LGPD

LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

MANUAL DE APLICAÇÃO NA ADMINISTRAÇÃO PÚBLICA

PGE
PROCURADORIA-GERAL
DO ESTADO DO PARÁ

GOVERNO DO PARÁ
POR TODO O PARÁ

LGPD

LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

MANUAL DE APLICAÇÃO NA ADMINISTRAÇÃO PÚBLICA

GOVERNO DO PARÁ
POR TODO O PARÁ

RICARDO NASSER SEFER
Procurador-Geral do Estado

ADRIANA FRANCO BORGES GOUVEIA
Procuradora-Geral Adjunta Administrativa

GUSTAVO TAVARES MONTEIRO
Procurador-Chefe da Procuradoria de Assessoramento Jurídico à Chefia do Poder Executivo

GRUPO DE TRABALHO:

CAROLINA ORMANES MASSOUD
Procuradora do Estado - Presidente

ENORÊ CORRÊA MONTEIRO
Procurador do Estado

RAFAEL FELGUEIRAS ROLO
Procurador do Estado

FABRÍCIO VASCONCELOS DE OLIVEIRA
Procurador Autárquico e Fundacional

JOÃO DE AQUINO PINTO NETO
Procurador Autárquico e Fundacional

NAGILA DA SILVA SAUAIA SOUSA
Procuradora Autárquica e Fundacional

APRESENTAÇÃO

A edição da Lei Geral de Proteção de Dados em 2018 e, mais recentemente, a entrada em vigor de parte relevante de suas disposições, fez nascer a necessidade de dar à Administração Pública subsídios para o tratamento de dados pessoais estabelecido pela norma. Daí por que a Procuradoria-Geral do Estado, como não poderia deixar de ser, instituiu Grupo de Trabalho para analisar a LGDP, o qual contou com a participação de Procuradores do Estado e de Procuradores Autárquicos e Fundacionais, a demonstrar a importância da advocacia pública atuante no Estado do Pará.

Como fruto do trabalho do Grupo, foi elaborado o presente Manual sobre a Aplicação da Lei Geral de Proteção de Dados Pessoais (LGPD) na Administração Pública, o qual, na esteira de outros materiais elaborados pela PGE, pretende orientar a atuação dos órgãos e entidades estaduais, desta feita quanto ao tratamento de dados pessoais de que dispõem, alcançando o fim último da norma federal.

O trabalho aborda conceitos, princípios, orienta sobre o tratamento de dados pessoais, em especial sob a ótica do Poder Público, bem como, dentre outros, propõe valiosíssimo roteiro de adequação e etapas de implementação do Programa de Governança em Privacidade, a auxiliar a Administração nesse importante mister.

Apresento-lhes, pois, o Manual sobre a Aplicação da Lei Geral de Proteção de Dados Pessoais (LGPD) na Administração Pública, e, ao tempo em que parabenizo o Grupo de Trabalho pela qualidade do produto entregue, recomendo sua leitura atenta por todos aqueles que compõem a Administração, que certamente serão recompensados com o brilhantismo de seu conteúdo.

RICARDO NASSER SEFER
Procurador-Geral do Estado do Pará

CAPÍTULO 1 - DISPOSIÇÕES GERAIS

Noções Gerais

A Lei Federal n. 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados – LGPD), dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural, devendo ser observada pela União, Estados, Distrito Federal e Municípios, ou seja, ela regula o tratamento de dados pessoais feito por pessoa jurídica de direito público ou privado, aí incluídos a Administração direta e indireta, inclusive fundações, empresas públicas e sociedades de economia mista.

Obrigatório atentar que os dispositivos legais se aplicam tanto a dados digitais, quanto a dados físicos.

Ao aplicar os dispositivos da disciplina da Lei Geral de Proteção de Dados, entenda que o legislador quer que você: respeite a privacidade; a autodeterminação informativa; a liberdade de expressão, de informação, de comunicação e de opinião; a inviolabilidade da intimidade, da honra e da imagem; o desenvolvimento econômico e tecnológico e a inovação; a livre iniciativa, a livre concorrência e a defesa do consumidor; e os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

Autodeterminação informativa é saber quais dados pessoais estão sendo coletados e qual a finalidade.

A Lei Geral de Proteção de Dados aplica-se a qualquer operação de tratamento: realizada no território nacional; que tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de

dados de indivíduos localizados no território nacional; ou que tenham sido coletados no terr itór io nac ional, considerando-se coletados no território nacional os dados pessoais cujo titular nele se encontre no momento da coleta.

A Lei não se aplica ao tratamento de dados pessoais realizado para fins exclusivos de: segurança pública; segurança do Estado; ou atividades de investigação e repressão de infrações penais, sendo vedado, nestas hipóteses, o tratamento dos dados por pessoa de direito privado, 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. Em tempo, o tratamento de dados pessoais para estes fins será objeto de legislação específica.

Conceitos

A LGPD trouxe as seguintes definições em seu art. 5º:

a) dado pessoal: é toda informação relacionada a pessoa natural identificada ou identificável;

b) dado pessoal sensível: é toda informação que se refere à 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 relacionado a uma pessoa natural;

c) dado anonimizado: é o dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento, ou seja, o dado que, submetido a técnicas próprias, não possa ser levado a identificar uma pessoa;

d) banco de dados: é o conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico;

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

f) controlador: é a pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais, quem dá ordens. Em tempo, a própria entidade controladora poderá realizar o tratamento dos dados;

g) operador: é a pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador, quem executa as ordens dadas pelo controlador. É possível que o operador e o controlador sejam pessoas diferentes (se, por exemplo, uma pessoa jurídica armazena dados a pedido de uma autarquia, a autarquia será controladora e a pessoa jurídica será operadora);

h) 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);

i) agentes de tratamento: são o controlador e o operador;

j) tratamento: é 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: é a utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo;

l) consentimento: é a manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada; m) bloqueio: é a suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados;

n) eliminação: é a exclusão de dado ou de conjunto de dados arma zenados em banco de dados, independentemente do procedimento empregado;

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

p) uso compartilhado de dados: é a 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;

q) relatório de impacto à proteção de dados pessoais: é a 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: é o 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; e

s) Autoridade Nacional: é o órgão da Administração Pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional. Suas competências e estrutura regimental constam na LGPD e no Decreto Federal n. 10.474, de 26 de agosto de 2020.

Princípios

Toda atividade de tratamento de dados pessoais deverá observar a boa-fé e, também, os seguintes princípios (art. 6º):

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

b) adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;

c) necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados per-

tinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;

d) 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;

e) 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;

f) 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;

g) 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;

h) prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;

i) não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos; e

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

CAPÍTULO 2 - DO TRATAMENTO DE DADOS PESSOAIS

Hipóteses autorizadoras

A Lei LGPD traz em seu art. 7º as hipóteses autorizadoras para o tratamento de dados pessoais, assim como prevê os requisitos para a sua execução.

No entanto, ainda que a situação fática enquadre-se em um dos incisos do art. 7º, é imprescindível saber que existem limites para a operação de tratamento. A validade da operação de tratamento de dados pessoais depende: a) do enquadramento da situação fática em um dos incisos do art. 7º; b) da observância dos princípios de proteção listados no art. 6º; e c) do respeito ao princípio da boa-fé objetiva.

Especificamente no caso do setor público, o tratamento de dados pessoais, além do dever de obediência aos princípios do art. 6º e ao da boa-fé, somente poderá ser realizado se estiver relacionado à execução de políticas públicas previstas em lei, regulamentos, convênios, contratos administrativos e instrumentos congêneres ou para cumprimento de obrigação legal ou regulatória da Administração.

Hipótese I - consentimento fornecido pelo titular dos dados

A regra geral estabelecida pela LGPD é a de que as operações de tratamento somente poderão ocorrer mediante consentimento do titular dos dados. O consentimento pode ser tido, após simples leitura da LGPD, como a "regra de ouro", pela qual se pauta toda a norma.

Para ser válido, precisa ser dado pelo titular de forma inequívoca, livre, desembaraçada e sem vícios, no bojo do qual ele manifesta sua concordância com o tratamento de seus dados pessoais para uma finalidade determinada.

Sobre o tópico, três situações merecem enfoque.

