LGPD

LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

MANUAL DE INTERPRETAÇÃO DA LGPD

ADVOCACIA-GERAL DO ESTADO

MINAS GERAIS

GOVERNO DIFERENTE. ESTADO EFICIENTE.

AGE MINAS GERAIS

AGE
MINAS GERAIS

SÉRGIO PESSOA DE PAULA CASTRO
Advogado-Geral do Estado

ANA PAULA MUGGLER RODARTE
Advogada-Geral Adjunta do Estado

MARGARIDA MARIA PEDERSOLI
Advogada-Geral Adjunta do Estado

TÉRCIO LEITE DRUMMOND
Chefe de Gabinete

SUMÁRIO

MENSAGEM DO ADVOGADO-GERAL DO ESTADO

O regime jurídico brasileiro de proteção de dados pessoais encontra na Lei Federal nº 13.709, de 14 de agosto de 2018, a Lei Geral de Proteção de Dados Pessoais (LGPD) um marco que se destaca pela importância da regulamentação ampla produzida, ao passo que também gera incertezas quanto à sua aplicação. Essa constatação não é de surpreender: além do caráter inaugural e inovador do diploma normativo, a proteção de dados pessoais envolve uma ampla gama de ações e comportamentos de uma série de atores.

A Administração Pública não pode se escusar de observar esse regime da forma mais efetiva possível. Ao mesmo tempo em que o tratamento de dados pessoais revela-se essencial para a eficiência de uma série de atividades do setor público, o respeito aos princípios que norteiam esse campo e aos direitos do cidadão não pode ser negligenciado. Dessa forma, revela-se necessária a implantação e evolução contínua de uma cultura de integridade e proteção aos direitos dos titulares de dados pessoais sob tutela da Administração, o que envolve um amadurecimento dos órgãos e entidades da Administração Direta e Indireta em todos os níveis, desde as decisões superiores e o planejamento estratégico de cada órgão, passando pelas soluções de tecnologia utilizadas, até as operações mais rotineiras, a envolver o comportamento de cada membro e servidor.

Nesse cenário, a Advocacia-Geral do Estado de Minas Gerais, reafirmando seu compromisso com uma cultura de integridade e buscando desempenhar seu papel de ser vetor de segurança jurídica na atuação da Administração Pública mineira, traz a público a presente cartilha. Além de conter um estudo das principais normas relativas à proteção de dados pessoais e sua pertinência ao setor público, o documento reúne as manifestações da Consultoria Jurídica exaradas até o momento por meio de pareceres e notas jurídicas. Com a expectativa de que a consulta a essa cartilha seja um momento de aprendizado e esclarecimento nesse cenário de transformações e inquietações pelo qual passa a Administração Pública, desejamos a todas e todos uma boa leitura!

Sérgio Pessoa de Paula Castro

1.1 Direito fundamental à proteção de dados pessoais

A proteção de dados pessoais, de acordo com a teoria jurídica moderna e a jurisprudência mais recente do Supremo Tribunal Federal, constitui um direito fundamental autônomo. Essa autonomia da proteção de dados pessoais enquanto um direito fundamental foi chancelado pelo STF ao declarar a inconstitucionalidade da Medida Provisória 954/2020, que dispunha sobre o compartilhamento de dados de usuários dos serviços de telefonia fixa e móvel de milhões de brasileiros com o IBGE. Nesse sentido, consta no Informativo 976 do STF:

> **A fim de instrumentalizar tais direitos, a CF prevê, no art. 5º, XII, a inviolabilidade do 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 penal.**
>
> **O art. 2º da MP 954/2020 impõe às empresas prestadoras do STFC e do SMP o compartilhamento, com o IBGE, da relação de nomes, números de telefone e endereços de seus consumidores, pessoas físicas ou jurídicas.**
>
> **Tais informações, relacionadas à identificação – efetiva ou potencial – de pessoa natural, configuram dados pessoais e integram o 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). Sua manipulação e seu tratamento, desse modo, devem observar, sob pena de lesão a esses direitos, os limites delineados pela proteção constitucional.**
>
> **Decorrências dos direitos da personalidade, o respeito à privacidade e à autodeterminação informativa foram positivados, no art. 2º, I e II, da Lei 13.709/2018 (Lei Geral de Proteção de Dados Pessoais), como fundamentos específicos da disciplina da proteção de dados pessoais.**

A afirmação de um direito fundamental autônomo à privacidade e à proteção de dados pessoais deriva de uma compreensão integrada do texto da Constituição Federal de 1988, lastreada (i) no direito fundamental à dignidade da pessoa humana; (ii) na proteção constitucional à intimidade, sobretudo em consideração com os novos riscos à sua violação em virtude do avanço da tecnologia; e (iii) no reconhecimento do habeas data enquanto instrumento central de tutela material do direito à autodeterminação informativa.[1]

[1] **ADPF 695 MC/DF.**

A partir desses três elementos, identifica-se a dupla dimensão do direito fundamental à proteção de dados. A primeira delas, a dimensão subjetiva, consiste na proteção do indivíduo contra os riscos que ameaçam a sua personalidade em face da coleta, processamento, utilização e circulação dos dados pessoais e a atribuição ao indivíduo da garantia de controlar o fluxo de seus dados[2]. Já a outra, a dimensão objetiva, por sua vez, consiste na imposição ao Poder Público, sobretudo ao legislador, de um dever de proteção do direito à autodeterminação informacional, o qual deve ser remediado a partir da previsão de mecanismos institucionais de salvaguarda traduzidos em normas de organização e procedimento e normas de proteção.

Com o escopo de proteger os direitos da personalidade, da liberdade, do respeito à privacidade e do livre desenvolvimento da personalidade da pessoa natural, foi promulgada a Lei Federal nº. 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados – LGPD, que dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado.

1.2 Noções gerais

A Lei Geral de Proteção de Dados, Lei Federal nº. 13.709, de 14 de agosto de 2018, nos termos do caput do seu art. 1º, dispõe sobre o tratamento de dados pessoais com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

As normas contidas na LGPD são normas de interesse nacional, ou seja, que visam promover os grandes propósitos do Estado, independentemente da vontade de seus governantes, e que devem ser cumpridas pela União, Estados, Distrito Federal e Municípios (parágrafo único do art. 1º). Ao encontro disso, reconhecendo caráter nacional das normas da LGPD e a importância de cumpri-las, o Estado de Minas Gerais institui grupo de trabalho por meio da Resolução Conjunta SEPLAG/CGE/SEF/AGE/PRODEMGE Nº 10.064, de 29 de julho de 2019, cujo resultado das atividades pode ser acessado no portal www.lgpd.mg.gov.br. Além disso, foi recentemente publicado o Decreto Estadual nº 48.237, que dispõe sobre a proteção de dados pessoais no âmbito do Estado de Minas Gerais, valendo destacar a constituição do Comitê Estadual de Proteção de Dados Pessoais, órgão colegiado e consultivo com diversas competências afetas à proteção de dados listadas no art. 5º do referido decreto.

Ainda sobre esse ponto, é importante observar que, ao regular o tratamento de dados pessoais realizado por pessoas jurídicas de direito público ou privado, as normas dispostas na LGPD também incluem no rol de pessoas que devem observá-la as fundações, empresas públicas e sociedades de economia mista.

[2] MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014, p. 140., p. 176-177.

Cabe observar que a LGPD visa a proteger tanto os dados mantidos em meios físicos, quanto digitais. Nesse aspecto, é importante observar que o risco de vazamento de dados não envolve apenas a cibersegurança dos meios digitais, mas também questões que envolvem a forma como os dados são coletados, armazenados e tratados em documentos físicos, devendo seguir os requisitos exigidos pela legislação.

Em relação às operações de tratamento dos dados pessoais aos quais a LGPD se aplica, nos termos do art. 3º da Lei, verifica-se que abrange qualquer operação de tratamento: (i) realizada no território nacional; (ii) que tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; (iii) ou que tenham sido coletados no território nacional. São considerados "coletados no território nacional" os dados pessoais cujo titular nele se encontre no momento da coleta.

Por outro lado, a LGPD deixou explícito (art. 4º) que ela não se aplica nos casos de tratamento de dados pessoais realizados (i) por pessoa natural para fins exclusivamente particulares e não econômicos; (ii) realizado para fins exclusivamente jornalísticos e artísticos ou acadêmicos. Ademais, também não se aplica para fins exclusivos de (iii) segurança pública; (iv) segurança do Estado; (v) ou atividades de investigação e repressão de infrações penais. Em relação à última hipótese, a lei vedou o tratamento dos dados por pessoa de direito privado (art. 4º, § 2º), exceto em procedimentos sob tutela de pessoa jurídica de direito público, que serão objeto de informe específico à Autoridade Nacional, não podendo, em hipótese alguma, a totalidade dos dados pessoais de banco de dados ser tratada por pessoa de direito privado, a menos que possua capital integralmente constituído pelo Poder Público.

1.3. Fundamentos da LGPD

O art. 2º da LGPD estabelece que são fundamentos da legislação, ou seja, são os sustentáculos da disciplina de proteção de dados, os seguintes:

I - **O respeito à privacidade:** a privacidade possui posição de destaque nos fundamentos da LGPD. Está em consonância com a Declaração Universal dos Direitos Humanos (art. 12), bem como com a nossa Constituição Federal (art. 5º, X), segundo as quais o direito à privacidade é garantia fundamental do ser humano, tratando-se de condição essencial para o livre desenvolvimento da personalidade humana. A proteção da privacidade, conforme a LGPD, tem como objetivo primordial garantir ao titular dos dados pessoais o controle sobre o acesso de terceiros à sua vida privada. Por esse motivo, a legislação versa sobre as condições e hipóteses de tratamento dos dados pessoais.

II - A autodeterminação informativa: desdobramento do direito à privacidade, o segundo fundamento abriga a filosofia de que o indivíduo titular de dados pessoais deve ser o protagonista das matérias relacionadas ao tratamento de seus dados pessoais, trazendo ao sujeito o foco das operações, em preocupação perpétua com a privacidade. Ou seja, o indivíduo titular de dados pessoais deve ter controle, ou ao menos plena transparência, sobre a destinação dada às suas informações pessoais, bem como as metodologias utilizadas para tanto.

III - A liberdade de expressão, de informação, de comunicação e de opinião: em virtude do fato da LGPD ser uma legislação regulatória no que tange à informação, o tratamento e a transmissão de dados, está intimamente ligada a outros princípios constitucionais soberanos do Estado Democrático de Direito, qual sejam, o da liberdade de expressão, informações e opinião (arts. 5º, IV e IX, da CF/88). Assim, o fundamento contido no art. 2º, III, da LGPD visa a garantir que as interpretações ao seu texto sejam realizadas em observância das liberdades de expressão, informação, comunicação e opinião, afastando qualquer entendimento que importe em censura.

IV - A inviolabilidade da intimidade, da honra e da imagem: assim como o respeito à privacidade, o legislador cuidou de incluir os demais direitos da personalidade no rol de fundamentos da LGPD, direitos estes garantidos também por força do art. 5º, X, da CF/88. De acordo com esse fundamento, todas as operações de tratamento de dados pessoais devem vem observar o cuidado com a intimidade, a honra e a imagem dos titulares dos dados pessoais.

V - O desenvolvimento econômico e tecnológico e a inovação: a promoção e incentivo ao desenvolvimento econômico e científico é dever do Estado, garantido pela Constituição Federal (arts. 218 e 219), devendo ser interpretados como princípios funcionais da República Federativa do Brasil quanto ao desenvolvimento nacional. Assim, a inclusão do desenvolvimento econômico e tecnológico e da inovação dentre os fundamentos LGPD aponta que a lei não foi elaborada a fim de impor freios ao livre avanço da tecnologia e de suas utilidades, mas sim garantir que o seu desenvolvimento seja compatível à proteção dos dados pessoais.

VI - A livre iniciativa, a livre concorrência e a defesa do consumidor: a Constituição brasileira de 1988 define a livre iniciativa como fundamento da ordem econômica (art. 170, caput), a garantia da propriedade privada dos meios de produção como direito individual fundamental, o estabelecimento da livre concorrência como princípio da ordem econômica (art. 170, IV) e, finalmente, a liberdade de atuação como base da economia nacional (art. 170, p. único). A inclusão de tais fundamentos na LGPD tem como escopo, novamente, demonstrar a plena aplicabilidade das normas de proteção dos dados pessoais com o desenvolvimento econômico do país.

VII - Os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais: as inclusões desses fundamentos na LGPD demonstram, mais uma vez, a preocupação do legislador em garantir os objetivos traçados no caput do art. 1º da própria lei, isto é, a proteção dos direitos fundamentais à liberdade e à privacidade e ao livre desenvolvimento da personalidade da pessoa natural. Visa a ampliar a proteção do titular dos dados pessoais para além dos direitos da personalidade, reafirmando a proteção à liberdade. A dignidade e a cidadania são fundamentos da República Federativa do Brasil, também reafirmados pela LGPD.

1.4 Conceitos

A LGPD, em seu art. 5º, trouxe conceitos-chave para a melhor compreensão da norma. São eles:

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

b) **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;

c) **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;

d) **Banco de dados:** conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico;

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

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

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

h) **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);

i) **Agentes de tratamento:** o controlador e o operador;

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

k) **Anonimização:** 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;

l) **Consentimento:** manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;

m) **Bloqueio:** suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados;

n) **Eliminação:** exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado;

o) **Transferência internacional de dados:** transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro;

p) **Uso compartilhado de dados:** comunicação, difusão, transferência internacional, inter- conexão 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 modalida- des de tratamento permitidas por esses entes públicos, ou entre entes privados;

q) **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;

r) **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;

s) **Autoridade nacional:** órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento da desta Lei em todo o território nacional.

1.5 Princípios

De acordo com a LGPD, as atividades de tratamento de dados pessoais deverão observar, além da boa-fé, outros dez princípios elencados no art. 6º.

Antes de tratar dos dez princípios previstos nos incisos do art. 6º é importante tratar da regra geral da boa-fé, prevista no caput do dispositivo.

A boa-fé trata-se de um princípio de conduta ética fundamental em todos os campos do direito. Consiste em proceder com correção e dignidade, com a atitude pautada nos princípios da honestidade, da boa intenção e no propósito de a ninguém prejudicar.[3] Em se tratando de dados pessoais, a boa-fé mostra-se basilar no equilíbrio dos interesses envolvidos, tendo em vista os riscos que envolvem a coleta e a utilização dos dados pessoais alheios.

Desta feita, ao lado dos artigos 187 e 422 do Código Civil de 2002, além de dispositivos do Código de Defesa do Consumidor, entre os quais os arts. 4º, III e 51, IV, que já traziam o princípio da boa-fé, estabeleceram-se, no art. 6º da LGPD, que "as atividades de tratamento de dados pessoais deverão observar a boa-fé".

Os outros princípios elencados no art. 6º da LGPD, expostos a seguir, são, no fundo, desdobramentos dos deveres da boa-fé.

a) Princípio da finalidade

> *"Realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades; "*

Por propósitos legítimos, depreende-se a finalidade movida pelo bom senso, razão, legalidade, bons costumes e boa-fé. Distancia-se da iniciativa subalterna, emulativa, emocional, ilícita e de má fé.

Ao tratar de propósitos específicos, enfatiza a preocupação de que o tratamento dos dados se volte para um objetivo certo e determinado.

Por propósitos explícitos o dispositivo busca ressaltar o aspecto unívoco do tratamento dos dados, ou seja, que não admite ambiguidade ou equivocidade, sendo objetivo e claro no que tange às intenções de seu uso.

[3] RODRIGUES, Silvio. Direito Civil. 3º Volume. 28ª ed. São Paulo: Ed. Saraiva. p. 60.

Esses propósitos, integradamente, conformam o princípio da finalidade admitida pela LGPD. Eles devem ser informados ao titular dos dados, o qual, com a sua concordância, delimitará o objeto do tratamento. Esse domínio não poderá ser subsequentemente modificado, salvo com posterior concordância específica e expressa do mesmo titular.

b) Princípio da adequação

> *"Compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento";*

A adequação, no âmbito da LGPD, diz respeito ao nexo e pertinência lógica de conformidade que se estabelece entre o tratamento e a finalidade objetivada, tal como

c) Princípio da 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; "*

De acordo com esse princípio, somente deverão ser tratados os dados pertinentes, ou seja, aqueles que se mostrem imprescindíveis para que o objetivo previamente tracejado seja atingido.

A proporcionalidade, no âmbito da LGPD, admite a realização do tratamento dos dados, nos limites do que se mostrar imprescindível e necessário para que o objetivo, previamente delimitado e aprovado pelo titular dos dados correspondentes, seja alcançado.

d) Princípio do 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; "*

A LGPD garante aos titulares dos dados, antes da realização do tratamento, que sejam cientificados acerca da forma através da qual poderão acessar gratuitamente os dados tratados.

Ademais, prestigia as pessoas naturais titulares de seus respectivos dados, após estes sofrerem o tratamento correspondente, assegurando o acesso e conhecimento da integralidade dos seus dados.

