2023

MANUAL

Aplicabilidade da Lei Geral de Proteção de Dados, no Âmbito da Administração Pública

PROCURADORIA-GERAL DO ESTADO DE ALAGOAS
CENTRO DE ESTUDOS

PGE

Apresentação

Em 14 de agosto de 2018, foi publicada a Lei Federal n. 13.709, que dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Vale destacar que, considerando as grandes inovações trazidas pelo marco regulatório de proteção de dados pessoais e, consequentemente, a necessidade de adequação das sociedades empresárias e demais instituições, estabeleceu-se uma vigência gradativa, de tal sorte que a aplicabilidade integral do referido diploma normativo apenas ocorreu em 01 de agosto de 2021, quando se tornou possível a incidência das sanções administrativas previstas nos artigos 52 a 54.

O Estado, na posição de principal agente de tratamento, curva-se aos procedimentos e diretrizes necessários ao resguardo do direito fundamental à proteção de dados pessoais[12]. Assim, não poderá agir em desarmonia com o sistema normativo, de modo a desvirtuar a finalidade para a qual os dados são utilizados, nem, tampouco, poderá ficar alheio aos mecanismos de segurança informacional.

Assim, surge para a Administração Pública estadual o dever de orientar os seus agentes, com o fito de possibilitar o regular exercício de suas competências legais, em compasso com as novas diretrizes de proteção de dados alinhavadas na legislação de regência.

Nesse cenário, a Procuradoria-Geral do Estado de Alagoas (PGE), enquanto instituição responsável pela tutela da ordem jurídica, elaborou esta cartilha com o objetivo de fornecer orientações de boas práticas e de governança aos órgãos e entidades da Administração Pública direta e indireta do Estado de Alagoas, no tocante ao tratamento de dados pessoais, em consonância, precipuamente, com os artigos 23 a 30 e 50 da Lei Geral de Proteção de Dados - LGPD.

---

1. Sobre análise da proteção de dados pessoais para além da privacidade, são válidas as considerações tecidas por Danilo Doneda: “A proteção de dados pessoais, em suma, propõe o tema da privacidade, porém, modifica seus elementos; aprofunda seus postulados e toca nos pontos centrais dos interesses em questão.” (DONEDA, Danilo. Da privacidade à proteção de dados pessoais. 3ª ed. São Paulo: Thomson Reuters Brasil, 2021, p. 178.)
2. Através da Emenda Constitucional nº 115, de 2022, foi incluído, no art. 5º da Constituição Federal, o inciso LXXIX, cujos termos dispõe sobre o direito fundamental à proteção de dados pessoais: “art. 5º. LXXIX - é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais.”

PAULO SURUAGY DO AMARAL DANTAS
Governador

SAMYA SURUAGY DO AMARAL BARROS PACHECO
Procuradora-Geral do Estado de Alagoas

LUÍS MANOEL BORGES DO VALE
Procurador do Estado
Coordenador do Centro de Estudos

Sumário

INTRODUÇÃO **5**

1. DAS DISPOSIÇÕES PRELIMINARES **9**

1.1. Fundamentos (Art. 2º) 9

1.2. Aplicabilidade (Art. 3º) 12

1.3. Não Aplicabilidade (Art. 4º) 14

1.4. Conceitos Específicos (Art. 5º) 16

1.5. Princípios (Art. 6º) 20

2. DO TRATAMENTO DE DADOS PESSOAIS **23**

2.1. Hipóteses autorizadoras dotratamento de dados pessoais 23

2.1.1. Hipótese I - mediante o fornecimento de consentimento pelo titular 24
2.1.2. Hipótese 2 - para o cumprimento de obrigação legal ou regulatória pelo controlador 25
2.1.3. Hipótese 3 - 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 27
2.1.4. Hipótese 4 - estudos por órgão de pesquisa 28
2.1.5. Hipótese 5 - 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 29
2.1.6. Hipótese 6 - para o exercício regular de direitos em processo judicial, administrativo ou arbitral (lei nº 9.307/1996 - lei de arbitragem) 30
2.1.7. Hipótese 7– para a proteção da vida ou da incolumidade física do titular ou de terceiro 30
2.1.8. Hipótese 8 - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária 31
2.1.9. Hipótese 9 – 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 31
2.1.10. Hipótese 10 - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente 32

2.2. Do tratamento de dados pessoais sensíveis 33

2.2.1. Hipótese 1 - quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas 35
2.2.2. Hipótese 2 - para cumprimento de obrigação legal ou regulatória pelo controlador 35

2.2.3. Hipótese 3 - para tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos 35
2.2.4. Hipótese 4 - para realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis 36
2.2.5. Hipótese 5 - para o exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral (lei nº 9.307/1996 - lei de arbitragem) 36
2.2.6. Hipótese 6 - para a proteção da vida ou da incolumidade física do titular ou de terceiro 36
2.2.7. Hipótese 7 - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária..... 36
2.2.8. Hipótese 8 - para a garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º da Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais 36

2.3. Do Tratamento de Dados Pessoais de Crianças e de Adolescentes 38

2.4. Do Término do Tratamento de Dados (Arts. 15 e 16)..... 39

3. DOS DIREITOS DO TITULAR..... 41

3.1. Noções Gerais 41

3.2. Dos direitos específicos 42

3.2.1. Direito à confirmação da existência de tratamento 42
3.2.2. Direito de acesso aos dados 43
3.2.3. Direito de correção de dados incompletos, inexatos ou desatualizados 44
3.2.4. Direito de anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto na LGPD 44
3.2.5. Direito de portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial 45
3.2.6. Direito à eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 da LGPD 46
3.2.7. Direito à informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados 46
3.2.8. Direito à informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa 47
3.2.9. Direito à revogação do consentimento..... 47

4. DO TRATAMENTO DE DADOS PESSOAIS PELO PODER PÚBLICO .49

4.1. Noções gerais 49

4.2. Dos serviços notariais e de registro exercidos em caráter privado, por delegação do Poder Público..... 50

4.3. Das empresas públicas e sociedades de economia mista 51

4.4. Do formato interoperável e estruturado para o uso compartilhado de dados pessoais pelo Poder Público..... 51

4.5. Da fiscalização e responsabilidade 53

5. DOS AGENTES DE TRATAMENTO DE DADOS PESSOAIS 54
5.1. Do controlador e do operador 54
5.1.1. Da Responsabilidade 55
5.2. Do encarregado 56

6. DA SEGURANÇA E DAS BOAS PRÁTICAS 58
6.1. Das medidas de segurança e padrões técnicos 58
6.2. Da garantia da segurança da informação e comunicação em caso de acidentes 59
6.3. Das boas práticas e da governança 60

7. DA FISCALIZAÇÃO E SANÇÕES ADMINISTRATIVAS 62
7.1. Noções gerais 62
7.2. Das sanções aplicadas à Administração Pública 63
7.3. Da conciliação extrajudicial 64

8. DO GUIA ORIENTATIVO DA ANPD SOBRE TRATAMENTO DE DADOS PESSOAIS PELO PODER PÚBLICO 65

REFERÊNCIAS BIBLIOGRÁFICAS 67

ANEXOS 69
ANEXO I– Proposta de programa de governança em privacidade 70
ANEXO II – Modelo de termo aditivo para inclusão de regra de proteção de dados pessoais 71
ANEXO III – Modelo de termo de compromisso de confidencialidade de informações e proteção de dados pessoais e sensíveis 77
ANEXO IV – Modelo de relatório de impacto à proteção de dados pessoais - RIPD 79

Introdução

Que veleje nesse informar
Que aproveite a vazante da infomaré
Que leve um oriki do meu velho orixá
Ao porto de um disquete de um micro em Taipé
Gilberto Gil

A Lei Federal n. 13.709 (LGPD), de 14 de agosto de 2018, é considerada o marco regulatório do Brasil para a proteção de dados pessoais, inclusive em meios digitais, de pessoa natural identificada ou identificável, em consonância com direitos fundamentais da personalidade, tais como a honra, a imagem, a privacidade e a identidade, ínsitos no art. 5º da CF/1988, além de estabelecer inovadoras sanções administrativas, em caso de descumprimento de suas determinações.

Desde o final do século XX, em decorrência do avanço tecnológico e, consequentemente, do aumento do fluxo de informações, vive-se a Era Digital ou do *Big Data*[1]. Os dados pessoais deixaram de ser mero insumo para se transformarem na *commodity* mais valorizada do atual contexto, sendo até chamados de "novo petróleo".[2]

Observou-se, com isso, a necessidade de se criarem mecanismos de controle do tratamento dos dados pessoais, pois, ao passo que as informações eram disseminadas de forma mais rápida e em maior volume, na mesma proporção surgiam inúmeros escândalos de vazamentos de dados.

Nesse cenário, diante dos graves riscos à violação de direitos fundamentais da personalidade, vários países buscaram a edição de leis e regulamentos

1."*Big data* é um termo recente e por isso não existente na maior parte de dicionários de estatística. São dados multivariados e de elevada dimensão, geralmente criados em tempo real e apresentam um crescimento exponencial (na escala temporal), nomeados de megadados. Quanto mais dados são gerados, maior é o esforço para extrair informações, e os centros de dados tiveram que aprender a lidar com o crescimento exponencial de dados gerados e tiveram que desenvolver ferramentas que fossem para além de bancos de dados relacionais e sistemas paralelos de bancos de dados. Sendo assim, a velocidade para obter a informação faz parte do sucesso que o big data pode proporcionar em sua empresa. (...) ". Disponível em: < https://pt.wikipedia.org/wiki/Big_data> Acesso em: 20 de setembro de 2021.

2.Disponível em: https://www.seudinheiro.com/2018/br-malls/os-dados-sao-o-novo-petroleo-do--mundo-dos-negocios/>Acesso em: 07 de outubro de 2021.

que protegessem os dados pessoais de seus cidadãos, principalmente aqueles constantes de bancos de dados públicos ou privados.

Além disso, é preciso sublinhar que, no âmbito do Poder Público, a operacionalização correta de dados pessoais é algo que pode engendrar transformações coletivas de significativa envergadura, através da implementação de políticas públicas personalizadas, as quais estejam em compasso com a realidade fática subjacente. Nesse sentido, cumpre destacar o teor do art. 24, da Lei 14.129, de 29 de março de 2021 (Governo Digital):

> Art. 24. Os órgãos e as entidades responsáveis pela prestação digital de serviços públicos deverão, no âmbito de suas competências:
> (...)
> VII - **realizar a gestão das suas políticas públicas com base em dados e em evidências por meio da aplicação de inteligência de dados em plataforma digital;** (Grifos nossos)

No contexto internacional, destaca-se a atuação da União Europeia que, no art. 8º da Carta de Direitos Fundamentais, promulgada no ano de 2000, reconhece a existência do direito fundamental à proteção de dados pessoais. Embora já tivesse editado várias leis esparsas sobre o tema, o bloco europeu aprovou o Regulamento Geral de Proteção de Dados - Regulamento 2016/679 (GDPR), o qual entrou em vigor 25 de maio de 2018, prevendo, inclusive, punições severas a sociedades empresárias e pessoas físicas que realizem operações de tratamento de dados pessoais em dissonância com o arcabouço legal.

Com a promulgação da GDPR, o Brasil tratou como prioridade a edição de uma lei específica, mormente em razão do receio de gerar possíveis bloqueios das operações comerciais, em decorrência da não observância de normas sobre a proteção de dados pessoais. Além disso, a mudança das relações intersubjetivas, em uma sociedade digitalizada, exigiu a tutela desse novo direito fundamental, cuja autonomização se fez imprescindível.

Por oportuno, vale destacar que, antes da edição da LGPD, já existiam no ordenamento jurídico pátrio alguns enunciados normativos que garantiam, de alguma forma, a proteção aos dados pessoais, tais como o art. 5º, X e LXXII, da CF/1988, o Código de Defesa do Consumidor (Art. 43 do Lei n. 8.078/1990), o Código Civil (Arts. 11, 12, 16, 17 e 21 da Lei n. 10.406/2002), a Lei do Habeas Data (Art. 7º da Lei n. 9.507/1997), o art. 313-A do Código Penal (Crime de inserção de dados falsos em sistemas de informações da administração pública), a Lei do Cadastro Positivo (Art. 5º da Lei 12.414/2011), a Lei de Acesso à informação (Art. 4º da Lei n. 12.527/ 2011 - LAI), Marco Civil da Internet (Lei n. 12.965/2014), entre outros, contudo, nenhum diploma normativo havia sistematizado a matéria, de modo a detalhar aspectos conceituais, procedimentais e punitivos.

Assim, a edição da LGPD representou um verdadeiro marco para a efetiva implementação de um regime jurídico que desse conta da tutela dos dados pessoais, nas mais variadas esferas de tratamento, impondo, por conseguinte, deveres imprescindíveis aos agentes públicos e privados.

É preciso pontuar que, após a consolidação da LGPD, no julgamento da Ação Direta de Inconstitucionalidade 6.387, Rel. Min. Rosa Weber, o Supremo Tribunal Federal reconheceu a existência de um direito fundamental autônomo à proteção de dados pessoais e à autodeterminação informacional. Essa linha foi endossada com a publicação da Emenda Constitucional 115, de 10 de fevereiro de 2022, que positivou esse direito fundamental no art. 5º, inciso LXXIX, da Constituição Federal.

Com vistas a promover a real concretização à proteção de dados pessoais, a cada dia que passa, constata-se que a LGPD se fortalece, inclusive com o adequado aparelhamento da Autoridade Nacional de Proteção de Dados – ANPD, entidade da administração pública federal responsável por zelar, implementar e fiscalizar o cumprimento da LGPD em todo o território nacional, nos termos do Decreto Federal n. 10.474/2020 (alterações empreendidas pelo Decreto nº 10.975, de 22 de fevereiro de 2022, e, posteriormente, pelo Decreto nº 11.202, de 21 de setembro de 2022.)

Nesse sentido, é relevante grafar que, em junho de 2023, a Autoridade Nacional de Proteção de Dados (ANPD) lançou a versão 2.0 do Guia Orientativo sobre Tratamento de Dados Pessoais pelo Poder Público, a fim de auxiliar entidades e órgãos públicos nas atividades de adequação e de implementação da LGPD.

Ante o exposto, a fim de primar pela densificação da segurança jurídica, é que a Procuradoria do Estado de Alagoas (PGE/AL) elaborou esta cartilha, para orientar os órgãos e entidades da Administração Pública quanto à adequada aplicação da Lei Geral de Proteção de Dados – LGPD. O documento está dividido em 8 (oito) capítulos, os quais estão estruturados da seguinte forma:

Capítulo 1 – Das Disposições Preliminares
Capítulo 2 – Do Tratamento de Dados Pessoais
Capítulo 3 – Dos Direitos do Titular
Capítulo 4 – Do Tratamento de Dados Pessoais pelo Poder Público
Capítulo 5 – Dos Agentes de Tratamento de Dados Pessoais
Capítulo 6 – Da Segurança e Boas Práticas
Capítulo 7 – Da Fiscalização e Sanções Administrativas
Capítulo 8 – Do Guia Orientativo sobre Tratamento de Dados Pessoais Pelo Poder Público da ANPD

e, por fim, alguns anexos:

ANEXO I – Proposta de programa de governança em privacidade;
ANEXO II – Modelo de termo aditivo para inclusão de regra de proteção de dados pessoais
ANEXO III – Modelo de termo de compromisso de confidencialidade de informações e proteção de dados pessoais e sensíveis
ANEXO IV – Modelo de relatório de impacto à proteção de dados pessoais – RIPD.

PAULO SURUAGY DO AMARAL DANTAS
Governador

SAMYA SURUAGY DO AMARAL BARROS PACHECO
Procuradora-Geral do Estado de Alagoas

LUÍS MANOEL BORGES DO VALE
Procurador do Estado
Coordenador do Centro de Estudos

1. Das Disposições Preliminares

1.1. Fundamentos (Art. 2º)

Primeiramente, é preciso elucidar que os objetivos da LGPD não se confundem com os seus fundamentos. Nesse sentido, pronuncia-se Celso Ribeiro Bastos[1]: "a ideia de objetivos não pode ser confundida com a de fundamentos, muito embora, algumas vezes, isto possa ocorrer. Os fundamentos são inerentes ao Estado, fazem parte de sua estrutura. Quanto aos objetivos, estes consistem em algo exterior que deve ser perseguido".

Assim, resta claro que os objetivos são os propósitos da lei, aquilo que se pretende alcançar. Por outro lado, os fundamentos são as fontes em que se baseiam os objetivos.

O artigo 1º traz expressamente o objetivo da LGPD, qual seja: a proteção de dados pessoais de pessoa natural identificada ou identificável, seja em meio físico ou digital. Já o artigo 2º traz explicitamente os 7 (sete) fundamentos da Lei. São eles: I - o respeito à privacidade; II - a autodeterminação informativa; III - a liberdade de expressão, de informação, de comunicação e de opinião; IV - a inviolabilidade da intimidade, da honra e da imagem; V - o desenvolvimento econômico e tecnológico e a inovação; VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

A seguir, serão detalhados os fundamentos da LGPD, em consonância com a Constituição Federal de 1988, legislação infraconstitucional, doutrina e jurisprudência:

I - o respeito à privacidade;	A privacidade é uma garantia fundamental, prevista no art. 5º, X e XII, da CF/88[2], bem como está amparada pelo art. 21 do CC/02[3]. Sobre os seus contornos conceituais,

1.BASTOS, Celso Ribeiro. Curso de Direito Constitucional. 20ª edição atualizada. São Paulo: Saraiva, 1999. pp. 159-160.

2.Art. 5º, CF/88 (...) X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação; (...) XII - é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal;

3.Art. 21, CC/02 A vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado,

I - o respeito à privacidade;	manifesta-se Danilo Doneda[4]:"A moderna doutrina do direito à privacidade, cujo início podemos considerar como sendo o célebre artigo de Brandeis e Warren, *The right to privacy*, apresenta uma clara linha evolutiva. Em seus primórdios, marcada por um individualismo exacerbado e até mesmo egoísta, portava a feição do direito a ser deixado só. A esse período remonta o paradigma da privacidade como uma *zero-relationship*, pelo qual representaria, no limite, a ausência de comunicação entre uma pessoa e as demais. Essa concepção foi o marco inicial posteriormente temperado por uma crescente consciência de que a privacidade seria um aspecto fundamental da realização da pessoa e do desenvolvimento da sua personalidade." Ademais, em 07/05/2020, na ADI nº 6387, de relatoria da Ministra Rosa Weber, o Tribunal Pleno proferiu decisão com fundamento no princípio em comento, entre outros.[5]

adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma.