A primeira é a de que o consentimento do titular, nos casos em que o seu dado pessoal é tornado manifestamente público, não precisa ser expresso, podendo se dar de forma tácita, na forma como preconiza o §4° do art. 7°. Nesse caso, 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 de proteção listados no art. 6°.

A segunda é o fato de que o ônus da prova quanto ao consentimento fornecido pelo titular cabe ao controlador, que deverá demonstrar que o obteve sem qualquer tipo de vício[1].

A terceira refere-se à necessidade do controlador, quando compartilhar os dados pessoais obtidos com outros controladores, de obter consentimento específico do titular para esse fim, ressalvadas as hipóteses de dispensa de consentimento previstas em lei. Isso porque o consentimento autoriza tão somente o agente que o obteve, não se estendendo a outras pessoas.

Hipótese II - cumprimento de obrigação legal ou regulatória pelo controlador

A LGPD dispensa o consentimento do titular quando o tratamento de seus dados for efetuado com base nessa hipótese legal.

Nos casos de cumprimento de obrigação legal ou regulatória pelo controlador, é importante ter em mente que a LGPD não revoga ou impede a aplicação de normas setoriais que também regulamentam dados pessoais, as quais devem continuar sendo observadas[2].

Um exemplo típico de aplicação dessa hipótese é o cumprimento pelo Poder Público de requisições oriundas dos órgãos de controle,

1 São vícios de consentimento, o erro, o dolo, a coação, o estado de perigo e a lesão, previstos no Capítulo IV do Código Civil brasileiro.
2 A título de exemplo, temos as seguintes leis: Lei Federal n. 12.527/2011 (Lei de Acesso à Informação), Lei Federal n. 12.965/2014 (Marco Civil da Internet) e Lei Estadual n. 8.972/2020 (Lei do Processo Administrativo na Administração Pública Estadual).

solicitando a ficha funcional de determinado servidor público para fins de investigação de eventual irregularidade administrativa. A Administração não precisará do consentimento do servidor titular para realizar o tratamento e o compartilhamento de seus dados, pois estará cumprindo obrigação legal.

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

Muito embora a LGPD dispense o consentimento do titular, quando o tratamento de seus dados pessoais for efetuado ou utilizado pela Administração, para execução de políticas públicas, ele (o titular dos dados) tem o direito de conhecer as hipóteses legais que autorizam o processamento de seus dados, a finalidade do tratamento e a forma como o dado será tratado pelo Poder Público, devendo, ainda, ser observadas as regras previstas no art. 23 a 30.

Nesse aspecto, exige a LGPD que Administração Pública dê a devida publicidade, preferencialmente por informação clara e atualizada em seu sítio eletrônico, quando efetuar a operação de tratamento de dados pessoais, coletados por qualquer meio (online, digital ou analógico).

Hipótese IV - realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais[3]

O órgão de pesquisa pode ser tanto público (por exemplo, universidades públicas e institutos de pesquisa públicos) quanto privado.

A LGPD trouxe, ainda, quanto ao tópico, as seguintes regras:

3 A anonimização é uma técnica de processamento de dados que remove ou modifica informações que possam identificar uma pessoa. Essa técnica resulta em dados anonimizados.

a) desnecessidade de consentimento do titular do dado;

b) a divulgação dos resultados ou excertos do estudo ou pesquisa não poderá revelar dados pessoais;

c) o órgão de pesquisa será responsável pela segurança da informação e não poderá transferir os dados obtidos a terceiros;

d) na realização 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, conforme práticas de segurança previstas em regulamento específico e que incluam, sempre que possível, a anonimização ou pseudonimização dos dados, bem como considerem os devidos padrões éticos relacionados a estudos e pesquisas; e

e) 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 no âmbito de suas competências.

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

Essa hipótese exige consentimento específico do titular do dado, que poderá ser dado no momento da formalização do ajuste, não sendo necessário a renovação do consentimento, caso mantida a finalidade original.

Hipótese VI - para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei Federal n. 9.307, de 23 de setembro de 1996 (Lei de Arbitragem)

De acordo com a LGPD, é viável o tratamento de dados pessoais de servidores ou empregados públicos para fins de defesa dos inte-

resses da Administração Pública em processos judiciais, arbitrais ou administrativos, bem como permite-se às partes o direito de produzir provas umas contra outras, ainda que se refiram a dados pessoais do adversário, sem a necessidade de consentimento do titular do dado.

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

Essa hipótese retrata típico caso de dispensa de consentimento do titular do dado, citando-se, por exemplo, o tratamento de dados pessoais realizado no âmbito de atuação da Defesa Civil, visando a proteger a vida ou incolumidade física do titular ou de terceiro.

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

De acordo com a LGPD, hospitais públicos, serviços de saúde, assim como demais entidades sanitárias estão autorizadas a realizar o tratamento de dados sensíveis dos pacientes, sem o seu consentimento específico, visando à tutela da saúde.

Além disso, nos casos em que os dados relacionados à saúde de pacientes (dados sensíveis) se mostrarem indispensáveis à concretização de políticas públicas, o tratamento poderá ser efetuado no âmbito da Administração sem a necessidade de sequer informar o titular do dado. Nessa hipótese, além da dispensa de consentimento, também é dispensado o Poder Público do dever de informar o titular do dado acerca do tratamento realizado.

A Lei Federal n. 13.853/2019 conferiu a possibilidade de se acrescentar novas finalidades ao tratamento de dados pessoais de saúde que são de acesso público ou foram tornados públicos pelo titular, de acordo com as necessidades do tratamento.

Por fim, salienta-se que essa hipótese de tratamento é exclusiva

para procedimentos realizados por profissionais de saúde, serviços de saúde ou autoridade sanitária, voltando-se, tão somente, para a tutela da saúde do paciente titular do dado.

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

Trata-se de hipótese subsidiária, a ser aplicável por órgãos e entidades públicas somente se não houver o enquadramento da situação fática nos incisos II e III do art. 7º, ou seja, se a hipótese de tratamento não disser respeito à consecução de políticas públicas ou competências legais do controlador.

A LGPD não precisou quais seriam esses "interesses legítimos" do controlador ou de terceiro que justificariam o tratamento de dados. Não obstante, respaldado nas disposições da própria Lei, pode-se afirmar que é lícito o tratamento de dados pessoais fundado no legítimo interesse do controlador quando tiver por finalidade o "apoio e promoção de atividades do controlador" (art. 10, I), como seria o caso, por exemplo, de oferta de produtos e serviços. O mesmo pode se dizer com relação ao tratamento destinado à "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" (art. 10, II).

Para o correto enquadramento nesse inciso, deve-se ponderar, ainda, o seguinte:

a) quando o tratamento for baseado no legítimo interesse do controlador, somente os dados pessoais estritamente necessários para a finalidade pretendida poderão ser tratados;

b) o controlador deverá adotar medidas para garantir a transparência do tratamento de dados baseado em seu legítimo interesse,

ou seja, o titular do dado deverá ser comunicado sobre o tratamento realizado com base na hipótese legal citada, ainda que não seja necessário o seu consentimento específico;

c) 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: c.1) apoio e promoção de atividades do controlador; e c.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, nos termos da LGPD; e

d) ao optar pela utilização da base legal do legitimo interesse, a Administração Pública precisa avaliar eventual risco jurídico que essa opção pode apresentar, tendo em vista que os seus elementos deverão ser avaliados e documentados em relatório de impacto à proteção de dados pessoais, documento esse que poderá ser revisado e até contestado pela Autoridade Nacional de Proteção de Dados.

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

Dentre as leis que versam sobre proteção de dados pessoais no mundo, a brasileira é a única a prever a proteção ao crédito como uma de suas bases legais para o tratamento de dados.

A previsão possibilitou que a Lei Federal n. 12.414/2011 (Lei do Cadastro Positivo), recentemente alterada por intermédio da Lei Complementar Federal n. 166/2019, esteja em consonância com a LGPD, já que não é mais necessário obter o consentimento do titular/cadastrado para usar os seus dados conforme as finalidades previstas naquela Lei (formação de histórico de crédito). Sob esse aspecto, os dois textos convergem e conversam entre si.