Além disso, exige que os titulares sejam cientificados da duração do tratamento, ou seja, não só do tempo a ser despendido para a sua realização, como também o período em que os dados tratados serão utilizados para a finalidade correspondente ser atingida.

Cumpre destacar que o princípio do livre acesso somente será observado, caso tais condições e respectivas concordâncias sejam satisfeitas e, expressamente, colhidas, dos respectivos titulares, na forma e no tempo adequados.

e) Princípio da 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; "*

No contexto da LGPD, o termo "exatidão" remete à ideia de precisão, do liame estrito estabelecido entre dados, tratamento e finalidade.

O termo "clareza", por sua vez, associa-se à noção de que tal relação seja assentada em palavras e procedimentos que, indubitavelmente, esclareçam os destinatários da mensagem, sobretudo a pessoa natural titular dos dados a serem tratados, assim como para que se voltem, certeiramente, para o resultado almejado.

A "relevância" indica que o tratamento em questão somente será realizado quando permitir atingir a finalidade previamente objetivada e, também, que, antecipadamente, tenha sido aprovada pelo titular dos dados.

Por fim, "atualização" é o elemento que enfatiza o aspecto temporal e dinâmico dos dados.

f) Princípio da 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 princípio da transparência destaca a importância que a LGPD dispensa à fluidez da informação para o titular dos dados tratados.

"Informações claras" remetem à ideia de que a utilização de conteúdo excessivamente técnico e até hermético não é adequado aos propósitos da LGPD. Visa-se garantir às pessoas naturais, independentemente do nível cultural, social e cognitivo, a plena compreensão do que se trata a informação.

Observe-se que a LGPD cuidou em garantir a proteção de segredos comerciais e industriais aos seus respectivos detentores, de maneira que se constituem em limites a serem observados ao se utilizarem da transparência relativa aos tratamentos realizados com dados de pessoas naturais.

g) Princípio da 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; "***

A ideia central desse princípio é a de preservar, sempre em ambiente seguro, os dados das pessoas naturais objeto do tratamento, sejam eles em meios digitais ou físicos. Para tanto deverão ser utilizadas, sempre, técnicas modernas de segurança e cibersegurança.

h) Princípio da prevenção

> ***"Adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais; "***

Derivado do princípio da segurança, a LGPD cuidou de reiterar o dever de proteção dos dados antes, durante e após o tratamento, imposto àqueles que os acessam e sobre eles dispõem.

i) Princípio da não discriminação

> ***"Impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos; "***

A impossibilidade de admitir a prática do ilícito é intrínseca a todo o ordenamento jurídico e foi enfatizada na LGPD. Deriva do princípio da boa-fé, segundo o qual o titular que dispõe seus dados presume que serão utilizados para fins lícitos.

No que tange à abusividade, a LGPD cuidou de proteger os titulares quanto ao manuseio excessivo ou imoderado dos seus dados, transbordando, inclusive, o nexo lógico e jurídico estabelecido pelo trinômio dado-tratamento-finalidade.

j) Princípio da responsabilização e da 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. "***

Esse último princípio elencado na LGPD está relacionado à rastreabilidade, ou seja, à comprovação de procedimentos e dos atos praticados relacionados aos dados das pessoas naturais. Refere-se à adoção de posturas sérias, técnicas e respeitosas pelo agente em relação aos dados do tratamento.

2.1 Hipóteses autorizadoras (I a X)

Em seu art. 7º, a LGPD traz de forma taxativa as bases legais, ou hipóteses autorizadoras, que permitem que o tratamento de dados pessoais seja realizado. Desta feita, pela dicção da LGPD, o agente de tratamento de dados pessoais terá o ônus de fundamentar as suas operações de tratamento de dados pessoais em um dos incisos do art. 7º. Esses incisos contemplam as variadas autorizações para o tratamento dos dados pessoais: desde o consentimento (inciso I), passando pelo cumprimento de obrigação legal ou regulatória pelo controlador (inciso II), bem como uma das bases legais mais desafiadoras ao controlador, que é o denominado interesse legítimo (inciso IX).

Os parâmetros de aferição quanto à adequação da escolha da base legal podem ser extraídos do conjunto das regras e princípios da LGPD, valendo citar a boa-fé, a finalidade, a adequação, a transparência, a responsabilização e a prestação de contas. Cabe pontuar que é razoável a interpretação do caput do art. 7º da LGPD no sentido de que seja permitido o enquadramento da operação de tratamento de dados pessoais em mais de uma base legal.

São as bases legais para o tratamento de dados pessoais expressamente previstas na LGPD:

a) Hipótese I - consentimento fornecido pelo titular dos dados

Trata-se da regra geral estabelecida pela LGPD, de que as operações de tratamento de dados apenas podem ocorrer mediante o consentimento de seu titular. A LGPD exige que o consentimento seja fornecido por escrito ou por outro meio que demonstre a manifestação inequívoca de vontade do titular (art. 8º).

O consentimento dado deve ser livre, informado, inequívoco, explícito e específico, ou seja, não cabe o consentimento genérico. Embora não seja necessário que o consentimento seja exclusivamente escrito em documento formal e padrão, é indispensável que ele seja dado de forma clara e direta dentro dos parâmetros e limites impostos na própria LGPD.

Quando o consentimento se der por escrito, ele deverá constar em uma cláusula destacada das demais contratuais, que não pode ser genérica, justamente para que seja comprovado que aquele consentimento foi dado para uma finalidade específica de tratamento (art. 8º, § 1º).

Em relação ao consentimento tácito, não expresso, mas manifestamente público, ou seja, nos casos em que qualquer pessoa poderá ter acesso aos dados tornados públicos pelo próprio titular, a LGPD dispõe que o tratamento deve ser realizado com cautela, respeitando-se os direitos do titular e os princípios elencados no art. 6º (art. 7º, §4º).

O titular do dado deve ser, primeiramente, informado pelo agente de tratamento sobre as finalidades do seu processamento para, então, poder autorizá-lo, consolidando-se a sua participação na operação.

No que tange ao ônus da prova do consentimento, o art. 7º, §2º, determina que cabe ao controlador provar que o consentimento foi obtido em conformidade com o disposto na LGPD, ou seja, que não há qualquer vício de consentimento, quais sejam, o erro, dolo, coação, estado de perigo e lesão.

Ademais, cumpre observar que o consentimento é estrito e limitado à finalidade, autorizando somente o agente que o obteve a realizar o tratamento, não estendendo automaticamente a outras pessoas. Desta feita, para o controlador compartilhar dados pessoais obtidos com outros controladores, faz-se necessário o consentimento específico do titular para esse fim, ressalvadas as hipóteses de dispensa de consentimento previstas em lei.

Importante observar também que a base legal do consentimento do titular é considerada um autorizador temporário, uma vez que pode ser revogado a qualquer momento, mediante manifestação expressa do titular, por procedimento gratuito e facilitado (art. 8º, § 5º).

Interessa pontuar que a obtenção de consentimento específico do titular não é exigida quando a Administração Pública efetuar o tratamento de dados com base nas outras hipóteses autorizadoras (art. 7º, II, III, IV, VI, VII, VIII, IX e X da LGPD) ou mesmo quando compartilhar os dados pessoais obtidos com outros órgãos ou entidades públicas para atender as exigências de determinada política pública ou para cumprir atribuição legal do órgão ou entidade. Contudo, frisa-se que a dispensa do consentimento não desobriga a Administração das limitações previstas na LGPD.

b) Hipótese II - cumprimento de obrigação legal ou regulatória pelo controlador

A segunda base legal para tratamento de dados pessoais prevista pela LGPD no art. 7º é o cumprimento de obrigação legal ou regulatória pelo controlador. Trata-se de um autorizador da LGPD que possibilita que a lei não entre em conflito com outros instrumentos normativos vigentes no ordenamento jurídico brasileiro.

No caso de uma obrigação decorrente de lei, ou regulação, acarretar um tratamento de dados pessoais por parte de uma empresa, por exemplo, essa estará autorizada a tratá-los de modo a cumprir a dita exigência legal ou regulatória. Outro exemplo refere-se ao cumprimento pelo Poder Público de requisições de dados pessoais de servidores públicos oriundas dos órgãos de controle, não precisando de consentimento dos titulares para realizar o compartilhamento dos dados.

c) Hipótese III - tratamento e uso compartilhado de dados pela Administração Pública, necessários à execução de políticas públicas previstas em lei e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres

Os órgãos da Administração Pública estão autorizados, por força do inciso III, do art. 7º da LGPD, a tratarem e compartilharem dados pessoais para execução de políticas públicas ou respaldadas em contratos, convênios ou instrumentos congêneres, sem a necessidade de consentimento dos titulares.

Contudo, a Administração Pública precisa se adequar e cumprir as disposições na LGPD, sendo obrigada a fornecer ao titular dos dados informações claras e inequívocas sobre a base legal para o tratamento dos dados, a finalidade e quais os procedimentos utilizados ao longo do ciclo de vida do dado dentro dos sistemas da Administração Pública. Ademais, deve observar os princípios preconizados na Lei e, especificamente, as regras previstas nos arts. 23 a 30.

Interessa recordar que a Administração Pública somente não está obrigada a cumprir com as exigências da LGPD no caso de tratamento de dados feito exclusivamente para fins de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação ou de repressão de infrações penais, nos termos do art. 4º.

d) Hipótese IV - realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais

A LGPD também permitiu, no inciso IV do art. 7º, o tratamento de dados pessoais para a realização de estudos por órgãos de pesquisa, preconizando que, sempre que possível, esses dados serão anonimizados, a fim de garantir a privacidade dos titulares e evitar possíveis vazamentos.

Nesse sentido, é valido recordar dois conceitos específicos da LGPD, quais sejam, o de órgãos de pesquisa e o de anonimização dos dados pessoais.

O primeiro termo, órgão de pesquisa, refere-se ao "órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos le-

galmente constituídos 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".

Já a anonimização significa a utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo. Ou seja, são aqueles dados que tornam impossível identificar o seu titular.

No que tange ao tratamento de dados pelos órgãos de pesquisa, públicos ou privados, a LGPD, de modo geral, trouxe os seguintes regramentos:

1) é desnecessário o consentimento do titular do dado, desde que anonimizado;

2) a divulgação dos resultados da pesquisa não poderá revelar dados que permitam a identificação pessoal dos titulares;

3) o órgão será responsável pela segurança da informação e não poderá compartilhar os dados com terceiros;

4) em casos de estudos em saúde pública, os órgãos de pesquisa poderão ter acesso a bases de dados pessoais, que serão tratados exclusivamente dentro do órgão e estritamente para a finalidade de realização de estudos e pesquisas e mantidos em ambiente controlado e seguro; e

5) o acesso a dados pessoais pelos órgãos de pesquisa para fins de realização de estudos em saúde pública será objeto de regulamentação pela ANPD (Autoridade Nacional de Proteção de Dados) e das autoridades da área de saúde e sanitárias.

e) Hipótese V - execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados

Outra hipótese autorizadora para o tratamento de dados pessoais, prevista no inciso V do art. 7º da LGPD, refere-se à necessidade do tratamento para a execução de um contrato ou de procedimentos preliminares relacionados a um contrato que o titular dos dados figurará como integrante.

Tal hipótese assemelha-se com o tratamento de dados via consentimento, diferenciando-se no fato de que o titular dos dados não poderá revogar o seu fornecimento a qualquer momento, uma vez que a outra parte estará resguardada pela LGPD para poder manter os dados fornecidos pelo titular enquanto durar a vigência do do contrato, desde que mantida a finalidade original.

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

Outra base legal que autoriza o tratamento de dados (art. 7º, VI) é para o exercício regular de direitos em processo judicial, administrativo ou arbitral. Esse autorizador contido na LGPD visa a garantir o direito de produção de provas de uma parte em face da outra em um processo judicial, administrativo ou arbitral, ainda que não exista o consentimento do titular do dado. Trata-se de dispositivo que objetiva assegurar os preceitos constitucionais da ampla defesa e do contraditório.

g) Hipótese VII - proteção da vida ou da incolumidade física do titular ou de terceiro

A LGPD admite o tratamento de dados, ainda que sem o consentimento do titular, para proteger a vida ou a incolumidade física do titular dos dados ou de terceiros. Trata-se de um autorizador legal com o escopo de garantir a proteção de bens de elevado interesse público, tais como a vida e a incolumidade física, desde que devidamente comprovada essa necessidade e exposta a finalidade do tratamento dos dados nessa situação.

h) Hipótese VIII - tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária

A LGPD incluiu nas hipóteses autorizadoras (art. 7º, VIII) o tratamento de dados para a tutela da saúde, desde que realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária. Trata-se de uma base legal que tem como plano de fundo o interesse público no tratamento dos dados pessoais e é exclusiva aos profissionais da saúde, serviços de saúde ou autoridade sanitária, voltando-se unicamente para a tutela da saúde do paciente titular do dado.

Assim, de acordo com o regramento da LGPD, os hospitais públicos, serviços de saúde e entidades sanitárias estão autorizadas a realizar o tratamento de dados sensíveis dos pacientes, sem o seu consentimento específico, visando à tutela da saúde. Mais além, nos casos em que os dados relacionados à saúde de pacientes se mostrarem indispensáveis à concretização de políticas públicas, o tratamento poderá ser efetuado no âmbito da Administração Pública sem a necessidade de informar o titular do dado.

i) Hipótese IX - 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

A LGPD elencou dentre as hipóteses autorizadoras de tratamento (art. 7º, IX) a necessidade de atendimento de interesses legítimos do controlador ou de terceiros. Trata-

-se de uma base legal de utilização subsidiária, ou seja, quando não houver outra base legal aplicável ao caso, tendo em vista o seu elevado grau de abstração.

Isso porque a LGPD não cuidou de definir o que seria considerado "legítimo interesse" do controlador ou terceiro, de modo que torna dificultoso sopesar até que ponto esse legítimo interesse sobrepõe o do titular dos dados ou fere algum direito ou outra disposição prevista na própria LGPD.

Nesse sentido, o art. 10 da LGPD determinou que o legítimo interesse do controlador somente poderá fundamentar tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas, que incluem, mas não se limitam a: (1) apoio e promoção de atividades do controlador; e (2) proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais.

Em suma, para a utilização dessa hipótese autorizadora para o tratamento de dados, mostra-se necessário: (1) identificar um interesse inequivocamente legítimo do controlador ou de terceiro; (2) demonstrar que o tratamento de dados é necessário para se atingir tal objetivo; e (3) atentar para não violar nenhum dispositivo legal ou nenhum direito do titular daqueles dados.

j) Hipótese X - proteção do crédito, inclusive quanto ao disposto na legislação pertinente

A última base legal elencada no inciso X do rol taxativo do art. 7º da LGPD refere-se à autorização para se realizar o tratamento de dados pessoais para a proteção do crédito, em observância às regras especificas para esse tema. Trata-se de uma autorizadora que revela a intenção do legislador de evitar que titulares de dados pessoais se utilizem de uma brecha legislativa para criarem mecanismos de escaparem de cobranças por dívidas contraídas.

Nesse sentido, a Lei Complementar Federal nº 166/2019 alterou a Lei Federal nº 12.414/2011, que trata da formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito, para compatibilizar ao disposto na LGPD, de modo a não precisar mais do consentimento do titular/cadastrado para usar seus dados conforme as finalidades de formação de histórico de crédito.

2.2 Dados sensíveis

Em relação ao conceito de dados pessoais sensíveis, vale lembrar, a LGPD definiu que se trata de "dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político,

dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural" (art. 5º, II, da LGPD). Importante pontuar que tal definição não é taxativa ou exaustiva, ou seja, enumera de maneira exemplificativa algumas das hipóteses em que serão identificados os dados pessoais que tenham natureza considerada sensível, podendo abarcar outras situações não previstas.

Nesse sentido, a doutrina conceitua os dados sensíveis como "uma espécie de dados pessoais que compreendem uma tipologia diferente em razão de o seu conteúdo oferecer uma especial vulnerabilidade, discriminação[4] ". A partir dessa compreensão, tem-se a noção de que tratam de dados com potencialidade discriminatória, ou de uso abusivo, no seu tratamento. Por esse motivo, a LGPD cuidou em conferir tratamento próprio, em sentido mais protetivo, para esses dados. A tutela jurídica especial que envolve os dados sensíveis encontra-se disciplinada nos arts. 11 a 13 da LGPD.

Para o tratamento de dados pessoais sensíveis a LGPD elencou um rol de hipóteses taxativas específico em seu art. 11.

A primeira das hipóteses, que constitui a regra geral, refere-se ao consentimento - livre e esclarecido - do titular. De forma diversa da previsão contida no art. 7º, para o tratamento de dados em geral, o consentimento que legitima o tratamento de dados sensíveis deve ser específico, inequívoco e expresso e, ainda, para finalidades determinadas. Desta feita, mostra-se essencial a clareza nas informações que serão passadas ao titular a respeito do tratamento que será feito com os seus dados pessoais sensíveis.