4. DONEDA, Danilo. Da privacidade à proteção de dados pessoais. 3ª ed. São Paulo: Thomson Reuters Brasil, 2021, p. 30.

5. EMENTA MEDIDA CAUTELAR EM AÇÃO DIRETA DE INCONSTITUCIONALIDADE. REFERENDO. MEDIDA PROVISÓRIA Nº 954/2020. EMERGÊNCIA DE SAÚDE PÚBLICA DE IMPORTÂNCIA INTERNACIONAL DECORRENTE DO NOVO CORONAVÍRUS (COVID-19). COMPARTILHAMENTO DE DADOS DOS USUÁRIOS DO SERVIÇO TELEFÔNICO FIXO COMUTADO E DO SERVIÇO MÓVEL PESSOAL, PELAS EMPRESAS PRESTADORAS, COM O INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA. FUMUS BONI JURIS. PERICULUM IN MORA. DEFERIMENTO. 1. **Decorrências dos direitos da personalidade, o respeito à privacidade e à autodeterminação informativa foram positivados, no art. 2º, I e II, da Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais), como fundamentos específicos da disciplina da proteção de dados pessoais. 2. Na medida em que relacionados à identificação – efetiva ou potencial – de pessoa natural, o tratamento e a manipulação de dados pessoais hão de observar os limites delineados pelo âmbito de proteção das cláusulas constitucionais assecuratórias da liberdade individual (art. 5º, caput), da privacidade e do livre desenvolvimento da personalidade (art. 5º, X e XII), sob pena de lesão a esses direitos. O compartilhamento, com ente público, de dados pessoais custodiados por concessionária de serviço público há de assegurar mecanismos de proteção e segurança desses dados.** 3. O Regulamento Sanitário Internacional (RSI 2005) adotado no âmbito da Organização Mundial de Saúde exige, quando essencial o tratamento de dados pessoais para a avaliação e o manejo de um risco para a saúde pública, a garantia de que os dados pessoais manipulados sejam "adequados, relevantes e não excessivos em relação a esse propósito" e "conservados apenas pelo tempo necessário." (artigo 45, § 2º, alíneas "b" e "d"). 4. Consideradas a necessidade, a adequação e a proporcionalidade da medida, não emerge da Medida Provisória nº 954/2020, nos moldes em que editada, interesse público legítimo no compartilhamento dos dados pessoais dos usuários dos serviços de telefonia. 5. Ao não definir apropriadamente como e para que serão utilizados os dados coletados, a MP nº 954/2020 desatende a garantia do devido processo legal (art. 5º, LIV, da CF), na dimensão substantiva, por não oferecer condições de avaliação quanto à sua adequação e necessidade, assim entendidas como a compatibilidade do tratamento com as finalidades informadas e sua limitação ao mínimo necessário para alcançar suas finalidades. 6. Ao não apresentar mecanismo técnico ou administrativo apto a proteger, de acessos não autorizados, vazamentos acidentais ou utilização indevida, seja na transmissão, seja no tratamento, o sigilo, a higidez e, quando o caso, o anonimato dos dados pessoais compartilhados, a MP nº 954/2020 descumpre as exigências que exsurgem do texto constitucional no tocante à efetiva proteção dos direitos fundamentais dos brasileiros. 7. Mostra-se excessiva a conservação de dados pessoais coletados, pelo ente público, por trinta dias após a decretação do fim da situação de emergência de saúde pública, tempo manifestamente excedente ao estritamente necessário para o atendimento da sua finalidade declarada. 8. Agrava a ausência de garantias de tratamento adequado e seguro dos

II - a autodeterminação informativa;	Trata-se do indivíduo saber com exatidão quais dos seus dados pessoais estão sendo coletados e a sua finalidade, a fim de decidir se autoriza fornecê-los. A efetividade desse fundamento veio no Capítulo III da LGPD, que dispõe sobre os direitos dos titulares. O precedente do STF citado no item anterior também é aplicado a este fundamento.
III - a liberdade de expressão, de informação, de comunicação e de opinião;	A livre manifestação do pensamento, sendo vedado o anonimato, bem como a livre expressão da atividade intelectual, artística, científica e de comunicação, independente de censura ou de licença, são alçadas como garantias fundamentais e estão previstas no art. 5º, IV e IX, da CF/88.
IV - a inviolabilidade da intimidade, da honra e da imagem;	Direitos fundamentais previstos no art. 5º, X, da CF/88.
V - o desenvolvimento econômico e tecnológico e a inovação;	Fundamentos que dialogam com o progresso da sociedade e estão previstos nos artigos 218 e 219 da CF/88. 'Nesse sentido, Viviane Nóbrega Maldonado e outros se manifestaram.[6]
VI - a livre iniciativa, a livre concorrência e a defesa do consumidor;	São princípios gerais da ordem econômica, nos termos do art. 1º e 170 da CF/88, que devem coabitar de forma equilibrada, a fim de possibilitar o desenvolvimento do país.
VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.	Traz de forma robusta a preservação da dignidade da pessoa humana, pois, ao proteger os dados pessoais do titular, de cunho íntimo, estará tutelando também a sua personalidade e, consequentemente, o exercício da sua cidadania.

dados compartilhados a circunstância de que, embora aprovada, ainda não vigora a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018), definidora dos critérios para a responsabilização dos agentes por eventuais danos ocorridos em virtude do tratamento de dados pessoais. O fragilizado ambiente protetivo impõe cuidadoso escrutínio sobre medidas como a implementada na MP nº 954/2020. 9. **O cenário de urgência decorrente da crise sanitária deflagrada pela pandemia global da COVID-19 e a necessidade de formulação de políticas públicas que demandam dados específicos para o desenho dos diversos quadros de enfrentamento não podem ser invocadas como pretextos para justificar investidas visando ao enfraquecimento de direitos e atropelo de garantias fundamentais consagradas na Constituição.** 10. Fumus boni juris e periculum in mora demonstrados. Deferimento da medida cautelar para suspender a eficácia da Medida Provisória nº 954/2020, a fim de prevenir danos irreparáveis à intimidade e ao sigilo da vida privada de mais de uma centena de milhão de usuários dos serviços de telefonia fixa e móvel. 11. Medida cautelar referendada.*(grifos nossos)*

6. "Ainda, ao dissertar sobre a moderna economia baseada em dados, o STND deixa claro ser elemento estratégico para o crescimento do País aproveitar as oportunidades advindas da crescente disponibilidade e do grande volume de dados, provendo: a criação de forte ecossistema para desenvolvimento de infraestrutura de telecomunicações e à atração de data centers ao País; capacidades técnicas e humanas relativas ao uso e tratamento de grandes volumes de dados; e um ambiente jurídico-regulatório que estimule investimentos e inovação, a fim de conferir segurança aos dados tratados e adequada proteção aos dados pessoais." (MALDONADO, Viviane; BLUM, Renato, coordenadores. Lei Geral de Proteção de Dados Comentada. São Paulo: Thomson Reuters, 2019. p.38.)

1.2. Aplicabilidade (Art. 3º)

De início, o art. 3º elenca as hipóteses de incidência da LGPD, destacando que o diploma normativo se aplica 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".

O sujeito tutelado pela LGPD é a pessoa natural identificada ou identificável. Consideram-se, portanto, também aqueles dados que possam de alguma forma ser vinculados a uma pessoa, tal como o endereço IP[7] do computador.

Ademais, não estão tuteladas as operações de tratamento de dados relativas à Pessoa Jurídica, até porque os dados protegidos são os pessoais, aqueles que são ínsitos à Pessoa Humana, os quais podem acarretar lesão aos direitos da personalidade, como a privacidade, honra e a imagem, considerados como prerrogativas fundamentais dos cidadãos e garantidos pela Constituição Federal, com o status de cláusula pétrea.

De maneira diversa, a legislação de proteção de dados uruguaia também tutela as pessoas jurídicas, nos moldes do que dispõe o art. 2º, da Lei 18.331/08: "Ambito subjetivo.- El derecho a la protección de los datos personales se aplicará por extensión a las personas jurídicas, en cuanto corresponda."

Embora o fluxo de informações tenha se intensificado na "Era Digital", momento em que surgiram vários escândalos de vazamentos de informações, como o caso da sociedade empresária britânica *Cambridge Analytica*, que obteve acesso a dados de usuários do *Facebook*[8], a LGPD veicula, tanto no artigo 1º ("inclusive em meios digitais"), quanto no artigo 3º ("independente do meio"), expressões que albergam a aplicação material da lei no tratamento de dados realizado em meio físico ou digital.

Assim, o campo de aplicação material da LGPD se tornou bastante amplo, quando comparado com o do Marco Civil da Internet (art. 3º), o qual apenas

7."O IP (ou Internet Protocol) é uma identificação única para cada computador conectado a uma rede. Podemos imaginá-lo como um documento de identificação único, como o CPF, por exemplo." BRITO, Edivaldo. O que é o IP? Descubra para que serve e qual é seu número. Disponível em: <https://www.techtudo.com.br/artigos/noticia/2013/05/o-que-e-o-ip-descubra-para-o-que-serve-e-qual-e-seu-numero.html)>Acesso em: 15 de setembro de 2021.

8."O escândalo da Cambridge Analytica, organização de consultoria política britânica, em 2018, foi um dos casos mais emblemáticos da utilização indevida de dados pessoais por entidades privadas. A empresa foi acusada de obter informações de usuários do Facebook, mesmo tendo sido declarado, anteriormente, pelo aplicativo, que informações sobre os perfis não seriam compartilhadas com terceiros. Tais dados foram utilizados, entre outras circunstâncias, na campanha de Donald Trump à presidência dos Estados Unidos em 2016. Inicialmente, a agência governamental norte-americana Federal Trade Commission (FTC) divulgou que o número de perfis, cujos dados teriam sido coletados e compartilhados, era de 50 a 65 milhões, contagem elevada, posteriormente, para 85 milhões de usuários". SATIRA, Roberta. O maior escândalo de "vazamento" de dados, o caso Facebook - Cambridge Analytica, e a importância da Lei Geral de Proteção de Dados Pessoais (LGPD) no Brasil. Disponível em: <https://pt.wikipedia.org/wiki/Cambridge_Analytica> Acesso em: 21 de setembro de 2021.

se restringe à proteção de dados no ciberespaço. A Lei Geral de Proteção de Dados, por seu turno, compreende informações pessoais constantes inclusive em bibliotecas físicas ou virtuais, tratados de forma *on line* ou *offline*, constantes em livros, memórias de computador e etc.

No tocante ao sujeito passivo da lei, quando se trata de pessoa física ou natural, considera-se apenas aquela que realiza o tratamento de dados para fins econômicos, consoante dispõe o art. 4º, I, da LGPD: "Art. 4º Esta Lei não se aplica ao tratamento de dados pessoais: I - realizado por pessoa natural para fins exclusivamente particulares e não econômicos;"

Além disso, no caso das pessoas jurídicas, a aplicação é ampla, de modo a incluir as de direito público, seja interno (União, Estados, Distrito Federal e Municípios, autarquias e as demais entidades de caráter público criadas por lei) ou externo (Estados estrangeiros e todas as pessoas que forem regidas pelo direito internacional público), e as de direito privado, como associações, partidos políticos, sociedades, fundações e entidades religiosas, nos termos dos artigos 40, 41, 42 e 44 do Código Civil.

Por fim, no contexto da abrangência territorial, a LGPD, no seu artigo 3º, traz 3 (três) hipóteses de aplicação, que são independentes entre si, bastando a incidência de uma delas para que o diploma normativo projete seus regulares efeitos: a) a operação de tratamento seja realizada no território nacional; b) 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 c) os dados pessoais objeto do tratamento tenham sido coletados no território nacional.

Os demais pontos estão detalhados na planilha a seguir.

Objeto da lei	Operação de tratamento de dados pessoais.
Sujeito tutelado pela Lei	Pessoa natural (física) identificada ou identificável.
Aplicação Material	A lei se aplica a atividades de tratamento realizadas em meio físico ou digital.
Sujeito que sofre a incidência da Lei	Pessoas físicas (que realizem tratamento de dados pessoais com finalidade econômica) ou jurídicas de direito público ou privado.
Abrangência Territorial	I) realização de tratamento dentro do território nacional; II) tratamento para oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional (localização geográfica - extraterritorialidade); ou III) dados pessoais objeto do tratamento tenham sido coletados no território nacional.

1.3. Não Aplicabilidade (Art. 4º)

O artigo 4º da LGPD elenca 4 (quatro) incisos com exceções à aplicabilidade da lei, ou seja, são as hipóteses que não sofrem sua incidência.

O inciso I versa sobre a hipótese de não incidência da Lei, nos casos de dados tratados por pessoa física para uso pessoal, sem fins econômicos, tais como listas de endereços de amigos em agenda telefônica física ou eletrônica. Por outro lado, caso essa lista seja de um celular corporativo de um representante comercial sofre a incidência da LGPD, pois tem finalidade lucrativa. Assim, trata-se de uma hipótese que também deve ser analisada em confronto com os riscos aos dados pessoais dos titulares.

Já o inciso II traz 3 (três) hipóteses de não incidência da LGPD. A primeira é a relativa ao tratamento de dados pessoais realizados para fins exclusivamente jornalísticos. Nesse ponto, o legislador tem a intenção de enfatizar a liberdade de expressão da atividade **exclusivamente** jornalística, seja ela desenvolvida por pessoa natural ou jurídica. Cumpre destacar que no julgamento do Recurso Extraordinário nº 511.961/SP, ao analisar a necessidade de qualificação para o exercício da atividade jornalística, o Ministro Gilmar Mendes reconheceu a sua importância no contexto da liberdade de expressão.[9]

Em seguida, como segunda hipótese do inciso II, há o tratamento de dados pessoais realizado para fins exclusivamente artísticos. Para que seja extraído o sentido da lei, como ponto de partida, é louvável a observância dos conceitos dispostos na Lei n. 9.610, de 19 de fevereiro de 1998, que trata sobre a proteção dos direitos autorais sobre obras artísticas, entre outras, visto que muitos deles dão concretude à hipótese trazida por este inciso, o qual veicula um conceito jurídico indeterminado.[10] Dessa forma, o legislador não quer criar obstáculos à criação artística, sendo ela essencial ao desenvolvimento intelectual e

9.“Qualquer controle desse tipo, que interfira na liberdade profissional no momento do próprio acesso à atividade jornalística, configura, ao fim e ao cabo, controle prévio que, em verdade, caracteriza censura prévia das liberdades de expressão e de informação, expressamente vedada pelo art. 5o , inciso IX, da Constituição.” (BRASIL. Supremo Tribunal Federal. Recurso Extraordinário nº511.961. São Paulo, 17 de junho 2019, p.50.)

10. Art. 7º São obras intelectuais protegidas as criações do espírito, expressas por qualquer meio ou fixadas em qualquer suporte, tangível ou intangível, conhecido ou que se invente no futuro, tais como: I - os textos de obras literárias, artísticas ou científicas;II - as conferências, alocuções, sermões e outras obras da mesma natureza;III - as obras dramáticas e dramático-musicais;IV - as obras coreográficas e pantomímicas, cuja execução cênica se fixe por escrito ou por outra qualquer forma;V - as composições musicais, tenham ou não letra;VI - as obras audiovisuais, sonorizadas ou não, inclusive as cinematográficas;VII - as obras fotográficas e as produzidas por qualquer processo análogo ao da fotografia;VIII - as obras de desenho, pintura, gravura, escultura, litografia e arte cinética;IX - as ilustrações, cartas geográficas e outras obras da mesma natureza;X - os projetos, esboços e obras plásticas concernentes à geografia, engenharia, topografia, arquitetura, paisagismo, cenografia e ciência;XI - as adaptações, traduções e outras transformações de obras originais, apresentadas como criação intelectual nova;XII - os programas de computador;XIII - as coletâneas ou compilações, antologias, enciclopédias, dicionários, bases de dados e outras obras, que, por sua seleção, organização ou disposição de seu conteúdo, constituam uma criação intelectual.

cultural de um Estado Democrático de Direito.

A terceira e última hipótese do inciso II diz respeito ao tratamento de dados pessoais para fins exclusivamente acadêmicos[11]. Trata-se de hipótese de **aplicação mitigada,** em face dela ser concretizável apenas se estiver em consonância com um dos requisitos ou bases legais dispostos nos artigos 7º e 11 da LGPD.

Inspirado pela GDPR[12], a LGPD, no inciso III, dispõe sobre as atividades públicas que estão excluídas da sua incidência, quais sejam: segurança pública, defesa nacional, segurança de Estado e atividades de investigação e repressão de infrações penais. São atividades exercidas exclusivamente pelo Estado e que possuem capítulo próprio na Constituição Federal.[13]

Impõe-se a necessidade de edição de lei específica, que venha a regular as operações de tratamento de dados pessoais realizadas nesses campos, a fim de preservar o estado democrático de direito, com o estabelecimento de medidas proporcionais e estritamente necessárias ao atendimento do interesse público, à preservação do devido processo legal, à tutela dos princípios gerais de proteção e ao resguardo dos direitos dos titulares dos dados tratados.

Ainda nesse contexto, a LGPD veda o tratamento dos dados por pessoa de direito privado, nas hipóteses veiculadas no inciso III, exceto se tutelada por pessoa jurídica de direito público e desde que não se refira à totalidade dos dados pessoais constante em banco próprio de armazenamento.

Para concluir as hipóteses de não incidência da LGPD, o inciso IV prevê o afastamento do diploma normativo em relação a dados pessoais 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.

Na planilha a seguir serão descritas, de forma consolidada, as hipóteses de não aplicabilidade da LGPD, com as observações respectivas.

HIPÓTESES	OBSERVAÇÕES
Tratamento de dados pessoais realizado por pessoa natural para fins exclusivamente particulares e não econômicos;	Dados de uso pessoal não sofrem a incidência da LGPD, e.g. agenda telefônica do celular.

11. Sobre o tema vale o destaque Guia Orientativo específico elaborada pela ANPD: "Portanto, o âmbito de incidência e o afastamento parcial da lgpd é restrito aos tratamentos de dados pessoais vinculados de forma estrita – isto é, exclusivamente – ao exercício da liberdade de expressão nos ambientes acadêmicos. Assim, sempre que o tratamento de dados pessoais atender a outros fins, que não aqueles estritamente vinculados à livre expressão acadêmica, a lgpd deverá ser plenamente observada." (https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/web-guia-anpd-tratamento-de-dados-para-fins-academicos.pdf. Acesso em 05/10/2023)

12. Art. 2º, 2, d, do *General Data Protection Regulation* - Regulamento Geral de Proteção de Dados, com entrada em vigor em 25 de maio de 2018.

13.Art. 144 da CF/1988.

Tratamento de dados pessoais realizado para fins exclusivamente jornalísticos;	As atividades jornalísticas são de cunho social e de interesse público, considerando a exclusividade da atividade por parte da pessoa natural ou jurídica, não sofrem a incidência da LGPD;
Tratamento de dados pessoais realizado para fins exclusivamente artísticos;	Tais como obras literárias, dramáticas, musicais, coreógrafas, cinematográficas, pinturas, gravuras, ilustrações, fotos etc., não sofrem a incidência da LGPD.
Tratamento de dados pessoais para fins exclusivamente acadêmicos;	De aplicabilidade mitigada, esta hipótese deve ser analisada sistematicamente com os artigos 7º e 11 da LGPD.
Tratamento de dados pessoais para fins exclusivamente de segurança pública, defesa nacional, segurança do Estado e atividades de investigação e repressão de infrações penais;	Trata-se de atividades de interesse público e de competência exclusiva do Estado, que não sofrem a incidência da LGPD, mas que para realizarem operações de tratamento de dados pessoais estarão sujeitas à legislação específica.
Tratamento de dados pessoais oriundos do exterior	Não se aplica a LGPD em relação a dados 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.

1.4. Conceitos Específicos (Art. 5º)

Com a finalidade de esclarecer conceitos adotados pela lei, o artigo 5º traz definições sobre dado pessoal, dado pessoal sensível, dado anonimizado, banco de dados, titular, controlador, operador, encarregado, agentes de tratamento, tratamento, anonimização, bloqueio, eliminação, transferência internacional de dados, uso compartilhado de dados, relatório de impacto à proteção de dados pessoais, órgão de pesquisa e autoridade nacional.

Embora seja um artigo autoexplicativo, existem algumas definições que merecem ser destacadas para uma adequada compreensão.

No tocante ao inciso I, foi adotada para o dado pessoal a definição expansionista, pois a lei se aplica tanto para dados identificados quanto para aqueles identificáveis, ou seja, os que tem o potencial de serem identificados, como dados de geolocalização. Não é a primeira vez que a legislação pátria utiliza

o conceito expansionista de dado pessoal, pois o Decreto n. 8.771/2016, que trata sobre as hipóteses admitidas de discriminação de pacotes de dados na internet e de degradação de tráfego, entre outras questões, já havia previsto de forma mais detalhada.[14]

Os dados pessoais sensíveis, descrito no inciso II, são aqueles que, quando do tratamento, podem gerar discriminações e, por conseguinte, acarretar danos maiores à personalidade dos titulares, na medida em veiculam informações de cunho religioso, racial, sexual, político etc.

Em seguida foi elucidada a definição de dado anonimizado (III). Além do conceito esmiuçado pela lei, o qual estará disposto na tabela ao final deste item, destaca-se que existe diferença entre dado anonimizado e pseudonimização. No que pertine ao primeiro, os dados pessoais utilizados não são possíveis de serem vinculados ao seu titular, no contexto de utilização de meios técnicos razoáveis e disponíveis na ocasião do tratamento, inclusive o artigo 12 descreve que a anonimização não pode sequer ser revertida. Já o último traz a ideia de reidentificação de dados pessoais que antes estavam criptografados, por exemplo, mas que após o tratamento puderam identificar o seu titular.

Já acerca do conceito de titular de dados pessoais (V), é preciso sublinhar que a lei tutela os dados da pessoa viva, nos termos bem delimitados pela doutrina:

Portanto, no Brasil, a tutela dos direitos existentes na LGPD se inicia com o feto, no mínimo diante da expectativa de direito sobre seus dados pessoais, em razão da sua personalidade jurídica formal, desde a sua concepção, e da personalidade jurídica material, relacionada aos direitos patrimoniais, adquirida com o nascimento com vida, e terminaria com o falecimento. [15]

O controlador (VI) e o operador (VII) são espécies do gênero “agente de tratamento” (IX). O primeiro é quem toma as decisões alusivas ao tratamento dos dados pessoais. Por sua vez, o operador é quem executa a atividade de tratamento, de acordo com as balizas traçadas pelo controlador. Ambos podem ser responsabilizados pela lei.

Ao definir “tratamento de dados” (X), a lei o fez de forma meramente exemplificativa, ou seja, podem ser abrangidas eventuais outras operações que, de alguma forma, estejam relacionadas ao uso de dados pessoais. Além disso, as condutas que descrevem a atividade de tratamento não são cumulativas, de tal modo que basta realizar uma delas, para que haja a incidência da LGPD em toda a sua extensão.