Sobre o tema, é importante ressaltar que a Segunda Seção do Superior Tribunal de Justiça, no julgamento do REsp 1.419.697/RS, sub-

metido ao regime dos recursos repetitivos, definiu que, no tocante ao sistema *scoring* de pontuação[4], apesar de desnecessário o consentimento do consumidor consultado, devem ser a ele fornecidos esclarecimentos (dever de informação), caso solicitados, acerca das fontes dos dados considerados (histórico de crédito), bem como sobre as informações pessoais valoradas[5].

Consentimento do titular do dado

Sendo a proteção de dados pessoais um aspecto da privacidade e, esta, por sua vez, um dos direitos da personalidade, é evidente que o processamento desses dados exige, via de regra, o consentimento do titular. A LGPD consagra a plena autonomia do indivíduo em controlar o fluxo de suas informações pessoais (protagonismo do consentimento).

---

4 Trata-se de um método desenvolvido para avaliação do risco de concessão de crédito, que confere uma nota ao consumidor a partir da análise de dados referentes a operações de crédito contratadas por ele anteriormente.

5 TEMA REPETITIVO 710/STJ - RECURSO ESPECIAL REPRESENTATIVO DE CONTROVÉRSIA (ART. 543-C DO CPC). TEMA 710/STJ. DIREITO DO CONSUMIDOR. ARQUIVOS DE CRÉDITO. SISTEMA "CREDIT SCORING". COMPATIBILIDADE COM O DIREITO BRASILEIRO. LIMITES. DANO MORAL.

I - TESES: 1) O sistema "credit scoring" é um método desenvolvido para avaliação do risco de concessão de crédito, a partir de modelos estatísticos, considerando diversas variáveis, com atribuição de uma pontuação ao consumidor avaliado (nota do risco de crédito) 2) Essa prática comercial é lícita, estando autorizada pelo art. 5º, IV, e pelo art. 7º, I, da Lei n. 12.414/2011 (lei do cadastro positivo).

3) Na avaliação do risco de crédito, devem ser respeitados os limites estabelecidos pelo sistema de proteção do consumidor no sentido da tutela da privacidade e da máxima transparência nas relações negociais, conforme previsão do CDC e da Lei n. 12.414/2011.

4) Apesar de desnecessário o consentimento do consumidor consultado, devem ser a ele fornecidos esclarecimentos, caso solicitados, acerca das fontes dos dados considerados (histórico de crédito), bem como as informações pessoais valoradas.

5) O desrespeito aos limites legais na utilização do sistema "credit scoring", configurando abuso no exercício desse direito (art. 187 do CC), pode ensejar a responsabilidade objetiva e solidária do fornecedor do serviço, do responsável pelo banco de dados, da fonte e do consulente (art. 16 da Lei n. 12.414/2011) pela ocorrência de danos morais nas hipóteses de utilização de informações excessivas ou sensíveis (art. 3º, §3º, I e II, da Lei n. 12.414/2011), bem como nos casos de comprovada recusa indevida de crédito pelo uso de dados incorretos ou desatualizados.

III - RECURSOS ESPECIAIS PARCIALMENTE PROVIDOS."

O consentimento dado deve ser livre, informado, inequívoco, explícito e específico. Não cabe o consentimento genérico ou "no vazio", como uma espécie de "cheque em branco" fornecido pelo titular. Muito embora não seja necessário que o consentimento seja colhido em documento formal e padrão, é indispensável que ele seja dado de forma clara e direta dentro do que a LGPD preconiza.

Nesse ponto, sugere-se quando houver necessidade de se colher o consentimento do titular, que se faça de modo destacado de outras cláusulas que compõem contratos, convênios e outros instrumentos congêneres celebrados pelo Poder Público.

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.

Ademais, o uso pelos agentes de tratamento dos dados autorizados deve limitar-se à finalidade que fora expressamente autorizada pelo titular, sendo que qualquer outro uso demanda novo consentimento. Se o titular discordar da alteração, poderá revogar o seu consentimento, a qualquer tempo, por procedimento simplificado e gratuito.

A LGPD dispõe, ainda, ser nulo o consentimento dado, caso as informações fornecidas ao titular tenham conteúdo enganoso ou abusivo ou não tenham sido apresentadas previamente com transparência, de forma clara e inequívoca.

Frise-se que a obtenção de consentimento especifico do titular não é exigida da Administração Pública, quando ela efetuar o tratamento de dados com base nos incisos II, III, IV, VI, VII, VIII, IX e X do art 7º 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.

Por outro lado, a dispensa do consentimento não desobriga a Administração das demais obrigações previstas na LGPD, especialmente da observância dos princípios gerais de proteção e da garantia dos direitos do titular.

Quanto à revogação do consentimento, a LGPD esclarece que ela poderá ocorrer, 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, nos termos do inciso VI do caput do art. 18 da Lei.

Dados sensíveis

Como o próprio conceito sugere, tais dados demandam uma tutela jurídica diferenciada, pois podem sujeitar o titular a uma especial vulnerabilidade, qual seja: a discriminação. Isso porque quando se pensa em dados que mostrem a origem racial ou étnica, convicção religiosa, a condição de saúde, a vida sexual e a opinião política de determinada pessoa surge, inevitavelmente, a preocupação se haverá ou não no meio social discriminação e distinção dessa pessoa por conta de tais atributos inerentes a sua personalidade.

Então como se daria essa tutela jurídica especial que envolve os dados sensíveis?

Primeiramente, é importante saber que os dados pessoais sensíveis também poderão ser tratados com base no consentimento do titular (via de regra). Diferentemente do que é previsto para o tratamento de dados em geral, contudo, o consentimento que legitima o tratamento de dados sensíveis tem de ser específico, inequívoco e expresso e, ainda, o ser para finalidades determinadas. Nesse caso, sugere-se inclusive que o consentimento conste de cláusula destacada do instrumento jurídico celebrado.

É imprescindível, assim, que haja clareza nas informações que serão passadas ao titular a respeito do tratamento que será feito com os seus dados pessoais sensíveis – assim como no caso de dados pessoais não sensíveis -, sendo recomendável que se faça constar esses esclarecimentos nas políticas de privacidade dos agentes de tratamento.

Em segundo lugar, o tratamento de dados pessoais sensíveis so-

mente poderá ocorrer nas hipóteses taxativamente listadas nos incisos do art. 11 da LGPD, observando-se, sempre, o postulado da boa-fé e os princípios de proteção do art. 6° da LGPD.

Também se permite o tratamento de dados pessoais sensíveis sem o consentimento do titular (é a exceção), desde que voltado, exclusivamente, para o cumprimento de obrigação legal ou regulatória pelo controlador (art. 11, II, "a"); realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis (art. 11, II, "c"); exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral (art. 11, II, "d"); proteção da vida ou da incolumidade física do titular ou de terceiro (art. 11, II, "e"); tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária (art. 11, II, "f") e garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos (art. 11, II, "g"), hipóteses essas muito semelhantes – mas não idênticas - àquelas previstas para o tratamento de dados pessoais em geral.

Ao contrário, porém, do que acontece com os dados pessoais em geral, 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.

No caso do Poder Público, algumas outras regras precisam ser observadas:

a) é exigência da LGPD de que 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, pela Administração Pública, de políticas públicas previstas em leis ou regulamentos, deem 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 com base nas alíneas "c", "d", "e", "f" e "g" do inciso II do art. 11 da LGPD, não exige o consentimento do titular, bem como dispensa a Administração de garantir a publicidade; e

c) o controlador, antes de efetuar o tratamento de um dado sensível, deverá demonstrar que a situação fática posta enquadra-se em uma das alíneas, do inciso II, do art. 11 da LGPD, bem como justificar, de forma fundamentada, que o tratamento do dado sensível é indispensável para a Administração.

Tratamento de dados sensíveis na saúde

Sabidamente, dentre os setores que utilizam informações pessoais para diferentes finalidades, a área da saúde é um dos mais impactados pela LGPD. Afinal de contas, inúmeros dados sensíveis de pacientes fazem parte de prontuários médicos e das informações que um hospital necessita para realizar o seu atendimento.

No âmbito do SUS, por exemplo, existe uma cadeia interligada, que vai do ambulatório ao hospital, perpassando pelo laboratório, divisão de imagem, farmácia, paciente e agentes de saúde.