De forma excepcional, o tratamento de dados pessoais sensíveis pode ocorrer sem o consentimento do titular, nas hipóteses em que for indispensável para:

a) cumprimento de obrigação legal ou regulatória pelo controlador;

b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;

c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;

d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);

[4] BIONI, Bruno Ricardo. Proteção de Dados Pessoais - A Função e os Limites do Consentimento. Forense, 10/2018. Saraiva. p. 60.

e) proteção da vida ou da incolumidade física do titular ou de terceiro;

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

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

Observa-se que são parecidas as hipóteses previstas de tratamento de dados em geral, porém não há previsão específica na LGPD para que seja realizado o tratamento de dados pessoais sensíveis com a finalidade de viabilizar a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, ou sob a justificativa de atender ao legítimo interesse do controlador.

Em relação ao tratamento de dados sensíveis na saúde, observa-se que a LGPD dispensa o consentimento expresso nos casos de proteção à vida ou tutela da saúde do titular, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária. Verifica-se que o profissional de saúde possui o dever de prestar a assistência, independentemente da assinatura de termo de consentimento pelo titular. Em que pese o consentimento ser desnecessário, as unidades de saúde devem infor- mar aos pacientes sobre a forma como seus dados serão recolhidos e tratados. Por fim, o tratamento e o compartilhamento de dados sensíveis da saúde só poderão ser realizados em benefício do titular, nunca com intuito lucrativo, e deverão coexistir com os princípios gerais previstos no art. 6º da LGPD.

Em relação aos órgãos de pesquisas, públicos e privados, de acordo com a LGPD, deve-se manter a anonimização ou pseudonimização[5] dos dados pessoais sensíveis obtidos, assim como a divulgação dos resultados ou de qualquer excerto do estudo ou da pesquisa, em nenhuma hipótese, poderá revelar dados pessoais, nem haver a transferência dos dados a terceiro. Ademais, importante lembrar que esses órgãos de pesquisa são responsáveis pela segurança da informação, devendo adotar condutas para proteger os dados pessoais sensíveis da utilização inadequada por terceiros.

No caso do Poder Público, em relação aos dados sensíveis, a LGPD impõe as seguintes normas:

[5] **Dados pseudonimizados são aqueles que, com a aplicação de estratégias de proteção, podem parecer anônimos em um primeiro momento, mas, na realidade, permitem que o processo de anonimização seja revertido. Esses dados ainda são protegidos pela LGPD, visto que não perdem a sua capacidade de identificar uma pessoa.**

a) os órgãos e entidades públicas que realizarem o tratamento de dados sensíveis para o cumprimento de obrigação legal ou regulatória pelo controlador ou para o tratamento compartilhado de dados necessários à execução de políticas públicas previstas em leis ou regulamentos, devem dar a devida publicidade da dispensa de consentimento do titular, preferencialmente em seus sítios eletrônicos (art. 23, I);

b) o tratamento de dados pessoais sensíveis pelo Poder Público fundamentado nas exceções previstas no inciso II do art. 11 da LGPD não exige o consentimento do titular, bem como dispensa a Administração de garantir a publicidade;

c) o controlador, antes de efetuar o tratamento de um dado sensível, deverá demonstrar que a situação fática posta se enquadra nas hipóteses de tratamento que dispensam o consentimento e deve justificar, de forma fundamentada, que o tratamento do dado sensível é indispensável para a Administração.

2.3 Tratamento de dados pessoais de crianças e de adolescentes

A LGPD também abordou de forma especial o tratamento de dados pessoais das crianças e adolescentes (Capítulo II, Seção III, art. 14). Nos termos da Lei, o tratamento de dados de crianças e adolescentes deve ser realizado de acordo com o melhor interesse desses, mediante consentimento específico e destacado dado por pelo menos um dos pais ou pelo responsável legal. O consentimento dos pais ou responsável legal é exigido ainda que se trate de execução de políticas públicas pelo controlador.

De forma excepcional, o consentimento dos pais é dispensado em duas hipóteses expressamente previstas na LGPD, quais sejam (art. 14, § 2º): (1) quando a coleta do dado for necessária para contatar os pais ou responsável legal; ou (2) para a própria proteção da criança/adolescente. Em ambos os casos, os dados só poderão ser utilizados uma única vez, vedado o seu armazenamento, e não poderão ser repassados a terceiro, salvo se houver consentimento específico na forma prevista na LGPD.

2.4 Término do tratamento de dados

O término do tratamento de dados consiste no momento do encerramento do tratamen to e, em regra, do descarte definitivo dos dados utilizados.

O art. 15 da LGPD determina, de forma clara, as hipóteses em que ocorrerá o término do tratamento. São elas:

a) Verificação de que a finalidade foi alcançada ou de que os dados deixaram de ser necessários ou pertinentes ao alcance da finalidade específica almejada: Nesse ponto, a

finalidade pretendida com a utilização do dado coletado já foi atingida. Trata-se da materialização do princípio da finalidade.

b) Fim do período de tratamento: Ocorre quando foi estabelecido um período prévio para o tratamento dos dados.

c) 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: A LGPD estabeleceu a possibilidade de revogação do consentimento do titular dos dados, a qualquer tempo.

d) Determinação da autoridade nacional, quando houver violação ao disposto na LGPD: Havendo a violação das regras e princípios dispostos na LGPD, a autoridade nacional poderá determinar ao agente o fim do tratamento de dados pessoais.

Após ocorrido o término de seu tratamento, nas hipóteses supracitadas, o art. 16 da LGPD estabelece que, regra geral, os dados serão eliminados no âmbito e nos limites técnicos das atividades. Contudo, a LGPD excepciona casos em que a conservação será autorizada, quais sejam: (i) em 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.

Verifica-se que, em todos os casos, os princípios da boa-fé e os demais princípios previstos no art. 6º devem ser sempre observados.

Em relação ao término do tratamento de dados pela Administração Pública, é importante pontuar que a eliminação de dados pessoais deve obedecer às disposições contidas, em âmbito federal, na Lei Federal nº 8.159/1991, que dispõe sobre a política nacional de arquivos públicos e privados e dá outras providências, e em âmbito estadual na Lei Estadual nº 19.420/2011, que estabelece a política estadual de arquivos no Estado de Minas Gerais, e no Decreto nº 46.398/2013, que institui instrumentos de gestão de documentos no âmbito da Administração Pública do Poder Executivo de Minas Gerais. Isso porque os dados pessoais coletados pelo Poder Público passam a integrar o "arquivo público" do órgão ou da entidade, devendo a sua eliminação obedecer aos dispostos nas legislações específicas.

3.1 Noções gerais

O titular dos dados pessoais vale lembrar, nos termos da LGPD, corresponde à pes- soa natural a quem se referem os dados/as informações que é objeto de tratamento pe- lo controlador.

É importante pontuar que a Lei Geral de Proteção de Dados deixou claro que os dados pessoais, ou seja, as informações que identificam ou que, em conjunto com outros dados, permitem a identificação de uma pessoa, pertencem ao indivíduo e não ao controlador dos dados, seja uma empresa privada ou órgão público. É nesse sentido que a LGPD garantiu, em seu art. 17, que toda pessoa natural tem assegurada a titularidade de seus dados pessoais (direito à titularidade dos dados pessoais) e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade. Note-se que a redação do dispositivo guarda vínculo com os princípios elencados no art. 6º da própria LGPD e com a Constituição Federal.

Os direitos dos titulares de dados pessoais são indicados no capítulo III, do artigo 17 ao 22, da Lei nº 13.709, de 2018. Interessa notar que os direitos que a LGPD visa a garantir não se limitam aos direitos em espécie dispostos nesse capítulo, devendo ser compreendida toda a sistemática de proteção que a LGPD buscou conferir ao titular dos dados pessoais.

3.2 Direitos em espécie

A LGPD destacou, sobretudo em seu art. 18, direitos em espécie dos titulares dos dados pessoais. Trata-se de prerrogativas oponíveis tanto em face do controlador, como ante o próprio operador desses dados, ambos responsáveis pelo tratamento de dados, nos termos da legislação.

São direitos dos titulares dos dados pessoais:

a) A confirmação da existência de tratamento (art. 18, I)

O direito à confirmação da existência de tratamento decorre lógica e juridicamente dos princípios do livre acesso e da transparência (art. 6º, IV e VI). Refere-se ao direito garantido ao titular de confirmar se o controlador ou operador realiza o tratamento de seus dados pessoais.

O direito à confirmação da existência de tratamento pode ser efetivado de forma simplificada e imediata (com a negativa ou afirmativa da existência do tratamento) ou em formato completo, no prazo de 15 dias, ou seja, através da declaração clara e completa, que indique a origem dos dados, a inexistência de registro, os critérios utilizados e a finalidade do tratamento (art. 19, I, II), respeitando-se os segredos comercial e industrial.

b) Acesso aos dados (art. 18, II)

O acesso aos dados, também decorrente dos princípios do livre acesso e da transparência (art. 6º, IV e VI), garante aos seus titulares o direito de obter uma cópia de seus dados pessoais, dentre outras informações relacionadas.

O direito de acesso compreende todas as informações constantes do art. 9º da LGPD, quais sejam: (1) informação sobre a finalidade específica do tratamento; (2) informações sobre a forma e a duração do tratamento, observados os segredos comercial e industrial; (3) a identificação do controlador; (4) informações de contato do controlador; (5) informações acerca do uso compartilhado de dados pelo controlador e a finalidade; (6) as responsabilidades dos agentes que realizarão o tratamento; e (7) os direitos do titular, com menção explícita aos direitos contidos no art. 18 desta Lei.

A consulta quanto à forma e duração do tratamento, assim como em relação à exatidão dos dados pessoais é gratuita, nos termos do art. 18, § 5º da LGPD.

Os dados devem ser armazenados em formato que favoreça o acesso pelo titular e poderão ser solicitados aos agentes de tratamento por via eletrônica ou impressa, conforme disposto no art. 19, § 2º, I e II. Assim como no caso da confirmação do tratamento, o titular pode requisitar o acesso em formato simplificado e imediato ou em formato completo, com o prazo de 15 dias para atender à solicitação.

c) Correção de dados incompletos (art. 18, III)

É garantido ao titular o direito à correção de dados incompletos, inexatos ou desatualizados, que consiste no direito de solicitar que os dados tratados sejam corrigidos ou atualizados. Trata-se de um direito que decorre do princípio da qualidade dos dados, previsto no art. 6º, V da LGPD.

Nos termos do art. 18, § 6º, a correção dos dados incompletos deve ser imediatamente realizada pelos agentes de tratamento.

d) Anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto na LGPD

O titular dos dados tem direito à anonimização. Essa prerrogativa, vale lembrar, consiste na "utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo" (art. 5º, XI). Cumpre observar que, uma vez anonimizados, os dados deixam de ser regidos pela LGPD, tendo em vista que perdem a qualidade de dados pessoais.

O bloqueio de dados, por sua vez, consiste na "suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados" (art. 5º, XIII). Esse bloqueio, nos termos da LGPD, é tanto um direito do titular (art. 18, III), quanto uma espécie de sanção a ser imposta pela Autoridade Nacional, nos termos do art. 52, X e XI da Lei.

A eliminação dos dados desnecessários, excessivos ou tratados em desconformidade com a legislação, por sua vez, decorre do princípio da necessidade (art. 6º, III).

e) Portabilidade dos dados (art. 18, V)

A LGPD prevê que o titular dos dados pode solicitar a portabilidade dos dados, ou seja, a transferência das suas informações pessoais a outro fornecedor de produto ou serviços. Para tanto, é necessária a requisição expressa, em conformidade com a regulamentação da autoridade nacional e observados os segredos comercial e industrial.

O direito do titular é regulamentado pelo § 7º do art. 18, o qual prevê que a portabilidade não pode incluir os dados já anonimizados do titular.

Em relação aos dados sensíveis, a LGPD autoriza ao titular de dados sensíveis solicitar a portabilidade, possibilitando a comunicação e o uso compartilhado, de forma excepcional à regra contida no art. 11, § 4º, I, que veda a *"comunicação ou o uso compartilhado entre controladores de dados pessoais sensíveis referentes à saúde com objetivo de obter vantagem econômica".*

A portabilidade dos dados trata-se de uma decorrência normativa da essencialidade da "autodeterminação informativa" do titular dos dados prevista no art. 2º, II, da LGPD.

f) Eliminação dos dados tratados com consentimento (art. 18, VI)

Em relação aos dados tratados com consentimento nos termos do art. 7º, I, a LGPD conferiu ao titular desses dados a prerrogativa de solicitar a eliminação dos dados, ou seja, a "exclusão de dado ou de conjunto de dados armazenados em banco de dados,

independentemente do procedimento empregado" (art. 5º, XIV), de forma definitiva e irreversível.

Contudo, a LGPD dispõe que há exceções a essa regra, ou seja, há situações em que o direito de eliminação de dados tratados com o consentimento não pode ser exercido. São elas as hipóteses previstas no art. 16 da LGPD, vale lembrar: (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.

g) Informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados (art. 18, VII)

Em decorrência do princípio da transparência (art. 6º, VI), a LGPD incluiu no rol de direitos do titular a garantia de informações sobre o compartilhamento de seus dados, ou seja, é direito do titular saber exatamente com quem, sejam entidades públicas ou privadas, o controlador está compartilhando os seus dados pessoais.

h) Informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa (art. 18, VIII)

Com fundamento no direito à autodeterminação informativa, aos princípios da boa-fé e da transparência, o titular dos dados pessoais deve ser informado sobre a possibilidade de não fornecer o consentimento e as consequências caso o consentimento seja negado. Esse direito está relacionado à premissa de que o consentimento deve ser pedido e concedido de forma clara, transparente e totalmente livre.

i) Revogação do consentimento, nos termos do § 5º do art. 8º desta Lei (Art. 18, IX)

O consentimento para o tratamento de dados pessoais (art. 7º, I), pode ser revogado a qualquer momento mediante manifestação expressa do titular, por procedimento gratuito e facilitado, ratificados os tratamentos realizados sob amparo do consentimento anteriormente manifestado, enquanto não houver requerimento de eliminação (art. 7º, § 5º). Esse direito do titular previsto na LGPD também decorre do direito de autodeterminação informativa.

Cumpre destacar que a revogação do consentimento não implica na eliminação automática de dados coletados valida e licitamente. Para tanto, a revogação do consentimento deve ser acompanhada, de forma expressa, com a requisição da eliminação dos dados, nos termos do art. 18, III da LGPD.

j) Direito à explicação e à revisão de dados (art. 20, caput e § 1º)

O direito à explicação corresponde ao direito do titular de receber informações suficientes para a compreensão da lógica e os critérios utilizados para o tratamento de seus dados. Já o direito à revisão diz respeito ao direito do titular de requisitar a revisão de uma decisão totalmente automatizada que possa ter um impacto nos seus interesses, sobretudo quando relacionados à definição de seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade.

k) Direito ao acesso à justiça

A LGPD também cuidou de enfatizar, em seu art. 22, que a defesa dos interesses e dos direitos dos titulares de dados poderá ser exercida em juízo, individual ou coletivamente, na forma do disposto na legislação pertinente, acerca dos instrumentos de tutela individual e coletiva.

CAPÍTULO 4 – TRATAMENTO DE DADOS PESSOAIS PELO PODER PÚBLICO

4.1 Introdução

Considerando o regime jurídico específico ao qual se submete a Administração Pública, a LGPD dedica um capítulo específico ao tratamento de dados pelo poder público. A opção é justificada, afinal, a atividade administrativa submete-se a princípios e regras específicas, ao mesmo tempo em que tem sua razão de existir da persecução do interesse público. Tal conjugação resulta, por um lado, em prerrogativas próprias e, por outro, na imposição de deveres e um regime fiscalizatório também distintos, cenário no qual se incluem as atividades que envolvem dados pessoais.

A utilização de dados é elemento estratégico para que a Administração atinja seus objetivos constitucionais na sociedade contemporânea. Nesse sentido, Miriam Wimmer afirma que *"[c]onhecer seus cidadãos é, para o Estado, pré-requisito para o desempenho de suas finalidades públicas."*[6] Mais do que uma ferramenta disponível, a gestão de dados com uso das tecnologias de informação modernas é uma agenda, uma medida a ser adotada em diversas frentes e que permite a realização dos fins constitucionais do Estado de modo eficiente. A compreensão é compartilhada pelo STF, que, no julgamento da medida cautelar na ADPF nº 695, pelo voto do Min. Gilmar Mendes, afirmou:

> É assente na literatura estrangeira o reconhecimento de que países comprometidos com uma agenda de um governo digital podem aprimorar os resultados de gestão utilizando novas tecnologias de forma responsiva, protetiva e transparente. Nesse aspecto, o tratamento de dados torna-se importantíssima ferramenta para o desenho, implementação e monitoramento de políticas e de serviços públicos essenciais. (ADPF nº 695, voto Min. Gilmar Mendes, fl. 25)

Por outro lado, a atuação do setor público mediante o uso desses recursos recursos não pode ser desmesurada, devendo sempre respeitar as garantias democráticas. É nesse sentido que, no precedente supracitado, o Tribunal propõe uma interpretação não dicotômica entre os interesses imediatos da Administração e os direitos dos seus tutelados, mas sim uma visão integradora e harmoniosa:

> (...) mesmo que se entenda que o direito fundamental à proteção de dados pessoais não é absoluto, é inequívoco que se deve buscar uma harmonização dos interesses do Estado tutelados constitucionalmente com os imperativos de proteção de garantias individuais. (ADPF nº 695, voto Min. Gilmar Mendes. 28)

[6] WIMMER, Miriam. Proteção de dados pessoais no Poder Público: incidência, bases legais e especificidades. Revista do Advogado, nº 144, nov/2019, p. 127.