É ônus da prova do controlador provar que houve o consentimento (XII), nos termos do artigo 8º, § 2º, com a manifestação livre, informada e inequívoca por

14.LGPD, Art. 14. Para os fins do disposto neste Decreto, considera-se: I - dado pessoal - dado relacionado à pessoa natural identificada ou identificável, inclusive números identificativos, dados locacionais ou identificadores eletrônicos, quando estes estiverem relacionados a uma pessoa;

15. MALDONADO, Viviane; BLUM, Renato, coordenadores. Lei Geral de Proteção de Dados Comentada. São Paulo: Thomson Reuters, 2019. p.103.

parte do titular. Se for no contexto de dados sensíveis, deve haver o consentimento de forma específica e em destaque (artigo 14, § 1º).

O bloqueio (suspensão temporária de qualquer operação de tratamento – inciso XIII) pode ser feito por requisição do titular dos dados, quando, por exemplo, houver excesso ou desconformidade legal (artigo 18, IV), bem como em caso de sanção administrativa (artigo 52, V), desde que aplicada, neste último caso, após procedimento administrativo que possibilite a oportunidade da ampla defesa, nos termos do § 1º do mesmo artigo.

A eliminação também está prevista como direito do titular (artigo 18, VI), bem como pode ser decorrência de aplicação de sanção administrativa (artigo 52, VI). Ademais, nos termos do artigo 18, § 6º, o controlador deve informar imediatamente aos demais agentes com os quais tenha realizado uso compartilhado de dados, que realizou a correção, a eliminação, a anonimização ou o bloqueio dos dados, para que estes repitam idêntico procedimento, exceto nos casos em que esta comunicação seja comprovadamente impossível ou implique esforço desproporcional.

O conceito de transferência internacional de dados (XV) deve ser compreendido em conjunto com o artigo 33, cujos termos elenca um rol taxativo de situações em que há a permissão de transferência internacional de dados pessoais.

Destaca-se que o compartilhamento de dados (XVI) pode se dar de forma ampla, ou seja, entre entes públicos, entre entes públicos e privados e vice-versa, desde que observados os parâmetros da LGDP, tal como as limitações expostas no art. 26. No mais, o titular tem o direito de ser informado sobre o compartilhamento de seus dados, incluindo-se a identificação do agente de tratamento, e a finalidade para a qual foram utilizados (artigo 9º, V e artigo 18, VII).

O controlador é responsável por gerar o relatório de impacto à proteção de dados pessoais (RIPD). O RIPD será incluído nos procedimentos de governança em privacidade do controlador (artigo 50, § 2º, I, d), com vistas a reduzir riscos, e deverá ser utilizado antes do início do tratamento.

Ao final deste artigo, a lei descreve a autoridade nacional (XIX), que também é tratada como Autoridade Nacional de Proteção de Dados - ANPD em outros trechos. Além das demais competências descritas no inciso, a autoridade também é responsável por aplicar sanções administrativas dispostas no Capítulo VIII da LGPD. A ANPD é autarquia de natureza especial, dotada de autonomia técnica e decisória, e é composta pelo Conselho Diretor, Conselho Nacional de Proteção de Dados Pessoais e da Privacidade, Corregedoria, Ouvidoria e unidades administrativas e unidades especializadas necessárias à aplicação da LGPD (artigo 55-C)

Demais informações estão contidas no quadro abaixo, nos termos do artigo 5º da LGPD.

Dado Pessoal	Informação relacionada a pessoa natural identificada ou identificável.
Dado Pessoal Sensível	Dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.
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. O artigo 5º, III, cumulado com o artigo 12.
Banco de Dados	Conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico
Títular	Pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.
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.
Encarregado	Pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD).
Agentes de Tratamento	O controlador e o operador.
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.
Anomização	Utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo.
Consentimento	Manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada.
Bloqueio	Suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados.

Eliminação	Exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado.
Transferência Internacional de Dados	Transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro.
Uso Compartilhado de Dados	Comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados.
Relatório de impacto à Proteção de Dados Pessoais	Relatório de impacto à proteção de dados pessoais: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco.
Órgão de Pesquisa	Órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no País, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico.
Autoridade Nacional	Órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional

1.5. Princípios (Art. 6º)

O artigo 6º da LGPD enumera os princípios que norteiam a proteção de dados pessoais, cuja relevância é indispensável para modelar adequadamente o comportamento de todos aqueles que estão submetidos à incidência da lei.

O caput do artigo 6º descreve o princípio da boa-fé, sob o aspecto objetivo. Tal princípio pauta a conduta do agente perante a sociedade, ao densificar a ideia de fidelidade, moralidade, probidade, confiança etc. Ressalta-se, ainda, que várias bases legais de tratamento são fundamentadas em contratos e este princípio é um dos pilares estruturantes do Direito Civil e Consumerista.[16]

Os incisos do art. 6º detalham 10 (dez) outros princípios específicos. O primeiro deles é o princípio da finalidade (I), o qual ressalta a importância de delimitar o objetivo do tratamento, a fim de se evitarem possíveis abusos. O

16. CC, Art. 113. Os negócios jurídicos devem ser interpretados conforme a boa-fé e os usos do lugar de sua celebração.

princípio da adequação (II) está voltado para a escolha assertiva dos procedimentos adotados, segundo as finalidades informadas. Já o princípio da necessidade (III) busca nortear o agente de tratamento para a utilização de dados estritamente necessários à finalidade proposta. O princípio do livre acesso (IV), também citado no artigo 9º, deixa claro a garantia do titular em ter acesso aos seus dados, por meio de uma requisição (artigo 18), para que possa controlar o fluxo de informações a seu respeito. O princípio da qualidade dos dados (V) objetiva garantir ao titular dos dados pessoais a correta coleta e tratamento dos seus dados, a fim de evitar imprecisão que possa acarretar danos à sua personalidade.[17] A transparência (VI), também apontada no artigo 20, § 1º, é via hábil à consolidação dos demais princípios, na medida em que, com a transparência das informações, principalmente sobre a realização do tratamento e os respectivos agentes de tratamento, o titular consegue verificar se os outros princípios foram atendidos plenamente. O princípio da segurança (VII) retrata a importância dos agentes de tratamento se preocuparem em adotar medidas aptas a proteger os dados pessoais, inclusive de eventos acidentais, nos termos do artigo 46 e seguintes da lei. A prevenção (VIII) objetiva mitigar os riscos de violação de dados pessoais, além de determinar que o controlador elabore o RIPD, conforme anteriormente mencionado. O princípio da não discriminação (IX), com fundamento na dignidade da pessoa humana e da igualdade material, tem a finalidade de evitar condutas discriminatórias no tratamento de dados pessoais. Os últimos princípios citados pelo legislador foram os da responsabilização e prestação de contas (X), os quais traduzem a necessidade de 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.

A seguir será apresentado um quadro-resumo dos princípios dispostos no art. 6º da LGPD.

GERAL	Boa-fé	Único princípio geral expresso da LGPD, disposto no caput do art. 6º. A boa-fé objetiva densifica a ideia de que as partes possuem o dever de agir à luz de valores éticos e morais da sociedade. Desse princípio é possível extrair deveres anexos, tais como a lealdade, a transparência, a colaboração, a probidade, dentre outros. É o que se observa nas palavras de Paulo Brasil Dill Soares. [18]

17. "A previsão de correção de dados já encontra previsão constitucional por meio do *habeas data*, mas diferentemente do que se propõe o presente texto legislativo de proteção de dados, o *habeas data* garante ao cidadão tão somente a sua defesa contra as arbitrariedades do governo, o que significa pelas consequências do período ditatorial, que influenciou diretamente o constituinte de 1988". (TEIXEIRA E ARMELIN, 2020, p. 52, apud SARDETO, 2011, p. 55).

18. "Boa-fé objetiva é um "standart" um parâmetro genérico de conduta. Boa-fé objetiva significa, portanto, uma atuação "refletida", pensando no outro, no parceiro atual, respeitando seus interesses legítimos, suas expectativas razoáveis, seus direitos, agindo com lealdade, sem abuso,

	Finalidade	Realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades
	Adequação	Compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento.
	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
	Livre Acesso	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.
ESPECÍFICO	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.
	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.
	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.
	Prevenção	Adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais.
	Não Discriminação	Impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos.
	Responsabilização e Prestação de Contas	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

sem obstrução, sem causar lesão ou desvantagem excessiva, gerando para atingir o bom fim das obrigações: o cumprimento do objetivo contratual e a realização de interesses das partes." (SOARES, Paulo Brasil Dill. Princípios Básicos de Defesa do Consumidor: Institutos de Proteção ao Hipossuficiente. Leme/SP: LED, 2001. p.219-220)

2. Do Tratamento de Dados Pessoais

2.1. Hipóteses autorizadoras do tratamento de dados pessoais

As operações de tratamento de dados previstas no art. 3º da LGPD devem ser realizadas mediante o enquadramento de uma das hipóteses autorizadoras ou bases legais dispostas nos art. 7º e 11. Por exemplo, uma sociedade empresária brasileira, em regra, apenas é autorizada a realizar a coleta e tratamento de dados pessoais no Brasil, quando existe o consentimento livre, informado e específico do seu titular, na forma dos artigos 5º, XII, 8º e seguintes da lei.

Destaca-se que os artigos 7º e 11 descrevem bases legais taxativas, as quais legitimam o tratamento de dados pessoais. Apesar disso, algumas bases legais possuem conceitos jurídicos indeterminados (amplos), tais como a que aborda o interesse legítimo do controlador ou de terceiros, ocasionando, assim, maior subjetividade quando do seu enquadramento.

O artigo 7º da LGPD descreve 10 (dez) bases legais de tratamento de dados pessoais, bastando a adequação em qualquer uma delas para o tratamento ser considerado legítimo. Por outro lado, nada impede que o tratamento de dados pessoais se adeque a mais de uma base legal, mas é prudente que seja escolhido a mais segura e adequada.[1]

A primeira hipótese descrita no inciso I , do artigo 7º, da LGPD, é aquela que admite o tratamento, desde que seja fornecido o consentimento do titular. As outras 9 (nove) bases legais prescindem de anuência da pessoa natural aos quais os dados se referem.

A seguir serão tratadas, com detalhes, cada uma das hipóteses autorizadoras de tratamento de dados pessoais previstas no Art. 7º, da Lei Geral de Proteção da de dados Pessoais.

1. "(...) Entende-se que, ainda que seja possível utilizar mais de uma base legal para determinado tratamento de dados, é preciso buscar a base mais adequada e segura para a situação concreta". (DONEDA, Danilo ... (et al.). Tratado de proteção de dados pessoais. Rio de Janeiro: Forense, 2021. p.133)

2.1.1. Hipótese I - mediante o fornecimento de consentimento pelo titular

O inciso I, do artigo 7º, da LGPD, descreve o permissivo legal para tratamento de dados pessoais, mediante o fornecimento de consentimento pelo titular.

Destaca-se que o consentimento é considerado um negócio jurídico, de tal forma devem estar presentes todos os requisitos de validade dispostos no Código Civil de 2002, especialmente no artigo 104, quais sejam: agente capaz; objeto lícito, possível, determinado ou determinável; e forma prescrita ou não defesa em lei. [2]

O caput do artigo 8º da Lei descreve que o consentimento deve ser fornecido por escrito ou por outro meio que demonstre de forma inequívoca a manifestação de vontade do titular, tais como vídeo, áudio etc., vinculada àquele determinado tratamento. Não é admitido consentimento tácito.

Caso seja escrito, o consentimento deve constar de cláusula destacada das demais, que pode ser em documento anexo ou no mesmo documento, desde que em negrito, fonte maior, sublinhado, etc.[3] O que se quer é a clareza das informações para se obter um consentimento inequívoco.

Em caso de dúvida quanto à validade do consentimento, o ônus da prova é do controlador[4]. Considera-se válido, ademais, o consentimento que se refere a finalidades determinadas. Portanto, sendo nulas as autorizações genéricas.[5]

É considerada a principal base legal disposta na lei e para ser considerada legítima essa manifestação deverá ser **livre, informada e inequívoca**, em consonância com o art. 5º, XII, do mesmo dispositivo legal.

A manifestação livre é aquela que não sofre nenhum vício no seu consentimento[6], tais como erro ou ignorância, dolo, coação, estado de perigo, lesão, fraude contra credores e simulação.[7]

A manifestação inequívoca é aquela que não deixa nenhuma dúvida ao controlador quanto ao consentimento do titular para o fornecimento dos dados pessoais. Assim, não se admitem formulários pré-preenchidos ou sem nenhuma ação do titular.

A manifestação informada é aquela em que os titulares foram cientificados acerca da: finalidade específica do tratamento; forma e duração do tratamento, observados os segredos comercial e industrial, identificação do controlador; informações de contato do controlador; informações acerca do uso compartilhado de dados pelo controlador e a finalidade; responsabilidades dos agentes que realizarão o tratamento; e direitos do titular, com menção explícita aos direitos

---

2. COTS, Márcio; OLIVEIRA, Ricardo. Lei geral de proteção de dados pessoais comentada. 3ª edição. São Paulo: Thomson Reuters Brasil, 2019. p.92.
3. Artigo 8º, § 1º, LGPD.
4. Artigo 8º, § 2º, LGPD
5.Artigo 8º, § 4º, LGPD.
6. Artigo 8º, § 3º, LGPD.
7.Artigos 138-165, do Código Civil/2002.

contidos no art. 18 da Lei.[8]

Todos os registros devem ser armazenados pelo Controlador, em caso de necessidade de comprovação posterior de que o consentimento atendeu aos ditames legais.

O titular dos dados pode, a qualquer momento, revogar o seu consentimento, desde que mediante manifestação expressa, por procedimento gratuito e facilitado, mas serão ratificados os tratamentos até aquele momento, enquanto não houver requerimento para eliminá-los. [9]

A Lei autoriza o compartilhamento de dados pessoais entre controladores, mas exige consentimento específico do titular para esse fim,[10] o que deve ser entendido como uma cláusula no termo ou contrato com a identificação do controlador que receberá os dados.

O artigo 7º, §§ 3º e 4º, dispõe sobre o tratamento de dados pessoais cujo acesso o titular tenha tornado manifestamente público. Neste caso, a lei não exige o consentimento do titular para o tratamento de dados, num primeiro momento, desde seja considerada a finalidade, a boa-fé e o interesse público que justificaram sua disponibilização.

Entretanto, o § 7º do mesmo artigo, admite o tratamento posterior de dados pessoais, cujo titular tenha tornado público, para novas finalidades, desde que observados os propósitos legítimos e específicos para o novo tratamento, preservando-se os direitos do titular, assim como os fundamentos e os princípios previstos na LGPD.

A seguir será exposto um quadro com os requisitos do consentimento nos termos da LGPD.

[Início Tabela 6]

Requisitos do Consentimento	Manifestação livre	Artigo 5º, XII
	Manifestação inequívoca	Artigo 5º, XII
	Manifestação informada	Artigo 5º, XII
	Referir-se a finalidades determinadas	Artigo 8º, § 4º
	Escrito ou por outro meio que demonstre a manifestação de vontade do titular	Artigo 8º, caput

2.1.2. Hipótese 2 - para o cumprimento de obrigação legal ou regulatória pelo controlador

O inciso II do artigo 7º legitima o tratamento de dados pessoais para o cumprimento de obrigação legal ou regulatória pelo controlador. A título exemplificativo, pode-se citar o tratamento de dados para atendimento à legislação

8. Artigo 9º da LGPD.
9.Artigo 8º, § 5º, LGPD.
10.Artigo 7º, § 5º, LGPD.

trabalhista e previdenciária, nos casos em que o empregador tem o dever de cumprimento de obrigações acessórias, tal como o translado da Guia de Recolhimento do FGTS e de Informações à Previdência Social (GFIP).

No âmbito administrativo, pode-se citar como exemplo o dever de um agente público lotado na área de gestão de pessoas do Estado de Alagoas, independente de requerimento, acessar e divulgar nos sítios oficiais as informações sobre remunerações dos servidores lotados na Administração Pública, em decorrência de determinação legal.

Sobre o tema, são válidas as orientações expedidas pela ANPD, no Guia Orientativo sobre Tratamento de Dados Pessoais pelo Poder Público[11]:

De forma geral, a aplicação desses dispositivos será efetuada em dois contextos normativos distintos, que se diferenciam em razão da espécie de norma jurídica que estabelece a obrigação a ser cumprida. **É o caso, em especial, das normas de conduta e das normas de organização.** Na primeira hipótese, a obrigação legal decorre de uma norma de conduta, isto é, uma regra que disciplina um comportamento, em geral estabelecendo um fato ou uma hipótese legal, com uma possível consequência jurídica em caso de descumprimento. Caso o responsável não cumpra a obrigação legal (como, por exemplo, a divulgação da agenda de compromissos públicos de autoridades, conforme art. 11 da Lei nº 12.813/2013), poderá ser objeto das penalidades administrativas previstas na legislação.

Nessas situações, o tratamento de dados pessoais é necessário para atender a uma regra específica, ou seja, uma determinação legal expressa ou uma obrigação de natureza regulatória estabelecida por um órgão regulador. Não há, por isso, um vínculo necessário e direto entre o tratamento de dados e o exercício de atribuições e competências legais do controlador. Já na segunda hipótese, a obrigação legal decorre de normas de organização, assim entendidas as normas que estruturam órgãos e entidades e estabelecem suas competências e atribuições. Nesse contexto normativo, o tratamento de dados pessoais é parte essencial do exercício de prerrogativas estatais típicas, uma vez que necessário para viabilizar a própria execução das atribuições, competências e finalidades públicas da entidade ou do órgão público.

Assim, diferentemente das normas de conduta, que estabelecem obrigações de forma direta e expressa, prevendo uma consequência específica em caso de descumprimento, as normas de organização estabelecem obrigações que estão associadas, de forma mais geral, ao próprio cumprimento e à execução de atribuições legais típicas da entidade ou do órgão público responsável pelo tratamento de dados pessoais. (Grifos nossos)

Nesse contexto, frise-se que não se enquadra nessa base legal as obrigações assumidas por meio de contratos. O que o dispositivo legal respalda são

11. https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/guia-poder-publico-anpd-versao-final.pdf. Acesso em 10/10/2023.

as obrigações decorrentes de determinações legais, inclusive aquelas provenientes de legislação internacional.[12]

2.1.3. Hipótese 3 - 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

Na terceira hipótese veiculada no inciso III, da LGPD, o tratamento e uso compartilhado de dados pessoais é permitido, desde que sejam necessários à execução de políticas públicas, previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres.[13]

Tal base legal deve ser lida em conjunto com os artigos 23 a 32 do mesmo dispositivo legal, que descreve regras específicas sobre tratamento de dados pessoais pelo poder público.

O caput do artigo 23 informa que as **pessoas jurídicas de direito público** abrangidas pela Lei são as mesmas dispostas no artigo 1º da Lei nº 12.527/2011 (Lei de Acesso à Informação), quais sejam: órgãos públicos integrantes da administração direta dos Poderes Executivo, Legislativo, incluindo as Cortes de Contas, e Judiciário e do Ministério Público, as autarquias, as fundações públicas, as empresas públicas, as sociedades de economia mista e demais entidades controladas direta ou indiretamente pela União, Estados, Distrito Federal e Municípios.

Ressalte-se, porquanto oportuno, que, segundo o artigo 24 da LGPD, as empresas públicas e as sociedades de economia mista que atuam em regime de concorrência, sujeitas ao disposto no art. 173 da Constituição Federal, terão o mesmo tratamento empregado às pessoas jurídicas de direito privado particulares.

Ademais, o tratamento de dados pessoais deve ser realizado em atendimento à finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público, e desde que: 1) sejam informadas aos seu titulares as hipóteses em

---

12. "Ademais, eventuais determinações previstas na **legislação internacional**, bem como em melhores práticas comprovadamente seguidas por um nicho da indústria, também poderão ser entendidos como fundamento para o tratamento de dados, sob pena de serem criados entraves de consequências relevantes, especialmente a companhias internacionais." (MALDONADO, Viviane; BLUM, Renato, coordenadores. Lei Geral de Proteção de Dados Comentada. São Paulo: Thomson Reuters, 2019. p.183.)

13. "A administração pública poderá realizar o uso compartilhado de dados (...), desde que tal se dê com o estrito objetivo de executar políticas públicas (o conceito de **políticas públicas** não é o único, mas, em linhas gerais, podemos considerá-lo como sendo toda atividade realizada por qualquer ente da administração pública com o objetivo de solucionar demandas da sociedade, englobando setores, tais como saúde, educação, economia, entre outros) expressamente previstas na legislação. (MALDONADO, Viviane; BLUM, Renato, coordenadores. Lei Geral de Proteção de Dados Comentada. São Paulo: Thomson Reuters, 2019. p.183.)

que, no exercício de suas competências, realizam o tratamento de dados pessoais, fornecendo informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos; 2) seja indicado um encarregado quando realizarem operações de tratamento de dados pessoais, nos termos do art. 39 da LGPD; [14]

2.1.4. Hipótese 4 - estudos por órgão de pesquisa

A LGPD, no inciso IV, do artigo 7º, autoriza o tratamento de dados para a realização de estudos por órgão de pesquisa, ressaltando, porém, a importância de se garantir, sempre que possível, a anonimização dos dados pessoais.