Um ponto importante da LGPD na saúde é que o setor não está obrigado a ter o consentimento expresso do titular em todas as situações de tratamento de dados (são as hipóteses de exceção tratadas principalmente nos arts. 7º, 10 e 11. A dispensa ocorre nos casos de proteção à vida ou tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; obrigação legal ou regulatória; para execução de contratos com o titular dos dados; em processos judiciais ou administrativos; quando há legítimo interesse do controlador; ou, ainda, no caso de estudo por órgãos de pesquisa.

A parte final do inciso VIII do art. 7º da LGPD, porém, deixou claro que a tutela da saúde refere-se exclusivamente a procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária.

Significa dizer que, no âmbito da assistência em saúde, aquelas prestadas tão somente por profissionais da área, a assinatura do consentimento do titular para o tratamento de seus dados pessoais de saúde não é essencial à prestação do serviço. Logo, o profissional de saúde possui o dever de prestar a assistência, independentemente da assinatura de termo de consentimento pelo titular.

De qualquer modo, mesmo nos casos em que o consentimento não é necessário, clínicas, prontos-socorros e hospitais estão obrigados a informar aos pacientes sobre a forma como os seus dados serão recolhidos e tratados. Recomenda-se, diante do princípio da transparência, que o profissional, hospital, pronto-socorro ou clínica, elabore uma declaração escrita, assinada pelo paciente, que se limite a informar que ele tomou conhecimento das informações.

Além disso, a Lei revela que 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 à prestação de serviços de saúde, de assistência farmacêutica e de assistência à saúde, incluídos os serviços auxiliares de diagnose e terapia, em benefício dos interesses dos titulares de dados.

Percebe-se, assim, que agora o tratamento e o compartilhamento de dados da saúde só poderão ser realizados em benefício do titular (jamais com mero intuito lucrativo) e deverão coexistir com os princípios gerais previstos na Lei Geral de Proteção de Dados, para que haja o respeito à boa-fé, à finalidade do tratamento, adequação, limitação do tratamento ao mínimo necessário para o cumprimento do seu propósito, garantia aos titulares do livre acesso aos seus dados, garantia da qualidade dos dados e de sua transparência, garantia de proteção aos dados, prevenção de danos em virtude do tratamento e a demonstração pelo agente de que adotou medidas eficazes e capazes de comprovar a observância das normas de proteção.

Tratamento de dados sensíveis voltado à realização de estudos por órgãos de pesquisas

Deve-se recordar a regra aplicável aos órgãos de pesquisa, públicos ou privados, quanto ao tratamento de dados pessoais, na realização de estudos em saúde pública.

De acordo com a LGPD, sempre que possível, deve-se manter a anonimização ou pseudoanonimização dos dados pessoais 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, a LGPD determina a adoção de práticas de segurança e a responsabilidade do órgão de pesquisa pela segurança da informação, visando a proteger os dados pessoais de eventual utilização indevida de terceiros.

Tratamento de dados pessoais de crianças e de adolescentes

O tratamento de dados de crianças e adolescentes deve ser realizado de acordo com o melhor interesse do menor, 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 (o que não ocorre no caso dos maiores de 18 anos).

Somente é dispensado referido consentimento em duas situações taxativamente previstas na LGPD: a) quando a coleta do dado for necessária para contatar os pais ou responsável legal; ou b) para a própria proteção da criança/adolescente. Nesses dois casos, os dados só poderão ser utilizados uma vez, vedado o seu armazenamento, e não poderão ser repassados a terceiro, salvo se houver consentimento específico na forma preconizada pela LGPD.

Instituições de ensino, públicas ou privadas, deverão se adequar aos ditames preconizados na LGPD, a fim de garantir maior transparência e zelo quando do tratamento de dados pessoais de crianças e

adolescentes estudantes. Portanto, é imprescindível que o agente de tratamento envide todos os seus esforços para colher o consentimento do responsável legal desses estudantes, sendo seu o ônus da prova de que o consentimento foi dado.

Dados anonimizados e pseudoanonimizados

A importância de se delimitar um dado como anônimo ou não é que a LGPD não se aplica a dados anonimizados.

Nesse aspecto, o legislador brasileiro optou pela utilização do critério da razoabilidade para delimitar o espectro dos dados pessoais. Assim, se para a ligação entre um dado e uma pessoa for demandado esforço fora do razoável, não há que se falar em dados pessoais. O dado, nesse caso, será considerado como anônimo. Vale frisar que um dado só é considerado efetivamente anonimizado se não permitir que, por via meios técnicos e outros, reconstrua-se o caminho para descobrir quem era a pessoa titular do dado - se de alguma forma a identificação ocorrer, então ele não é, de fato, um dado anonimizado.

A determinação do que é razoável deverá levar em consideração fatores objetivos, como custo e tempo necessários para reverter a anonimização, de acordo com as tecnologias disponíveis à época, e a utilização exclusiva de meios próprios. Finalmente, fica estabelecido que a Autoridade Nacional poderá dispor sobre padrões e técnicas utilizadas em processos de anonimização.

Já dados pseudonomizados são aqueles que, com a aplicação de diferentes estratégias de proteção, à primeira vista, podem parecer anônimos, mas, na realidade, permitem que o processo de anonimização seja revertido. Apenas os dados anonimizados estão efetivamente fora do escopo da LGPD. Uma vez que os dados pseudonimizados não perderam a sua capacidade de identificar uma pessoa, eles ainda são protegidos pela Lei.

É importante mencionar que, ao operar um processo de anonimização e manter a base de dados com todas as informações originais,

o controlador não está anonimizando os dados em questão, mas meramente adotando uma técnica de pseudonomização. Isso porque, ao manter a base de dados original em sua posse, o controlador pode, a qualquer momento, reverter o processo de anonimização e restaurar o caráter identificável dos dados.

Término do tratamento de dados

O término do tratamento dos dados é o evento que culmina no encerramento do tratamento e, via de regra, no descarte dos dados utilizados. As hipóteses de encerramento estão previstas nos incisos I a IV do art. 15 da LGPD, que assim dispõe:

a) quando a finalidade foi alcançada ou os dados deixaram de ser necessários ou pertinentes ao alcance da finalidade específica almejada: trata-se da concretização do princípio da finalidade previsto no art. 6º da LGPD, pois alcançada a finalidade pretendida com o dado coletado, o seu tratamento deverá ser encerrado;

b) fim do período de tratamento;

c) comunicação do titular, inclusive no exercício de seu direito de revogação do consentimento, resguardado o interesse público: a LGPD estabelece como um dos direitos do titular dos dados, a possibilidade de revogação do consentimento dado, a qualquer tempo, devendo o agente de tratamento criar condições para que a revogação possa se dar da forma mais simplificada e clara possível. A partir da revogação, o agente de tratamento deverá excluir os dados pessoais do revogante de seu banco de dados. Quando o Poder Público realizar o tratamento de dados, inclusive dados sensíveis, enquadrando-o em uma das hipóteses legais autorizadoras da dispensa de consentimento, eventual ato de revogação por parte do titular não produzirá quaisquer efeitos jurídicos na órbita do controlador, que poderá continuar realizando o tratamento; e

d) determinação da Autoridade Nacional, quando houver violação a LGPD: havendo violação a algum dispositivo da LGPD, a Autoridade

Nacional poderá determinar ao agente o fim do tratamento de dados pessoais, o que pode impactar severamente determinadas pessoas jurídicas, em especial aquelas que efetuam rotineiramente o tratamento de dados pessoais.

Término do tratamento e Administração Pública

No caso da Administração Pública direta ou indireta, a eliminação de dados pessoais tratados, deve obedecer, rigorosamente, as disposições contidas na Lei Federal n. 8.951/1991[6] e na Lei Estadual n. 8.543/2017[7].

Isso porque, os dados pessoais coletados pelo Poder Público passam a integrar o que se denomina "arquivo público" do órgão ou da entidade[8] e, portanto, sua eliminação deve obedecer à classificação arquivística pertinente contida em tabela de temporalidade de documentos[9].

Além disso, toda a eliminação de documentos no âmbito do Poder Executivo do Estado do Pará deverá ser precedida da Listagem de Eliminação de Documentos, de autorização prévia do Arquivo Público do Estado e da publicação de Edital de Ciência de Eliminação dos Documentos. Ao final, será levada a termo pelo Termo de Eliminação de Documentos.

