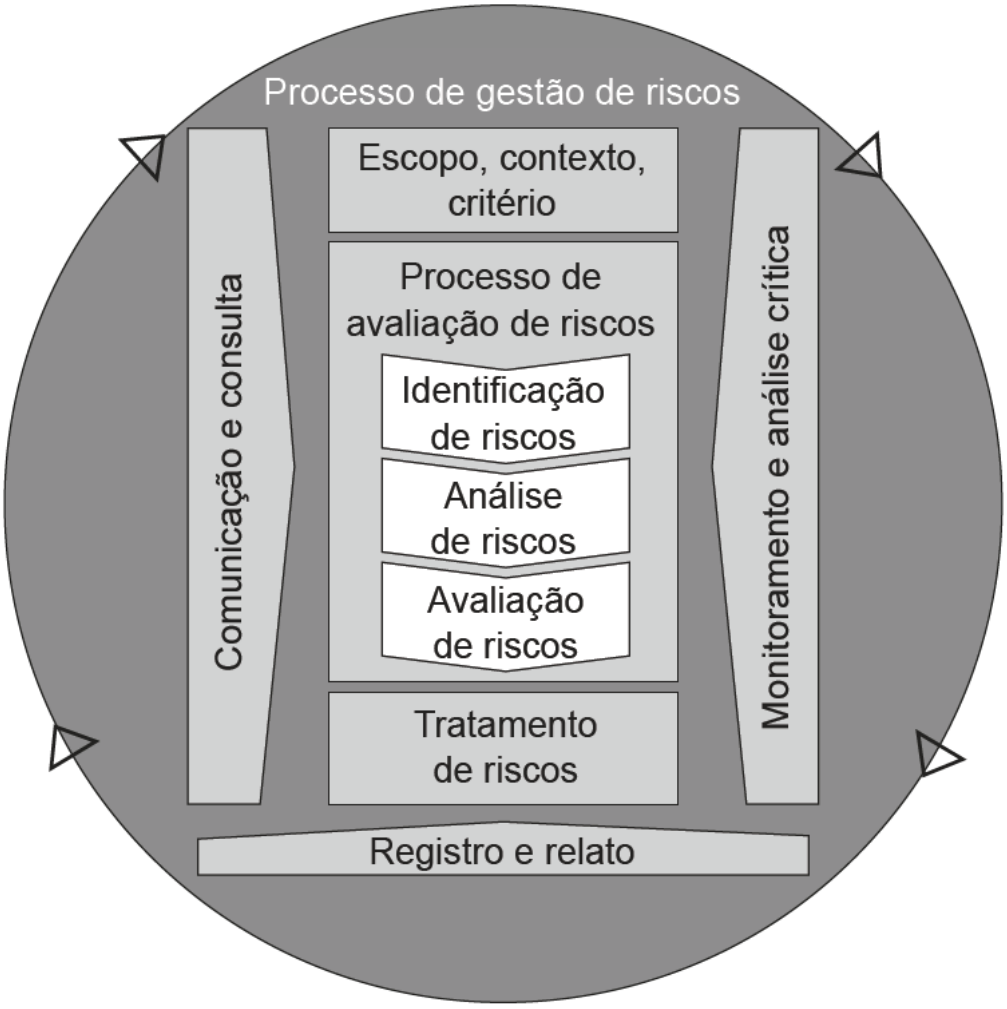

Figura 15. Processos de gestão de riscos

Fonte: ISO 31000:2018 (ISO, 2018)

Descrição: A imagem apresenta o processo de gestão de riscos, indicando todas as atividades.

Além de apresentar informações básicas, princípios e diretrizes para a implementação da gestão de riscos, a ISO 31000:2018 estabelece esquema de processos de gerenciamento de riscos que envolve a aplicação sistemática de políticas, procedimentos e práticas para as atividades de comunicação e consulta, estabelecimento do contexto e avaliação, tratamento, monitoramento, análise crítica, registro e relato de riscos (Figura 15).