Diante desta base legal, é essencial relembrar o conceito de **órgão de pesquisa** descrito no artigo 5º, inciso XVIII, da LGPD, vejamos: "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".

As pessoas jurídicas de direito privado com fins lucrativos não estão abrangidas por esta hipótese, conforme se observa do conceito legal acima descrito. Nessa linha de intelecção, são relevantes os apontamentos da ANPD, no "Guia Orientativo sobre Tratamento de Dados Pessoais para fins Acadêmicos e para a Realização de Estudos e Pesquisas"[15]:

A LGPD não incluiu as pessoas jurídicas de direito privado com fins lucrativos no rol de agentes de tratamento que podem recorrer à hipótese legal de realização de estudos por órgãos de pesquisa. Isso significa que, mesmo detendo entre suas finalidades constitutivas a realização de pesquisa, não se torna possível a utilização dessa hipótese legal específica por essas organizações. Para tais agentes, o tratamento de dados pessoais para fins de estudos e pesquisas deverá ser realizado com amparo em outras hipóteses legais, a exemplo do consentimento ou do legítimo interesse.

Há recomendação, no permissivo legal apontado, de que os órgãos de pesquisa promovam a **anonimização dos dados pessoais**, através da utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento, pois não poderão ser identificados.

Ainda acerca dessa base legal, a LGPD, no caput do artigo 13, aventa a possibilidade de, ao realizarem "**estudos em saúde pública**, os órgãos de pesquisa terem acesso a bases de dados pessoais, que serão tratados exclusivamente dentro do órgão e estritamente para a finalidade de realização de estudos

14. Artigo 23, I ao IV, da LGPD

15. https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/web-guia-anpd-tratamento-de-dados-para-fins-academicos.pdf. Acesso em 10/10/2023.

e pesquisas e mantidos em ambiente controlado e seguro, conforme práticas de segurança previstas em regulamento específico e que incluam, sempre que possível, a anonimização ou pseudonimização dos dados, bem como considerem os devidos padrões éticos relacionados a estudos e pesquisas".

Ainda no contexto dos estudos em saúde pública, os parágrafos do artigo 13 veiculam as seguintes determinações: "§ 1º - a divulgação dos resultados ou de qualquer excerto do estudo ou da pesquisa de que trata o caput, em nenhuma hipótese, poderá revelar dados pessoais; § 2º o órgão de pesquisa será o responsável pela segurança da informação prevista no caput, não permitida, em circunstância alguma, a transferência dos dados a terceiro; § 3º - e o acesso desses dados será objeto de regulamentação por parte da autoridade nacional e das autoridades da área de saúde e sanitárias, no âmbito de suas competências."

Por fim, a **pseudonimização** descrita no § 4º, do artigo 13, da LGPD, para os casos de estudos em saúde pública, "é o tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro", como a criptografia que posteriormente pode ser revertida.

2.1.5. Hipótese 5 - 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

A quinta hipótese autorizadora, disposta no inciso V, do artigo 7º, da LGPD, admite a legitimidade de tratamento de dados para execução de contrato ou procedimentos preliminares pré-contrato (e.g. proposta ou contrato preliminar) do qual seja parte o titular, mediante o seu pedido.

Pode-se considerar que essa hipótese se assemelha a do inciso I do mesmo dispositivo, mediante consentimento do titular, mas neste caso o titular dos dados não pode revogar o consentimento a qualquer tempo já que a parte adversa poderá manter os dados fornecidos se o tratamento for necessário durante a execução contratual, como exemplo as instituições financeiras em relação a determinada pessoa, anteriormente a concessão do crédito e durante a vigência do contrato.[16]

16.DONEDA, Danilo ... (et al.). Tratado de proteção de dados pessoais. Rio de Janeiro: Forense, 2021. p.135-136.

2.1.6. Hipótese 6 - para o exercício regular de direitos em processo judicial, administrativo ou arbitral (lei nº 9.307/1996 - lei de arbitragem)

O inciso VI, do artigo 7º, da LGPD, autoriza o tratamento de dados pessoais 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), sem o consentimento do titular dos dados pessoais, desde que para o atendimento de finalidades específicas e pelo tempo que subsistir a necessidade.

Trata-se de hipótese autorizadora ampla, que converge com os direitos e garantias fundamentais processuais, dentre eles o devido processo legal, o legítimo exercício do direito de ação, o contraditório e a ampla defesa.[17]Não seria possível impedir, nesse sentido, que o autor apresentasse dados pertinentes ao réu, a fim de viabilizar sua regular citação, ou que uma das partes veiculasse informações necessárias à intimação de uma determinada testemunha.

2.1.7. Hipótese 7– para a proteção da vida ou da incolumidade física do titular ou de terceiro

Trata-se de hipótese autorizadora de tratamento de dados pessoais, descrita no inciso VII, do artigo 7º, da LGPD, para a proteção da vida ou da incolumidade física do titular ou de terceiros.

Tal disposição é para ser aplicada de forma restritiva, ou seja, em situações de gravidade que podem gerar risco à vida ou à incolumidade física do cidadão, como o caso de obtenção de dados de geolocalização de dispositivos de telefone celular, na hipótese de desaparecimento ou ocorrência de acidente grave, e.g. desabamento de um prédio[18], ou para tratamento de dados importantes para conter o avanço de pandemias etc.[19]

Destaca-se que tanto a vida/incolumidade física do indivíduo quanto a privacidade são direitos e garantias fundamentais tutelados pela Constituição Federal de 1988[20], mas, diante de situações graves/urgentes, deve-se ponderar a necessidade de tratamento de dados, mesmo que sem o devido consentimento

17.CF/1988 - Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes: (...) XXXV - a lei não excluirá da apreciação do Poder Judiciário lesão ou ameaça a direito; (...) LV - aos litigantes, em processo judicial ou administrativo, e aos acusados em geral são assegurados o contraditório e ampla defesa, com os meios e recursos a ela inerentes;

18.COTS, Márcio; OLIVEIRA, Ricardo. Op., cit.. p. 185.

19. DONEDA, Danilo ... (et al.). Tratado de proteção de dados pessoais. Rio de Janeiro: Forense, 2021. p.137

20.CF/1988, Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do **direito à vida**, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes: (...) III - ninguém será submetido a tortura nem a tratamento desumano ou degradante; (...) X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;

do titular.

Na própria CF/1988, o direito à vida está localizado no caput do artigo 5º, com uma função norteadora em relação aos demais direitos fundamentais dispostos nos incisos do mesmo dispositivo, sendo considerado como pilar estruturante do Estado Democrático de Direito.

Assim, em situações urgentes, excepcionais e específicas é aplicada esta hipótese autorizadora de tratamento de dados pessoais, a fim de proteger a vida ou incolumidade física do titular dos dados ou terceiros, em detrimento do direito à privacidade.

2.1.8. Hipótese 8 - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária

A oitava hipótese autorizadora, descrita no inciso VIII do artigo 7º da LGPD, legitima o tratamento de dados pessoais para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária.

Percebe-se que o legislador buscou destacar, mais uma vez, a exemplo do inciso anterior, a importância do princípio da proteção à vida e da incolumidade física do indivíduo, em face do princípio da privacidade.

Esta base legal só pode ser utilizada em procedimentos realizados por "profissionais de saúde" (médicos, dentistas, psicólogos, fisioterapeutas etc.), no desempenho de suas atividades profissionais, quando do tratamento de dados, bem como por "serviços da saúde" e "entidades sanitárias"[21], tornando-se, assim, ainda mais restritiva que a anterior.

2.1.9. Hipótese 9 – 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 inciso IX, do artigo 7º, da LGPD, autoriza, quando necessário, que seja realizado o tratamento de dados para atendimento dos 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.

Mas afinal, o que seria considerado interesse legítimo? Por se tratar de um conceito aberto, com alto grau de subjetividade, esta hipótese gera muita discussão.

Nesse contexto, quando do tratamento de dados pessoais baseado no

21."(...) entidades sanitárias são entes de direito público da administração direta dedicada à algum aspecto da preservação da saúde pública. Não é muito destacar que tal incumbência é dos entes integrantes do Sistema Único de Saúde – SUS, nos termos do artigo 200 da Constituição Federal". (COTS, Márcio; OLIVEIRA, Ricardo. Lei geral de proteção de dados pessoais comentada. 3ª edição. São Paulo: Thomson Reuters Brasil, 2019. p. 89.)

legítimo interesse, o controlador deve considerar os fundamentos dispostos nos parágrafos do artigo 10 da LGPD: 1) atendimento às finalidades legítimas; 2) aplicação em situações concretas; 3) utilização somente dos dados pessoais estritamente necessários para a finalidade pretendida (princípio da necessidade)[22]; 4) adoção de medidas para garantir a transparência do tratamento de dados (princípio da transparência)[23]; 5) caso seja solicitado pela autoridade nacional, apresentação de relatório de impacto à proteção de dados pessoais, observados os segredos comercial e industrial.

Atenta-se que a escolha dessa base legal deve ser muito bem fundamentada a ponto de dispensar o consentimento do titular dos dados, pois, caso contrário o controlador será responsabilizado e estará sujeito as sanções da Lei.

2.1.10. Hipótese 10 - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente

Trata-se da última hipótese autorizadora do artigo 10, a qual legitima o tratamento de dados para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

Não é a primeira vez que a legislação pátria prevê essa proteção. Pode-se vislumbrar a tutela ao crédito por meio da Lei do Cadastro Positivo (Lei n. 12.414), de 09 de julho de 2011, que disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito, e do Código de Defesa do consumidor (Lei n. 8.078), de 11 de setembro de 1990, especialmente no artigo 43, que previu a formação de bancos de dados pelas sociedades empresárias que trabalham com serviços de proteção ao crédito.

Ressalta-se que, ao proteger o crédito, o legislador busca fomentar a economia, garantindo às instituições a análise dos riscos, o que garante uma maior solidez no mercado financeiro. Em linha de convergência, manifestam-se Tarcísio Teixeira e Ruth Maria Guerreiro da Fonseca Armelin: “Essa hipótese engloba ainda o tratamento de dados pessoais para compor o *score* (pontuação em português) do indivíduo e para a prevenção antifraude a ser adotada pelo agente de tratamento.”[24]

A seguir, por meio de um quadro sinóptico, será feito um resumo das hipóteses autorizadoras do artigo 7º, da LGPD, com seus respectivos fundamentos legais.

HIPÓTESES	DESCRIÇÃO	BASE LEGAL
Hipótese 1	mediante o fornecimento de consentimento pelo titular	Art. 7º, I

22.LGPD, artigo 6º, III.

23.LGPD, artigo 6º, VI.

24. TEIXEIRA, Tarcísio; ARMELIN, Ruth Maria Guerreiro da Fonseca. Lei Geral de Proteção de Dados Pessoais: comentada artigo por artigo. 2ª ed. Salvador: Juspodim, 2020, p. 59.

Hipótese 2	para o cumprimento de obrigação legal ou regulatória pelo controlador	Art. 7º, II
Hipótese 3	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	Art. 7º, III
Hipótese 4	para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais	Art. 7º, IV
Hipótese 5	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	Art. 7º, V
Hipótese 6	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)	Art. 7º, VI
Hipótese 7	para a proteção da vida ou da incolumidade física do titular ou de terceiro	Art. 7º, VII
Hipótese 8	para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária	Art. 7º, VIII
Hipótese 9	quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais	Art. 7º, IX
Hipótese 10	para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente	Art. 7º, X

2.2. Do tratamento de dados pessoais sensíveis

Antes de adentrar nas 8 (oito) hipóteses autorizadoras de tratamento de dados pessoais sensíveis, convém relembrar o conceito de dado pessoal sensível descrito no inciso II do artigo 5º da LGPD: “II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural”.

Assim, dados pessoais sensíveis são aqueles que, se expostos

indevidamente, podem implicar em maiores danos à personalidade do titular, na medida em que tem o condão de ensejar situações discriminatórias.[25]

Diante disso, o legislador reserva uma seção na LGPD (Capítulo II – Seção II – Art. 11) para tratar de regras específicas relativas ao tratamento de dados pessoais sensíveis, uma vez que pode ferir diretamente os direitos e liberdades fundamentais, e, por conseguinte, a dignidade da pessoa humana, fundamento da República Federativa do Brasil, conforme disposto no artigo 1º, inciso III, da Constituição Federal de 1988.

Das 10 (dez) hipóteses autorizadoras descritas no artigo 7º, 3 (três) delas não podem ser utilizadas no tratamento de dados sensíveis, quais sejam: 1) para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados; 2) para atender aos interesses legítimos do controlador ou de terceiro; e 3) para a proteção do crédito.

Ao todo o artigo 11 lista 8 (oito) hipóteses autorizadoras para tratamento de dados sensíveis, sendo que, dentre elas, 7 (sete) já estão descritas no artigo 7º, com regramento mais rígido em algumas situações, a fim de conferir maior proteção a essa espécie de dados. São elas: 1) quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas; 2) para o cumprimento de obrigação legal ou regulatória pelo controlador; 3) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos; 4) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis; 5) 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); 6) proteção da vida ou da incolumidade física do titular ou de terceiro; e 7) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; e 8)para garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos. Sendo esta última específica aos dados pessoais sensíveis.

25. "A criação de uma categoria de dados sensíveis foi fruto da observação pragmática sobre a diferença dos efeitos do tratamento desta categoria de dados em relação aos demais. E foi este idêntico impulso pragmático que fez com que se percebesse mais claramente a necessidade de exorbitar os cânones "tradicionais" ligados à privacidade, ao revelar a presença de um outro valor digno de tutela como fundamento da tutela da pessoa neste caso, que é o princípio da igualdade material." DONEDA, Danilo. Da privacidade à proteção de dados pessoais: fundamentos da lei geral de proteção de dados – 2ª edição – São Paulo: Thomson Reuters Brasil, 2019. p. 143)

2.2.1. Hipótese 1 - quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas

O inciso I do artigo 11 da LGPD legitima o tratamento de dados pessoais sensíveis, quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades concretas.

Portanto, além da manifestação do consentimento ser livre, informada e inequívoca[26], também precisa ser específica e destacada, nos termos enunciados por Chiara Spadaccini de Teffé e Mario Viola[27]:

Específico deve ser compreendido como um consentimento manifestado em relação a propósitos concretos e claramente determinados pelo controlador e antes do tratamento dos dados, havendo também aqui, e com mais ênfase, as obrigações da granularidade. Destacado pode ser interpretado no sentido de que é importante que o titular tenha pleno acesso ao documento que informará todos os fatos relevantes sobre o tratamento, devendo tais disposições vir destacadas para que a expressão do consentimento também o seja. Além de se referir a dados determinados e haver declaração de vontade que esteja ligada a objetivo específico, a manifestação de vontade deverá vir em destaque no instrumento de declaração que autoriza o tratamento.

As próximas hipóteses autorizadoras serão legitimadas sem o consentimento do titular dos dados pessoais sensíveis.

2.2.2. Hipótese 2 - para cumprimento de obrigação legal ou regulatória pelo controlador

Comentários remissivos ao item 3.1.2 desta Cartilha (Hipótese 2 - para o cumprimento de obrigação legal ou regulatória pelo controlador).

2.2.3. Hipótese 3 - para tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos

Comentários remissivos ao item 3.1.3 desta Cartilha (Hipótese 3 - 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), exceto no tocante aos contratos, convênios ou instrumentos congêneres, os quais não são aplicáveis a tal hipótese.

26.LGPD, Artigo 5º, XII.

27. TEFFÉ, Chiara Spadaccini de; VIOLA, Mario. Tratamento de dados pessoais na LGPD: estudo sobre as bases legais. civilistica.com, v. 9, n. 1, p. 1-38, 9 mai. 2020.

2.2.4. Hipótese 4 - para realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis

Comentários remissivos ao item 3.1.4 desta Cartilha (Hipótese 4 - estudos por órgão de pesquisa).

2.2.5. Hipótese 5 - para o exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral (lei nº 9.307/1996 - lei de arbitragem)

Comentários remissivos ao item 3.1.6 desta Cartilha (Hipótese 6 - para o exercício regular de direitos em processo judicial, administrativo ou arbitral (lei nº 9.307/1996 - lei de arbitragem).

2.2.6. Hipótese 6 - para a proteção da vida ou da incolumidade física do titular ou de terceiro

Comentários remissivos ao item 3.1.7 desta Cartilha (Hipótese 7 – para a proteção da vida ou da incolumidade física do titular ou de terceiro).

2.2.7. Hipótese 7 - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária

Comentários remissivos ao item 3.1.8 desta Cartilha (Hipótese 8 - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária).

2.2.8. Hipótese 8 - para a garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º da Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais

Trata-se de base legal específica, prevista no artigo 11, inciso II, g, da LGPD, para o tratamento de dados sensíveis, quando for indispensável, para: 1) a garantia da prevenção à fraude; e 2) a garantia de prevenção à segurança do titular. Os dois casos são restritos aos processos de identificação e autenticação de cadastro em sistemas eletrônicos. A título exemplificativo, pode-se citar as situações nas quais os planos de saúde exigem dos seus segurados a biometria para liberação de exames, e.g.[28]

Destaca-se que, para legitimar esta hipótese, os agentes de tratamento

28.DONEDA, Danilo ... (et al.). Tratado de proteção de dados pessoais. Rio de Janeiro: Forense, 2021. p.141.

devem resguardar os direitos mencionados no art. 9º da Lei.[29]

Nesse contexto, a LGPD não autoriza o tratamento de dados pessoais sensíveis ,caso haja ameaça a direitos e liberdades fundamentais do titular.

A seguir, por meio de um quadro sinóptico, será feito um resumo das hipóteses autorizadoras do artigo 11 da LGPD (tratamento de dados sensíveis), com seus respectivos fundamentos legais.

[Início Tabela 8]

HIPÓTESES	DESCRIÇÃO	BASE LEGAL
Hipótese 1	Quando o titular ou seu responsável legal consentir, de forma específica e destacada, que o tratamento seja realizado para finalidades concretas.	Art. 11, I
Hipótese 2	Para cumprimento de obrigação legal ou regulatória pelo controlador.	Art. 11, II, a
Hipótese 3	Para tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos	Art. 11, II, b
Hipótese 4	Para realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis	Art. 11, II, c
Hipótese 5	Para o 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)	Art. 11, II, d
Hipótese 6	Para a proteção da vida ou da incolumidade física do titular ou de terceiro.	Art. 11, II, e
Hipótese 7	Para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária.	Art. 11, II, f
Hipótese 8	Para a garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º da Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.	Art. 11, g

29. LGPD, Art. 9º O titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca de, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso: I - finalidade específica do tratamento; II - forma e duração do tratamento, observados os segredos comercial e industrial; III - identificação do controlador; IV - informações de contato do controlador; V - informações acerca do uso compartilhado de dados pelo controlador e a finalidade; VI - responsabilidades dos agentes que realizarão o tratamento; e VII - direitos do titular, com menção explícita aos direitos contidos no art. 18 desta Lei.

2.3. Do Tratamento de Dados Pessoais de Crianças e de Adolescentes

A LGPD reserva uma seção específica (Capítulo II – Seção III – Art. 14) para regular o tratamento de dados pessoais de crianças e de adolescentes.

No ordenamento jurídico pátrio existem várias leis que amparam os direitos das crianças e adolescentes. A própria Carta Magna, no artigo 227, descreve que "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".

O principal marco legal e regulatório de proteção das crianças e adolescentes é a Lei n. 8.069 (Estatuto da Criança e do Adolescente - ECA), de 13 de julho de 1990. De acordo com o artigo 2º do ECA, considera-se criança a pessoa até 12 (doze) anos de idade incompletos, e adolescente aquela entre 12 (doze) doze e 18 (dezoito) dezoito anos de idade. Durante essas fases, o ser humano se encontra em desenvolvimento físico e psicológico e uma inadequada exposição de seus dados pessoais pode acarretar danos irreparáveis à sua personalidade pelo resto da vida.

No artigo 14, da LGPD, o legislador deixa claro que o tratamento de dados pessoais de crianças e adolescentes deverá ser realizado em seu **melhor interesse**. Ressalta-se ainda que, de acordo com o § 1º desse mesmo dispositivo, o tratamento de dados pessoais de **crianças deverá ser realizado com o consentimento específico e em destaque** por pelo menos um dos pais ou pelo responsável legal.

O § 5º, do art. 14, impõe o dever do controlador de realizar todos os esforços razoáveis para verificar se o consentimento específico e em destaque foi dado pelo responsável da criança e/ou do adolescente, consideradas as tecnologias disponíveis.