Frise-se, ainda, que caso um dado pessoal coletado pela Adminis-

---

6 Dispõe sobre a política nacional de arquivos públicos e privados e dá outras providências.

7 Dispõe sobre a temporalidade de documentos públicos do Estado do Pará e dá outras providências.

8 Lei Estadual n. 8.543/2017: "Art. 1° - Entende-se por arquivos públicos as documentações produzidas, recebidas e acumuladas por órgãos públicos da administração direta, autarquias, fundações, empresas públicas pelo Poder Público, bem como entidades privadas encarregadas da gestão de serviços públicos".

9 Lei Estadual n. 8.543/2017: "Art. 17 - São instrumentos básicos de gestão de documentos os Planos de Classificação de Documentos e as Tabelas de Temporalidade de Documentos".

tração componha o conceito de documento de valor permanente[10], mesmo após exaurida a finalidade da coleta, ele deverá ser definitivamente preservado, jamais eliminado[11].

Término do tratamento e conservação de dados pessoais

A regra é que os dados pessoais sejam excluídos após o término do tratamento.

Essa regra, além dos casos já relatados envolvendo a Administração Pública, admite quatro exceções, todas reguladas no art. 16 da LGPD:

a) por cumprimento legal ou regulatório do controlador: ainda nesse caso devem ser mantidos apenas os dados necessários a essa finalidade, descartando-se os demais;

b) destinada aos órgãos de pesquisa, que estão autorizados a conservar os dados pessoais mesmo após o término do tratamento, apenas para estudo, vedando-se a sua utilização para qualquer outra finalidade;

c) mediante a transferência dos dados a terceiro: essa previsão res-

---

10 Lei Estadual n. 8.543/2017: "Art. 9º Os documentos de arquivo são identificados como: (...) III - documentos permanentes aqueles com valor histórico, probatório e informativo, que devem ser definitivamente preservados;".

11 Lei Estadual n. 8.543/2017:

v"Art. 12 - Os documentos de arquivo de guarda permanente devem ser preservados, em razão das informações nele contidas, para a eficácia da ação administrativa, como prova, garantia de direitos ou fonte de pesquisa.

Art. 13 - São considerados documentos de guarda permanente:

I - os indiciados nas Tabelas de Temporalidade de Documentos, que serão definitivamente preservados;

II - os arquivos privados de pessoas físicas ou jurídicas declaradas de interesse público e

III - todos os processos, expedientes e demais documentos produzidos, recebidos ou acumulados pelos órgãos da administração pública estadual, considerados de valor histórico, probatório e informativo, a partir da primeira Constituição do Pará.

Art. 14 - Os documentos de guarda permanente não poderão ser eliminados após a microfilmagem, digitalização ou qualquer outra forma de reprodução, devendo ser preservados pelo próprio órgão produtor ou recolhidos ao Arquivo do Estado.

Parágrafo único. Aqueles documentos recolhidos ao Arquivo do Estado, deverão estar avaliados, organizados, higienizados, acondicionados e acompanhados de instrumento descritivo que permita sua identificação, acesso e controle".

guarda o direito à portabilidade, isto é, o direito do titular de migrar os dados a outro fornecedor de serviço ou produto, desde que observados os direitos do titular e os princípios que regem a LGPD; e

d) em caso de uso exclusivo do controlador: quando o tratamento está condicionado à anonimização dos dados.

CAPÍTULO 3 - DIREITOS DO TITULAR

Noções gerais

Toda e qualquer análise em torno dos direitos do titular deve levar em consideração as pretensões de defesa e de intervenção. O objetivo mestre do legislador com a LGPD seria o de fazer com que o indivíduo (entendido como a "pessoa natural determinada ou determinável") se torne, propriamente, o "senhor" de seus dados pessoais.

Assim, a LGPD se destina à proteção de direto complexo, dotado de característica preponderantemente extrapatrimonial, em todo caso relacionado à personalidade e, em especial, à tutela dos dados relativos à pessoa natural. Para a definição do que são dados relativos à condição de pessoa, deve-se ter em mente: a) primeiramente, aqueles dados vinculados ao nome de determinado titular ou cujo conteúdo ou contexto possa de alguma forma reconduzir, de modo imediato, à identificação do seu titular; e b) em segundo lugar, não sendo o caso de recondução imediata do dado concretamente à mão à informação a respeito de sua titularidade específica, há dado pessoal quando a identidade é, ainda assim, determinável por meio de uso de meios técnicos razoáveis e concretamente disponíveis.

A definição do que seria o "dado pessoal" é certamente relativa. É possível que a identidade seja "determinável" para um agente de tratamento específico, mas não para o outro. Tudo depende, de fato, das capacidades eventuais e razoáveis de tratamento de dados de modo a permitir a determinação de seu titular, pelo que a legislação deve ser interpretada à luz das precauções necessárias em face dessa condição.

Deve-se considerar concretamente a seguinte pergunta a cada momento: O dado em questão corresponde a elemento capaz de conduzir, considerando a utilização de meios técnicos tanto razoáveis, como disponíveis por ocasião do tratamento, à definição da pessoa direta-

mente interessada ou afetada pelo seu tratamento? Caso a resposta a essa pergunta seja positiva, haverá necessidade de enquadramento da situação à luz dos limites da Lei Geral de Proteção de Dados.

Assim, a proteção da informação pessoal, nos termos da LGPD, deve ser realizada de forma mais ampla possível, até mesmo, pois, em respeito ao direito de autodeterminação informacional, já mencionado, a consideração sobre o que seria uma informação "relativa à intimidade, vida privada, honra e imagem" não pode ser realizada exclusiva ou preponderantemente por uma autoridade pública qualquer no silêncio de seu gabinete, à revelia de considerações sobre a situação concreta em que o tratamento de dados é possível.

A proteção de dados pessoais, ademais, não corresponde à mera garantia derivada da noção de "privacidade", embora deva ser destacada a existência de importantes sobreposições entre a tutela da privacidade e a proteção de dados pessoais. A proteção de dados também possui relevância inconteste mesmo ante a informação pessoal produzida e tratada em espaços públicos, quando há informação inegavelmente "pública". Um exemplo nessa direção seria o caso do direito de acesso e retificação de que trata classicamente o habeas data, previsto inclusive na Constituição Federal de 1988, mas também seria o caso de se entender que a proteção de dados pessoais implica toda a gama de princípios destacados nos incisos do art. 6º da LGPD, bem como nos incisos do art. 18 da mesma Lei, todos os quais se aplicam ao setor público, irrestritamente. Assim, ainda que possa haver sobreposição entre a proteção da privacidade e a tutela dos dados pessoais, percebe-se a diferença entre um e outro, não havendo motivos para conferir interpretação restritiva à proteção conferida pela LGPD a partir daquilo que se entende como "esfera privada".

Direitos em espécie

Os direitos reconhecidos pela LGPD não estão todos listados no art. 18. Muito pelo contrário, estão espalhados ao longo dos dispositivos.

Os direitos reconhecidos ao longo de toda a LGPD são instrumentalizados e processualizados à luz das prerrogativas fixadas e estabelecidas no art. 18 da Lei.

As prerrogativas são oponíveis tanto em face do controlador, como ante o próprio operador desses dados, ambos responsáveis pelo tratamento de dados, nos termos da legislação.

Art. 18

- Confirmação da existência do tratamento e do acesso aos dados (art. 18, I e II)

Tanto a confirmação da existência de tratamento, quanto o acesso aos dados objeto de tratamento correspondem a prerrogativas que instrumentalizam e decorrem lógica e juridicamente dos princípios de "livre acesso" (que pressupõe, dentre outras condições, a gratuidade do acesso) e de "transparência" (art. 6º, IV e VI).

A confirmação da existência de dados, considerando a necessidade de comunicação da finalidade do tratamento (art. 6º, I), a importância que o consentimento assume na nova legislação (art. 7º, I, e 8º), que nem todas as hipóteses de tratamento, todavia, exigem o consentimento prévio do titular dos dados (art. 7º, II a X) e ante o direito existente ao "acesso facilitado" às informações sobre o tratamento (art. 9º), prescinde da requisição do titular para ser efetivado.