A partir da identificação, análise e avaliação de riscos, o órgão ou entidade poderá proceder ao tratamento dos riscos voltados à privacidade e segurança. Sabendo que somente depois dessa avaliação, e se ainda identificada a necessidade de redução do nível do risco, podem ser propostos novos controles, observados sempre critérios de eficiência e eficácia da sua implementação.

4.4 – Governança da Política Estadual de Proteção de Dados Pessoais

A Política Estadual de Proteção de Dados Pessoais, para formulação do seu modelo de governança, considerou a estrutura atualmente vigente com o Sistema Estadual de Informática de Governo - SEIG, instituído pela Lei Estadual nº 12.985/2006. O SEIG tem por finalidade a formulação da Política de Tecnologia da Informação e Comunicação do Estado - PTIC, o planejamento, a coordenação, o controle e a execução das atividades a ele relacionadas, no âmbito da administração direta e indireta do Poder Executivo Estadual.

O SEIG prevê duas estruturas permanentes de governança que são: Comitê Executivo de Governança Digital - CEGD e Comitê Técnico de Governança Digital - CTGD. Dessa forma, toda a Política Estadual de Proteção de Dados Pessoais estará alinhada às exigências da PTIC, considerando todas as evoluções e estratégias do Governo Digital.

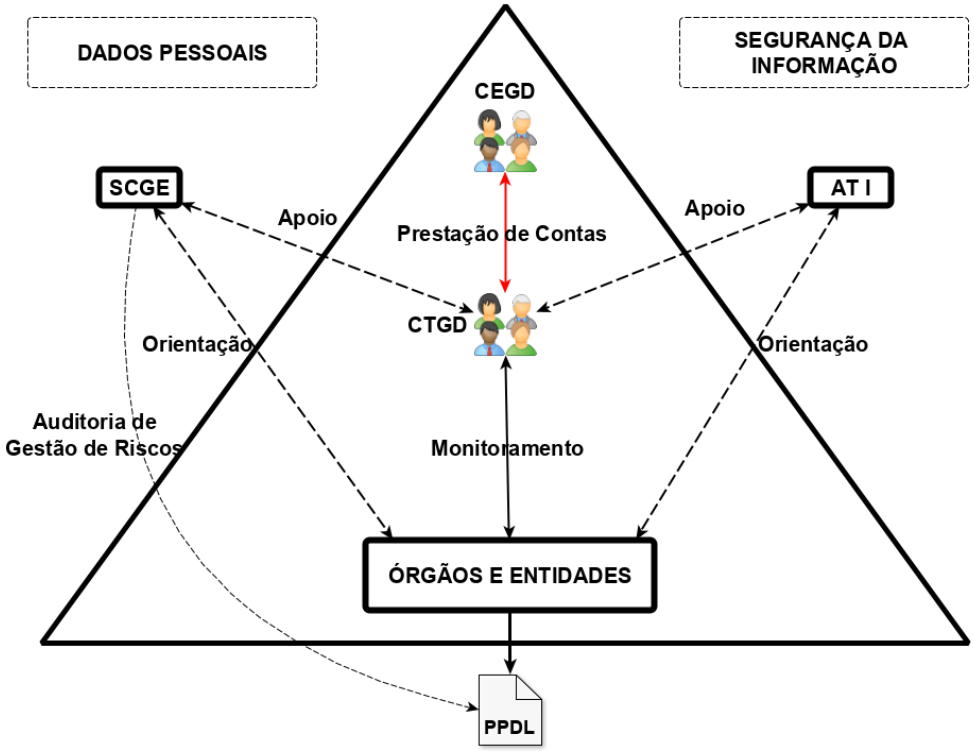

Figura 16. Estrutura de governança da Política Estadual de Proteção de Dados Pessoais

Fonte: Secretaria da Controladoria-Geral do Estado (SCGE-PE)

Descrição: A imagem apresenta o modelo de governança da PEPDP

Uma vez iniciadas as adequações necessárias dos negócios às exigências da LGPD, os órgãos e entidades da Administração Pública Estadual direta, autárquica e fundacional do Poder Executivo Estadual estarão sujeitos à seguinte estrutura de governança:

Tabela 4 - Atribuições das estruturas envolvidas na governança da Política Estadual de Proteção de Dados Pessoais

Comitê Executivo de Governança Digital - CEGD
Aprovar portaria de proteção de dados pessoais apresentada pela SCGE;
Aprovar o Plano Quadrienal;
Aprovar o parecer dos resultados da auditoria interna sobre a Política Estadual.
Comitê Técnico de Governança Digital - CTGD
Monitorar o desempenho e riscos produzidos pela Política Locais;
Assessorar a SCGE com informações que apoiem decisões e orientem ações estratégicas;
Deliberar a adoção de padrões para serviços e produtos;
Decidir sobre as questões de integração e de articulação;
Apoiar a promoção com a divulgação de ações e a criação de grupos de estudos de boas práticas;
Aprovar a padronização de cláusulas contratuais técnicas para fins de compartilhamento e tratamento.
Secretaria da Controladoria-Geral do Estado de Pernambuco - SCGE
Coordenar e orientar a rede de encarregados;
Elaborar o Plano Quadrienal;
Consolidar os resultados e apoiar o monitoramento;
Disponibilizar canal de atendimento ao titular;
Coordenar a qualidade do atendimento;
Produzir manuais, modelos de documentos e capacitações;
Auditoria interna.
Agência de Tecnologia da Informação – ATI
Orientar a aplicação de soluções de TIC relacionadas à proteção de dados pessoais;
Adequar as arquiteturas e as operações compartilhadas de TIC hospedadas no datacenter e na rede corporativa;

Propor padrões de desenvolvimento de novas soluções de TIC, desde a fase de concepção do produto e serviço até a sua execução.
Procuradoria-Geral do Estado
Disponibilizar consultoria jurídica para dirimir questões e emitir pareceres do significado e alcance LGPD;
Disponibilizar modelos de contratos, convênios e acordos de cooperação internacional aderentes à LGPD;
Disponibilizar modelo de termo de uso de sistema de informação da Administração Pública.

Cumpre destacar que o Decreto Estadual nº 49.265/2020 conferiu à Secretaria da Controladoria-Geral do Estado (SCGE) a competência para coordenar e orientar a rede de encarregados. Tal atribuição está alinhada com a estratégia da SCGE de "Contribuir para melhoria do desempenho das políticas públicas" ao promover a capacitação e a orientação dos servidores públicos estaduais quanto às normas de proteção de dados pessoais.

Apesar do monitoramento contínuo e das atividades orientativas e consultivas desempenhadas pela SCGE (proteção de dados), PGE (jurídico) e ATI (segurança da informação), haverá a necessidade de uma avaliação anual de implantação da LGPD. Nesse sentido, o CEGD assumirá um papel estratégico de deliberação sobre a adequabilidade das ações desempenhadas pelos órgãos e entidades. Ressalta-se que o Comitê Executivo terá conhecimento das ações estratégicas, das dificuldades e das fragilidades existentes no estado para subsidiar sua deliberação. Além disso, a SCGE produzirá relatório de auditoria de avaliação de gerenciamento de riscos que servirá de suporte para avaliação final da Política de cada órgão e entidade.

4.5 – O Encarregado e equipe de apoio

4.5.1 – A indicação

O encarregado é a pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador/operador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD) (art. 5º, VIII, LGPD).

Ademais, conforme inciso II do art. 12 do Decreto Estadual nº 49.265/2020, **a indicação do encarregado deverá ser feita por ato próprio do dirigente máximo. Ou seja, a designação deverá ser dada por Portaria do dirigente máximo de cada órgão ou entidade.**

Confira o Modelo de Portaria de Designação de Encarregado no site da SCGE.