O § 2º, por sua vez, trata do dever dos controladores de manterem pública a informação sobre os tipos de dados coletados, a forma de sua utilização e os procedimentos para o exercício dos direitos a que se refere o art. 18 da Lei, (confirmação da existência do tratamento; acesso aos dados; correção de dados incompletos inexatos ou desatualizados; anonimização, bloqueio ou eliminação de dados desnecessários ou tratados em desconformidade com a legislação; portabilidade de dados; eliminação de dados; informações sobre o compartilhamento de dados; revogação do consentimento etc.).

Por outro lado, o § 3º, do artigo 14, evidencia a legitimidade de tratamento de dados pessoais de crianças sem consentimento, quando a coleta for necessária para contatar os pais ou o responsável legal, desde que utilizados uma única

vez e sem armazenamento, ou para sua proteção. Ao mesmo tempo impõe que, em nenhum caso, os dados podem ser repassados a terceiro, sem que exista o consentimento de pelo menos um dos pais ou pelo responsável legal.

Além disso, o legislador também ressalta no § 4º que, para a participação das crianças em jogos, aplicações de internet ou outras atividades, os controladores deverão obter apenas as informações pessoais estritamente necessárias à atividade.

Por fim, o § 6º, do artigo 14, da LGPD, esclarece o dever dos controladores de fornecerem as informações sobre o tratamento de dados de crianças e/ou adolescentes de maneira simples, clara e acessível, consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, com uso de recursos audiovisuais, quando adequado, de forma a proporcionar a informação necessária aos pais ou ao responsável legal e adequada ao entendimento da criança.

2.4. Do Término do Tratamento de Dados (Arts. 15 e 16)

O artigo 15 da LGPD exemplifica 4 (quatro) hipóteses relacionadas ao término do tratamento de dados: I - verificação de que a finalidade foi alcançada ou de que os dados deixaram de ser necessários ou pertinentes ao alcance da finalidade específica almejada; II - fim do período de tratamento; III - comunicação do titular, inclusive no exercício de seu direito de revogação do consentimento conforme disposto no § 5º do art. 8º desta Lei, resguardado o interesse público; ou IV - determinação da autoridade nacional, quando houver violação ao disposto na Lei.

Mais uma vez, a LGPD resguarda os direitos do titular dos dados, ao determinar que o tratamento deve ter prazo certo, preferencialmente, e, portanto, após a sua utilização, tais informações devem ser eliminadas[30], pois não podem ser esquecidas em algum banco de dados, tornando-se vulneráveis ao vazamento ou à utilização para finalidades diversas daquelas previstas inicialmente e não legitimadas pela Lei.

No que pertine ao inciso I, do artigo 15, destaca-se que a referida previsão está em consonância com o princípio da finalidade, disposto no artigo 6º, inciso I, da LGPD[31], afinal de contas, quando não há mais necessidade de manutenção das informações, deve-se eliminá-las de imediato.

Nesse contexto, o artigo 16 da LGPD determina que os dados pessoais serão eliminados após o término de seu tratamento, no âmbito e nos limites

30. LGPD, Art. 5º (...) XIV - eliminação: exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado;

31. LGPD, Art. 6º I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;

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.

A eliminação deve ser de forma definitiva, caso seja possível a reversão, poderá ser considerada uma pseudoanomização, como já explicado anteriormente no item 2.5 (Conceitos Específicos).

Destaca-se que a gestão documental e a proteção especial a documentos de arquivos tratados pela Administração Pública devem obedecer às disposições contidas, especialmente, na Lei Federal nº 8.159/1991, que dispõe sobre a política nacional de arquivos públicos e privados e dá outras providências. No âmbito do Estado de Alagoas, é preciso que sejam observados os seguintes diplomas normativos: a) Lei nº 6.236, de 06 de junho de 2001, que institui o Sistema de Arquivos do Estado de Alagoas; b) Lei de nº 2.428, de 30 de dezembro de 1961, que dispõe sobre a criação do Arquivo Público de Alagoas e dá outras providências; e c) Decreto nº 9.228, de 13 de dezembro de 2010, que dispõe sobre o acesso aos documentos produzidos e acumulados por órgãos de inteligência e informação, especificamente aqueles relacionados ao período do Regime Militar no Brasil e dá outras providências. Portanto, a eliminação de tais documentos deve obedecer aos dispostos nas legislações específicas.

3. Dos Direitos do Titular

3.1. Noções Gerais

A sociedade passa, atualmente, por um processo de digitalização, o qual tem modificado a dinâmica das relações intersubjetivas. As interações multiplicadas no ciberespaço exigem que a normatividade não só dê conta dos desafios de proteção dos direitos e garantias fundamentais previstos constitucionalmente, mas que promova novos arranjos para tutelar contextos antes inimagináveis sob um olhar analógico.

É o tempo de consolidação, portanto, do nominado *homo digitalis*[32], cuja conectividade plena tem impactado o Direito, independentemente da área na qual se atue. Institutos clássicos não mais são suficientes para dar conta da necessidade de responder a um cenário complexificado, de tal modo que é preciso descontruir linhas antiquadas de raciocínio e refundar premissas.

Esse novo cenário é marcado por uma produção exponencial de dados, que são diuturnamente processados por sistemas computacionais inteligentes, promovendo a identificação de padrões e classificações antes operacionalmente não factíveis. Sem dúvida, os dados constituem uma das *commodities* mais valiosas do mercado e o seu tratamento em escala tem gerado, em alguns ambientes, grandes monopólios e oligopólios deveras questionáveis sob a premissa basilar da livre concorrência. Tem-se, portanto, a tão propalada *data-driven economy*[33] ou economia orientada por dados.

Na seara pública, estão mapeados os contornos de uma governabilidade digital, em consonância com o que dispõe a Lei 14.129, de 14 de março de 2021, de tal modo que a arquitetura de políticas públicas deve ser orientada por dados, possibilitando, assim, a alocação eficiente de recursos[34].

---

32. VESTING, Thomas. *Gentleman, Gesto, Homo Digitalis: a transformação da subjetividade jurídica na modernidade*. São Paulo: Contracorrente, 2022, p. 267.

33. FRAZÃO, Ana. *Fundamentos da proteção dos dados pessoais – Noções introdutórias para a compreensão da importância da Lei Geral de Proteção de Dados*. TEPEDINO, Gustavo *et al*. Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro. 3ª ed. São Paulo: Thomson Reuters Brasil, 2023, p. 35.

34. O art. 24, VII, da Lei 14.129, de 14 de março de 2021 assim dispõe: “art. 24. VII - realizar a gestão das suas políticas públicas com base em dados e em evidências por meio da aplicação de inteligência de dados em plataforma digital;”

Alçado à condição de direito fundamental autônomo[35], a proteção de dados pessoais, cujos delineamentos estão bem esquadrinhados na Lei Geral de Proteção de Dados – LGPD (Lei nº 13.709, de 14 de agosto de 2018), tem sido objeto de reiteradas violações, no bojo da sociedade digital, de tal sorte que é preciso amadurecer as discussões sobre os mecanismos de tutela adequada deste direito.

Nessa linha de intelecção, é preciso analisar, em extensão e profundidade o capítulo próprio da LGPD, cujos termos versam sobre os direitos do titular. O artigo 17, inserido em tal contexto, busca assegurar a titularidade dos dados pessoais e garantir os direitos fundamentais de liberdade, de intimidade e de privacidade. Considerando que a lei protege, exclusivamente, dados de pessoa natural, não cabe cessão ou transferência da titularidade, nos termos do artigo 11 do Código Civil, sob pena de os negócios jurídicos serem considerados nulos.[36]

Além dos artigos 17 ao 22, do Capítulo III – Dos Direitos do Titular, a LGPD descreve, em outros dispositivos (Art. 6º, I-X; Arts. 7º, I, e 8º; Art. 7º, III e IV; Art. 7º, § 6º; Art. 8º, §§ 2º, 4º e 5º; Art. 9º, § 1º; Art. 16), direitos subjetivos da pessoa natural, titular dos dados tratados, em face daqueles responsáveis pelo controle de dados.[37]

Portanto, o rol dos direitos elencados no Capítulo III – Dos Direitos do Titular é meramente exemplificativo, devendo o intérprete analisar todo o arcabouço legal, incluindo os objetivos, fundamentos e princípios, a fim de assegurar o pleno atendimento da tutela dos dados pessoais.

3.2. Dos direitos específicos

3.2.1. Direito à confirmação da existência de tratamento

O inciso I, do artigo 18, da LGPD descreve o primeiro direito específico do titular de dados pessoais, qual seja o de obter do controlador, em relação aos dados tratados, a qualquer momento e mediante requisição, a confirmação da

35. Antes mesmo da edição da Emenda Constitucional nº 115, de 10 de fevereiro de 2022, que, dentre outras alterações, acresceu o inciso LXXIX, ao art. 5º da Constituição Federal, com o objetivo de categorizar a proteção de dados pessoais como um direito fundamental, o Supremo Tribunal Federal já reconhecia a autonomia desse direito em relação à privacidade e à intimidade, nos termos do que restou pronunciado nas Ações Diretas de Inconstitucionalidade n. 6387, 6388, 6389, 6393 e 6390. Nesse sentido, é valido destacar excerto do inteiro teor do acórdão: "A proteção de dados pessoais e a autodeterminação informativa são direitos fundamentais autônomos, que envolvem uma tutela jurídica e âmbito de incidência específicos. Esses direitos são extraídos da interpretação integrada da garantia da inviolabilidade da intimidade e da vida privada (art. 5º, X), do princípio da dignidade da pessoa humana (art. 1º, III) e da garantia processual do habeas data (art. 5º, LXXII), todos previstos na Constituição Federal de 1988." (ADI 6387 MC-Ref, Relator(a): ROSA WEBER, Tribunal Pleno, julgado em 07/05/2020, PROCESSO ELETRÔNICO DJe-270 DIVULG 11-11-2020 PUBLIC 12-11-2020)

36.COTS, Márcio; OLIVEIRA, Ricardo. Lei geral de proteção de dados pessoais comentada. 3ª edição. São Paulo: Thomson Reuters Brasil, 2019. p. 126.

37. FEIGELSON, Bruno;Becker, DANIEL; CAMARINHA, Sylvia, coordenadores. Comentários à lei geral de proteção de dados: Lei 13.709/2018. São Paulo: Thomson Reuters Brasil, 2020. p.83-85.

existência de tratamento.

Trata-se de um direito bastante simples de ser exercido, sem necessidade de nenhuma justificativa por parte do titular, em consonância com o princípio do livre acesso e da transparência, dispostos no artigo 6º, IV e VI, da LGPD.

Os incisos I e II do artigo 19 buscam detalhar a forma e modo para o exercício do direito em questão, nos seguintes termos: 1) O titular receberá imediatamente as informações, quando optar pelo formato simplificado; e 2) Caso o titular deseje que seja emitida declaração completa[38], o controlador deverá atender o pedido no prazo de 15 (quinze) dias, contado da data do requerimento, mas a autoridade nacional poderá prever prazos diferentes para determinados setores, considerando a realidade destes e o volume de requisições.[39]

O artigo 18, §5º[40], determina que o exercício desse direito deve ser gratuito.

3.2.2. Direito de acesso aos dados

O artigo 18, II, da LGPD, descreve o segundo direito específico do titular, qual seja o de obter do controlador, a qualquer momento e mediante requisição, o acesso aos seus dados.

Como se pode observar, tal direito pressupõe o conhecimento prévio por parte do titular da existência de tratamento dos dados pessoais. O requerimento de acesso aos dados, que pode ser parcial ou integral, está em consonância com os princípios do livre acesso e da transparência, dispostos no artigo 6º, IV e VI, da LGPD, respectivamente[41].

O artigo 9º, da LGPD, em reforço à previsão inserta no art. 18, II, destaca que o titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva, conforme características já citadas no item 3.2.8. Ademais, o artigo 19 também densifica a garantia de que o acesso às informações será imediato, se as informações forem simples e não demandarem nenhuma diligência, ou no prazo de 15 (quinze) dias, caso as informações sejam completas, conforme já descrito no item anterior.

Com a nítida intenção de facilitar o exercício do direito de acesso às informações, os §§ 1º e 2º, do artigo 19, indicam que os dados podem ser fornecidos por qualquer meio, seja eletrônico ou impresso, a critério do titular. Quando

38. LGPD, Art. 19. A confirmação de existência ou o acesso a dados pessoais serão providenciados, mediante requisição do titular: (...) II - por meio de **declaração clara e completa, que indique a origem dos dados, a inexistência de registro, os critérios utilizados e a finalidade do tratamento, observados os segredos comercial e industrial,** fornecida no prazo de até 15 (quinze) dias, contado da data do requerimento do titular.

39.COTS, Márcio; OLIVEIRA, Ricardo. Lei geral de proteção de dados pessoais comentada. 3ª edição. São Paulo: Thomson Reuters Brasil, 2019. p. 135.

40. LGPD, Art. 18, § 5º O requerimento referido no § 3º deste artigo será atendido sem custos para o titular, nos prazos e nos termos previstos em regulamento.

41. LGPD, Art. 6º (...) VI - 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;

o tratamento tiver origem no consentimento do titular ou em contrato, o titular poderá solicitar cópia eletrônica integral de seus dados pessoais, observados os segredos comercial e industrial, nos termos de regulamentação da autoridade nacional, em formato que permita a sua utilização subsequente, inclusive em outras operações de tratamento.

Os artigos 6º, IV, e 18, §5º[42], determinam que o exercício do direito de acesso às informações deve ser gratuito.

3.2.3. Direito de correção de dados incompletos, inexatos ou desatualizados

O inciso III, do artigo 18, da LGPD, descreve o direito específico do titular de dados pessoais de obter do controlador, a qualquer momento e mediante requisição, a correção de dados incompletos, inexatos ou desatualizados.

Percebe-se que este direito está em consonância com o princípio da qualidade dos dados, disposto no artigo 6º, V, da LGPD.[43]

Nesse contexto, é primordial o exercício desse direito, até porque a falta de exatidão das informações pode propiciar um ambiente mais profícuo para a proliferação de fraudes.

Assim, mediante requisição do titular, a qualquer tempo, os dados pessoais podem ser completados, corrigidos ou atualizados, por decorrência, muitas vezes, da vida cotidiana, como mudança de nome no casamento, alteração de endereço ou telefone, tr de gênero etc.

O artigo 18, §5º, determina que o exercício desse direito deve ser gratuito.

Por fim, o artigo 18, §6º, determina que o responsável deverá informar, de maneira imediata, aos agentes de tratamento com os quais tenha realizado uso compartilhado de dados, a correção, para que repitam idêntico procedimento, exceto nos casos em que esta comunicação seja comprovadamente impossível ou implique esforço desproporcional.

3.2.4. Direito de anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto na LGPD

O inciso IV, do artigo 18, da LGPD, pode ser desdobrado em 3 (três) direitos do titular de dados, quais sejam: a) anonimização; b) bloqueio e c) eliminação. Tais direitos serão exercidos, quando a operação de tratamento envolver dados desnecessários, excessivos ou nas hipóteses de ações desenvolvidas pelo controlador que sejam contrárias à LGPD.

O primeiro deles assegura ao titular dos dados pessoais a anonimização

42. LGPD, Art. 18, § 5º O requerimento referido no § 3º deste artigo será atendido sem custos para o titular, nos prazos e nos termos previstos em regulamento.

43. LGPD, Art. 18 V - 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;

de suas informações, nos termos dos artigos 5º, III, e 12, e do item 2.5 desta cartilha.

Parte-se da ideia de que o dado anonimizado é aquele que, definitivamente, não possibilita mais a identificação do seu titular, o que difere da pseudonimização, pois, neste caso, o processo pode ser revertido.

O exercício do direito à anonimização não se dá de forma irrestrita, em algumas hipóteses relevantes, de acordo com os artigos 7º, IV, 11, II, c, 13, caput, e 16, II, da LGPD, não será exigível do controlador a adoção do processo de anonimização, se este se mostrar impossível.

O segundo direito é o de bloqueio, nos termos do artigo 5º, XIII, da LGPD, e do item 2.5- Conceitos Específicos desta cartilha, que pode ser assim definido: suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados.

Por último, tem-se o direito à eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto na LGPD, nos termos do artigo 6º, III. Assim, diante da plausabilidade do requerimento feito pelo titular, o controlar deverá eliminar esses dados, salvo justificativa legal.

O artigo 18, § 5º, determina que o exercício desses direitos deve ser gratuito.

3.2.5. Direito de portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial

O inciso V, do artigo 18, da LGPD, descreve o direito específico do titular de dados pessoais de obter do controlador, a qualquer momento e mediante requisição, a portabilidade dos seus dados para outro fornecedor de serviço ou produto, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial.

É frequente o exercício desse direito, na vida cotidiana dos indivíduos, como ocorre nos casos de portabilidade de salários de uma instituição bancária para outra, de números telefônicos de uma operadora de telefonia móvel para outra etc. Dessa forma, a LGPD confere ao titular de dados o direito de requerer a portabilidade de dados, de forma mais livre, tranquila e estruturada.

O artigo 18, § 5º, determina que o exercício desse direito deve ser gratuito.

Ressalta-se que não cabe a portabilidade, quando os dados já tiverem sido anonimizados pelo controlador.[44]

44. LGPD, Art. 18, § 7º A portabilidade dos dados pessoais a que se refere o inciso V do caput deste artigo não inclui dados que já tenham sido anonimizados pelo controlador.

3.2.6. Direito à eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 da LGPD

O inciso VI, do artigo 18, da LGPD, descreve o sexto direito específico do titular de dados pessoais, qual seja o de obter do controlador, a qualquer momento e mediante requisição, a eliminação dos dados pessoais tratados com o seu consentimento, exceto nas hipóteses previstas no art. 16 da LGPD.

Primeiramente, cumpre frisar que a eliminação de dados é medida indispensável, seja por revogação ou pelo término do prazo de tratamento. A eliminação tratada anteriormente, no item 4.2.4, está relacionada com informações desnecessárias, excessivas ou inexatas. Por sua vez, a hipótese atual versa sobre a eliminação de informações que foram tratadas com o consentimento do titular.

Nesse contexto, como ressaltado em linhas pretéritas, engloba-se, no presente caso, os tratamentos de dados que tiveram como base legal o consentimento do titular, na forma do artigo 7º, I. A partir do momento que o titular subtrai o seu consentimento, ele terá o direito de requerer a eliminação dos seus dados pessoais, exceto nas hipóteses previstas no artigo 16, em que é autorizada a conservação dos dados, após o esgotamento da sua finalidade, em decorrência de: 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, conforme já descrito no item 3.5 desta cartilha.

É importante destacar que, caso não seja possível a eliminação, conforme hipóteses acima descritas, o controlador imediatamente deve informar e justificar a recusa.

O artigo 18, § 5º, determina que o exercício desse direito deve ser gratuito.

3.2.7. Direito à informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados

O inciso VII, do artigo 18, da LGPD, trata do direito específico do titular de dados pessoais de obter do controlador, a qualquer momento e mediante requisição, informações das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados[45].

Trata-se de direito corolário do princípio da transparência, nos termos do artigo 6º, VI, da LGPD.

A partir do instante em que a lei autoriza o uso compartilhado de dados, ela também se preocupa em assegurar ao titular a possibilidade de obter informações acerca do compartilhamento. Com isso, garante-se, em amplitude, a

45. LGPD, Art. 5º, XVI

autodeterminação informacional.

Nessa linha de intelecção, em acréscimo às considerações pretéritas, cumpre destacar o teor do § 6º, do artigo 18, da LGPD: "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."

O artigo 18, § 5º, determina que o exercício desse direito deve ser gratuito.

3.2.8. Direito à informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa

O inciso VIII, do artigo 18, da LGPD, versa sobre o direito específico do titular de dados pessoais de obter do controlador, a qualquer momento e mediante requisição, a informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa.

Trata-se de direito que também deriva do princípio da transparência, nos termos do artigo 6º, VI, da LGPD, pois, ao titular, a partir de informações claras, precisas e facilmente acessíveis, será assegurada a possibilidade do não fornecimento do consentimento, mediante a apresentação das consequências da sua negativa. Tais informações devem ser prestadas de forma antecipada, preferencialmente.

O artigo 18, § 5º, determina que o exercício desse direito deve ser gratuito.

3.2.9. Direito à revogação do consentimento

O inciso IX, do artigo 18, da LGPD, regula o direito específico do titular de dados pessoais de revogar o seu consentimento, nos termos do § 5º do art. 8º da LGPD.

Trata-se de reiteração de direito já descrito no artigo 8º, § 5º, da LGPD. Assim, o consentimento pode ser revogado, a qualquer momento, mediante manifestação expressa do titular, por procedimento gratuito e facilitado, ratificados os tratamentos realizados sob o amparo do consentimento anteriormente manifestado.

O artigo 18, § 5º, determina que o exercício desse direito deve ser gratuito.