Importante destacar, quanto ao acesso aos dados, em se tratando de tratamento realizado sobre dados pessoais de crianças e adolescentes, o art. 14, §6º, impõe que as informações "deverão ser fornecidas de maneira simples, clara e acessível, consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, com uso de recursos audiovisuais quando adequado, de forma a proporcionar a informação necessária aos pais ou ao responsável legal e adequada ao entendimento da criança".

Tal destaque decorre da determinação genérica de "acesso facilita-

do" de que trata em especial o art. 9º, devendo ser aplicado de forma extensiva a todo e qualquer indivíduo portador de qualquer forma de deficiência físico-psíquico-motora.

Uma vez que os dados pessoais correspondem a emanações do direito da personalidade do indivíduo, os dados não são desatrelados dessa condição, mesmo após a confirmação do consentimento no seu tratamento, razão pela qual a gerência sobre os dados é sempre garantida ao seu titular, que pode revogar o consentimento a qualquer momento (arts. 8º, V, e 18, IX), bem como pode se opor ao tratamento realizado naquelas hipóteses de dispensa de consentimento, em caso de descumprimento ao disposto na Lei (art. 18, §2º).

O direito de acesso compreende todas aquelas informações constantes do art. 9º: (a) informação sobre a finalidade específica do tratamento; (b) informações sobre a forma e duração do tratamento, observados os segredos comercial e industrial; (c) a identificação do controlador; (d) informações de contato do controlador; (e) informações acerca do uso compartilhado de dados pelo controlador e a finalidade; (f) as responsabilidades dos agentes que realizarão o tratamento; e (g) os direitos do titular, com menção explícita aos direitos contidos no art. 18 desta Lei.

O direito de acesso é complementado pelo art. 19, o qual estabelece prazos e as formalidades mínimas para o fornecimento das informações solicitadas. Tratando-se de solicitação em "formato simplificado", a disponibilização da informação deve ser realizada de modo imediato. Somente naquelas hipóteses em que são requeridas informações que devam ser disponibilizadas por meio de "declaração clara e completa" é que se confere, para o seu fornecimento, o prazo de 15 (quinze) dias (dias corridos, diga-se), contados da data do requerimento do titular.

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

A correção de dados incompletos, por sua vez, é decorrência do princípio da qualidade dos dados (art. 6º, V).

A correção de dados deve ser realizada de forma imediata pelos agentes de tratamento com os quais se tenha realizado o uso compartilhado dos dados (art. 18, §6º).

- Anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com a LGPD (art. 18, IV)

O titular dos dados possui a prerrogativa da "anonimização" dos dados. Uma vez anonimizados de forma eficaz, os dados deixam de ser regidos pela LGPD, pois, na forma da definição legal, perdem a qualidade de "dados pessoais".

Por sua vez, o bloqueio de dados, na forma das definições fornecidas diretamente pela LGPD, corresponde à "suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados". Tal suspensão corresponde tanto de um direito do titular (pelo próprio art. 18, III) como uma espécie de sanção prevista na legislação, a ser imposta pela Autoridade Nacional (art. 52, X e XI).

Por fim, a eliminação dos dados desnecessários, excessivos ou tratados em desconformidade com a legislação também decorre do princípio da necessidade (art. 6º, III).

Uma vez verificadas as situações de desnecessidade, excesso e desconformidade legal, por definição, a eliminação é de rigor, como decorrência lógica da promessa de minimização dos dados pessoais à disposição do tratamento.

Nas hipóteses de comunicação e uso compartilhado de dados, o art. 18, §6º, da LGPD estabelece que o "responsável deverá informar, de maneira imediata, aos agentes de tratamento com os quais tenha realizado uso compartilhado de dados a correção, a eliminação, a anonimização ou o bloqueio dos dados, para que repitam idêntico procedimento", havendo exceção a esse dever unicamente quando se tratar daqueles casos em que essa "comunicação seja comprovadamente impossível ou implique esforço desproporcional". A legislação não especifica o que deve ser entendido por desproporcionalidade

do esforço de comunicação, pelo que a matéria ainda depende de ulterior conformação normativa.

- Portabilidade (art. 18, IV)

Trata-se de decorrência normativa do fundamento inscrito no art. 2º, II, da LGPD, o qual afirma a essencialidade da "autodeterminação informativa" do titular dos dados para a proteção de dados pessoais no Brasil.

A legislação, ao tratar do tema, não dispõe especificamente se a portabilidade corresponderia a caso de mero compartilhamento de dados, com a manutenção de dois bancos de dados paralelos com a mesma informação, ou se haveria transferência de responsabilidade pelo seu tratamento, mediante a cessão dos dados entre arquivos diferentes, com a consequente obsolescência da informação contida no primeiro banco de dados. Pressupõe-se que, a depender do caso, ambas as possibilidades podem ser configuradas, o que demanda algum cuidado do responsável pelo tratamento. Essa diferença não é meramente teórica, uma vez que, em se tratando de transferência de dados no segundo sentido sugerido, impõe-se a eliminação do dado desnecessário.

A prerrogativa é regulamentada adiante pelo art. 18, §7º, de modo que a portabilidade não pode incluir os dados já anonimizados do titular.

Especialmente no que diz respeito aos dados sensíveis, ademais, a LGPD traz disposição específica no art. 11, §4º, I, ao dispor sobre a vedação de "comunicação ou o uso compartilhado entre controladores de dados pessoais sensíveis referentes à saúde com objetivo de obter vantagem econômica", encontrando-se, dentre as exceções a essa vedação, a hipótese da portabilidade de dados quando solicitada pelo titular. Assim, é possível ao titular de dados solicitar a portabilidade de dados sensíveis, quando então será permitida a sua comunicação e seu uso compartilhado.

- Eliminação dos dados tratados com o consentimento do titular (art. 18, VI)

Em complemento ao art. 18, IV, e ao art. 16, o art. 18, VI, dispõe a respeito da eliminação de dados tratados licitamente, mediante o consentimento do titular.

Assim, mediante requerimento expresso, o titular pode solicitar a "exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado" (art. 5º, XIV). Trata-se de procedimento definitivo e irreversível.

- Informações das entidades públicas ou privadas com as quais o controlador realizou uso compartilhado de dados (art. 18, VII)

A Lei Geral de Proteção de Dados admite o compartilhamento de dados entre agentes de tratamento à informação, contudo, determina a necessidade de se informar o titular a respeito. Apesar de a legislação silenciar tanto quanto à necessidade de informar os dados de qualificação das entidades públicas e privadas com as quais houve compartilhamento, tal exigência decorre do princípio de transparência e encontra seu fundamento na premissa de autodeterminação informativa.

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

Como decorrência lógica do princípio da transparência e com fundamento tanto na boa-fé como no direito à autodeterminação informacional, o titular possui direito de ser informado sobre as consequências da negativa de seu consentimento.

- Revogação do consentimento (art. 18, IX)

Nas hipóteses do art. 7º, I, o consentimento corresponde ao fundamento do tratamento de dados, podendo tal autorização expressa ser,

de semelhante forma, revogada. Tal revogação pode ser solicitada a qualquer tempo, mediante procedimento gratuito e facilitado, tratando-se de direito potestativo do titular.

A revogação do consentimento não comporta a determinação para a eliminação automática dos dados coletados validamente, pelo que o ideal é que a requisição de eliminação, caso venha a ser solicitada juntamente com a revogação do consentimento (de que trata o art. 18, III), seja feita de forma expressa.

Art. 20.

O art. 20, da LGPD, especificamente no caput e no §1°, dispõe sobre os direitos à explicação e à revisão de dados, respectivamente.

Segundo a doutrina aplicada ao dispositivo[12]:

> *"Enquanto o direito à explicação diz respeito ao direito de receber informações suficientes e inteligíveis que permitam ao titular dos dados entender a lógica e os critérios utilizados para tratar seus dados pessoais para uma ou várias finalidades (§1°), o direito à revisão compreende o direito do titular de requisitar a revisão de uma decisão totalmente automatizada que possa ter um impacto nos seus interesses, principalmente os relacionados à definição de seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade (caput)".*

Com o veto do art. 20, §3°, da LGPD, quando da promulgação da Lei Federal n. 13.853/2019, foi excluída a previsão expressa que garantia a revisão humana das decisões proferidas pelos computadores. Apesar da revogação, entretanto, a possibilidade de assim proceder continua a existir normalmente. Especialmente no que tange à Admi-

12 MULHOLLAND, Caitlin (Org). A LGPD e o novo marco normativo no Brasil. Porto Alegre: Arquipélago, 2020, p. 345.

nistração Pública, ademais, tal possibilidade corresponde a verdadeiro poder-dever do gestor em face do tratamento de dados pessoais, não havendo qualquer óbice à revisão do entendimento adotado pela máquina de forma automatizada, sempre que tal medida vier a atender, de forma equânime e razoável, à finalidade jurídica legitimamente projetada pela Administração.