A posição não seria isolada na jurisprudência do Tribunal, mas o resultado de uma contínua evolução da sua compreensão sobre a matéria. Ao encontro disso, também podem ser mencionados como importantes precedentes a Suspensão de Liminar 1.103 MC, quando foi determinado ao IBGE que se abstivesse de fornecer ao Ministério Público Federal dados para a identificação de crianças sem registro de nascimento no município de Bauru/SP, e o Mandado de Segurança nº 36.150 MC, que determinou a cassação de determinação do Tribunal de Contas da União para que o Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira – INEP fornecesse dados individualizados à auditoria do Programa Bolsa Família, entendendo que a finalidade dos dados mantidos pelo INEP era distinta daquela para a qual seu uso estava sendo visado.

Nesse panorama, dando continuidade ao exame da LGPD, é pertinente retomar o princípio da legalidade, um dos princípios fundamentais previstos no art. 37 da Constituição da República e cuja incidência nesse âmbito significa que a Administração não poderá agir se não com base na lei. As atividades de tratamento de dados não fogem à regra. Outrossim, além de se submeterem às normas do ordenamento jurídico, a Administração não poderá se furtar de realizá-lo para cumprir suas obrigações e realizar suas finalidades, de modo que, conforme as hipóteses listadas no art. 11, II da LGPD, não será necessário o consentimento do titular dos dados.

Como não poderia deixar de ser, a atividade deve se dirigir à realização do interesse público. Além disso, devem ser disponibilizadas aos titulares dos dados, preferencialmente nos portais institucionais dos órgãos e entidades, informações claras e atualizadas sobre a previsão legal autorizadora da operação, a finalidade, os procedimentos e as práticas utilizadas pelo Poder Público. É essa a previsão do art. 23, que inaugura o capítulo da LGPD dedicado ao tratamento de dados na Administração Pública:

> **Art. 23. O tratamento de dados pessoais pelas pessoas jurídicas de direito público referidas no parágrafo único do art. 1º da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação), deverá ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público, desde que:**
>
> **I - 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;**
>
> **II - (VETADO); e**
>
> **III - seja indicado um encarregado quando realizarem operações de tratamento de dados pessoais, nos termos do art. 39 desta Lei; e**
>
> **IV - (VETADO).**

Vale mencionar que a necessidade de indicação de servidor encarregado, prevista no inciso III supracitado, é medida salutar para o controle e a fiscalização das operações.

4.2 A Administração Pública e o acesso à informação de interesse público

Outro princípio basilar da Administração Pública, também positivado no art. 37 da Constituição da República, é o princípio da publicidade, que detém importância intrínseca, além de promover o cultivo de virtudes cívicas e propiciar condições de fiscalização da atividade administrativa. Esse contexto não permite conclusão diversa daquela segundo a qual o fato de existirem institutos e procedimentos específicos instituídos pela legislação nacional de proteção de dados não exime a Administração de observar as demais normas relativas à transparência e ao acesso à informação.

Em outras palavras, a proteção à privacidade não pode impedir a divulgação de informações de inegável interesse público. Essa foi a tônica da manifestação exarada no Parecer nº 16.248, de 23 de julho de 2020, que destacou a necessidade de promover uma interpretação sistemática da LGPD e da Lei de Acesso à Informação (LIA), a Lei Federal nº 12.527, de 18 de novembro de 2011:

> 16. A harmonia entre a LAI e a LGPD é medida premente. E deve ser o mote a guiar o intérprete de ambas as normas. Quanto mais a própria Administração Pública, ao tratar de temas que lhe são confluentes.
>
> 17. Para isso, imperioso destacar que da aplicação de regras direcionadas à transparência no trato da coisa pública não deverá decorrer, necessariamente, a lesão a direitos e interesses de terceiros. E, eventualmente, se de um decorrer o outro, caberá à Administração Pública adotar via diversa em que haja, senão a extirpação, a mitigação de eventuais efeitos gravosos sobre o direito protegido. Exigindo-se, caso assim seja, a presença de elementos de razoabilidade entre o dano causado e o benefício gerado pelo "ato de transgressão".

Na ocasião analisada no citado parecer, a harmonia entre os valores envolvidos foi alcançada nas próprias sugestões apresentadas pela consulente, resultante das atividades de grupo de trabalho interinstitucional:

> A ocultação parcial de dados de candidatos aprovados em concursos públicos, de representantes de sociedades contratadas e de credores de despesas públicas nas divulgações promovidas pelo Portal da Transparência – a exemplo da omissão da integralidade do número de documentos de identidade e registro e do endereço residencial – é medida razoável a fim de compatibilizar os deveres de transparência e de proteção de dados pessoais.

Outra situação solucionada por essa proposta é a possibilidade de divulgação da remuneração de servidores públicos em portais da transparência. A medida, que teve repercussões significativas no debate público quando começou a ser implementada no país, encontra guarida na jurisprudência pátria, com destaque para o julgamento unânime do STF no ARE 652777, atende às normas de transparência e não restaram inviabilizadas com a edição da LGPD.

4.3 Proteção de dados na administração indireta

As empresas públicas e as sociedades de economia mista, embora possuam natureza jurídica de direito privado, também compõem a Administração, figurando no que se designa como administração indireta e realizando a descentralização das atividades administrativas. No campo da proteção de dados, a LGPD adotou a distinção, utilizada pela jurisprudência brasileira para solucionar diversas questões, entre aquelas entidades que prestam serviços públicos e aquelas que desempenham atividade econômica, em regime de concorrência, com base nas hipóteses autorizadoras do art. 173 da Constituição da República.

No último caso, o tratamento conferido às empresas públicas e sociedades de economia mista deve ser, nos termos constitucionais, "a sujeição ao regime jurídico próprio das empresas privadas, inclusive quanto aos direitos e obrigações civis, comerciais, trabalhistas e tributários". É essa a base constitucional da previsão do art. 24 da LGPD:

> Art. 24. 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 dispensado às pessoas jurídicas de direito privado particulares, nos termos desta Lei.
>
> Parágrafo único. 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, nos termos deste Capítulo.

Como exemplo pertinente, pode-se indicar o caso da Companhia de Tecnologia da Informação do Estado de Minas Gerais – Prodemge, sociedade de economia mista que presta serviços públicos com repercussão econômica, muitas vezes atendendo às necessidades do próprio Estado de Minas Gerais, o que não inviabiliza a produção e comercialização de bens e serviços para a iniciativa privada, conforme legítima previsão do seu estatuto social.

A submissão da Prodemge às normas da LGPD foi objeto do Parecer nº 16.164, de 20 de dezembro de 2019, que esclareceu a necessidade de observância de diversas condições para a observância plena, pela consulente, às normas vigentes de proteção de

dados pessoais. Outras situações a envolver a Prodemge foram objeto das Notas Jurídicas nº 5.445, de 31 de março de 2020, e nº 5.673, de 14 de dezembro de 2020, que contribuíram para a consolidação de um ambiente de segurança jurídica nas atividades concernentes à matéria, ainda que sujeitas à dinamicidade das situações enfrentadas pela Administração direta e indireta.

4.4 Serviços notariais e de registro

O regime constitucional de 1988 tratou a prestação dos serviços notariais e de registro em caráter privado, mediante delegação do Poder Público (art. 236), com fiscalização do Poder Judiciário. Não obstante, a atividade submete-se à mesma regulação conferida à Administração Pública pela LGPD, conforme expresso no seu art. 23, §4º.

A previsão consagra de modo adequado o interesse público envolvido em tais serviços, o que é igualmente garantido pela obrigação imposta às serventias de fornecer à Administração acesso, por meio eletrônico, aos dados que detém medida que pode ser de grande valia para que a Administração desempenhe suas funções, inclusive nas atividades de fiscalização e cobrança da dívida ativa. A matéria é regulamentada pelo Conselho Nacional de Justiça (Provimento nº 74, de 31 de julho de 2018) e pelos atos normativos dos Tribunais de Justiça de cada Estado, valendo mencionar o contexto de expansão das bases de dados nacionais no setor, a exemplo da Central Notarial de Serviços Eletrônicos Compartilhados – CENSEC.

4.5. Compartilhamento e interoperabilidade de dados pessoais na Administração Pública

Consagrando mais uma ferramenta para a realização das atividades da Administração na persecução do interesse público e prezando pela eficiência, a LGPD prevê que os dados pessoais serão mantidos em ambientes que permitam sua transmissão a todos os órgãos e entes que deles possam fazer proveito na realização dos seus objetivos institucionais:

> Art. 25. 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.

A implementação da norma é um desafio ao qual responde progressivamente o poder público, afinal, demanda a atualização e manutenção de sistemas e parques tecnológicos, sem negligenciar os aspectos de segurança envolvidos em tal compartilhamento.

As disposições do art. 26 da LGPD situam-se precisamente na busca desse equilíbrio entre eficiência (pela ampliação do compartilhamento de dados) e proteção à privacidade e à segurança dos titulares de dados pessoais. O meio encontrado pela legislação foi autorizar, de modo genérico, o compartilhamento de dados pelo Poder Público (ou, de modo mais preciso, o uso compartilhado de dados) para o estrito atendimento às finalidades, especificamente consideradas, de execução das políticas públicas e atribuições legais de cada órgão e entidade.

Ao mesmo tempo, o compartilhamento de dados com entidades privadas – lembre-se, como já indicado no item 4.3, o que inclui as empresas públicas e as sociedades de economia mista que atuam em regime de concorrência – foi objeto de um regime mais restritivo, sendo vedado como regra e permitido nas hipóteses contidas no art. 26, §1º da LGPD, quais sejam:

> § 1º É vedado ao Poder Público transferir a entidades privadas dados pessoais constantes de bases de dados a que tenha acesso, exceto:
>
> I - Em casos de execução descentralizada de atividade pública que exija a transferência, exclusivamente para esse fim específico e determinado, observado o disposto na Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação);
>
> II - (VETADO);
>
> III - nos casos em que os dados forem acessíveis publicamente, observadas as disposições desta Lei.
>
> IV - Quando houver previsão legal ou a transferência for respaldada em contratos, convênios ou instrumentos congêneres; ou (Incluído pela Lei nº 13.853, de 2019)
>
> V - 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.

Os instrumentos que venham a implementar tais hipóteses (contratos e convênios) devem, ainda, ser comunicados à Autoridade Nacional de Proteção de Dados.

4.6. Responsabilidade do poder público

O regime de responsabilidade por violação das normas de proteção de dados pessoais também é distinto no âmbito da Administração Pública, o que preserva a probidade administrativa e observância a todos aqueles princípios que regem a atividade administrativa, além de ser medida concernente com a lógica de operação da administração, que atua na persecução do interesse público, e não do retorno econômico, como as unidades que atuam no mercado.

Dessa forma, a LGPD sela o seu capítulo dedicado ao tratamento de dados na Administração Pública, em seus arts. 31 e 32, reforçando a submissão dos órgãos e entes à Autoridade Nacional de Proteção de Dados. A atuação desta se dará não apenas de modo repressivo, solicitando as medidas cabíveis para fazer cessar violações à Lei, mas também preventivo, podendo solicitar relatórios de impacto e sugerir a adoção de padrões e boas práticas, medida que deve ser compreendida em conjunto com a autonomia dos entes federados.

Reforçando a necessidade de uma atuação preventiva e segura, a atuação desta Advocacia-Geral revela-se de grande valia. A atividade consultiva tem sido capaz de fornecer segurança ao administrador e prevenir situações que poderiam porventura ser objeto de contestação. É o que se observou, por exemplo, no contexto de edição do supracitado Parecer nº 16.164, de 20 de dezembro de 2019, no qual diversas indicações foram feitas para adequação plena das atividades pretendidas pela Prodemge ao regime da LGPD; e no Parecer nº 16.248, 23 de julho de 2020, também já indicado, que chancelou as medidas propostas para a divulgação adequada de dados de candidatos aprovados em concursos públicos e de representantes legais de contratados e credores da Administração.

O mesmo panorama foi assegurado no âmbito das atividades objeto da Nota Jurídica nº 5.690, 29 de dezembro de 2020, a qual respondeu a questionamentos do Comitê de Orçamento e Finanças – COFIN relativos a dados mantidos pela Companhia de Habitação do Estado de Minas de Gerais – COHAB, cuja divulgação submetia-se às hipóteses da LGPD e encontrava motivação na persecução ao interesse público e à eficiência. Na hipótese, além de agregar segurança à fundamentação aos atos pretendidos, foram indicadas medidas de mitigação de riscos, com esteio nos procedimentos previstos da LIA e regulamentados neste Estado pelo Decreto Estadual nº 45.969, tudo isso de modo a reforçar um ambiente de segurança jurídica na atuação da Administração Pública.

CAPÍTULO 5 – AGENTES DE TRATAMENTO DE DADOS PESSOAIS

5.1 Agentes

Para uma compreensão adequada da dinâmica instituída pela LGPD faz-se necessário ainda compreender quais os papéis, ou funções por ela definidos. Trata-se de divisão de atribuições relacionadas à proteção de dados pessoais que deve ser sempre visualizada em cada caso concreto. Quando inobservada, a sistematização permite que sejam atribuídas responsabilidades, de modo a superar a situação de violação do sistema de proteção de dados.

a) Controlador:

O art. 5º da LGPD, em seu inciso VI, define o controlador como a "pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais". Na prática administrativa, serão os órgãos ou entidades que detêm o banco de dados.

Ao controlador cabe obter o consentimento do titular de dados a serem tratados, quando necessário (art. 7º, §5º). Também será sua responsabilidade verificar se os demais requisitos para tratamento de dados foram observados e decidir se eles poderão ser disponibilizados ou enviados a interessado, mediante consulta.

O controlador também deve ter especial atenção com dados sensíveis, já definidos acima. Em relação a tais dados, deve observar as diretivas e instruções feitas pela Autoridade Nacional de Proteção de Dados (vide art. 11, §3º). Houve, ainda, especial atenção do legislador aos dados sensíveis relativos à saúde, como se depreende da limitação positivada no §4º do art. 11:

> **§ 4º É vedada a comunicação ou o uso compartilhado entre controladores de dados pessoais sensíveis referentes à saúde com objetivo de obter vantagem econômica, exceto nas hipóteses relativas a prestação de serviços de saúde, de assistência farmacêutica e de assistência à saúde, desde que observado o § 5º deste artigo, incluídos os serviços auxiliares de diagnose e terapia, em benefício dos interesses dos titulares de dados, e para permitir:**
>
> **I - a portabilidade de dados quando solicitada pelo titular; ou**
>
> **II - as transações financeiras e administrativas resultantes do uso e da prestação dos serviços de que trata este parágrafo.**

Ainda, o controlador deve manter registro das operações de tratamento de dados pessoais que realizar (art. 37) e, quando solicitado pela autoridade nacional, emitir relatório de impacto à proteção de dados, na forma do art. 38 da LGPD. Tais medidas promovem a transparência nas atividades do setor público e permitem a manutenção de um ambiente de segurança, e, afinal, são condizentes com o arcabouço principiológico positivado no art. 6º, notadamente com os princípios da transparência, segurança e prevenção, afinal, têm o condão de possibilitar à própria Administração demonstrar o cumprimento de todas as normas do sistema nacional de proteção de dados, angariando a confiança de toda a sociedade. Inobstante, também atendem à necessidade de responsabilização por eventuais violações e prestação de contas, também alçados à condição de princípio pela legislação.

Já em relação à possibilidade de exigência de relatório de impacto pela autoridade nacional, sua definição e conteúdo mínimo encontram-se no art. 5º, XVII da Lei em estudo, consistindo em "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. "

Por fim, caberá ao controlador indicar o encarregado pelo tratamento de dados, figura analisada a seguir.

b) Operador

A LGPD define o operador, em seu art. 5º, VII, como a "pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador". Nesse sentido, o operador atuará sempre a partir das instruções e condições indicadas pelo controlador que, afinal, detém o banco de dados, de modo que deverá se submeter aos limites e seguir as instruções técnicas indicadas por este.

É o que prevê o art. 39 da LGPD e o que foi destacado por ocasião do **Parecer nº 16.164, de 20 de dezembro de 2019:**

> Partindo do pressuposto de que o órgão ou entidade pública que detém o banco de dados é o controlador e a Prodemge, a operadora, condições essas que demandam a confirmação técnica por parte da consulente, entendemos ser suficiente a autorização por parte daquele, a qual deverá conter todas as instruções necessárias ao tratamentos dos dados, conforme dispõe o art. 39 da LGPD, in verbis:
>
> Art. 39. O operador deverá realizar o tratamento segundo as instruções fornecidas pelo controlador, que verificará a observância das próprias instruções e das normas sobre a matéria.