4.5.2 – Das Responsabilidades

De acordo com o § 2º do art. 41 da Lei Federal nº 13.709/18, as atividades do encarregado correspondem a:

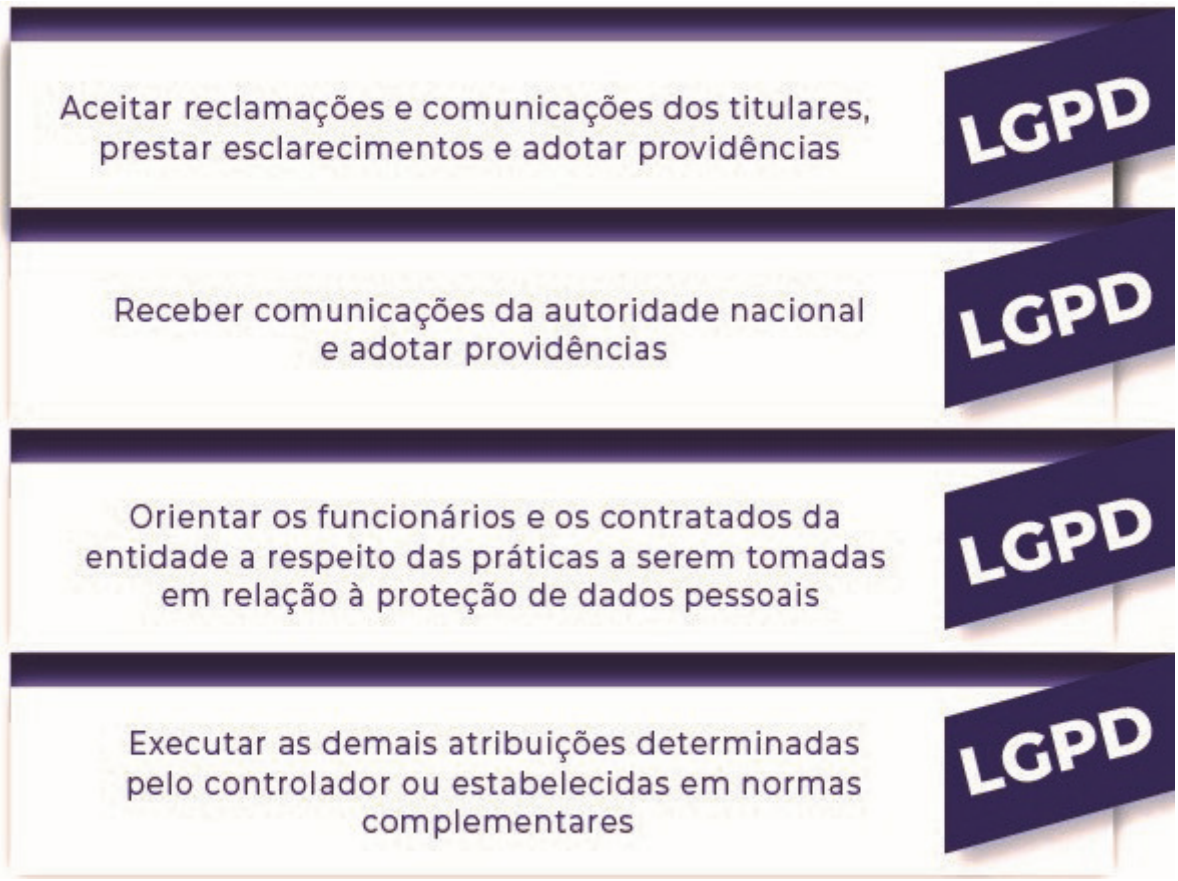

Figura 17. Atribuições do encarregado definidas pela LGPD.

?

O encarregado deve possuir dedicação exclusiva?

Diferentemente do RGPD, a LGPD não faz qualquer referência a esta questão, nem mesmo o Decreto Estadual nº 49.265/20. Entretanto, a dedicação exclusiva é considerada uma boa prática, visto que tornaria o processo de avaliação e orientação com maior grau de independência, além de haver a segregação de funções, evitando-se, assim, possíveis conflitos de interesses. Todavia, tal decisão ficará a cargo de cada órgão/entidade, segundo seu juízo de conveniência e percepção de relevância da função, considerando as atribuições do cargo, a estrutura organizacional disponível e dependerá da natureza e do volume de dados pessoais tratados.