CAPÍTULO 4 - TRATAMENTO DE DADOS PESSOAIS PELO PODER PÚBLICO

Noções gerais

O ponto de partida, no caso de tratamento de dados pessoais pelo Poder Público, é verificar, no caso concreto, qual a base legal será utilizada para a operação. E isso porque a Administração encontra-se jungida ao princípio constitucional da legalidade, necessitando, sempre, estar amparada em lei para as suas ações, o que inclui o tratamento de dados pessoais.

Nesse sentido, o art. 23 da LGPD preconiza que o tratamento de dados pessoais pelo Poder Público deverá ser realizado, independentemente do consentimento do titular (art. 11, II) 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.

Mesmo nesses casos, o tratamento só será válido se forem disponibilizadas ao titular do dado informações claras e atualizadas sobre a previsão legal autorizadora da operação, a finalidade, os procedimentos e as práticas utilizadas pelo Poder Público. De acordo com a LGPD, tais informações devem ser disponibilizadas preferencialmente nos sítios eletrônicos dos agentes de tratamento[13]. Além disso, a LGPD exige que seja indicado um encarregado responsável pela operação de tratamento de dados.

Tratamento de dados pessoais pelos serviços notariais e de registro

Os serviços notariais e de registro exercidos em caráter privado, por delegação do Poder Público, receberam da LGPD o mesmo trata-

13 A Autoridade Nacional de Proteção de Dados poderá dispor sobre outras formas de publicidade para as operações de tratamento no âmbito do Poder Público.

mento conferido às pessoas jurídicas de direito público integrantes da Administração Pública direta ou indireta.

Assim, somente podem efetuar o tratamento de dados pessoais para a persecução do interesse público, respeitados os princípios de proteção do art. 6º, e desde que sejam fornecidas as informações ao titular dos dados e nomeado um encarregado.

Sobre o tema, o Conselho Nacional de Justiça editou o Provimento n. 74, de 31 de julho de 2018, o qual dispõe sobre padrões mínimos de tecnologia de informação para a segurança, integridade e disponibilidade de dados para a continuidade da atividade pelos serviços notariais e de registro no Brasil.

O Provimento está em perfeita consonância com a LGPD, pois preconiza que os serviços notariais e de registro exercidos por delegação do Poder Público mantenham disponíveis informações claras sobre o tratamento de dados que realizam, inclusive contendo a obrigação prevista no §5º do art. 23 da LGPD, no que atina ao fornecimento de dados pessoais, por meio eletrônico, à Administração Pública para o atendimento de sua finalidade.

Tratamento de dados pessoais pelas estatais

As empresas públicas e as sociedades de economia mista são integrantes da Administração Pública indireta e consideradas instrumentos de atuação do Estado na consecução de seus fins.

Sabe-se que as atividades desempenhadas pelas estatais podem ser tanto a prestação de serviços públicos, quanto a exploração de atividade econômica, mas nesse último caso somente se houver imperativos de segurança nacional ou relevante interesse público, nos termos do que preconiza o art. 173 da Constituição Federal de 1988[14].

14 Constituição Federal de 1988: "Art. 173. Ressalvados os casos previstos nesta Constituição, a exploração direta de atividade econômica pelo Estado só será permitida quando necessária aos imperativos da segurança nacional ou a relevante interesse coletivo, conforme definidos em lei.".

Quando explorarem atividade econômica, as estatais se sujeitam ao regime jurídico das empresas privadas (art. 173, §1º, inciso II, da CF/1988), e isso inclui a operação de tratamento de dados pessoais que porventura realizem. No caso do BANPARÁ, por exemplo, quando estiver comercializando produtos bancários ou financeiros no mercado, estará sujeito à LGPD do mesmo modo que os entes privados.

No caso de prestação de serviços públicos pelas estatais ou quando estiverem operacionalizando políticas públicas, contudo, eventual tratamento de dados pessoais realizado se dará de forma idêntica àquela aplicada pelos órgãos e entidades do Poder Público.

Compartilhamento de dados pessoais na Administração Pública

Há que diferenciar, quanto ao compartilhamento de dados, duas situações, que ensejam consequências jurídicas diversas ao Poder Público.

A primeira diz respeito ao uso de dados pessoais compartilhados pela Administração Pública. A LGPD o permite, desde que tenha por objetivo: a) atender a finalidades específicas de execução de políticas públicas; e b) cumprir atribuição legal pelos órgãos e pelas entidades públicas, respeitados os princípios de proteção de dados pessoais elencados no art. 6º da Lei.

Situação completamente diferente é o compartilhamento dos dados pessoais constantes na base de dados da Administração Pública a pessoas jurídicas de direito privado. Nesse caso, a LGPD possui regramento específico, permitindo que o Poder Público compartilhe informações de seus bancos de dados, desde que: a) os dados sejam acessíveis publicamente; b) haja previsão legal ou a transferência for respaldada em contratos, convênios ou instrumentos congêneres; c) a transferência dos dados objetive exclusivamente a prevenção de fraudes e irregularidades, ou vise à proteção e resguardo da segurança e da integridade do titular dos dados, vedado o tratamento para outras finalidades; e d) seja caso de execução descentralizada de atividade

pública que exija a transferência, exclusivamente para esse fim específico e determinado.

Ademais, caso o Poder Público vislumbre, no caso concreto, não se encaixar em nenhuma das hipóteses legais autorizadoras do compartilhamento de dados pessoais com um ente privado, e, mesmo assim, pretenda efetuar o compartilhamento, deverá, obrigatoriamente, preencher aos seguintes requisitos: a) obter o consentimento expresso e destacado do titular do dado; e b) comunicar à Autoridade Nacional.

Em qualquer caso, deve-se ter em mente que o Poder Público, ao usar dados compartilhados ou efetuar o compartilhamento de dados constantes em sua base, deverá sempre perseguir o interesse público, não podendo agir sob fins não contemplados na Lei.

Interoperabilidade dos dados pessoais

Interoperabilidade é a capacidade de um sistema se comunicar de forma transparente (ou o mais próximo disso) com outro sistema, semelhante ou não ao seu.

A LGPD privilegia, no seu art. 25, a interoperabilidade no âmbito do Poder Público, afirmando que os dados pessoais devem ser mantidos em formato interoperável e estruturado com vistas à execução de políticas públicas, à prestação de serviços públicos, à descentralização de atividade pública e à disseminação e o acesso das informações pelo público em geral.

Assim, órgãos e entidades da Administração Pública deverão atuar de forma integrada em seus sistemas, de modo a facilitar o compartilhamento de dados, visando à prestação de serviços públicos e à execução de políticas públicas em benefício do cidadão, respeitados os protocolos de segurança da informação e a proteção dos dados pessoais.

Um banco de dados adequado, certamente, pode ajudar na implementação de inúmeras políticas públicas, e, em última análise, melhorias para a população local. No entanto, é imprescindível que os dados coletados possam transitar entre os diversos órgãos e entidades

públicas de forma interoperável e estruturada, sem perder de vista a finalidade precípua do compartilhamento, que é a proteção do interesse público.

Autoridade Nacional e normas complementares

Visando a dar maior proteção ao cidadão, a LGPD dispõe, ainda, que a Autoridade Nacional poderá estabelecer normas complementares, além das previstas na Lei, para regular a comunicação e o compartilhamento de dados pessoais pelo Poder Público.

Responsabilidade por infração à LGPD

A LGPD trata de forma específica a responsabilidade do Poder Público por infração as suas regras. Diferentemente dos entes privados, órgãos e entidades públicas não estão sujeitos a sanções pecuniárias.

Havendo infração em decorrência do tratamento de dados pessoais pelo Poder Público, a Autoridade Nacional poderá enviar informe com medidas cabíveis para fazer cessar a violação e também poderá solicitar a agentes do Poder Público a publicação de relatórios de impacto à proteção de dados pessoais e sugerir a adoção de padrões e de boas práticas para os tratamentos de dados pessoais, conforme os arts. 31 e 32.