Novamente salta aos olhos a importância de se identificar corretamente, em cada caso concreto, quais as figuras e papeis envolvidos no manejo de dados pessoais. Além disso, a sintonia entre controlador e operador é essencial para a realização da atividade de modo seguro – deve-se ter em conta, de todo modo, a possibilidade de responsabilização solidária, que será retomada no tópico seguinte. Não por outro motivo a legislação refere-se ao conjunto formado por controlador e operador como agentes de tratamento (art. 5º, VIII).

Ao encontro disso, a LGPD prevê, em seu art. 50, que entre eles poderão ser estipuladas regras de boas práticas e governança, que podem incluir padrões técnicos e condições de organização e segurança, o que será novamente abordado no capítulo seguinte. Por ora, cabe indicar que, conforme também sugerido no Parecer supracitado, tal ajuste poderá ser formalizado mediante a celebração de termo de cooperação técnica.

Por fim, como já indicado em relação ao controlador, a previsão de manutenção de registro das atividades de tratamento de dados constante do art. 37 da LGPD também se aplica ao operador.

c) Encarregado pelo tratamento de dados pessoais

Na definição do art. 5º, VIII, encarregado é a "pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD)". Trata-se de uma espécie de fiscal da observância das normas de proteção de dados naquele ambiente, razão pela qual é também designado por data protection officer (DPO).

Desse modo, o encarregado, ou DPO, será imprescindível, desempenhando tarefas operacionais e funcionando como canal de comunicação entre as partes envolvidas na manutenção e no tratamento de dados. Assim, deve ser máxima a publicidade sobre sua identificação e informações de contato, divulgadas preferencialmente no portal eletrônico do controlador (art. 41, §1º).

O art. 41, §2º lista de modo mais específico as funções do encarregado:

> **§ 2º As atividades do encarregado consistem em:**
>
> **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.

Verifica-se, pois, que o encarregado desempenha função primordial na rotina do órgão, de modo que sua escolha é decisão da maior importância. Não por outro motivo o Decreto Estadual nº 48.237/2021 previu duas competências do Comitê Estadual de Proteção de Dados Pessoais relacionadas aos encarregados dos órgãos e entidades do Estado. Conforme o inciso VII do art. 5º compete ao Comitê formular orientações sobre a indicação do encarregado e, conforme o inciso VIII, orientar a rede de encarregados responsáveis pela implementação da Política Estadual de Proteção de Dados Pessoais.

Vale destacar que a LGPD não define se o encarregado deve ser pessoa física ou jurídica (questão especialmente relevante para o setor privado), ou mesmo se deve ser servidor do órgão ou agente externo. A única recomendação da Autoridade Nacional sobre a questão é de que sua indicação seja realizada por ato formal (como um contrato de prestação de serviços, no setor privado, e ato administrativo, no setor público).[7]

Outro ponto de especial interesse é a possibilidade de criação de equipe de apoio ao encarregado. Esse modo de dar suporte às atividades do encarregado é especialmente relevante tendo-se em conta o caráter multifacetado das suas tarefas, as quais reclamam, além de conhecimento sobre os aspectos jurídicos envolvidos na proteção de dados, trato com sistemas e demais questões de ordem técnica. É nesse sentido que afirma a Autoridade Nacional:

> Também é importante observar que a LGPD não proíbe que o encarregado seja apoiado por uma equipe de proteção de dados. Ao contrário, considerando as boas práticas, é importante que o encarregado tenha recursos adequados para realizar suas atividades, o que pode incluir recursos humanos.[8]

5.2 Responsabilidade civil por irregularidade no tratamento de dados

Como afirmado no início da presente seção, a definição dos agentes responsáveis pela manutenção e tratamento de dados pessoais, além de indicar uma divisão de tarefas importante para fins operacionais, cumpre a função de prevenir danos e indicar os respectivos responsáveis, quando da sua ocorrência. Trata-se de realização do princípio da responsabilização (art. 6º, X da LGPD) e hipótese consentânea com a necessidade de proteção aos direitos fundamentais envolvidos nesse sistema. A sistemática não foge à regra geral do ordenamento: quando houver lesão a direito (in casu, aos direitos do titular

[7] 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, p. 22.

[8] Ibid.

de dados pessoais), surgirá a obrigação de reparação, e as figuras do controlador, operador e encarregado ajudam a identificar sobre quem deverá recair a obrigação de proceder a tal reparação.

Vale mencionar, de partida, que a lesão aos direitos do titular dos danos pode ter natureza patrimonial, moral, individual ou coletiva, na dicção do art. 42. A enumeração exaustiva visa a garantir uma proteção abrangente aos direitos individuais do titular dos dados, de modo consentâneo com a noção ampla de direito fundamental à proteção de dados pessoais anteriormente explicitada.

Note-se também que a transgressão pode ocorrer de modo não individualizado, mas coletivo. Nesse sentido, alguns institutos típicos do sistema de tutela de direitos coletivos revelam-se pertinentes, o que foi consagrado pela LGPD na medida em que indica explicitamente a possibilidade de ajuizamento de ação de reparação por danos coletivos (art. 42, §2º).

Ainda em relação a possíveis repercussões processuais do sistema em análise, o art. 42, §1º também previu a possibilidade de inversão do ônus probatório pelo juiz "quando, a seu juízo, for verossímil a alegação, houver hipossuficiência para fins de produção de prova ou quando a produção de prova pelo titular resultar-lhe excessivamente onerosa". Trata-se de medida atenta à situação típica de hipossuficiência técnica na qual se encontram titulares que têm seus dados submetidos ao controle e tratamento realizado pelos agentes descritos acima, o que reclama, de fato, uma orientação dinâmica do ônus probatório.

Ainda em relação a possíveis repercussões processuais do sistema em análise, o art. 42, §1º também previu a possibilidade de inversão do ônus probatório pelo juiz "quando, a seu juízo, for verossímil a alegação, houver hipossuficiência para fins de produção de prova ou quando a produção de prova pelo titular resultar-lhe excessivamente onerosa". Trata-se de medida atenta à situação típica de hipossuficiência técnica na qual se encontram titulares que têm seus dados submetidos ao controle e tratamento realizado pelos agentes descritos acima, o que reclama, de fato, uma orientação dinâmica do ônus probatório.

Além disso, nos casos em que estiver configurada relação de consumo - hipóteses que também podem restar configuradas em contextos que envolvem a Administração, a exemplo da prestação de serviços públicos em que há relação contratual com o cidadão, o que deve ser analisado em cada hipótese específica – as normas da legislação de proteção de dados não excluirão as regras de responsabilidade previstas no microssistema consume-

rista, conforme expressa previsão do art. 45 da LGPD.[9]

A lesão aos direitos do titular quando do tratamento dos seus dados pessoais deve ser identificada levando-se em conta todo o contexto real existente, de modo que, ao mesmo tempo em que deve ser oferecida proteção suficiente à sua dignidade, também não devem ser cometidos exageros na responsabilização de agentes que atuaram com a devida cautela e adotaram as medidas viáveis e disponíveis à época. O sistema normativo de proteção de dados, afinal de contas, não deve causar desmesurado temor ou impossibilitar a atuação do administrador público. Ao fazê-lo em observância às regras vigentes e com uso dos dispositivos ao seu alcance, sua atuação estará resguardada de responsabilidade. É nesse sentido que se nota a importância da previsão do art. 44 da LGPD, que enumera, de modo exemplificativo, circunstâncias que deverão ser levadas em conta nessa análise:

> Art. 44. O tratamento de dados pessoais será irregular quando deixar de observar a legislação ou quando não fornecer 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.

Além de levar em conta tais circunstâncias, a responsabilização também deve levar em conta as hipóteses excludentes do art. 43, de modo que não haverá responsabilização dos agentes de tratamento (controlador e operador) quando não tiver havido tratamento algum de dados pessoais, ainda que lhes tenha sido atribuída tal função; que houve tratamento nos estritos limites da legislação de proteção de dados; ou que o dano decorreu de culpa exclusiva de terceiro ou da vítima, o titular dos dados pessoais. Nota-se que as previsões são um influxo das normas gerais de responsabilidade civil.

Nesse panorama, a LGPD prevê que o controlador e o operador serão responsáveis pela reparação do dano causado por tratamento de dados em inobservância da legislação, podendo haver, inclusive, solidariedade entre eles (art. 42, §1º, I). Nesse sentido, há uma confluência das figuras, uma elevação do papel de operador ao de controlador, quando aquele agir em descumprimento da lei ou das instruções lícitas dadas por este.

[9] De se mencionar, aliás, que, como lembra Laura Schertel Mendes, foi o Código de Defesa do Consumidor, em seu art. 43, o primeiro diploma normativo infraconstitucional a disciplinar a privacidade e a proteção de dados no contexto da evolução de tecnologias de bancos de dados, positivando condições para sua utilização em proteção ao consumidor (MENDES, Laura Schertel. A Lei Geral de Proteção de Dados Pessoais: um modelo de aplicação em três níveis. SOUZA, Carlos Affonso; MAGRANI, Eduardo; SILVA, Priscila (Coords.). Lei Geral de Proteção de Dados–Caderno Especial. São Paulo: Revista dos Tribunais, 2019, p. 44).

Como já destacado, a hipótese revela a sintonia que deve haver entre os agentes de tratamento de dados e vai ao encontro da previsão do art. 39 da mesma Lei, que atribui ao controlador a atribuição de fornecer instruções técnicas e fiscalizar o seu cumprimento pelo operador. Deve o administrador estar atento a essa condição, razão pela qual a celebração de termos de cooperação técnica ou de outros instrumentos que reduzam a termos instruções claras e explícitas do controlador (detentor, afinal, da base de dados) ao operador (que procederá ao seu tratamento), como foi sugerido no Parecer nº 16.164, de 20 de dezembro de 2019.

Ademais, também há responsabilidade solidária entre controladores diversos (art. 42, §1º, II) e aquele que reparar o dano manterá direito de regresso aos demais responsáveis, na medida da responsabilidade de cada um (art. 42, §4º). Nesse sentido, medida que pode se revelar salutar é o cultivo de uma cultura de integridade entre os servidores dos órgãos que lidam com dados pessoais e mesmo a assinatura de termos de confidencialidade por todos os servidores e empregados públicos que possuírem acesso a bases de dados pessoais com acesso restrito.

Antes de concluir a presente seção, é pertinente indicar que o regime de responsabilidade aqui analisado deve ser aplicado sem prejuízo da apuração de responsabilidade na esfera administrativa, tema também regulamentado pela LGPD (art. 52). Aliás, pode-se concluir que o regime de responsabilidade civil, em conjunto com as medidas de fiscalização e aplicação de sanções administrativas, constitui um último nível de aplicação do sistema de proteção de dados, que busca conferir efetividade às normas de proteção de dados[10]

[10] **Laura Schertel Mendes compreende o sistema da LGPD a partir de um modelo de aplicação de três níveis interrelacionados:**

a) qualquer tratamento de dados pessoais somente pode ser iniciado se atendidas as condições para a sua legitimidade (condições de legitimidade);

b) atendidas as condições de legitimidade, todo o tratamento de dados deve cumprir determinados procedimentos, que se encontram na Lei tanto na forma de direitos do titular como de obrigações dos agentes de tratamento (procedimentos para garantir a proteção de dados pessoais); e

c) em caso de violação a esse direito, são aplicáveis sanções administrativas e civis (sanções e reparação). (MENDES, Laura Schertel. A Lei Geral de Proteção de Dados Pessoais: um modelo de aplicação em três níveis. SOUZA, Carlos Affonso; MAGRANI, Eduardo; SILVA, Priscila (Coords.). Lei Geral de Proteção de Dados–Caderno Especial. São Paulo: Revista dos Tribunais, 2019.p. 47)

6.1 Segurança da informação, privacidade e risco

A proteção dos direitos dos titulares de dados e a garantia da sua privacidade passam obrigatoriamente pela segurança no armazenamento e na utilização de suas informações. Por esse motivo, além de ser um dos princípios elencados no art. 6º da LGPD, a Lei dedicou ao tema um capítulo específico.

Antes de passar às medidas e práticas indicadas no referido capítulo, porém, faz-se pertinente uma reflexão sobre suas bases e os desenvolvimentos mais atuais das concepções de privacidade que devem permear a atuação de todos os agentes de tratamento de dados. Isso porque a garantia efetiva de segurança e privacidade são continuamente submetidas a um aparente conflito com as possibilidades trazidas com o desenvolvimento tecnológico e com as necessidades da Administração Pública. Nesse panorama, duas considerações iniciais são importantes: a necessidade de uma concepção de privacidade que seja ampla e passe por todos os momentos do ciclo de geração e utilização dos dados e a visualização de que uma abordagem adequada deve ter em conta o risco como elemento intrínseco a tais atividades, tratando-o de modo adequado.

Em relação à primeira, um conceito de referência na literatura sobre a temática é o de privacidade desde a concepção (privacy by design). Trata-se de compreender que a privacidade deve ser garantida desde a concepção do serviço até a sua execução, mesmo após o término do tratamento de dados, concepção que foi incorporada pela LGPD em seu art. 46, §2º, e art. 47. Assim, a privacidade deve ser protegida em todo o ciclo de vida do projeto ou serviço que se utilize de dados pessoais, o que significa levá-la em conta desde os momentos iniciais de planejamento, o que pode garantir que as ferramentas desenvolvidas ou escolhidas para a realização da atividade tenham configurações e opções suficientes para garantir a segurança na utilização dos dados.

Para melhor compreender essa concepção faz-se referência aos sete princípios do privacy by design sistematizados por Ann Cavoukian.[11]

1. **Proativo, e não reativo; preventivo, e não corretivo:** a privacidade desde a concepção é um modelo que busca antecipar-se e prevenir violações de privacidade. Tal princípio deve ter como consequência um compromisso claro, em todos os níveis hierárquicos do órgão

[11] CAVOUKIAN, Ann. Privacy by design: The 7 foundational principles. Information and privacy commissioner of Ontario, Canada, v. 5, p. 12, 2009.

ou entidade, da necessidade de estabelecer e preservar altos padrões de privacidade; que tal compromisso seja público, constituindo uma cultura em constante aperfeiçoamento; e que sejam estabelecidos procedimentos para identificar falhas e corrigi-las antes que alguma violação ocorra.

2. **Privacidade como padrão (privacy as default):** a privacidade deve ser a regra, o modelo básico, e não a exceção. Há verdadeira presunção em favor da privacidade e todos os sistemas e procedimentos, em seu funcionamento normal, devem garantir a proteção aos dados, sem necessidade de qualquer ação ou pedido do titular. O princípio desdobra-se em alguns corolários: especificação dos propósitos (para a coleta de informações pessoais); limitação da coleta e minimização dos dados; e limitação do uso, retenção e divulgação. Ou seja, a coleta de dados deve ser realizada para atender a finalidades específicas, apenas quando e na medida do estritamente necessário para atingir aquela finalidade e gerando o menor número de dados, armazenados no menor número de bancos quanto possível e utilizados e divulgados igualmente com a menor abrangência possível.

3. **Privacidade incorporada ao design:** sistemas de TI, softwares, procedimentos e práticas devem incorporar a defesa à privacidade como componente essencial, de modo a diminuir riscos operacionais que resultem na sua violação.[12]

4. **Funcionalidade total – um jogo de resultado positivo, e não de soma zero:** a garantia da privacidade não deve ser compreendida como um "jogo de soma zero", ou seja, baseado no conflito perene entre a privacidade e os outros valores envolvidos. Ao contrário, a abordagem indicada é a de harmonizar a privacidade com os objetivos legítimos perseguidos com as práticas que envolvem o uso de dados pessoais, alcançando resultados efetivos e benéficos. Em outras palavras, a garantia da privacidade não é um ônus a ser compensado com outros ganhos. Incorporar a privacidade em tecnologias e processos não deve acarretar o sacrifício aos seus demais objetivos.

5. **Segurança de ponta a ponta - proteção durante todo o ciclo de vida dos dados:** como resultado dos princípios anteriores e com o fato de se levar em conta a privacidade desde a concepção dos processos e serviços, ela é garantida em todas as etapas da coleta e tratamento dos dados pessoais.

6. **Visibilidade e transparência:** deve-se prezar pela publicidade, transparência e pela aquiescência (compliance) às normas de proteção de dados existentes, o que gera confiança na instituição e um ciclo positivo de implemento de uma cultura de respeito às

[12] Princípio consagrado no art. 49 da LGPD: Art. 49. 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 nesta Lei e às demais normas regulamentares.

boas práticas para a proteção de dados. Desdobra-se nos elementos da responsabilização, abertura e aquiescência.

7. **Respeito à privacidade do usuário:** os melhores resultados são alcançados quando os titulares de dados são levados em conta com o máximo respeito e consideração pelos seus interesses e decisões. Assim, o princípio desdobra-se em práticas que assegurem, nos processos de tratamento de dados, o consentimento livre e informado, a precisão (as informações fornecidas devem ser claras, precisas e abrangentes), o acesso e, novamente, a aquiescência.