No âmbito da Administração Pública Estadual direta, autárquica e fundacional do Poder Executivo Estadual, respaldadas em boas práticas internacionais e no modelo de governança instituído, foram adicionadas as seguintes atribuições ao encarregado na Política de Proteção de Dados Local (art. 13 do Decreto Estadual nº 49.265/2020):

Figura 18. Atribuições do encarregado no âmbito da Administração Pública direta, autárquica e fundacional do Poder Executivo Estadual, conforme Decreto Estadual nº 49.265/2020.

4.5.3 – Dos Requisitos

Conforme § 2º e § 3º do art. 12 do Decreto Estadual nº 49.265/2020, **o encarregado deve ser designado pelo controlador, representado pelo dirigente máximo do órgão ou entidade, a quem deverá estar diretamente vinculado.**

É importante ressaltar que tal condição visa dar ao encarregado independência para determinar as ações necessárias, bem como garantir o pronto apoio das

unidades subordinadas ao dirigente máximo no atendimento das demandas dos titulares de dados pessoais. Da mesma forma, tal situação visa dar amplo acesso à estrutura organizacional e à possibilidade de avaliar de maneira sistêmica a conformidade do órgão ou entidade e orientar os responsáveis pelas vulnerabilidades identificadas sem ressalvas.

4.5.4 – Do Perfil

Considerando todas as responsabilidades, é possível assumir que o encarregado no estado assumirá o papel de especialista de compliance da LGPD, realizando atividades como orientação, monitoramento e análise dos ditames legais de proteção de dados pessoais.

De acordo com MALDONADO (2021), das atribuições do encarregado previstas na lei brasileira, certamente a mais importante é "orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais" porque o objetivo da lei geral de proteção de dados é fundamentalmente esse: a proteção "dos direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural." (art. 1º).

A autora (MALDONADO, 2021) destaca que para ser capaz de orientar a respeito de práticas de proteção de dados pessoais é necessário um longo processo de formação em privacidade de dados. Essa disciplina ou área do conhecimento torna-se a essência para a correta implementação e interpretação da lei. Tal prática visa obedecer, dentre outros, o Princípio da Prevenção no tratamento de dados pessoais (inciso VIII do art. 6o da LGPD) ao evitar a materialização de incidentes no tratamento (coleta, eliminação, acesso, transmissão, armazenamento etc.) de dados pessoais. Para tanto, há um amplo espectro de conhecimentos dificilmente dominados por um profissional sem formação multidisciplinar (privacidade, segurança da informação, tecnologia, direito etc.).

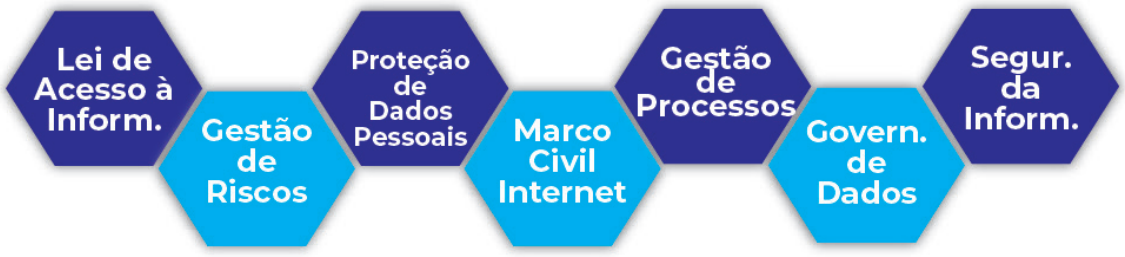

Figura 19. Áreas de conhecimento do encarregado.

Portanto, para assumir a função, o encarregado deve possuir conhecimento nos termos da LGPD, bem como demais normativos relativos à proteção de dados, Lei de Acesso à Informação (LAI), Marco Civil da Internet, noções de gestão de riscos e processos.

Quanto à segurança da informação, orienta-se que o encarregado tenha conhecimento em boas práticas produzidas pela International Organization for Standardization (ISO), em especial, as ISO 31000, 31010, 27001, 27002, 27004, 27005, 27701, 29100.