Outro ponto que merece destaque é o artigo 64 da LGPD, cujo teor é adiante transcrito: "Os direitos e princípios expressos nesta Lei não excluem outros previstos no ordenamento jurídico pátrio relacionados à matéria ou nos tratados internacionais em que a República Federativa do Brasil seja parte." Como exemplo, pode-se destacar a Lei n. 12.965/2014 (Marco Civil da Internet), que, mesmo após a edição da LGPD, permanece vigente, de tal modo que devem ser respeitados seus princípios, suas garantias, bem como observados os direitos

e deveres para o uso da internet no Brasil, notadamente no que pertine à privacidade e à proteção de dados pessoais.

Apresenta-se, a título de encerramento, um quadro-resumo dos direitos específicos do titular de dados pessoais, em conformidade com o artigo 18 da LGPD:

[Início Tabela 9]

DIREITOS ESPECÍFICOS	FUNDAMENTO LEGAL
Direito à confirmação da existência de tratamento.	Art. 18, I
Direito de acesso aos dados.	Art. 18, II
Direito de correção de dados incompletos, inexatos ou desatualizados.	Art. 18, III
Direito de anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto na LGPD.	Art. 18, IV
Direito de portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial.	Art. 18, V
Direito à eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 da LGPD.	Art. 18, VI
Direito à informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados.	Art. 18, VII
Direito à informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa.	Art. 18, VIII
Direito à revogação do consentimento, nos termos do § 5º do art. 8º da LGPD.	Art. 18, IX

4. Do Tratamento de Dados Pessoais pelo Poder Público

4.1. Noções gerais

De início, é preciso destacar que, em regra, a LGPD não exclui da sua incidência o Poder Público, na medida em que exige de todo aquele que trata dados pessoais a efetivação dos seus princípios e fundamentos, com a implantação de sistemas eficazes e seguros, desde a concepção até o término do tratamento. As situações que ensejem violação aos cânones da LGPD deverão ser apuradas, de modo a viabilizar a penalização dos agentes envolvidos, mormente quando forem constatados danos à personalidade do titular dos dados.[46]

A despeito disso, a Administração Pública possui peculiaridades, diante de seu constitucional papel de proteção do interesse coletivo, hábeis a ensejar a necessidade de estruturação de dispositivos próprios, na LGPD, a fim de resguardar o regular exercício de suas competências. Assim, é que o legislador dedicou o Capítulo IV, da Lei Geral de Proteção de Dados Pessoais, para regular o papel do Poder Público, quando atua na condição de agente de tratamento.

É preciso grafar, por oportuno, que a LGPD não incidirá, nas hipóteses descritas no inciso III do artigo 4º, quando o tratamento de dados for realizado pelo Poder Público, para fins exclusivos de: a) segurança pública; b) defesa nacional; c) segurança do Estado; ou d) atividades de investigação e repressão de infrações penais.

Por outro lado, o artigo 7º, III, da LGPD, enfatiza a proeminente base legal que autoriza a administração pública a tratar dados pessoais: "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". Isso não exclui a possibilidade de utilização de

46. "(...) na hipótese de algo se desviar do que legalmente se encontra determinado, será de rigor a adoção de medidas que busquem minorar prejuízos, apurar responsabilidades e gerar as devidas punições. Este último aspecto tem direta aplicação ao Poder Público, tendo em vista os deveres dos servidores públicos e os mecanismos para apuração e punição de eventuais desvios, sejam eles culposos ou dolosos". (OPICE, Renato. Proteção de dados: desafios e soluções na adequação à lei – Rio de Janeiro: Forense, 2020. p.87)

outras bases legais de tratamento, em situações específicas, tais como o consentimento, o legítimo interesses e o cumprimento de obrigação legal/regulatória.

O artigo 23, da LGPD, frisa que as pessoas jurídicas de direito público abrangidas pela legislação são aquelas descritas no art. 1º da Lei nº 12.527/2011 (Lei de Acesso à Informação), conforme detalhado no item 3.1.3 desta cartilha.

Ademais, o tratamento de dados pessoais implementado pela Administração deverá ser realizado em atendimento à finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público, desde que: 1) sejam informadas aos seu titulares as hipóteses em que, no exercício de suas competências, realizam o tratamento de dados pessoais, fornecendo informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos; 2) seja indicado um encarregado quando realizarem operações de tratamento de dados pessoais, nos termos do art. 39 da LGPD.

Ainda no artigo 23, o § 1º elenca a possibilidade de a Autoridade Nacional de Proteção de Dados - ANPD dispor sobre as formas de publicidade das operações de tratamento de dados pessoais realizadas pelo poder público. Os § 2º e 3º, do art. 23, preveem, respectivamente, que o disposto na LGPD não dispensa as pessoas jurídicas de direito público de instituírem as autoridades de que trata a Lei de Acesso à Informação, e que os prazos e procedimentos para o exercício dos direitos do titular perante o Poder Público observarão o disposto em legislação específica, em especial as disposições constantes da Lei do Habeas Data, da Lei Geral do processo Administrativo e da Lei de Acesso à Informação.[47]

4.2. Dos serviços notariais e de registro exercidos em caráter privado, por delegação do Poder Público

Os §§ 4 e 5º, do artigo 23, determinam que os serviços notariais e de registro exercidos em caráter privado, por delegação do Poder Público, terão o mesmo tratamento dispensado às pessoas jurídicas de direito público.

Ademais, tais órgãos devem fornecer acesso aos dados, por meio eletrônico, para a Administração Pública, tendo em vista o atendimento às finalidades coletivas.

47.FEIGELSON, Bruno; Becker, DANIEL; CAMARINHA, Sylvia, coordenadores. Comentários à lei geral de proteção de dados: Lei 13.709/2018. São Paulo: Thomson Reuters Brasil, 2020. p.106

4.3. Das empresas públicas e sociedades de economia mista

O artigo 24 da LGPD determina que as empresas públicas e sociedades de economia mista que atuam em regime de concorrência, sujeitas ao disposto no art. 173 da CF/1988[48], terão o mesmo tratamento dispensado às pessoas jurídicas de direito privado.

Por outro lado, no parágrafo único do mesmo dispositivo, a lei destaca que as empresas públicas e as sociedades de economia mista, quando estiverem operacionalizando políticas públicas e no âmbito da execução delas, terão o mesmo tratamento dispensado aos órgãos e às entidades do Poder Público.

4.4. Do formato interoperável e estruturado para o uso compartilhado de dados pessoais pelo Poder Público

O artigo 25, da LGPD, ressalta que os dados deverão ser mantidos em formato interoperável e estruturado para o uso compartilhado, com vistas à execução de políticas públicas, à prestação de serviços públicos, à descentralização da atividade pública e à disseminação e ao acesso das informações pelo público em geral. No mesmo sentido, está delineado o art. 38, da Lei nº 14.129/21 (Lei do Governo Digital):

Art. 38. Os órgãos e as entidades responsáveis pela prestação digital de serviços públicos detentores ou gestores de bases de dados, inclusive os controladores de dados pessoais, conforme estabelecido pela **Lei nº 13.709, de 14 de agosto de 2018** (Lei Geral de Proteção de Dados Pessoais), deverão gerir suas ferramentas digitais, considerando:

I - **a interoperabilidade de informações e de dados sob gestão dos órgãos e das entidades referidos no art. 2º desta Lei, respeitados as**

48. CF/88, Art. 173. Ressalvados os casos previstos nesta Constituição, a exploração direta de atividade econômica pelo Estado só será permitida quando necessária aos imperativos da segurança nacional ou a relevante interesse coletivo, conforme definidos em lei. § 1º A lei estabelecerá o estatuto jurídico da **empresa pública, da sociedade de economia mista** e de suas subsidiárias que explorem atividade econômica de produção ou comercialização de bens ou de prestação de serviços, dispondo sobre: I - sua função social e formas de fiscalização pelo Estado e pela sociedade; II - a sujeição ao regime jurídico próprio das empresas privadas, inclusive quanto aos direitos e obrigações civis, comerciais, trabalhistas e tributários; III - licitação e contratação de obras, serviços, compras e alienações, observados os princípios da administração pública; IV - a constituição e o funcionamento dos conselhos de administração e fiscal, com a participação de acionistas minoritários; V - os mandatos, a avaliação de desempenho e a responsabilidade dos administradores. § 2º As empresas públicas e as sociedades de economia mista não poderão gozar de privilégios fiscais não extensivos às do setor privado. § 3º A lei regulamentará as relações da empresa pública com o Estado e a sociedade. § 4º A lei reprimirá o abuso do poder econômico que vise à dominação dos mercados, à eliminação da concorrência e ao aumento arbitrário dos lucros. § 5º A lei, sem prejuízo da responsabilidade individual dos dirigentes da pessoa jurídica, estabelecerá a responsabilidade desta, sujeitando-a às punições compatíveis com sua natureza, nos atos praticados contra a ordem econômica e financeira e contra a economia popular.

restrições legais, os requisitos de segurança da informação e das comunicações, as limitações tecnológicas e a relação custo-benefício da interoperabilidade; (Grifos nossos)

No caput do artigo 26, observa-se que o uso compartilhado deve atender a finalidades específicas de execução de políticas públicas e atribuição legal pelos órgãos e pelas entidades públicas, respeitados os princípios de proteção de dados pessoais elencados no art. 6º, conforme descrito no item 2.6 desta Cartilha.

Neste sentido, o Supremo Tribunal Federal, no bojo da ADI 6649, validou o compartilhamento de dados pessoais, no âmbito da Administração Pública, estabelecendo alguns parâmetros de observância cogente[49]:

respeito aos princípios da finalidade, adequação e necessidade, nos termos do art. 6º, I, II e III, da LGPD;

cumprimento integral dos requisitos, garantias e procedimentos estabelecidos na Lei Geral de Proteção de Dados, no que for compatível com o setor público;

rigorosa observância do art. 23, I, da LGPD, o qual determina a publicidade das hipóteses em que cada entidade governamental compartilha ou tem acesso a banco de dados pessoais;

o compartilhamento de informações pessoais em **atividades de inteligência** deve observar a adoção de medidas proporcionais e estritamente necessárias ao atendimento do interesse público; a instauração de procedimento administrativo formal, acompanhado de prévia e exaustiva motivação, para permitir o controle de legalidade pelo Poder Judiciário; a utilização de sistemas eletrônicos de segurança e de registro de acesso, inclusive para efeito de responsabilização em caso de abuso;

o tratamento de dados pessoais promovido por órgãos públicos ao arrepio dos parâmetros legais e constitucionais importará a responsabilidade civil do Estado pelos danos suportados pelos particulares, na forma dos arts. 42 e seguintes da Lei 13.709/2018, associada ao exercício do direito de regresso contra os servidores e agentes políticos responsáveis pelo ato ilícito, em caso de culpa ou dolo; e

a transgressão dolosa ao dever de publicidade estabelecido no art. 23, inciso I, da LGPD, fora das hipóteses constitucionais de sigilo, importará a responsabilização do agente estatal por ato de improbidade administrativa, nos termos do art. 11, inciso IV, da Lei 8.429/92, sem prejuízo da aplicação das sanções disciplinares previstas nos estatutos dos servidores públicos federais, municipais e estaduais.

O § 1º do artigo 26 veda, em regra, a transferência de dados pessoais das entidades públicas para as entidades privadas, ressalvadas as 4 (quatro) exceções adiante listadas: 1) em casos de execução descentralizada de atividade

49. ADI 6649, Relator(a): GILMAR MENDES, Tribunal Pleno, julgado em 15/09/2022, PROCESSO ELETRÔNICO DJe-s/n DIVULG 16-06-2023 PUBLIC 19-06-2023

pública que exija a transferência, exclusivamente para esse fim específico e determinado, observado o disposto na Lei de Acesso à Informação; 2) nos casos em que os dados forem acessíveis publicamente, observadas as disposições da LGPD; 3) quando houver previsão legal ou a transferência for respaldada em contratos, convênios ou instrumentos congêneres; 4) na hipótese de a transferência dos dados 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. O § 2º, por sua vez, determina que os contratos e convênios referenciados no item 3 deverão ser comunicados à ANPD.

Cumpre destacar, ainda, que a comunicação ou o uso compartilhado de dados pessoais de pessoa jurídica de direito público a pessoa de direito privado será informado à autoridade nacional e dependerá de consentimento do titular, exceto: I - nas hipóteses de dispensa de consentimento previstas na Lei; II - nos casos de uso compartilhado de dados, em que será dada publicidade, desde que sejam informadas as hipóteses em que, no exercício de suas competências, realizam o tratamento de dados pessoais, fornecendo informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos; ou III - nas exceções constantes do § 1º do art. 26, citadas no parágrafo anterior.

4.5. Da fiscalização e responsabilidade

O artigo 29 da LGPD autoriza a autoridade nacional solicitar, a qualquer momento, aos órgãos e às entidades do poder público a realização de operações de tratamento de dados pessoais, informações específicas sobre o âmbito e a natureza dos dados e outros detalhes do tratamento realizado e poderá emitir parecer técnico complementar para garantir o cumprimento da LGPD.

No tocante às responsabilidades imputadas ao Poder Público pelas atividades de tratamento realizadas, os artigos 31 e 32, da LGPD, destacam a possibilidade de a ANPD enviar informe com medidas cabíveis para fazer cessar eventual a violação, bem como solicitar a agentes do Poder Público a publicação de relatórios de impacto à proteção de dados pessoais e sugerir a adoção de padrões e de boas práticas para os tratamentos de dados pessoais pelo Poder Público.[50]

50. "Vislumbram-se nesses dispositivos a base legal para a eventual responsabilização pessoal dos servidores públicos cujas consutas se enquadrem na Lei de Improbidade Administrativa". FEIGELSON, Bruno; Becker, DANIEL; CAMARINHA, Sylvia, coordenadores. Comentários à lei geral de proteção de dados: Lei 13.709/2018. São Paulo: Thomson Reuters Brasil, 2020. p.118.

5. Dos Agentes de Tratamento de Dados Pessoais

5.1. Do controlador e do operador

Antes de iniciar a explicação deste item, convém recordar que os incisos VI, VII, VIII e IX, do artigo 5º, da LGPD, destacam o conceito de controlador, operador, encarregado e agentes de tratamento[51], respectivamente.

A LGPD destina os artigos 37 a 45, do capítulo VI, para tratar, em especial, das obrigações e responsabilidades dos agentes de tratamento de dados pessoais.

O artigo 37 determina como primeira obrigação do controlador e do operador a manutenção do registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseadas no legítimo interesse. Nesse ponto, ressalta-se que o conceito de interesse legítimo foi abordado no item 3.1.9, em consonância com o artigo 10 da LGPD.

À luz dos princípios que regem a proteção de dados pessoais, como a finalidade, adequação, necessidade, transparência, segurança, responsabilização e prestação de contas, dispostos nos artigos 6º da Lei, fica evidente que a obrigação outrora mencionada também tem o objetivo de possibilitar a fiscalização da ANPD.

Além disso, quando houver determinação da ANPD, o controlador é obrigado a elaborar relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente a suas operações de tratamento de dados, nos termos de regulamento, observados os segredos comercial e industrial, em consonância com o artigo 38. O relatório deve conter, no mínimo, a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados.

51. Art. 5º Para os fins desta Lei, considera-se: (...) VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais; VII - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador; VIII - encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD); IX - agentes de tratamento: o controlador e o operador;

No caso do operador, o artigo 39 determina que este deverá realizar o tratamento, segundo as instruções fornecidas pelo controlador, que verificará a observância das próprias instruções e das normas sobre a matéria.

Para finalizar este item, cumpre destacar que o artigo 40, da LGPD, trata do direito à portabilidade. Para tornar possível tal direito, a lei deixa claro que os dados pessoais pertencem ao seu titular, de forma que a destinação destes está sob o seu regular controle.[52]

5.1.1. Da Responsabilidade

A Seção III, do Capítulo VI, da LGPD, trata da responsabilidade civil dos agentes de tratamento, bem como do eventual ressarcimento de danos.

No artigo 42, a lei determina que, se em razão do exercício de atividade de tratamento de dados pessoais, o controlador ou o operador causar dano a outrem (patrimonial, moral, individual ou coletivo), em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo. Trata-se de uma responsabilização ampla que envolve os danos patrimoniais ou morais, bem como danos individuais ou coletivos.

Em seguida, no § 1º do mesmo dispositivo, a LGPD cria 2 (duas) hipóteses de responsabilidade solidária: 1) do **operador com o controlador** pelos danos causados, podendo o titular dos danos responsabilizar ambos ou qualquer deles, de forma integral, quando o operador descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador, hipótese em que o operador se equipara ao controlador, salvo nos casos de exclusão previstos no art. 43; e 2) dos **controladores** que estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados, salvo nos casos de exclusão previstos no art. 43. O § 4º, por sua vez, versa sobre o direito de regresso daquele que reparou o dano contra os demais responsáveis, na medida de suas respectivas participações na prática do ato ilícito.

No contexto da produção de prova judicial, o § 2º trata da possibilidade de aplicação do instituto da inversão do ônus da prova, a fim de assegurar efetividade à proteção dos dados pessoais, principalmente diante de situações de vulnerabilidade e hipossuficiência dos titulares, em face de sociedade empresárias ou do Poder Público.

A lei também elenca algumas hipóteses excludentes de responsabilidade dos agentes de tratamento, desde que seja provado: I - que não realizaram o tratamento de dados pessoais que lhes é atribuído; II - que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados; ou III - que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiro.

52.MALDONADO, Viviane; BLUM, Renato, coordenadores. Lei Geral de Proteção de Dados Comentada. São Paulo: Thomson Reuters, 2019. p.311.

Para uma melhor compreensão, a lei conceitua, no artigo 44, que o tratamento de dados irregular ocorre quando os operadores deixarem de observar a legislação ou quando não fornecerem a segurança que o titular dele pode esperar, consideradas as circunstâncias relevantes, entre as quais: I - o modo pelo qual é realizado; II - o resultado e os riscos que razoavelmente dele se esperam; III - as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado. Já o parágrafo único do dispositivo mencionado destaca que: "Responde pelos danos decorrentes da violação da segurança dos dados o controlador ou o operador que, ao deixar de adotar as medidas de segurança previstas no art. 46 desta Lei, der causa ao dano."

Ressalta-se, ao final, que o artigo 45 positivou que, diante de relações de consumo, prevalecem as regras de responsabilidade previstas no Código de Defesa do Consumidor.

5.2. Do encarregado

É preciso destacar, preliminarmente, que a LGPD não incluiu o encarregado como agente de tratamento, nos termos do artigo 5º, IX. Com isso, o que se pode depreender é que o encarregado não está diretamente envolvido no tratamento de dados pessoais, pois atua como um canal de comunicação entre o controlador, os titulares dos dados e a ANPD.

Cabe ao controlador promover a indicação do encarregado, na forma do artigo 41. Ademais, no § 1º do mesmo dispositivo, destaca-se que, após a indicação, a identidade e as informações de contato do encarregado deverão ser divulgadas publicamente, de forma clara e objetiva, preferencialmente no sítio eletrônico do controlador.

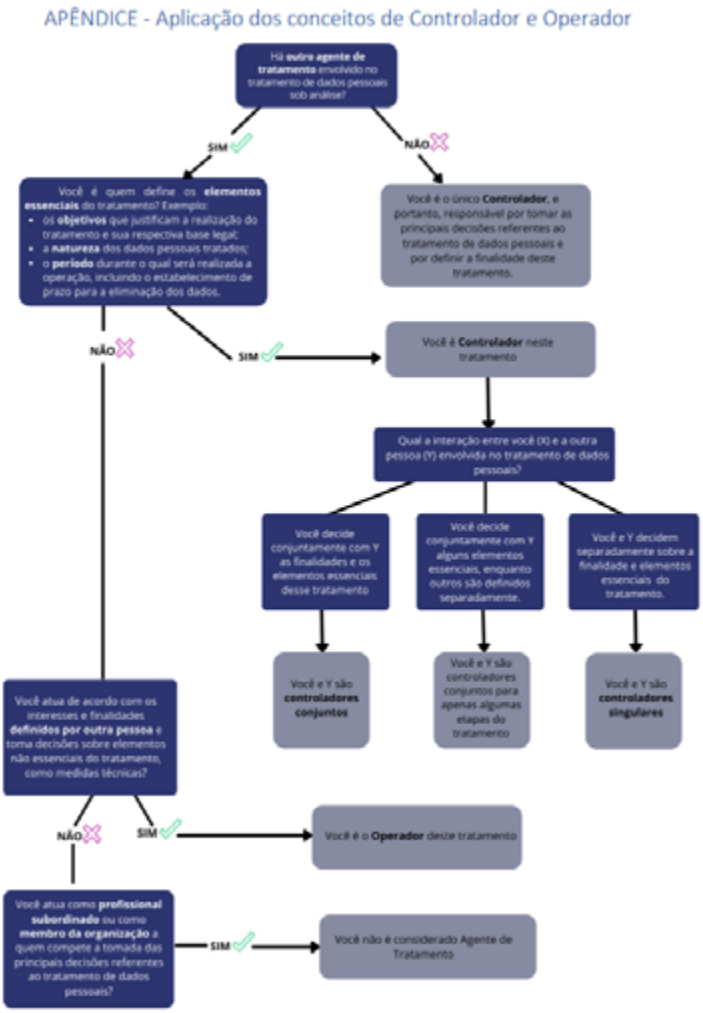
De forma destacada, no § 2º, do art. 41, a LGPD lista as atribuições do encarregado, as quais seguem adiante grafadas: I - aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências; II - receber comunicações da autoridade nacional e adotar providências; III - orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e IV - executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.