6.2 Medidas de segurança

Os sete princípios acima são referências para as práticas que envolvam a coleta e uso de dados pessoais em todos os setores, incluindo a Administração Pública. Ocorre que sua aplicação não garante, em absoluto, que incidentes nunca ocorrerão, afinal, trata-se de atividade que envolve risco. O que se propõe é a sua mitigação pela atuação preventiva e constante: devem ser avaliados recorrentemente os riscos envolvidos nas operações e, a partir desse mapeamento, implementadas soluções que previnam a ocorrência de incidentes de segurança.[13]

Com efeito, o mapeamento de riscos é atividade essencial para a garantia da privacidade. Igualmente, o registro das operações de tratamento é outra medida, esta com previsão expressa no art. 37 da LGPD.

Por fim, é pertinente citar que a LGPD indica que a autoridade nacional poderá dispor sobre padrões técnicos mínimos para garantia da segurança dos dados pessoais (art. 46, §1º). Deve-se mencionar, porém, que, além de eventuais diretivas que a autoridade nacional venha a editar, orientações com medidas de segurança e boas práticas podem ser encontradas em outros materiais e documentos, como as normas publicadas pela Associação Brasileira de Normas Técnicas. Nesse sentido, vale mencionar, com valor meramente de referência, que o Guia de Boas Práticas para Implementação da LGPD na Administração Pública Federal[14] contém recomendações para implementação do padrão técnica indicado pela ABNT (ABNT NBR ISO/IEC 27001, ABNT NBR ISO/IEC 27002, ABNT NBR ISO/IEC 27701 e ABNT NBR ISO/IEC 27002; ISO/IEC 29151 – Code of practice for personally identifiable information protection; CIS® (Center for Internet Security, Inc.®) Controls™ e ISO/IEC 29134 - Guidelines for privacy impact assessment.

[13] Vide SOMBRA, Thiago Luís; CASTELLANO, Ana Carolina H. Plano de Resposta a Incidentes de Segurança: reagindo rápido e de forma efetiva. *Revista do Advogado*, nº 144, nov/2019, pp. 168-173, p. 169.

[14] BRASIL. Guia de Boas Práticas. Lei Geral de Proteção de Dados. V. 2.0. Governo Federal, agosto/2020. Disponível em: https://www.gov.br/governodigital/pt-br/governanca-de-dados/guia-de-boas-praticas-lei-geral-de-protecao-de-dados-lgpd. Acesso em: 20 de maio de 2021.

Além disso, a ANPD publicou no dia 28/05/2021 o Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado, no qual, dentre as diversas diretivas não vinculantes e esclarecimentos sobre o regime nacional de proteção de dados pessoais, destacam-se os esclarecimentos relativos às funções de cada agente de proteção de dados. O guia pode ser acessado pelo link.

6.3 Incidentes de segurança e sua comunicação

Concretizado o risco referido acima, tem-se a ocorrência de um incidente de segurança, conceito que não encontra definição expressa na LGPD, que se limitou a trazer um rol exemplificativo, no caput do seu art. 46, de fatos assim considerados: acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

A partir de tais exemplos e dos conceitos da literatura sobre segurança da informação, pode-se chegar à seguinte definição: incidente de segurança é "qualquer evento adverso, confirmado ou sob suspeita, que afete a tríade da segurança da informação: confidencialidade, a integridade ou disponibilidade dos dados."[15]

Diante da sua ocorrência, uma providência exigida pela LGPD é a comunicação, pelo controlador, à autoridade nacional (art. 48). Algumas observações sobre esse expediente são necessárias. Em primeiro lugar, verifica-se que não é absolutamente todo evento adverso que ensejará tal comunicação, mas apenas aqueles que, no termo do dispositivo citado, *"possa[m] acarretar risco ou dano relevante aos titulares"*. A abertura deixada pelo conceito indeterminado de *"risco ou dano relevante"* deve ser suprida com a atuação motivada e transparente do administrador, observando a razoabilidade e comunicando apenas os incidentes reputados graves.

O mesmo raciocínio aplica-se ao prazo para realização de tal comunicação, que não foi fixado pela LGPD (fala-se em "prazo razoável" no art. 48, §1º) e se submete, igualmente, à razoabilidade aferida no caso concreto. Em relação aos casos em que a comunicação não for imediata, os motivos disso devem ser expostos, conforme previsão do art. 48, §1º, V.

Deve-se destacar também que os incidentes que reclamam comunicação à autoridade independem da existência de dolo ou culpa por parte de qualquer agente. Havendo o evento imprevisto e relevante, deve haver a comunicação, independentemente da constatação de elemento subjetivo por parte de qualquer agente. Não é relevante, ademais, para verificação do dever de comunicar, portanto, se o fato é oriundo de situação acidental ou incidental.

[15] SOMBRA, Thiago Luís; CASTELLANO, Ana Carolina H. Plano de Resposta a Incidentes de Segurança: reagindo rápido e de forma efetiva. Revista do Advogado, nº 144, nov/2019, pp. 168-173, p. 169.

Apesar de o art. 48 referir-se ao controlador como aquele obrigado a realizar a comunicação, vislumbra-se a possibilidade de que a tarefa seja realizada pelo operador, o que pode ser estabelecido por cláusula contratual ou cláusula em termo de cooperação técnica – novamente pertinente a referência ao Parecer nº 16.164, de 20 de dezembro de 2019.

A comunicação deve ser abrangente e transparente, levando ao conhecimento da autoridade nacional o maior número de informações e as mais aprofundadas tanto quanto possível. Ademais, há um conteúdo mínimo a ser observado, previsto nos incisos do art. 48, §1º:

> 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.

Recebida a comunicação, a autoridade nacional avaliará o incidente e poderá impor medidas ao controlador em resposta ao incidente: a ampla divulgação do fato em meios de comunicação; e medidas para reverter ou mitigar os efeitos do incidente (art. 48, §2º). Tais medidas, não obstantes, devem ser adotadas pelo controlador, operador ou encarregado logo que identificar o incidente, evitando sua perpetuação.

Por fim, a adoção de medidas adequadas será levada em conta pela autoridade no momento em que avaliar a gravidade do incidente. Conforme a previsão do art. 48, §3º, ele deverá perceber, notadamente, se "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."

Uma das medidas preventivas que deve ser adotada e se revelará importante para uma rápida e efetiva reação aos incidentes é a elaboração de um plano de resposta a incidentes e remediação. Trata-se de medida prevista pela LGPD para os planos de governança das instituições (art. 50, §2º, I, g), o que será retomado a seguir.

Thiago Sombra e Ana Carolina Castellano ensinam que o plano deverá ser formulado em três etapas.[16] A primeira, a fase de preparação, ocorre antes dos incidentes. Nela será

[16] SOMBRA, Thiago Luís; CASTELLANO, Ana Carolina H. Plano de Resposta a Incidentes de Segurança: reagindo rápido e de forma efetiva. Revista do Advogado, nº 144, nov/2019, pp. 168-173, p. 170 ss.

elaborado um documento que conterá, entre outras informações, a especificação dos procedimentos e responsabilidades para atuação diante do incidente, como a indicação de um comitê de gestão de crise e os canais a serem acionados. Já na fase de preparação, devem ser realizados testes e treinamento dos envolvidos na resposta ao incidente, última fase, na qual as medidas previstas no plano de resposta serão acionadas. Deverá haver a reunião das pessoas indicadas para atuar, identificação do incidente, acionamento das medidas mitigatórias, isolamento da área ou sistema em que ocorreu o incidente, para evitar seu alastramento e adoção das medidas de combate à ameaça e contenção de novos ataques. Ainda, as lesões devem ser avaliadas, assim como os riscos de novos incidentes, e todas as atividades devem ser registradas. Tais atividades poderão envolver consultorias e peritos externos, devendo haver sua previsão no plano de resposta.

6.4 Das boas práticas e da governança

Por fim, a LGPD traz dispositivos relacionados à implementação de boas práticas e de um sistema de governança que possibilitem tomadas de decisão transparentes e seguras para o trato de dados pessoais:

> Art. 50. Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais.
>
> § 1º Ao estabelecer regras de boas práticas, o controlador e o operador levarão em consideração, em relação ao tratamento e aos dados, a natureza, o escopo, a finalidade e a probabilidade e a gravidade dos riscos e dos benefícios decorrentes de tratamento de dados do titular.

A previsão é salutar. A implementação da segurança efetiva em relação aos direitos dos titulares é uma tarefa paulatina e que envolve o cultivo de uma cultura institucional de segurança e respeito. As boas práticas e os sistemas de governança são, assim, vetores para a efetivação dos princípios positivados no art. 6º da LGPD, de modo sensível às particularidades de cada caso e primando pela segurança.

Como já se pôde observar isso implica, para a Administração Pública, não apenas um dever de se abster de realizar operações lesivas ou excessivamente perigosas para a segurança dos dados pessoais, mas também uma atuação proativa no sentido de criar mecanismos que garantam sua proteção diante do risco existente nas operações de tratamento, âmbito no qual se insere o cultivo de boas práticas.

Trata-se, afinal, de uma dupla dimensão do direito à proteção de dados pessoais[17], reconhecida pela jurisprudência (vide, sobretudo, a decisão na ADI 6387). Além de uma dimensão subjetiva, que protege a autodeterminação informacional de cada indivíduo, o direito ostenta também uma dimensão objetiva, que transcende o âmbito individual para informar, sobretudo ao legislador, a necessidade de adoção de medidas amplas que determinem proteção geral aos dados pessoais pela adoção de mecanismos procedimentais e institucionais:

> Já em uma dimensão objetiva, a afirmação do direito fundamental à proteção de dados pessoais impõe ao legislador um verdadeiro dever de proteção (Schutzpflicht) do direito à autodeterminação informacional, o qual deve ser colmatado a partir da previsão de mecanismos institucionais de salvaguarda traduzidos em normas de organização e procedimento (Recht auf Organisation und Verfahren) e normas de proteção (Recht auf Schutz).
>
> Essas normas devem ser positivadas justamente para garantir o controle efetivo e transparente do indivíduo relativamente à circulação dos seus dados, tendo como chave-interpretativa da juridicidade desse controle a noção de consentimento. (ADI 6387, voto Min. Gilmar Mendes, fl. 26).

É essa, portanto, a diretriz positivada no dispositivo supracitado da LGPD, a proteger a dimensão objetiva do direito à autodeterminação informacional através da instituição de boas práticas e da governança. Esses são instrumentos para a efetivação daquele direito. Vale ressaltar, ainda, que tais regras devem ser sensíveis às particularidades de cada instituição, dos dados a serem mantidos e tratados e aos fins para os quais se direcionam o tratamento de dados, como se depreende do art. 50, §1º, da Lei.

Não obstante, deve-se destacar que a adoção de um programa de governança é medida facultativa. Sua adoção, portanto, submete-se aos juízos de oportunidade e conveniência e deve acompanhar um contexto de amadurecimento institucional no sentido da integridade e da segurança no tratamento de dados. Caso adotado, o programa de governança deve observar um conteúdo mínimo previsto pela LGPD no seu art. 50, §2º:

> I - implementar programa de governança em privacidade que, no mínimo:
>
> a) demonstre o comprometimento do controlador em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais;
>
> b) seja aplicável a todo o conjunto de dados pessoais que estejam sob seu controle, independentemente do modo como se realizou sua coleta;
>
> c) seja adaptado à estrutura, à escala e ao volume de suas operações, bem como à sensibilidade dos dados tratados;
>
> d) estabeleça políticas e salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade;

[17] MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014, p. 140., p. 176-177.

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;

Vale destacar a previsão de existência de planos de resposta a incidentes de segurança, instrumento já explicado na seção anterior, e a necessidade de constante atualização, não apenas levando em conta os avanços tecnológicos, mas também a evolução da realidade institucional e da cultura de preservação da segurança progressivamente implementada no órgão ou entidade.

Embora não seja obrigatória, a adoção de um programa de governança em privacidade de dados pessoais, assim como de todos os demais instrumentos destinados à prevenção de incidentes e minimização de danos, será levada em consideração quando da aplicação de eventual sanção, pela Autoridade Nacional de Proteção de Dados, aos agentes de tratamento de dados (art. 52, §1º, VIII e IX).

7.1 Noções gerais

Como já indicado acima, o sistema instituído pela LGPD pode ser visualizado como um modelo de aplicação em três níveis: (a) condições de legitimidade para que se inicie uma operação de tratamento de dados; (b) procedimentos de observância obrigatório para a realização de tais operações (direitos dos titulares e obrigações dos agentes de tratamento); (c) e, por fim, respostas aos casos de violação de direitos e procedimentos previstos na lei.[18]

Até aqui, tivemos como foco as duas primeiras etapas, abordando a terceira, parcialmente, no item 5.2 e em alguns tópicos do capítulo anterior. O presente capítulo é destinado à continuação do estudo desse terceiro nível, abordando a fiscalização e responsabilização administrativa pela violação da norma de proteção de dados, expedientes ligados à efetividade do sistema e que respondem à positivação, no art. 6º, X, da LGPD, da responsabilização e prestação de contas como princípios desse regime.

A criação da Autoridade Nacional de Proteção de Dados (art. 55-A) dá-se nesse sentido. Trata-se de órgão da Administração Pública federal, integrante da Presidência da República e dotado de autonomia técnica e decisória (art. 55-B), previsão compatível com as funções a ele atribuídas pela LGPD. Já vimos que à Autoridade cumpre editar atos normativos e solicitar relatórios técnicos; também vimos que incidentes de segurança devem ser comunicado a ela, previsão que tem relação com a função fiscalizatória e sancionatória da Autoridade. Além de zelar pela proteção de dados, de modo geral, cabe a ela "fiscalizar e aplicar sanções em caso de tratamento de dados realizado em descumprimento à legislação, mediante processo administrativo que assegure o contraditório, a ampla defesa e o direito de recurso" (art. 55-J, IV).

7.2 Compatibilização da LGPD com o regime público e as sanções aplicáveis

O estudo das sanções aplicáveis no âmbito da Administração Pública demanda uma interpretação dos dispositivos da LGPD sistemática e atenta às particularidades do regime do serviço público. Essa interpretação aponta, de modo geral, para a inaplicabilidade de sanções pecuniárias e pela convivência do regime sancionatório da LGPD com aqueles previstos na legislação administrativa de cada ente.

[18] MENDES, Laura Schertel. A Lei Geral de Proteção de Dados Pessoais: um modelo de aplicação em três níveis. SOUZA, Carlos Affonso; MAGRANI, Eduardo; SILVA, Priscila (Coords.). Lei Geral de Proteção de Dados–Caderno Especial. São Paulo: Revista dos Tribunais, 2019. p. 47

O próprio texto da LGPD foi atento às particularidades do setor público ao prever, no §3º do seu art. 52, que apenas algumas das sanções previstas no rol do seu caput serão aplicadas às entidades e aos órgãos públicos. Dessa forma, as sanções aplicáveis nesse âmbito são as seguintes:

a) advertência, com indicação de prazo para adoção de medidas corretivas;

b) publicização da infração, após devidamente apurada e confirmada a sua ocorrência;

c) bloqueio dos dados pessoais objeto da infração, até a sua regularização;

d) eliminação dos dados pessoais objeto da infração;

e) suspensão parcial do funcionamento do banco de dados objeto da infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador;

f) suspensão do exercício da atividade de tratamento dos dados pessoais objeto da infração pelo período máximo de 6 (seis) meses, prorrogável por igual período;

g) proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados.

Como se pôde notar, a LGPD excluiu do rol de sanções aplicáveis aos órgãos e entes públicos as sanções de caráter pecuniário, como a multa simples e a multa diária, previstas nos incisos II e III do art. 52, respectivamente. A escolha do legislador leva em conta o fato de que eventual aplicação de multa seria suportada pelos cofres públicos do ente político e que o patrimônio da Administração é utilizado na persecução do interesse público, e não do lucro. Ademais, subsiste a possibilidade de responsabilização para fazer frente aos direitos lesados do titular de dados (vide item 4.6), sanção de outra natureza e que não se confunde com as sanções de ordem administrativa ora analisadas. Além disso, as multas previstas nos incisos supracitados têm como base de cálculo o faturamento da pessoa jurídica de direito privado, grupo ou conglomerado, o que inviabiliza sua aferição em relação à Administração.

Em outro giro, a LGPD também positivou de modo expresso a convivência do seu regime sancionatório com os mecanismos sancionatórios presentes em outros diplomas. É o que se depreende do §2º do art. 52: "O disposto neste artigo não substitui a aplicação de sanções administrativas, civis ou penais definidas na Lei nº 8.078, de 11 de setembro de 1990 (Código de Defesa do Consumidor), e em legislação específica."

É também o que se depreende do já referido §3º do mesmo artigo, que prevê a aplicação das sanções listadas acima "sem prejuízo do disposto na Lei nº 8.112, de 11 de dezembro de 1990 [regime jurídico dos servidores públicos civis da União, das autarquias e das fundações públicas federais; aplica-se, nesse caso, o estatuto dos servidores civis do Estado], na Lei nº 8.429, de 2 de junho de 1992 (Lei de Improbidade Administrativa), e na Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação)."