Ademais, será preciso realizar cursos de aperfeiçoamento e desenvolvimento no tema, principalmente os promovidos pela SCGE e pela Agência de Tecnologia da Informação (ATI).

Tal orientação decorre da condição prevista no § 3º do art. 12 do Decreto ao exigir ao encarregado experiência em gestão, com assessoria jurídica e tecnológica, e poderes para tratar questões que afetem os operadores.

Ressalte-se que a escolha adequada do encarregado afetará, positiva ou negativamente, toda a governança do órgão/entidade que garanta a conformidade do agente de tratamento com a LGPD e com a Política Estadual e demais normativos aplicáveis, devendo ser extremamente criteriosa.

4.5.5 – Equipe de Apoio

O art. 13. do Decreto Estadual nº 49.265/2020 prevê a existência de uma equipe de apoio com objetivo subsidiar as responsabilidades do encarregado.

Considerando as particularidades da gestão estadual, a SCGE considera fundamental a participação de, ao menos, quatro áreas de suporte:

- **Jurídica:** consultas e pareceres sobre direito digital e proteção de dados pessoais; gestão do risco jurídico; proposições normativas; adequação dos instrumentos contratuais; elaboração das políticas de privacidade e termo de uso.
- **Tecnologia da Informação:** gestão de aplicações, considerando a proteção de dados pessoais; gestão da segurança da informação; diagnósticos de vulnerabilidades; e proposições de soluções de TIC.
- **Ouvidoria:** processo de transparência e atendimento ao titular do dado pessoal.

• **Controle Interno:** técnicas e métodos de gestão de riscos; diagnósticos de vulnerabilidades; planos de adequação aos normativos; e prestação de contas.

Figura 20. Equipe de apoio de adequação à LGPD no âmbito da Administração direta, autárquica e fundacional do Poder Executivo Estadual.

Fonte: Secretaria da Controladoria-Geral do Estado (SCGE-PE).

Descrição: A imagem apresenta a relação do encarregado com a equipe de apoio.

É importante, portanto, que cada órgão e entidade da Administração Pública Estadual direta, autárquica e fundacional estabeleça a governança de proteção de dados com a instituição de suas respectivas Políticas de Proteção de Dados Pessoais Local (PPDPL), definindo, além de aspectos gerais, as atribuições de cada unidade administrativa na proteção de dados pessoais, em especial as áreas destacadas como apoio.

Bibliografia

ANPD; Perguntas Frequentes – ANPD — Português (Brasil) (www.gov.br), 2021. [Online] Acessado em 02 de maio de 2021;

ANPD; Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado, maio de 2021, Brasília/DF. [Online] Disponível em: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/outros-documentos-externos/anpd_guia_agentes_de_tratamento.pdf. Acessado em 30 de agosto de 2021;

BLUM, Renato Opice; MALDONADO, Viviane Nóbrega (Coordenadores.). Comentários ao GDPR: Regulamento Geral de Proteção de Dados da União Europeia. São Paulo: Thomson Reuters Brasil, 2018;

BLUM, Renato Opice; VAINZOF, Rony; MORAES, Henrique Fabretti (Coordenadores). Data Protection Office (Encarregado): teoria e prática de acordo com a LGPD e GDPR. São Paulo: Thomson Reuters, 2020;

CÂMARA FEDERAL; Projeto de Lei da Câmara nº 53/2018, 2018. [Online]. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/133486. Acessado em 02 de abril de 2021;

CNS – CONSELHO NACIONAL DE SAÚDE; Código de Boas Práticas: Proteção de Dados para Prestadores Privados de Saúde; [Online]. Disponível em: cnsaude.org.br/wp-content/uploads/2021/03/Boas-Praticas-Protecao-Dados-Prestadores-Privados-CNSaude_ED_2021.pdf, 2021. Acessado em 02 de maio de 2021;

COMISSÃO EUROPEIA, article 29 data protection working party, Opinion 1/2010 on the concepts of "controller" and "processor", 2010, [Online] Disponível em: MARKT-2001-05060-00-00-FR-TRA-00 (EN) (europa.eu), Acessado em 01 de abril de 2021;