Ao final, o § 3º, do artigo 41, deixa claro que nem sempre será obrigatória a indicação de encarregado, mas compete à ANPD estabelecer hipóteses de dispensa da necessidade de sua indicação, conforme a natureza e o porte da entidade ou o volume de operações de tratamento de dados.

Não obstante a LGPD tenha apenas abordado a responsabilidade civil do controlador e operador, entende-se que o encarregado está também sujeito a responder por seus atos na esfera cível, administrativa ou penal, em decorrência de irregularidades ou má execução de suas atribuições, contudo o seu

fundamento é extraído de outras previsões normativas, tal como o disposto nos artigos 186, 187 e 927 do Código Civil, no artigo 13 do Código Penal, na Lei de Improbidade Administrativa (8.429/92) e nas legislações próprias que regem a atuação dos servidores públicos.[53]

Enfeixando tais considerações, cumpre colacionar quadro esquemático estruturado pela ANPD que bem delineia os papéis dos agentes de tratamento[54]:



53.COTS, Márcio; OLIVEIRA, Ricardo. Lei geral de proteção de dados pessoais comentada. 3ª edição. São Paulo: Thomson Reuters Brasil, 2019. p.177-178.

54. https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia_agentes_de_tratamento_e_encarregado___defeso_eleitoral.pdf. Acesso em 24/10/2023.

6. Da Segurança e das Boas Práticas

6.1. Das medidas de segurança e padrões técnicos

O artigo 6º, VII, da LGPD, dispõe sobre o princípio da segurança, a fim de reforçar a importância de utilização de medidas técnicas e administrativas aptas a protegerem os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão.

Por isso, o capítulo VII, da LGPD, está destinado, notadamente, a tratar das medidas de segurança e boas práticas que devem ser adotadas pelos agentes de tratamento de dados pessoais. O artigo 46, por exemplo, impõe que os agentes de tratamento possuam estrutura necessária à tutela dos dados, impedindo, por exemplo, situações de vazamento.

O § 1º, do art. 46, da LGPD, confere à ANPD o poder de dispor sobre padrões técnicos mínimos para tornar mais seguro o controle de acessos aos dados, evitando o vazamento ou perda destes, especialmente quando se estiver a tratar de dados sensíveis.

Convém citar, por oportuno, que, no Marco Civil da Internet, existe título específico "Da Proteção aos Registros, aos Dados Pessoais e às Comunicações Privadas", o qual poderá ser utilizado, subsidiariamente, na falta de norma regulamentadora sobre a matéria, bem como servir de referencial de boas práticas.[55]

Por fim, o § 2º, do art. 44, da LGPD, versa sobre o moderno conceito de *privacy by design*[56], quando descreve que os agentes de tratamento deverão observar as medidas de segurança, técnicas e administrativas, desde a fase de concepção do produto ou do serviço até a sua execução.

55.COTS, Márcio; OLIVEIRA, Ricardo. Lei geral de proteção de dados pessoais comentada. 3ª edição. São Paulo: Thomson Reuters Brasil, 2019. p.193.

56. "(...) Busca-se, assim, a criação de confiança não apenas no método, no procedimento de coleta e tratamento de dados, mas também na própria arquitetura do sistema. Objetiva-se com a chamada *privacy by design* dar ao usuário mais ferramentas de confiança na rede." (DONEDA, Danilo ... (et al.). Tratado de proteção de dados pessoais. Rio de Janeiro: Forense, 2021. p.450)

6.2. Da garantia da segurança da informação e comunicação em caso de acidentes

O artigo 47 dispõe acerca da obrigatoriedade, tanto do controlador/operador quanto de qualquer outra pessoa, de garantia da segurança dos dados pessoais, em todas as fases do tratamento, mesmo após o seu término.

Constata-se, com esse dispositivo, que a obrigação de segurança da informação perdura mesmo após o término do tratamento, o que faz necessária a referência aos artigos 15 e 16 da Lei, descritos no item 3.4 desta Cartilha, os quais regulam as normas específicas acerca do fim do tratamento.

Ainda sob o aspecto da segurança, à luz do princípio da transparência, o artigo 48 determina que, quando ocorrer incidente de segurança que possa acarretar risco ou dano relevante aos titulares, o controlador deverá comunicar à autoridade nacional e ao titular a ocorrência. Nos termos do § 1º, a comunicação ocorrerá em prazo razoável, definido pela autoridade nacional, e deverá mencionar, no mínimo: I - a descrição da natureza dos dados pessoais afetados; II - as informações sobre os titulares envolvidos; III - a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial; IV - os riscos relacionados ao incidente; V - os motivos da demora, no caso de a comunicação não ter sido imediata; e VI - as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.

Nesse cenário, na forma do § 2º do mesmo dispositivo, a autoridade nacional verificará a gravidade do incidente e poderá, caso necessário, para a salvaguarda dos direitos dos titulares, determinar ao controlador a adoção de providências, tais como: I - ampla divulgação do fato em meios de comunicação; e II - medidas para reverter ou mitigar os efeitos do incidente.

A ANPD, nos termos do §3º do mesmo dispositivo, ao realizar o juízo de gravidade do incidente, avaliará eventual comprovação de que foram adotadas medidas técnicas adequadas que tornem os dados pessoais afetados ininteligíveis, no âmbito e nos limites técnicos de seus serviços, para terceiros não autorizados a acessá-los.

Ressalta-se que os sistemas utilizados para o tratamento de dados pessoais devem ser estruturados de forma a atender aos requisitos de segurança, aos padrões de boas práticas e de governança e aos princípios gerais previstos na Lei e às demais normas regulamentares, em consonância com o artigo 49.

Consideram-se como padrões de boas práticas e de governança aqueles reconhecidos mundialmente, como, por exemplo, a Norma Técnica ABNT NBR ISSO/IEC 27002, a capacitação de empregados, a adoção de políticas internas de segurança e informação e de proteção de dados pessoais etc.[57]

57.MALDONADO, Viviane; BLUM, Renato, coordenadores. Lei Geral de Proteção de Dados Comentada. São Paulo: Thomson Reuters, 2019. p.348.

Ademais, como mencionado antes, os princípios que regem a proteção de dados pessoais são aqueles insertos nos incisos I ao X do artigo 6º (finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação, bem como responsabilização e prestação de contas). Já as demais normas regulamentadoras são aquelas que criadas, principalmente pela ANPD, a fim de implementar e fiscalizar o cumprimento da LGPD, tal como o enunciado CD/ANPD nº 01, de 22 de maio de 2023, cujos termos estão assim lavrados: "O tratamento de dados pessoais de crianças e adolescentes poderá ser realizado com base nas hipóteses legais previstas no art. 7º ou no art. 11 da Lei Geral de Proteção de Dados Pessoais (LGPD), desde que observado e prevalecente o seu melhor interesse, a ser avaliado no caso concreto, nos termos do art. 14 da Lei."

6.3. Das boas práticas e da governança

Em decorrência da importância de estimular culturalmente os indivíduos quanto à proteção de dados pessoais, a LGPD possui uma seção específica para tratar de boas práticas e governança, as quais estão descritas nos artigos 50 e 51.

Logo no caput do artigo 50, constata-se que há permissão, e não obrigatoriedade, dos controladores e operadores, individualmente ou por meio de associações, formularem regras de boas práticas e de governança, que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais.

Quando do estabelecimento de regras de boas práticas, tanto no tocante à procedimentalização do tratamento quanto aos dados, os agentes devem levar em consideração a natureza, o escopo, a finalidade e a probabilidade e a gravidade dos riscos e dos benefícios decorrentes de tratamento de dados do titular, na forma do § 1º do artigo 50.

O inciso I, do § 2º, do art. 50, da LGPD, prevê que os agentes de tratamento, ao implementarem programa de governança em privacidade, devem atentar aos seguintes requisitos mínimos: a) demonstre o comprometimento do controlador em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais; b) seja aplicável a todo o conjunto de dados pessoais que estejam sob seu controle, independentemente do modo como se realizou sua coleta; c) seja adaptado à estrutura, à escala e ao volume de suas operações, bem

como à sensibilidade dos dados tratados; d) estabeleça políticas e salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade; e) tenha o objetivo de estabelecer relação de confiança com o titular, por meio de atuação transparente e que assegure mecanismos de participação do titular; f) esteja integrado a sua estrutura geral de governança e estabeleça e aplique mecanismos de supervisão internos e externos; g) conte com planos de resposta a incidentes e remediação; e h) seja atualizado constantemente com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas.

O § 3º do mesmo dispositivo determina que as regras de boas práticas e de governança deverão ser publicadas e atualizadas periodicamente e poderão ser reconhecidas e divulgadas pela autoridade nacional.

É imperioso destacar, em relação ao tema, que a ANPD observará a adoção de políticas de boas práticas e governança quando da aplicação de sanções administrativas, nos termos do art. 52, §1º, VIII e IX.

Além disso, a Lei busca estimular a cultura institucional de proteção de dados, no âmbito da Administração Pública, pois permite que a ANPD solicite aos agentes do Poder Público a publicação de relatórios de impacto à proteção de dados pessoais, bem como sugira a adoção de padrões e de boas práticas para os tratamentos de dados pelo Poder Público. [58]

Como já tratado no item 7.2 desta Cartilha, a adoção de boas práticas e governança deve ser observada sob o filtro do *privacy by design*, por se tratar de um padrão de estruturação dos sistemas de tratamento de dados pessoais.

Ao final, o artigo 51 ressalta a importância de a ANPD estimular a adoção de padrões técnicos que facilitem o controle pelos titulares dos seus dados pessoais.

58.DONEDA, Danilo ... (et al.). Tratado de proteção de dados pessoais. Rio de Janeiro: Forense, 2021. p.361-362.

7. Da Fiscalização e Sanções Administrativas

7.1. Noções gerais

Os artigos 52 a 54, da Seção I, do Capítulo VIII, da LGPD, positivam as sanções administrativas, quando do descumprimento da Lei.

Ressalta-se, porquanto oportuno, que os artigos 52 a 54 apenas entraram em vigor em 01 de agosto de 2021, conforme artigo 65, I-A, com a finalidade de conceder um maior tempo de adaptação das instituições ao novo regramento legal.

As sanções administrativas, dentre outras funções, destinam-se, inclusive, a evitar condutas ilícitas no futuro, uma vez que impõem, por exemplo, a necessidade de adoção de medidas de segurança, com vistas a impossibilitar futuros vazamentos de dados. O caput do artigo 52 deixa claro que as penalidades serão aplicadas apenas contra os agentes de tratamento (controlador e operador), através de regular processo administrativo instaurado pela ANPD (atualmente a Resolução nº 01, de 28 de outubro de 2021, da ANPD, regula o processo de fiscalização e sanção).

São 9 (nove) tipos de sanções administrativas dispostas na lei, quais sejam: 1) advertência, com indicação de prazo para adoção de medidas corretivas; 2) multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração; 3) multa diária, observado o limite total a que se refere o inciso II; 4) publicização da infração após devidamente apurada e confirmada a sua ocorrência; 5) bloqueio dos dados pessoais a que se refere a infração até a sua regularização; 6) eliminação dos dados pessoais a que se refere a 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 da atividade de tratamento pelo controlador; 8) suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período;9) proibição parcial ou total do exercício de atividades relacionadas a

tratamento de dados.

Cumpre frisar, nos termos do § 1º do mesmo dispositivo, que as sanções serão aplicadas após procedimento administrativo que possibilite a oportunidade da ampla defesa, de forma gradativa, isolada ou cumulativa, de acordo com as peculiaridades do caso concreto e considerados os seguintes parâmetros e critérios: I - a gravidade e a natureza das infrações e dos direitos pessoais afetados; II - a boa-fé do infrator; III - a vantagem auferida ou pretendida pelo infrator; IV - a condição econômica do infrator; V - a reincidência; VI - o grau do dano; VII - a cooperação do infrator; VIII - 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 desta Lei; IX - a adoção de política de boas práticas e governança; X - a pronta adoção de medidas corretivas; e XI - a proporcionalidade entre a gravidade da falta e a intensidade da sanção.

Em julho de 2023, a ANPD aplicou a primeira multa por descumprimento da LGPD à uma sociedade empresária que estaria ofertando uma listagem de contatos de WhatsApp de eleitores, para fins de disseminação de material de campanha eleitoral. Ao fim do processo administrativo sancionador, a CGF/ANPD concluiu que a sociedade empresária infringiu os arts. 7º e o 41 da LGPD, além do art. 5º do Regulamento de Fiscalização da ANPD, por conseguinte, foram aplicadas as sanções de multa simples e advertência[59].

Outrossim, as sanções administrativas dispostas no artigo 52 não substituem a aplicação de sanções administrativas, civis ou penais definidas pelo Código de Defesa do Consumidor, e em legislação específica, nos termos do § 2º do mesmo dispositivo.

O § 6º aduz que as sanções de suspensão parcial do funcionamento do banco de dados, suspensão do exercício da atividade de tratamento dos dados pessoais e proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados, previstas nos incisos X, XI e XII, do artigo 52, consideradas mais gravosas, serão aplicadas: I - somente após já ter sido imposta ao menos 1 (uma) das sanções de que tratam os incisos II, III, IV, V e VI do caput deste artigo para o mesmo caso concreto; e II - em caso de controladores submetidos a outros órgãos e entidades com competências sancionatórias, ouvidos esses órgãos.

7.2. Das sanções aplicadas à Administração Pública

É notório que a Administração Pública está sujeita aos ditames da LGPD e, consequentemente, às suas sanções administrativas. Contudo, não são

59. https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-aplica-a-primeira-multa-por-descumprimento-a-lgpd

aplicadas ao Poder Público todas as penalidades dispostas na Lei, por expressa previsão legal.

O § 3º, do artigo 52, da LGPD, dispõe que as sanções de natureza pecuniária, ou seja, multa simples e multa diária, não podem ser aplicadas à Administração Pública. Tal opção legislativa tem o objetivo de não onerar o erário, o que poderia causar precarização dos serviços prestados.

Lado outro, é preciso destacar que as sanções eventualmente aplicadas à Administração Pública, em decorrência das previsões da LGPD, não excluem outras previstas em diplomas diversos, tais como: a) Lei Estadual nº 5.247/1991, que dispõe sobre o Estatuto do Servidor Público Estadual de Alagoas e a b) Lei nº 8.429/1992 (Lei de Improbidade Administrativa).

Por fim, é preciso sublinhar que a ANPD já aplicou as primeiras sanções à Administração Pública, consoante as decisões proferidas no Processo Administrativo Sancionador nº 00261.001886/2022-51[60] e no Processo Administrativo Sancionador nº 00261.001969/2022-41[61], de tal modo que se faz necessário atentar, principalmente, para a adoção de processos seguros de implementação da LGPD.

7.3. Da conciliação extrajudicial

Os vazamentos individuais ou os acessos não autorizados de que trata o caput do art. 46, da LGPD, poderão ser objeto de conciliação direta entre controlador e titular e, caso não haja acordo, o controlador estará sujeito à aplicação das penalidades de que trata o art. 52.

60. https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-sanciona-mais-um-orgao-publico/Relatorio_4_2023_e_DOU_versopblica.pdf. Acesso em 24/10/2023.

61. https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/sei_4286376_relatorio_2_2023.pdf. Acesso em 24/10/2023.

8. Do Guia Orientativo da ANPD Sobre Tratamento de Dados Pessoais pelo Poder Público

A Autoridade Nacional de Proteção de Dados (ANPD) foi criada pela Medida Provisória nº 869, de 2018, convertida na Lei nº 13.853, de 08 de julho de 2019. Contudo, somente, em 05 de novembro de 2020, passou a funcionar efetivamente com a nomeação de seu primeiro Diretor-Presidente.

Já a estrutura regimental e o quadro de cargos da ANPD foi aprovada pelo Decreto nº 10.474, de 26 de agosto de 2020, e posteriormente alterada pelo Decreto nº 10.975, de 22 de fevereiro de 2022.

Nos termos do caput art. 55-A da LGPD, a ANPD é órgão da administração pública federal, integrante da Presidência da República.

No mais, o art. 55-B do mesmo diploma dispõe que a ANPD possui autonomia técnica e decisória. Quanto à sua competência, é responsável por zelar pela proteção dos dados pessoais, e por orientar, regulamentar e fiscalizar o cumprimento da legislação, destacando-se as seguintes[62]:

Elaborar as diretrizes para a Política Nacional de Proteção de Dados e da Privacidade;

Promover na população o conhecimento das normas e das políticas públicas sobre proteção de dados pessoais e das medidas de segurança;

Promover e elaborar estudos sobre as práticas nacionais e internacionais de proteção de dados pessoais e privacidade;

Estimular a adoção de padrões para serviços e produtos que facilitem o exercício de controle dos titulares sobre seus dados pessoais;

Fiscalizar e aplicar sanções em caso de tratamento de dados realizado em descumprimento à legislação.

Dito isto, em 28 de janeiro de 2022, com vistas a zelar pela proteção de dados, notadamente no âmbito dos órgãos e entidades públicos, a Autoridade Nacional de Proteção de Dados (ANPD) lançou o Guia Orientativo sobre Tratamento de Dados Pessoais pelo Poder Público. Posteriormente, em junho de 2023, foi lançada a versão 2.0 do referido documento.

62. Disponível em: <https://www.gov.br/anpd/pt-br/acesso-a-informacao/institucional/base-juridica>. Acesso em: 11/03/2022.

Com o objetivo de auxiliar órgãos e entidades públicas nas atividades de adequação e implementação da LGPD, o guia dispõe: 1) breve explanação sobre a LGPD, o conceito de Poder Público e as competências da ANPD; 2) bases legais mais comuns; 3) os princípios mais relevantes no tratamento de dados; 4) duas operações específicas de tratamento de dados pessoais pelo Poder Público: o compartilhamento e a divulgação de dados pessoais; e, na parte final, 5) Anexos I e II com os sumários das recomendações apresentadas na análise dos dois casos específicos mencionados no item anterior.

Trata-se, portanto, de leitura obrigatória para os agentes de tratamento do Poder Público, disponibilizada no site da ANPD e pode ser acessada através do link: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos--de-publicacoes/guia-poder-publico-anpd-versao-final.pdf

REFERÊNCIAS BIBLIOGRÁFICAS

BASTOS, Celso Ribeiro. Curso de Direito Constitucional. 20ª edição atualizada. São Paulo: Saraiva, 1999.

BRASIL. Guia Orientativo. Tratamento de dados pessoais pelo Poder Público. V. 2.0. Governo Federal, junho/2023. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-vpublicacoes/guia--poder-publico-anpd-versao-final.pdf. Acesso em: 29 de setembro de 2023

BRASIL. Guia de Boas Práticas. Lei Geral de Proteção de Dados. V. 2.0. Governo Federal, agosto/2020. Disponível em: https://www.gov.br/governo-digital/pt-br/seguranca-e-protecao-de-dados/guias/guia_lgpd.pdf. Acesso em: 04 de outubro de 2021.

BRASIL. Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado. Governo Federal, Autoridade Nacional de Proteção de Dados, maio/2021. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/2021.05.27GuiaAgentesdeTratamento_Final.pdf. Acesso em 04/10/2021.

BRASIL. COMO PROTEGER SEUS DADOS PESSOAIS: Guia do Núcleo de Proteção de Dados do Conselho Nacional de Defesa do Consumidor em parceria com a ANPD e a SENACON. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/arquivos-de-documentos-de-publicacoes/guia-do-consumidor_como-proteger-seus-dados-pessoais-final.pdf. Acesso em 04/10/2021.

BIONI, Bruno. Proteção de dados pessoais: a função e os limites do consentimento. 2ª edição – Rio de Janeiro: Forense, 2020.

OPICE, Renato. Proteção de dados: desafios e soluções na adequação à lei – Rio de Janeiro: Forense, 2020.

DONEDA, Danilo. Da privacidade à proteção de dados pessoais: fundamentos da lei geral de proteção de dados – 2ª edição – São Paulo: Thomson Reuters Brasil, 2019.

POZZO, Augusto; MARTINS, Ricardo, coordenadores. LGPD e a administração pública: uma análise ampla dos impactos. São Paulo: Thomson Reuters, 2020.

MALDONADO, Viviane; BLUM, Renato, coordenadores. Lei Geral de Proteção de Dados Comentada. São Paulo: Thomson Reuters, 2019.