Desse modo, o cometimento de infrações e a respectiva sanção aplicada pela Autoridade Nacional de Proteção de Dados não inviabiliza a aplicação, pela Administração do Estado, de sanções ao servidor que tenha violado o regime disciplinar ao qual se submete ou que tenha realizado conduta ímproba, como não poderia deixar de ser. Para tanto, deverão ser utilizadas as vias ordinárias das sindicâncias e processos administrativos disciplinares.

Em relação às sanções listadas acima, cabe apontar, ainda, que aquelas previstas nos incisos X, XI e XII do art. 52 (suspensão de banco de dado, suspensão e proibição, parcial ou total, da atividade de tratamento de dados), por serem sanções mais gravosas que as demais, só poderão se aplicadas com a observância de requisitos especiais. Nesse sentido, o §2º do art. 52 indica que só serão aplicadas após a imposição de ao menos uma das sanções previstas nos incisos IV, V e VI do mesmo dispositivo (os incisos II e III, como já explicado, não se aplicam à Administração Pública) pela mesma violação concreta das normas de proteção de dados e prevê que sejam ouvidos os órgãos com competência sancionatória aos quais o controlador esteja submetido, caso existam.

Em todo caso, as sanções poderão ser aplicadas cumulada ou isoladamente, mediante processo administrativo que garante a ampla defesa e em atenção às peculiaridades do caso concreto. Quanto a esta última condição, o §1º do art. 52 indica condições que sempre deverão ser levadas em conta:

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.

Vale ressaltar que a LGPD prevê expressamente a conciliação como veículo de resolução de conflitos no caso de vazamento de dados pessoais. A medida vai ao encontro do entendimento hodierno relativo à possibilidade de adoção do mecanismo no âmbito da Administração Pública e da cultura que tem sido cultivada por esta Advocacia-Geral. Nesse sentido, vale destacar a atuação da Câmara de Prevenção e Resolução Administrativa de Conflitos (CPRAC), unidade que tem sido vetor da implementação dessa cultura de solução consensual dos conflitos na Administração mineira.

Por fim, é pertinente indicar que o regime sancionatório da LGPD (arts. 52, 53 e 54) entrará em vigor no dia 1º de agosto de 2021, nos termos do art. 65, I-A, tendo optado o legislador por conferir maior tempo para o aprofundamento do conhecimento do regime de proteção de dados e implementação dos seus procedimentos, antes que possa haver punições pela sua violação.

REFERÊNCIAS

BIONI, Bruno Ricardo. Proteção de Dados Pessoais - A Função e os Limites do Consentimento. Forense, 10/2018.

BRASIL. Guia de Boas Práticas. Lei Geral de Proteção de Dados. V. 2.0. Governo Federal, agosto/2020. Disponível em: https://www.gov.br/governodigital/pt-br/governanca-de-dados/guia-de-boas-praticas-lei-geral-de-protecao-de-dados-lgpd. Acesso em: 20 de maio 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/assuntos/noticias/2021-05-27-guia-agentes-de-tratamento_final.pdf. Acesso em 26/07/2021.

CAVOUKIAN, Ann. Privacy by design: The 7 foundational principles. Information and privacy commissioner of Ontario, Canada, v. 5, p. 12, 2009.

GOVERNO DO ESTADO DO PARÁ. Procuradoria-Geral do Estado do Pará. LGPD: Lei Geral de Proteção de Dados Pessoais – Manual de Aplicação na Administração Pública. Disponível em: https://www.pge.pa.gov.br/sites/default/files/upload/ebook_lgpd_pge_gov_pa_2021_a5_b_10fev.pdf. Acesso em 27 de maio de 2021.

MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014.

_____. A Lei Geral de Proteção de Dados Pessoais: um modelo de aplicação em três níveis. SOUZA, Carlos Affonso; MAGRANI, Eduardo; SILVA, Priscila (Coords.). Lei Geral de Proteção de Dados–Caderno Especial. São Paulo: Revista dos Tribunais, 2019.

RODRIGUES, Silvio. "Direito Civil", São Paulo, 3º Volume, Ed. Saraiva,, 28ª ed, p. 60.

SOMBRA, Thiago Luís; CASTELLANO, Ana Carolina H. Plano de Resposta a Incidentes de Segurança: reagindo rápido e de forma efetiva. Revista do Advogado, nº 144, nov/2019, pp. 168-173.

WIMMER, Miriam. Proteção de dados pessoais no Poder Público: incidência, bases legais e especificidades. Revista do Advogado, nº 144, nov/2019.

ANEXO I - TABELA DE PARECERES E NOTAS JURÍDICAS DA CONSULTORIA JURÍDICA DA ADVOCACIA-GERAL DO ESTADO

PARECER/NOTA JURÍDICA	CLASSIFICAÇÃO TEMÁTICA	EMENTA
Parecer 16.164, de 20 de dezembro de 2019	Administração Pública Indireta. Sociedade de economia mista. Lei Geral de Proteção de Dados.	ADMINISTRAÇÃO PÚBLICA INDIRETA. SOCIEDADE DE ECONOMIA MISTA PRESTADORA DE SERVIÇO PÚBLICO. PRODEMGE. EXPLORAÇÃO DE ATIVIDADE ECONÔMICA EM SENTIDO ESTRITO. POSSIBILIDADE EM SITUAÇÕES ESPECÍFICAS. PREVISÃO NA LEI DE AUTORIZAÇÃO E NO ESTATUTO SOCIAL. ATRAÇÃO DO REGIME JURÍDICO DE DIREITO PRIVADO E AFASTAMENTO DO REGIME PÚBLICO, A DEPENDER A CARACTERIZAÇÃO DA ATIVIDADE. LEI GERAL DE PROTEÇÃO DE DADOS. NECESSIDADE DE ATENDIMENTO DAS INSTRUÇÕES DO CONTROLADOR DOS DADOS.
Parecer 16.248, de 23 de julho de 2020	Direito Administrativo e outras matérias de Direito Público. Transparência. Lei de Acesso à Informação. Lei Geral de Proteção de Dados.	DIREITO ADMINISTRATIVO. DIVULGAÇÃO DE DADOS PELA ADMINISTRAÇÃO PÚBLICA DO PODER EXECUTIVO. DADOS PESSOAIS. CANDIDATOS APROVADOS, REPRESENTANTES LEGAIS DE CONTRATADOS E CREDORES. CPF E OUTROS DADOS. PORTAL DA TRANSPARÊNCIA. LEI DE ACESSO À INFORMAÇÃO. LEI GERAL DE PROTEÇÃO DE DADOS. CONFLITO APARENTE. PONDERAÇÃO ENTRE PRINCÍPIOS CONSTITUCIONAIS.
Nota Jurídica 5.204, de 27 de fevereiro de 2019	Direito Administrativo e outras matérias de Direito Público. Convênios Administrativos. Termo de Cooperação.	MINUTA DE ACORDO DE COOPERAÇÃO QUE ENTRE SI CELEBRAM A ADVOCACIA-GERAL E A POLÍCIA CIVIL. COMPARTILHAMENTO DE BASES DE DADOS. REGISTROS DE PROPRIEDADE VEICULAR DO DEPARTAMENTO DE TRÂNSITO (DETRAN-MG), REGISTROS DE INFRAÇÕES ADMINISTRATIVAS, DADOS DE CADASTRO DE PESSOAS FÍSICAS E JURÍDICAS DISPONIBILIZADOS NA SUPERINTENDÊNCIA DE INFORMAÇÕES E INTELIGÊNCIA POLICIAL (SIIP) E DEMAIS REPOSITÓRIOS. BASE DE CADASTRO DE PESSOAS DO TRIBUNUS. LEI DE PROTEÇÃO DE DADOS PESSOAIS, LEI Nº 13.709/2018.

Nota Jurídica 5.252, de 15 de maio de 2019.	Direito Administrativo e outras matérias de Direito Público. Convênios Administrativos.	MINUTA DE ACORDO DE COOPERAÇÃO QUE ENTRE SI CELEBRAM A ADVOCACIA-GERAL DO ESTADO E O INSTITUTO MINEIRO DE AGROPECUÁRIA. COMPARTILHAMENTO DE BASES DE DADOS. REGISTROS DE PROPRIEDADES RURAIS, PRODUTORES E ESTABELECIMENTOS AGROINDUSTRIAIS. INFORMAÇÕES SOBRE O TRÂNSITO E ESTOQUE DE VEGETAIS, SEMOVENTES E MATERIAIS GENÉTICOS CORRELATOS. LEI DE PROTEÇÃO DE DADOS PESSOAIS, LEI N° 13.709/2018.
Nota Jurídica 5.445, de 31 de março de 2020	Acesso à informação. Proteção de dados pessoais.	DESENVOLVIMENTO DE PLATAFORMA DE APIS (INTERFACES DE PROGRAMAÇÃO DE APLICA) PELA PRODEMGE, EM PARCERIA COM O DETRAN-MG, PARA SERVIÇOS RELACIONADOS A VEÍCULOS E HABILITAÇÃO. DISPONIBILIZAÇÃO DE DADOS PESSOAIS MEDIANTE O CONSENTIMENTO DO RESPECTIVO TITULAR. PREVISÃO NA LEI DE ACESSO À INFORMAÇÃO. NECESSIDADE DE OBSERVÂNCIA DO PARECER JURÍDICO AGE/CJ 16.164 E DA LGPD.
Nota Jurídica 5.673, de 14 de dezembro de 2020	Acesso à informação. Proteção de dados pessoais. Compensação de dívidas. Cessão de uso.	LEI GERAL DE PROTEÇÃO DE DADOS. DISPONIBILIZAÇÃO DE DADOS CONTROLADOS PELO DETRAN/MG CONFIGURA FATO GERADOR DO TRIBUTO DENOMINADO TAXA DE SEGURANÇA PÚBLICA. PRESTAÇÃO DE SERVIÇOS QUE, AO MENOS HIPOTETICAMENTE, NÃO SE ENQUADREM NO FATO GERADOR DA EXAÇÃO. PRESTAÇÃO DE SERVIÇO PÚBLICO REMUNERADO POR PREÇO PÚBLICO (TARIFA). COMPENSAÇÃO FINANCEIRA DO DETRAN/MG. POSSIBILIDADE DE COMPENSAÇÃO DE DÍVIDAS QUE TENHAM ENTRE SI O DETRAN/MG E A PRODEMGE. PROIBIÇÃO À COMERCIALIZAÇÃO DE SISTEMAS" DE PROPRIEDADE DO ESTADO.
Nota Jurídica 5.690, de 29 de dezembro de 2020	Administrativo e outras matérias de Direito Público. Publicidade de informações. LAI e LGPD.	DIREITO ADMINISTRATIVO. COHAB. PUBLICIDADE DE INFORMAÇÕES. FUNDO ESTADUAL DE HABITAÇÃO. AUTORIZAÇÃO PARA A APRESENTAÇÃO DOS DADOS FINANCEIROS DOS CONTRATOS DE FINANCIAMENTO. VIABILIZAÇÃO DA CONSTITUIÇÃO DE FUNDO DE INVESTIMENTO EM DIREITOS CREDITÓRIO. LEI DE ACESSO À INFORMAÇÃO. LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS.

Nota Jurídica 5.708	Ato administrativo/Ato Normativo.	DIREITO ADMINISTRATIVO. ANÁLISE DE MINUTA DE DECRETO QUE REGULAMENTA A APLICAÇÃO DA LEI FEDERAL Nº 13.709, DE 14 DE AGOSTO DE 2018 – LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD) – NO ÂMBITO DA ADMINISTRAÇÃO PÚBLICA ESTADUAL DIRETA E INDIRETA.

ANEXO II – QUADROS SINÓPTICOS

Dos fundamentos da LGPD

FUNDAMENTO	DISPOSITIVO LEGAL DA LGPD	CONCEITO
Respeito à privacidade	Art. 2°, I	Tem como objetivo primordial garantir ao titular dos dados pessoais o controle sobre o acesso de terceiros à sua vida privada.
Autodeterminação informativa	Art. 2°, II	O indivíduo titular de dados pessoais deve ter controle, ou ao menos plena transparência, sobre a destinação dada às suas informações pessoais, bem como das metodologias utilizadas para tanto.
Liberdade de expressão, de informação, de comunicação e de opinião	Art. 2°, III	Visa garantir que as interpretações ao seu texto sejam realizadas em observância das liberdades de expressão, informação, comunicação e opinião, afastando qualquer entendimento que importe em censura.
Inviolabilidade da intimidade, da honra e da imagem.	Art. 2°, IV	Todas as operações de tratamento de dados pessoais devem observar o cuidado com a intimidade, a honra e a imagem dos titulares dos dados pessoais.
Desenvolvimento econômico e tecnológico e a inovação	Art. 2°, V	Visa garantir que o desenvolvimento da tecnologia e de suas utilidades seja compatível à proteção dos dados pessoais.
Livre iniciativa, a livre concorrência e a defesa do consumidor.	Art. 2°, VI	Tem como escopo demonstrar a plena aplicabilidade das normas de proteção dos dados pessoais com o desenvolvimento econômico do país.
Direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais	Art. 2°, VII.	Visa ampliar a proteção do titular dos dados pessoais para além dos direitos da personalidade, reafirmando a proteção à liberdade. A dignidade e a cidadania são fundamentos da República Federativa do Brasil, também reafirmados pela LGPD.

Principais conceitos da LGPD

TERMO/ EXPRESSÃO	DISPOSITIVO LEGAL DA LGPD	CONCEITO
Dado pessoal	Art. 5°, I	informação relacionada a pessoa natural identificada ou identificável;
Dado pessoal sensível	Art. 5°, II	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	Art. 5°, III	dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;
Banco de dados	Art. 5°, IV	conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico;
Titular	Art. 5°, V	pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;
Controlador	Art. 5°, VI	pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;
Operador	Art. 5°, VII	pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;
Encarregado	Art. 5°, VIII	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	Art. 5°, IX	o controlador e o operador;

Tratamento	Art. 5º, X	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;
Anonimização	Art. 5º, XI	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	Art. 5º, XII	manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;
Bloqueio	Art. 5º, XIII	suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados;
Eliminação	Art. 5º, XIV	exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado;
Transferência internacional de dados	Art. 5º, XV	transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro;
Uso compartilhado de dados	Art. 5º, XVI	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	Art. 5º, XVII	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	Art. 5º, XVIII	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	Art. 5º, XIX	órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento da LGPD em todo o território nacional.

Princípios da LGPD

PRINCÍPIO	DISPOSITIVO LEGAL DA LGPD	CONCEITO
Princípio da boa-fé	Art. 6°, caput.	Consiste em proceder com correção e dignidade, com a atitude pautada nos princípios da honestidade, da boa intenção e no propósito de a ninguém prejudicar. Em se tratando de dados pessoais, a boa-fé mostra-se basilar no equilíbrio dos interesses envolvidos, tendo em vista os riscos que envolvem a coleta e a utilização dos dados pessoais alheios.
Princípio da finalidade	Art. 6°, I	”realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades; ”
Princípio da adequação	Art. 6°, II	“compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento”;
Princípio da necessidade	Art. 6°, III	“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;”
Princípio do livre acesso	Art. 6°, IV	”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;”
Princípio da qualidade dos dados	Art. 6°, V	“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;”
Princípio da transparência	Art. 6°, VI	“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;”

Princípio da segurança	Art. 6°, VII	“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;”
Princípio da prevenção	Art. 6°, VIII	adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;
Princípio da não discriminação	Art. 6°, IX	“impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;”
Princípio da responsabilização e da prestação de contas	Art. 6°, X	“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.”