COSO - Committee of Sponsoring Organizations of the Treadway Commission, "COSO Gerenciamento de Riscos Corporativos - Estrutura Integrada". 2007, Acessado: jul. 07, 2019. [Online]. Disponível em: https://www.coso.org/Documents/COSO-ERM-Executive-Summary-Portuguese.pdf;

DA MOTA ALVES, LGPD: Mais que uma lei de obrigações, uma lei de direitos – Migalhas, 2021, [Online]. Disponível em: https://www.migalhas.com.br/depeso/342256/lgpd-mais-que-uma-lei-de-obrigacoes-uma-lei-de-direitos. Acessado em 08 de maio de 2021;

DONEDA, Danilo. Da Privacidade à Proteção de Dados Pessoais: Fundamentos da Lei Geral de Proteção de Dados Pessoais. – 2.ed. – São Paulo: Thomson Reuters, 2019;

DONEDA, D. e MENDES, L. S.; Reflexões iniciais sobre a nova Lei Geral de Proteção de Dados. Revista de Direito do Consumidor, vol. 120/2018, 2018;

ICO – Information Commissioner's Office ; [Online]. Disponível em: Controllers and processors | ICO, 2021. Acessado em 02 de maio de 2021;

ICO – Information Commissioner's Office; [Online]. Disponível em: Legitimate interests | ICO,2021. Acessado em 03 de maio de 2021;

ISO – *International Organization For Standardization (ISO), "ISO 31000:2018 Risk management* — Guidelines". 2018, Acessado: jun. 11, 2020. [Online]. Disponível em: https://www.iso.org/obp/ui#iso:std:iso:31000:ed-2:v1:en;

LAPIN, Laboratório de Políticas Públicas e Internet. Controlador ou Operador: quem sou eu? – Cartilha sobre agentes de tratamento de dados pessoais, abril de 2021. [Online]. Disponível em: Controlador ou operador: quem sou eu? Cartilha sobre agentes de tratamento de dados pessoais (lapin.org.br).

LIMA, A. (04 de julho de 2020). LGPD e o relacionamento com demais leis e regulamentos de segmentos de mercado. São Paulo, Brasil;

MAIA, Fernanda (Coordenadora); LGPD: Aplicação Prática das Bases Legais – Acadêmico - Creative Commons Publicado em 19.08.2020, [Online] Disponível em: ebook.indd (bibliotecadeseguranca.com.br), 2020. Acessado em 02 de maio de 2021;

MALDONADO, V. N. (Coordenadora). LGPD: Lei Geral de Proteção de Dados Pessoais: Manual de Implementação. São Paulo: Thomson Reuters, 2019;

MALDONADO, V. N.; Encarregado, Controlador e Operador: quem é quem na LGPD?, [Online]. Disponível em: Encarregado, Controlador e Operador: quem é quem na LGPD? (nextlawacademy.com.br), 2021. Acessado em 02 de maio de 2021;

MENDES, L.S., DONEDA, D., SARLET, I.W., RODRIGUES JR., O.L., BIONI, B. (Coordenadores); Tratado de Proteção de Dados Pessoais – Rio de Janeiro, Forense, 2021;

PGE – PROCURADORIA GERAL DO ESTADO DE PERNAMBUCO, Parecer PGE nº 492/2020 (SAJ 2020.02.4099), 2020;

UNIÃO, Guia de Boas Práticas: Lei Geral de Proteção de Dados (LGPD), 2020. [Online]. Disponível em: GuiaLGPD.pdf (www.gov.br). Acessado em 01 de abril de 2021;

UNIÃO, Guia de elaboração de Termo de Uso e Política de Privacidade para serviços públicos, 2020. [Online]. Disponível em: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_tupp.pdf . Acessado em 01 de abril de 2021;

VAINZOF, R.; Dados pessoais, tratamento e princípios. In: BLUM, Renato Opice; MALDONADO, Viviane Nóbrega (Coordenadores.). Comentários ao GDPR: Regulamento Geral de Proteção de Dados da União Europeia. São Paulo: Thomson Reuters Brasil, 2018, p.37/83.