TEIXEIRA, Tarcísio; ARMELIN, Ruth. Lei geral de proteção de dados pessoais: comentada artigo por artigo. 2ªedição – Salvador: Editora JusPodivm, 2020.

SOARES, Paulo Brasil Dill. Princípios Básicos de Defesa do Consumidor: Institutos de Proteção ao Hipossuficiente. Leme/SP: LED, 200.

DONEDA, Danilo ... (et al.). Tratado de proteção de dados pessoais. Rio de Janeiro: Forense, 2021.

COTS, Márcio; OLIVEIRA, Ricardo. Lei geral de proteção de dados pessoais comentada. 3ª edição. São Paulo: Thomson Reuters Brasil, 2019.

FEIGELSON, Bruno; Becker, DANIEL; CAMARINHA, Sylvia, coordenadores. Comentários à lei geral de proteção de dados: Lei 13.709/2018. São Paulo: Thomson Reuters Brasil, 2020.

ANEXOS

ANEXO I - Proposta de programa de governança em privacidade;

ANEXO II – Modelo de termo aditivo para inclusão de regra de proteção de dados pessoais;

ANEXO III – Modelo de termo de compromisso de confidencialidade de informações e proteção de dados pessoais e sensíveis;

ANEXO IV – Modelo de relatório de impacto à proteção de dados pessoais – RIPD.

ANEXO I– Proposta de programa de governança em privacidade[1]

Etapa 1 - Iniciação e planejamento:

1. Nomeação do encarregado;
2. Alinhamento de Expectativas com a Alta Administração;
3. Análise da maturidade da Organização;
4. Análise e adoção de medidas de segurança, inclusive diretrizes e cultura interna;
5. Estabelecimento de uma estrutura organizacional para governança e gestão da proteção de dados pessoais, de acordo com o porte da instituição;
6. Inventário de Dados Pessoais;
7. Levantamento de Contratos relacionados a Dados Pessoais;

Etapa 2 – Construção e execução:

8. Políticas e práticas para proteção da privacidade do cidadão;
9. Cultura de segurança e proteção de dados e Privacidade desde a Concepção (privacy by design);
10. Relatório de Impacto à Proteção de Dados Pessoais (RIPD);
11. Medidas e Política de Segurança da Informação e Política de Privacidade;
12. Adequação Cláusulas Contratuais;
13. Termo de Uso;

Etapa 3 – Monitoramento:

14. Indicadores de Performance
15. Gestão de Incidentes
16. Análise de resultados; e
17. Reporte de Resultados.

1. Disponível em: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_governanca_privacidade.pdf. Acesso em 05/10/2021.

ANEXO II – Modelo de termo aditivo para inclusão de regra de proteção de dados pessoais[1]

XXX TERMO ADITIVO AO CONTRATO **(...) Nº - (...)/(...)**, QUE ENTRE SI CELEBRAM O ESTADO DE ALAGOAS, POR INTERMÉDIO DA(O) **(...ÓRGÃO...),** E A EMPRESA **(...)**.

CONTRATANTE: O Estado de Alagoas, por intermédio da(o) (...órgão...), inscrita(o) no CNPJ sob o nº (...) e com sede na (...endereço...), representado pelo (...cargo do ordenador de despesas...), Sr. (...nome...), inscrito no CPF sob o nº (...);

CONTRATADA: A empresa (...nome...), inscrita no CNPJ sob o nº (...) e estabelecida na (...endereço...), representada pelo seu (...cargo do representante legal...), Sr. (...nome...), inscrito no CPF sob o nº (...), de acordo com a representação legal que lhe é outorgada por (...procuração/contrato social/estatuto social...);

Os CONTRATANTES, nos termos do Processo nº (...), inclusive Parecer PGE-PLIC nº (...), aprovado pelos Despachos PGE-PLIC-CD nº (...) e PGE-GAB nº (...), e em observância às disposições com fulcro no art. 65, inciso I, alínea "a", da Lei n° 8.666/1993 e suas alterações ou art. 81, inciso I, da Lei 13.303/2016, e o Contrato Original, celebram o presente Termo Aditivo, mediante as cláusulas e condições a seguir enunciadas.

CLÁUSULA PRIMEIRA - DO OBJETO:

1.1 Estabelecer regra de proteção de dados pessoais no contrato **(...) Nº - (...)/(...)**.

1. Disponível em: https://www.transparencia.serpro.gov.br/acesso-a-informacao/licitacoes-e-contratos/documentos/minutas-padrao-de-editais-e-documentos-contratuais/padrao__t_a_clausula_protecao_de_dados_pessoais.pdf. Acesso em 05/10/2021.

CLÁUSULA SEGUNDA – DA ESPECIFICAÇÃO DO OBJETO:

2.1 Incluir na Cláusula xxxxxx – OBRIGAÇÕES DA CONTRATADA o seguinte item:

X.X Da Proteção de Dados Pessoais

XX.1 O ESTADO DE ALAGOAS e a CONTRATADA se comprometem a proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural, relativos ao tratamento de dados pessoais, inclusive nos meios digitais, garantindo que:

a) o tratamento de dados pessoais dar-se-á de acordo com as bases legais previstas nas hipóteses dos arts. 7º, 11 e/ou 14 da Lei 13.709/2018 às quais se submeterão os serviços, e para propósitos legítimos, específicos, explícitos e informados ao titular;

b) o tratamento seja limitado às atividades necessárias para o alcance das finalidades do serviço contratado ou, quando for o caso, ao cumprimento de obrigação legal ou regulatória, no exercício regular de direito, por determinação judicial ou por requisição da ANPD;

c) em caso de necessidade de coleta de dados pessoais dos titulares mediante consentimento, indispensáveis à própria prestação do serviço, esta será realizada após prévia aprovação do ESTADO DE ALAGOAS, responsabilizando-se a CONTRATADA pela obtenção e gestão. Os dados assim coletados só poderão ser utilizados na execução dos serviços especificados neste contrato, e em hipótese alguma poderão ser compartilhados ou utilizados para outros finalidades;

c.1) eventualmente, podem as partes convencionar que o ESTADO DE ALAGOAS será responsável por obter o consentimento dos titulares;

d) os sistemas que servirão de base para armazenamento dos dados pessoais coletados, seguem um conjunto de premissas, políticas, especificações técnicas, devendo estar alinhados com a legislação vigente e as melhores práticas de mercado;

e) os dados obtidos em razão deste contrato serão armazenados em um banco de dados seguro, com garantia de registro das transações realizadas na aplicação de acesso (log), adequado controle baseado em função (role based access control) e com transparente identificação do perfil dos credenciados, tudo

estabelecido como forma de garantir inclusive a rastreabilidade de cada transação e a franca apuração, a qualquer momento, de desvios e falhas, vedado o compartilhamento desses dados com terceiros;

e.1) no caso de haver transferência internacional de dados pessoais pela CONTRATADA, para atender ao acima, esta garante que:

e.1.1) a legislação do país para o qual os dados foram transferidos, asseguram o mesmo nível de proteção que a legislação brasileira em termos de privacidade e proteção de dados, sob pena de encerramento da relação contratual, em vista de restrição legal prevista no ordenamento jurídico brasileiro;

e.1.2) os dados transferidos serão tratados em ambiente da CONTRATADA;

e.1.3) o tratamento dos dados pessoais, incluindo a própria transferência, foi e continuará a ser feito de acordo com as disposições pertinentes da legislação sobre proteção de dados aplicável e que não viola as disposições pertinentes do Brasil;

e.1.4) sempre que necessário, orientará o ESTADO DE ALAGOAS durante o período de tratamento de dados pessoais, também em relação aos dados transferidos para país estrangeiro, para que ocorra em conformidade com a legislação sobre proteção de dados aplicável e com as cláusulas do contrato;

e.1.5) oferecerá garantias suficientes em relação às medidas de segurança técnicas e organizativas, e as especificará formalmente ao contratante, não compartilhando dados que lhe sejam remetidos com terceiros;

e.1.6) as medidas de segurança são adequadas para proteger os dados pessoais contra a destruição acidental ou ilícita, a perda acidental, a alteração, a divulgação ou o acesso não autorizados, nomeadamente quando o tratamento implicar a sua transmissão por rede, e contra qualquer outra forma de tratamento ilícito e que estas medidas asseguram um nível de segurança adequado em relação aos riscos que o tratamento representa e à natureza dos dados a proteger, atendendo aos conhecimentos técnicos disponíveis e aos custos resultantes da sua aplicação;

e.1.7) zelará pelo cumprimento das medidas de segurança;

e.1.8) tratará os dados pessoais apenas em nome do ESTADO DE ALAGOAS e em conformidade com as suas instruções e as cláusulas do contrato; no caso de não poder cumprir estas obrigações por qualquer razão, concorda

em informar imediatamente ao ESTADO DE ALAGOAS, que neste caso poderá suspender a transferência de dados e/ou de rescindir o contrato;

e.1.9) a legislação que lhe é aplicável não o impede de respeitar as instruções recebidas do ESTADO DE ALAGOAS e as obrigações do contrato e que, no caso de haver uma alteração nesta legislação que possa ter efeito adverso substancial nas garantias e obrigações conferidas pelas cláusulas do contrato, comunicará imediatamente essa alteração ao ESTADO DE ALAGOAS, que neste caso poderá suspender a transferência de dados e/ou de rescindir o contrato;

e.1.10) notificará imediatamente o ESTADO DE ALAGOAS sobre: qualquer solicitação juridicamente vinculativa de divulgação de dados pessoais por uma autoridade fiscalizadora responsável pela aplicação da lei, a menos que seja proibido de outra forma, como uma proibição da lei penal de preservar a confidencialidade de uma investigação policial; qualquer acesso acidental ou não autorizado;

e.1.11) responderá rápida e adequadamente todas as solicitações de informação do ESTADO DE ALAGOAS, relacionadas ao tratamento dos dados pessoais objeto da transferência e que se submeterá aos conselhos da autoridade fiscalizadora no que diz respeito ao processamento dos dados transferidos;

e.1.12) a pedido do ESTADO DE ALAGOAS, apresentará as informações necessárias sobre o tratamento relacionado com os dados pessoais objeto da transferência ou as informações solicitadas pela Autoridade fiscalizadora.

e.1.13) em caso de subcontratação, informará previamente o ESTADO DE ALAGOAS que poderá anuir por escrito;

e.1.14) os serviços de processamento pelo subcontratado, serão executados de acordo com o disposto neste contrato;

e.1.15) enviará imediatamente ao ESTADO DE ALAGOAS uma cópia de qualquer acordo de subcontratação que celebrar sobre o objeto deste contrato.

XX.2 A CONTRATADA dará conhecimento formal aos seus empregados das obrigações e condições acordadas nesta cláusula, inclusive no tocante à Política de Privacidade do ESTADO DE ALAGOAS.

XX.3 O eventual acesso, pela CONTRATADA, às bases de dados que contenham ou possam conter dados pessoais ou segredos de negócio, implicará

para a CONTRATADA e para seus prepostos – devida e formalmente instruídos nesse sentido – o mais absoluto dever de sigilo, no curso do presente contrato e pelo prazo de até 10 anos contados de seu termo final.

XX.4 As partes cooperarão entre si no cumprimento das obrigações referentes ao exercício dos direitos dos Titulares previstos na LGPD e nas Leis e Regulamentos de Proteção de Dados em vigor e também no atendimento de requisições e determinações do Poder Judiciário, Ministério Público, Órgãos de controle administrativo;

XX.5 Uma parte deverá informar à outra, sempre que receber uma solicitação de um Titular de Dados, a respeito de Dados Pessoais da outra Parte, abstendo-se de responder qualquer solicitação, exceto nas instruções documentadas ou conforme exigido pela LGPD e Leis e Regulamentos de Proteção de Dados em vigor.

XX.6 O Encarregado da CONTRATADA manterá contato formal com o Encarregado do ESTADO DE ALAGOAS, no prazo de 24 (vinte e quatro) horas da ciência da ocorrência de qualquer incidente que implique violação ou risco de violação de dados pessoais de que venha a ter conhecimento ou suspeita, devendo a parte responsável, em até 10 (dez) dias corridos, tomar as medidas necessárias.

XX.7 A critério do Encarregado de Dados do ESTADO DE ALAGOAS, a CONTRATADA poderá ser provocada a colaborar na elaboração do relatório de impacto à proteção de dados pessoais (RIPD), conforme a sensibilidade e o risco inerente dos serviços objeto deste contrato, no tocante a dados pessoais.

XX.8 Encerrada a vigência do contrato ou não havendo mais necessidade de utilização dos dados pessoais, sensíveis ou não, a CONTRATADA interromperá o tratamento e, em no máximo (30) dias, sob instruções e na medida do determinado pelo ESTADO DE ALAGOAS, eliminará completamente os Dados Pessoais e todas as cópias porventura existentes (em formato digital, físico ou outro qualquer), salvo quando necessite mantê-los para cumprimento de obrigação legal ou outra hipótese legal prevista na LGPD.

XX.9 Eventuais responsabilidades das partes, serão apuradas conforme estabelecido neste contrato e também de acordo com o que dispõe a Seção III, Capítulo VI da LGPD.

CLÁUSULA TERCEIRA – DAS DISPOSIÇÕES FINAIS:

3.1 Permanecem inalteradas as demais Cláusulas e disposições do Contrato original, desde que não conflitem com o disposto neste Instrumento.

E, por estarem justas e contratadas, o presente Termo Aditivo foi lavrado em 2 (duas) vias de igual teor, o qual, depois de lido e achado em ordem, vai assinado pelos contratantes.

Maceió (AL), em **(...)** de **(...)** de **(...)**.

_____

CONTRATANTE

_____

CONTRATADA

_____

TESTEMUNHA CPFN

_____

TESTEMUNHA CPFN

ANEXO III – Modelo de termo de compromisso de confidencialidade de informações e proteção de dados pessoais e sensíveis

I. Reconheço que em razão da utilização das ferramentas tecnológicas disponibilizadas pelo ESTADO DE ALAGOAS, poderei ter acesso a diversas informações pessoais, sensíveis, estratégicas, entre outras - confidenciais ou não - armazenadas nos sistemas informatizados sob a responsabilidade do ESTADO DE ALAGOAS;

II. Tenho ciência de que as credenciais de acesso (login e senha) são de uso pessoal e intrasferível e de conhecimento exclusivo. É de minha inteira responsabilidade todo e qualquer prejuízo causado pelo fornecimento de minha senha pessoal a terceiros, independentemente do motivo;

III. Reconheço que para os fins deste documento serão consideradas confidenciais todas as informações, transmitidas por meios escritos, eletrônicos, verbais ou quaisquer outros e de qualquer natureza, incluindo, mas não se limitando a:

a) Dados pessoais - qualquer informação que possa tornar uma pessoa física identificada ou identificável;

b) Dados sensíveis - qualquer dado pessoal que diga respeito a origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, bem como dado referente à saúde ou à vida sexual, dado genético ou biométrico;

c) Técnicas, design, especificações, desenhos, cópias, modelos, fluxogramas, croquis, fotografias, software, mídias, contratos, acordos ou instrumentos similares, processos, tabelas, projetos, nomes de servidores, agentes políticos ou empregados públicos, resultados de pesquisas, dados orçamentários e/ou financeiros, dentre outros;

IV. Tenho conhecimento ainda da Lei Federal n. 13.709/2018, que dispõe sobre a proteção de dados pessoais;

V. Tenho conhecimento ainda de que o ESTADO DE ALAGOAS possui um programa de governança de dados pessoais e de segurança da informação, em relação aos quais tenho obrigação de obedecer e auxiliar o cumprimento;

VI. Assumo o compromisso de não utilizar qualquer informação a que tenha acesso, classificada como confidencial ou não, para fins diversos daqueles para os quais tive autorização de acesso;

VII. Estou ciente de que é proibida a cópia, de qualquer informação para dispositivos estranhos à estrutura do ESTADO DE ALAGOAS, bem como a divulgação e compartilhamento, exceto se a referida ação seja estritamente necessária para a prestação dos serviços contratados, devendo ser realizada com a maior segurança possível e com expressa e prévia autorização do encarregado do ESTADO DE ALAGOAS;

VIII. Reconheço que os prejuízos causados por mim ao ESTADO DE ALAGOAS, em razão da quebra de confidencialidade, disponibilidade ou integridade das informações a que tenho acesso, poderão ser reclamados, judicial ou extrajudicialmente e, caso caracterizada qualquer infração penal, poderei ser pessoalmente responsabilizado;

IX. Reconheço que meus dados pessoais utilizados para acesso aos sistemas disponibilizados pelo ESTADO DE ALAGOAS serão conservados durante o tempo em que estiver vigente a relação contratual com o ente público ao qual estou vinculado e, após esta finalizar, durante os períodos de retenção de dados legalmente exigíveis, de forma estritamente necessária, tais como, mas não se limitando, pelos prazos prescricionais para ajuizamento de ação penal ou civil, assim como para o exercício do direito de defesa em processo judicial de qualquer natureza ou para outra finalidade por período não excessivo adotado pelo ESTADO DE ALAGOAS, garantida a transparência, confidencialidade, integridade e disponibilidade das minhas informações pessoais, bem como o exercício dos direitos previstos na Lei Federal n. 13.709/2018, na vigência da relação contratual, assim como após o término da referida relação;

X. Reconheço, neste ato, ter lido, compreendido e sanado todas as dúvidas sobre o Termo de Compromisso de Confidencialidade de Informação e Proteção de Dados Pessoais e Sensíveis.

Maceió/AL, XX de XXX de 2021.

_____

ANEXO IV – Modelo de relatório de impacto à proteção de dados pessoais - RIPD[1]

OBJETIVO
O Relatório de Impacto à Proteção de Dados Pessoais visa descrever os processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco. **Referência:** Art. 5º, XVII da Lei 13.709/2018 (LGPD).

1 – IDENTIFICAÇÃO DOS AGENTES DE TRATAMENTO E DO ENCARREGADO

Controlador

Operador

Encarregado	
E-mail Encarregado	**Telefone Encarregado**

2 – NECESSIDADE DE ELABORAR O RELATÓRIO

3 – DESCRIÇÃO DO TRATAMENTO

3.1 – NATUREZA DO TRATAMENTO
3.2 – ESCOPO DO TRATAMENTO
3.3 – CONTEXTO DO TRATAMENTO
3.4 – FINALIDADE DO TRATAMENTO

1. Disponível em: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_template_ripd.docx/view. Acesso em 05/10/2021.

4 – PARTES INTERESSADAS CONSULTADAS

5 – NECESSIDADE E PROPORCIONALIDADE

6 – IDENTIFICAÇÃO E AVALIAÇÃO DE RISCOS

Id	Risco referente ao tratamento de dados pessoais	P1	I2	Nível de Risco (P x I) 3

Legenda: P – Probabilidade; I – Impacto.

[1] Probabilidade: chance de algo acontecer, não importando se definida, medida ou determinada objetiva ou subjetivamente, qualitativa ou quantitativamente, ou se descrita utilizando-se termos gerais ou matemáticos (ISO/IEC 31000:2009, item 2.19).

[2] Impacto: resultado de um evento que afeta os objetivos (ISO/IEC 31000:2009, item 2.18).

[3] Nível de Risco: magnitude de um risco ou combinação de riscos, expressa em termos da combinação das consequências e de suas probabilidades (ISO/IEC 31000:2009, item 2.23 e IN SGD/ME nº 1, de 2019, art. 2º, inciso XIII).

7 – MEDIDAS PARA TRATAR OS RISCOS

Risco	Medida(s)	Efeito sobre o Risco1	Risco Residual2			Medida(s) 3 Aprovada(s)
			P	I	Nível (P x I)	

Legenda: P – Probabilidade; I – Impacto. Aplicam-se as mesmas definições de Probabilidade e Impacto da seção 6.

[1] Efeito resultante do tratamento do risco com a aplicação da(s) medida(s) descrita(s) na tabela. As seguintes opções podem ser selecionadas: Reduzir, Evitar, Compartilhar e Aceitar.

[2] Risco residual é o risco que ainda permanece mesmo após a aplicação de medidas para tratar o risco.

[3] Medida aprovada pelo controlador dos dados pessoais. Preencher a coluna com: Sim ou Não.

8 – APROVAÇÃO

RESPONSÁVEL PELA ELABORAÇÃO DO RELATÓRIO DE IMPACTO	ENCARREGADO
_____ <Nome do responsável> **Matrícula:** xxxxx <Local>, <dia> de <mês> de <ano>	_____ <Nome do encarregado> **Matrícula:** xxxxx <Local>, <dia> de <mês> de <ano>

AUTORIDADE REPRESENTANTE DO CONTROLADOR	AUTORIDADE REPRESENTANTE DO OPERADOR
_____ <Nome do representante> **Matrícula:** xxxxx <Local>, <dia> de <mês> de <ano>	_____ <Nome do representante> **Matrícula:** xxxxx <Local>, <dia> de <mês> de <ano>