Hipóteses de tratamento de dados pessoais

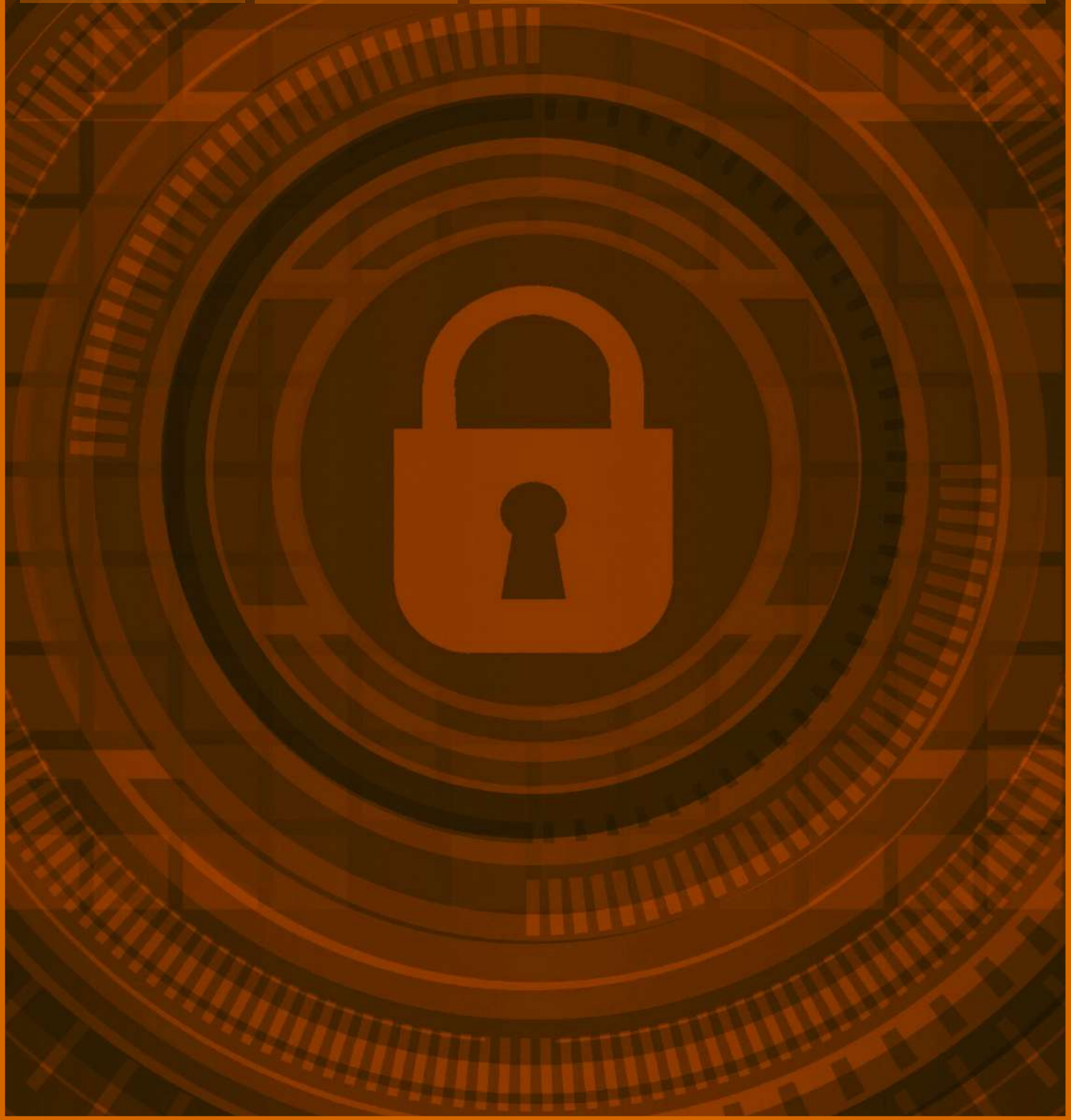
HIPÓTESES DE TRATAMENTO DE DADOS PESSOAIS	DISPOSITIVO LEGAL DA LGPD
Mediante o fornecimento de consentimento pelo titular	Art. 7°, I
Para o cumprimento de obrigação legal ou regulatória pelo controlador	Art. 7°, II
Pela administração pública, para o tratamento e uso compartilhado de dados necessários 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. 7°, III
Para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;	Art. 7°, IV
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. 7°, V
Para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei n° 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);	Art. 7°, VI
Para a proteção da vida ou da incolumidade física do titular ou de terceiro;	Art. 7°, VII
Para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária	Art. 7°, VIII

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; ou	Art. 7°, IX
Para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.	Art. 7°, X

Hipóteses de tratamento de dados sensíveis

HIPÓTESE DE TRATAMENTO DE DADOS SENSÍVEIS	DISPOSITIVO LEGAL DA LGPD	COMENTÁRIOS
Mediante consentimento expresso do titular	Art. 11, I	O consentimento precisa se dar de forma específica e destacado em cláusula própria
Cumprimento de obrigação legal ou regulatória	Art. 11, II, “a”	
Execução de políticas públicas	Art. 11, II, “b”	A política pública precisa estar prevista em lei ou em regulamentos (decretos ou portarias), não se admitindo, para esse caso, previsões constantes apenas em contratos, convênios e instrumentos congêneres
Estudos por órgãos de pesquisa	Art. 11, II, “c”	O órgão de pesquisa pode ser público ou privado e deve garantir sempre que possível a anonimização dos dados
Exercício regular de direitos	Art. 11, II, “d”	Hipótese que pode ser utilizada tanto para o titular quanto para o agente de tratamento e, inclusive, em contrato, processo administrativo e arbitral
Proteção da vida ou da incolumidade	Art. 11, II, “e”	A proteção pode ser do titular ou de terceiro
Tutela da saúde	Art. 11, II, “f”	Depende que o procedimento seja realizado exclusivamente por profissional de saúde, serviço de saúde ou autoridade sanitária

Prevenção à fraude e à segurança do titular	Art. 11, II, “g”	Apenas os processos de identificação e autenticação de cadastros em meio eletrônico não dependem de consentimento do titular, quando usados para prevenir fraudes. Isso inclui, por exemplo, o tratamento de dados necessários à gravação de voz para confirmação da identidade do titular ou a exigência de que o titular coloque o seu polegar em um leitor biométrico para confirmar sua identidade



Direitos em Espécie dos titulares dos dados pessoais

DIREITO EM ESPÉCIE	DISPOSITIVO LEGAL DA LGPD	CONCEITO	PRINCÍPIO/ NORMA RELACIONADO
A confirmação da existência de tratamento	Art. 18, I	Refere-se ao direito garantido ao titular de confirmar se o controlador ou operador realiza o tratamento de seus dados pessoais.	Princípios do livre acesso e da transparência
Acesso aos dados	Art. 18, II	Direito de obter uma cópia de seus dados pessoais, dentre outras informações relacionadas.	Princípios do livre acesso e da transparência
Correção de dados incompletos	Art. 18, III	Consiste no direito de solicitar que os dados tratados sejam corrigidos ou atualizados	Princípio da qualidade dos dados
Anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto na LGPD	Art. 18, IV	Anonimização: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo" (art. 5°, XI). Bloqueio de dados: suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados (art. 5°, XIII).	Princípio da necessidade.
Portabilidade dos dados		O titular dos dados pode solicitar a transferência das suas informações pessoais a outro fornecedor de produto ou serviços.	Decorrência normativa da "autodeterminação informativa"

Eliminação dos dados tratados com consentimento	Art. 18, VI	Solicitar a eliminação dos dados, ou seja, a “exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado” (art. 5º, XIV).	Decorrência normativa da “autodeterminação informativa”
Informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados	Art. 18, VII	Direito do titular saber exatamente com quem, seja entidades públicas ou privadas, o controlador está compartilhando os seus dados pessoais.	Princípio da transparência
Informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa	Art. 18, VIII	O titular dos dados pessoais deve ser informado sobre a possibilidade de não fornecer o consentimento e as consequências caso o consentimento seja negado.	Direito à autodeterminaçã o informativa eprincípios da boa-fé e da transparência
Revogação do consentimento	Art. 18, IX	O consentimento para o tratamento de dados pessoais (art. 7º, I), pode ser revogado a qualquer momento mediante manifestação expressa do titular, por procedimento gratuito e facilitado, ratificados os tratamentos realizados sob amparo do consentimento anteriormente manifestado enquanto não houver requerimento de eliminação (art. 7º, § 5º).	Decorre do direito de autodeterminaçã o informativa

Direito à explicação e à revisão de dados	Art. 20, caput e § 1°	O direito à explicação corresponde ao direito do titular de receber informações suficientes para a compreensão da lógica e os critérios utilizado para o tratamento de seus dados. Já o direito à revisão diz respeito ao direito do titular de requisitar a revisão de uma decisão totalmente automatizada que possa ter um impacto nos seus interesses, sobretudo quando relacionados à definição de seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade.	
Direito ao acesso à justiça	Art. 22	A defesa dos interesses e dos direitos dos titulares de dados poderá ser exercida em juízo, individual ou coletivamente, na forma do disposto na legislação pertinente, acerca dos instrumentos de tutela individual e coletiva.	

ANEXO III – PERGUNTAS E RESPOSTAS RELACIONADAS À LGPD

1) De acordo com a LGPD, quem é considerado parte do setor público?

Ao tratar do tratamento de dados pessoais pelo poder público, a LGPD faz menção às pessoas jurídicas listadas no parágrafo único do art. 1º da Lei de Acesso à Informação, quais sejam:

- os órgãos públicos integrantes da administração direta dos Poderes Executivo, Legislativo, incluindo os Tribunais 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.

O enquadramento das empresas públicas e sociedades de economia mista, porém, deve ser compreendido conforme o art. 24 da LGPD. Dessa forma, não estão incluídas no sentido de Administração Pública, para fins de aferição das regras de proteção de dados aplicáveis, aquelas que desempenham atividade econômica em regime de concorrência (sujeitas ao disposto no art. 173 da Constituição Federal). A elas, portanto, é dispensado o mesmo tratamento do setor privado.

De seu turno, empresas públicas e sociedades de economia mista que desempenham atividade econômica em regime de monopólio ou que prestam serviço público estarão submetidas ao tratamento dispensado ao setor público. Neste último caso, cabe apontar que a redação da LPGD é abrangente: “quando estiverem operacionalizando políticas públicas e no âmbito da execução delas”.

Diante disso, no caso de empresas públicas e sociedades de economia mista, o que se recomenda é uma análise cautelosa, em cada caso concreto, para verificar a qual tipo de atividade está relacionada (política ou serviço público ou atividade econômica, e, neste caso, em regime de mercado ou não) e, assim, indicar o regime da LPGD aplicável.

Por fim, é pertinente lembrar que a LGPD equiparou aos entes públicos os serviços notariais e de registro (art. art. 23, §4º).

2) Em quais hipóteses a Administração Pública pode tratar dados pessoais?

As hipóteses gerais (para o setor público e privado) autorizadoras estão listadas no art. 7º da LGPD:

I - mediante o fornecimento de consentimento pelo titular;

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

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

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

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

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

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

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

IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou

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

Em relação à Administração Pública cabe indicar que as hipóteses autorizativas são mais amplas, destacando a indicada no inciso três, qual seja, a execução de políticas públicas previstas em leis, decretos, portarias, contratos, convênios ou instrumentos congêneres (acordos de parceria, termos de cooperação, termos de ajustamento de conduto). Vale pontuar que, em todas as hipóteses listadas (incisos II a X), não é necessário o consentimento específico do titular, o que não desobriga a Administração de observar as demais regras e procedimentos da LGPD.

3) Quais obrigações o Poder Público assume ao realizar o tratamento de dados pessoais?

É importante que a Administração atue sempre de modo transparente, motivado e no estrito cumprimento dos procedimentos previstos na LGPD e em outros diplomas normativos. Algumas obrigações, porém, merecem destaque.

Em primeiro lugar, a Administração deverá indicar, com precisão, o enquadramento do caso concreto em uma das hipóteses autorizadas listadas acima. Além de indicar a hipótese, o ato deverá ser motivado e voltado para propósitos legítimos, informador ao titular.

Como já indicado, muitas das vezes não haverá necessidade de consentimento do titular, notadamente para a realização de políticas públicas. Não obstante, há exceções, como no caso de tratamento de dados de crianças e adolescentes, em que é imprescindível o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal (art. 14, §1º da LGPD), salvo nas hipóteses excepcionais previstas no §2º do mesmo artigo: quando a coleta do dado for necessária para contatar os pais ou responsável legal ou para a própria proteção da criança ou adolescente, vedado o armazenamento e transferência dos dados assim obtidos.

O órgão ou entidade também deverá divulgar, preferencialmente em seu portal na internet, informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades (art. 23, I da LGPD).

Além disso, é importante a indicação, pelo controlador, de um servidor que cumprirá a função de encarregado do tratamento de dados pessoais.

Também haverá necessidade de manter registro das operações de tratamento pelo controlador e pelo operador (art. 37).

Por fim, vale mencionar que também deverão ser observadas as normas que venham a ser emitidas pela Autoridade Nacional de Proteção de Dados (art. 30) e que alguns atos deverão ser comunicados a ela, como a realização de contratos e convênios que prevejam a transferência de dados pessoais pela Administração a entidade privada (art. 27), relatórios de impacto, quando por ela exigidos (art. 32) e a ocorrência de incidentes de segurança que possam acarretar risco ou dano significativos (art. 48).

4) A Administração Pública deverá informar o titular sempre que efetuar o tratamento dos seus dados pessoais?

Não haverá necessidade de consentimento ou de publicidade sobre a hipótese de tratamento nos seguintes casos:

a) realização de estudos por órgão de pesquisa (desde que anonimizados);

b) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral;

c) proteção da vida ou da incolumidade física do titular ou de terceiro;

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

e) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos.

Vale ressaltar que essa autorização para o tratamento não dispensa a administração da adoção de outras cautelas previstas na LGPD, notadamente quando houver tratamento de dados sensíveis.

5) Quais os instrumentos que podem ser utilizados pelo Poder Público como bases legais justificadoras do tratamento de dados pessoais?

Poderão ser emitidas portarias ou atos normativos similares das autoridades superiores, indicando as hipóteses autorizadoras, finalidades, procedimentos e práticas adotadas naquele órgão ou entidade, ato que deverá ser amplamente divulgado, preferencialmente em portais na internet (art. 23, I).

Também é recomendado que sejam incluídas cláusulas que prevejam e delimitem as atividades de tratamento de dados que porventura venham a ser realizadas em convênios, contratos, termos de cooperação técnica, acordos de pareceria e instrumentos congêneres. Esses instrumentos deverão ser utilizados, inclusive, para estipulação de boas práticas e regras de governança, padrões técnicas e condições de organização e segurança entre controladores e operadores (conforme previsão do art. 50 da LGPD).

Foi essa uma das recomendações indicadas no Parecer nº 16.164, de 20 de dezembro de 2019, cuja leitura é recomendada.

6) O sistema instituído pela LGPD altera as obrigações instituídas pela Lei de Acesso à Informação (LAI)?

Os sistemas de proteção de dados pessoais e de acesso à informação de interesse público devem conviver de maneira harmoniosa. Somente assim a Administração responderá, ao mesmo tempo, aos princípios da publicidade e ao direito à autodeterminação informacional.

Nesse sentido, a publicação da LGPD não destitui a Administração de cumprir as obrigações decorrentes da LAI, embora possa reclamar a adoção de determinadas cautelas a serem identificadas em cada caso concreto. É o que foi destacado no Parecer nº 16.248, de 23 de julho de 2020:

> (...) da aplicação de regras direcionadas à transparência no trato da coisa pública não deverá decorrer, necessariamente, a lesão a direitos e interesses de terceiros. E, eventualmente, se de um decorrer o outro, caberá à Administração Pública adotar via diversa em que haja, senão a extirpação, a mitigação de eventuais efeitos gravosos sobre o direito protegido

Dessa forma, pode se revelar necessária a anonimização de dados e procedimentos como a ocultação parcial de dados (por exemplo, a omissão da integralidade dos números de documentos de identificação).

7) A LGPD permite a divulgação de remuneração de servidores públicos?

A divulgação da remuneração de servidores públicos já era considerada, pela jurisprudência, medida legítima, afinal, trata-se de informação sobre a qual paira inegável interesse público e que não ofende a integridade ou privacidade dos titulares. Esse entendimento não foi alterado com a publicação da LGPD.

8) A Administração deve registrar as operações de tratamento de dados pessoais que realizar?

Sim, trata-se de obrigação expressamente prevista no art. 37 da LGPD: "[o] controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse."

Além disso, a Autoridade Nacional de Proteção de Dados poderá requisitar relatório de impacto à proteção de dados pessoais (art. 38), com conteúdo mínimo definido no definido pela lei: descrição dos tipos de dados coletados, metodologia utilizada para a coleta e para a garantia da segurança das informações e análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados.

9) Quais sanções podem ser aplicadas pela Autoridade Nacional de Proteção de Dados e a quem poderão ser aplicadas?

Os órgãos e entes da Administração não sofrerão sanções de cunho pecuniário, podendo sofrer as seguintes sanções:

a) advertência, com indicação de prazo para adoção de medidas corretivas;

b) publicização da infração, após devidamente apurada e confirmada a sua ocorrência;

c) bloqueio dos dados pessoais objeto da infração, até a sua regularização;

d) eliminação dos dados pessoais objeto da infração;

e) suspensão parcial do funcionamento do banco de dados objeto da infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador;

f) suspensão do exercício da atividade de tratamento dos dados pessoais objeto da infração pelo período máximo de 6 (seis) meses, prorrogável por igual período;

g) proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados.

Tais sanções serão aplicadas ao órgão ou entidade da Administração, ou equiparado, e não aos servidores, e não prejudicam a apuração de responsabilidade cível, penal ou no âmbito administrativo.

10) A fiscalização e a aplicação de sanções pela Autoridade Nacional de Proteção de Dados influenciam a apuração de irregularidade na esfera administrativa?

Ao encontro do que já se expôs acima, o poder disciplinar exercido pela Autoridade Nacional não se confunde, nem impede a atuação das autoridades administrativas do Estado. Há independência entre tais instâncias.

Dessa forma, servidores que cometam irregularidades ao lidarem com dados pessoais também poderão ser penalizados no âmbito administrativo, com base no estatuto dos servidores públicos do Estado, ao fim de processo administrativo disciplinar. Também poderão ser penalizados por cometimento de ato de improbidade administrativa.

Vale ressaltar, por fim, que a Autoridade Nacional deverá ouvir os respectivos órgãos com competência sancionatória quando aplicar as penalidades de suspensão do banco de dados e proibição parcial ou total de realização do tratamento, devendo considerar as informações colhidas para efeito de dosimetria da sanção.