CAPÍTULO 5 - AGENTES DE TRATAMENTO DE DADOS PESSOAIS

Agentes

A LGPD trouxe diversos conceitos quanto aos agentes - controlador, operador e encarregado -, que se distinguem, inclusive, para fins de responsabilização (art. 37 e ss.), conforme estabelecido no Capítulo I.

Impende notar que os papeis ficam bem definidos na LGPD, em que o controlador está obrigado a fornecer instruções ao operador, que àquele se vincula hierarquicamente (art. 39). Caberá ao controlador verificar a observância de suas instruções e das normas alusivas à matéria. Veja-se que a atuação do operador não se limita a cumprir apenas as instruções do controlador, mas adotar medidas em observância à legislação e de natureza técnica e organizacional de segurança, em cumprimento ao disposto no art. 46.

Ademais, o controlador indicará o encarregado pelo tratamento de dados (art. 41) e a Lei apontou a necessidade de acesso a ele, por meio da divulgação pública de sua identidade e informações de contato, de forma clara e objetiva, preferencialmente no sítio eletrônico do controlador (art. 41, §1º).

Ao encarregado, por seu turno, incumbem as seguintes atividades (art. 41, §2º):

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

b) receber comunicações da Autoridade Nacional e adotar providências;

c) orientar os servidores/empregados públicos e os contratados a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e

d) executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.

Podem ser editadas normas complementares pela Autoridade Nacional, em relação à definição e às atribuições do encarregado, inclusive quanto à dispensa da necessidade de sua indicação, conforme a natureza e o porte do órgão/entidade ou o volume de operações de tratamento de dados (art. 41, §3º).

Registros e do relatório de impacto à proteção de dados pessoais

A Lei obriga que o controlador e o operador mantenham registro das operações relativas ao tratamento de dados pessoais que realizarem, principalmente quando baseado no legítimo interesse (art. 37). Esses registros são importantes para demonstrar o cumprimento da Lei e em caso de apuração de responsabilidade. O legítimo interesse ainda aprece como um conceito jurídico indeterminado, a reforçar a necessidade dos registros.

No que tange à forma, uma vez considerado o princípio da responsabilização e prestação de contas (art. 6º, X), os registros deverão ser escritos, mesmo que armazenados eletronicamente.

Por outro lado, a Lei prevê a possibilidade de a Autoridade Nacional determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, inclusive quanto aos dados sensíveis, de acordo com o previsto no art. 38. Veja-se que o art. 10, §3º, indica que o relatório poderá ser solicitado quando o tratamento tiver como fundamento o interesse legítimo. O parágrafo único do art. 38 já estabelece um regramento quanto às exigências mínimas desse documento, definido no art. 5º, XVII:

a) descrição dos tipos de dados coletados;

b) metodologia utilizada para a coleta e para a garantia da segurança das informações; e

c) análise do controlador em relação a medidas, salvaguardas e mecanismos de mitigação de riscos.

Também se possibilitou à Autoridade Nacional dispor sobre padrões de interoperabilidade para fins de portabilidade, livre acesso

aos dados e segurança, assim como sobre o tempo de guarda dos registros, em face da necessidade e da transparência (art. 40).

Recomendações

O controlador deverá se preocupar com as atividades dos operadores, considerando a eventual responsabilidade solidária (art. 42, §1º, I).

Na Administração Pública, é recomendável que sejam firmados termos de confidencialidade com todos os servidores/empregados públicos e contratados que tiverem acesso a sistema que opere o tratamento de dados ou no qual estejam inseridas informações de acesso restrito, a fim de garantir maior segurança quanto à confidencialidade.

Responsabilidades

A LGPD indicou que o tratamento de dados será irregular quando deixar de observar a legislação ou não fornecer a segurança que o titular dele pode esperar, consideradas determinadas circunstâncias relevantes, dentre as quais: o modo pelo qual é realizado; o resultado e os riscos que razoavelmente dele se esperam; e as técnicas de tratamento de dados disponíveis à época em que foi realizado (art. 44).

O controlador ou o operador é obrigado a reparar os danos patrimoniais, morais, individuais ou coletivos causados em razão do tratamento de dados pessoais (art. 42), inclusive de forma solidária, nos termos da LGPD. A Lei também determina a responsabilidade do controlador ou do operador quanto aos danos decorrentes da violação da segurança dos dados, se, ao deixar de adotar as medidas de segurança previstas no art. 46, der causa ao dano (art. 44, parágrafo único).

O operador será responsabilizado "quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador, hipótese em que o operador equipara-se ao controlador" (art. 42, §1º, I).

Os controladores serão responsabilizados quando estiverem diretamente envolvidos no tratamento de dados do qual decorreram danos ao titular (art. 42, §1°, II).

De todo modo, a LGPD prevê a escusa de responsabilização dos agentes nas seguintes hipóteses (art. 43):

a) quando não realizaram o tratamento de dados pessoais que lhes é atribuído;

b) quando, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados; ou

c) quando o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiro.

No âmbito do processo judicial, o juiz "poderá inverter o ônus da prova a favor do titular de dados quando, a seu juízo, for verossímil a alegação, houver hipossuficiência para fins de produção de prova ou quando a produção de prova pelo titular resultar-lhe excessivamente onerosa" (art. 42, §2°). Ademais, as ações de reparação por danos coletivos que tenham por objeto a responsabilização de que trata o art. 42, caput, podem ser exercidas coletivamente em juízo, observado o disposto na legislação aplicável (art. 42, §3°).

A Lei garantiu ainda o direito de regresso àquele que reparar o dano ao titular contra os demais responsáveis, na medida de sua participação no evento danoso (art. 42, §4°).

Cumpre suscitar que "as hipóteses de violação do direito do titular no âmbito das relações de consumo permanecem sujeitas às regras de responsabilidade previstas na legislação pertinente" (art. 45).

CAPÍTULO 6 - SEGURANÇA E DAS BOAS PRÁTICAS

Medidas de segurança

Sem segurança da informação não há proteção de dados, razão pela a LGPD, além de elencá-la expressamente como um de seus princípios norteadores (princípio da segurança - art. 6, VII), dedicou-lhe ainda um capítulo exclusivo (SOMBRA; CASTELLANO: 2019, 169)[15], o qual inicia estabelecendo que é dever dos agentes de tratamento adotar medidas técnicas e administrativas, aptas a proteger os dados pessoais de acessos não autorizados, de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou irregular (art. 46).

Para fins de regularidade, a Lei também direcionou especial atenção ao modo pelo qual o tratamento é realizado, o resultado e os riscos que razoavelmente dele se esperam e as técnicas disponíveis à época de sua execução, sendo incisiva ao considerar como irregular todo o tratamento de dados pessoais que não observe a legislação ou não forneça a segurança que o titular dele pode esperar (art. 44, caput, incisos e parágrafo único).

Outrossim, deixou claro ainda, que as medidas de segurança adequadas devem ser observadas desde a concepção do produto ou do serviço até a sua execução (privacy and security by design), obrigando controladores, operadores ou qualquer outra pessoa que intervenha em uma das fases do processamento, a garantir a proteção necessária, mesmo após o término do tratamento (art. 46, §2º, e art. 47).

A despeito da imposição reiterada do dever de proteção dos da-

15 SOMBRA, Thiago Luís, CASTELLANO, Ana Carolina Heringer. Plano de Resposta a Incidentes de Segurança: reagindo rápido e de forma efetiva, in Revista do Advogado, in Proteção de dados: desafios e soluções na adequação à lei / Organizador OPICE BLUM, Renato. 2019 v. 39 n. 144 nov. pp. 168-173.

dos pessoais, a LGPD não especifica ou indica quais seriam as medidas de segurança recomendáveis ou pertinentes para o alcance da conformidade. Por ter uma abordagem baseada em risco, acaba por transferir aos agentes de tratamento de dados pessoais a responsabilidade de, no contexto e complexidade de suas operações, analisar quais as salvaguardas necessárias e pertinentes a serem adotadas.

É, portanto, a partir dos riscos identificados, que devem ser implementadas as ferramentas que assegurem um nível adequado de proteção equivalente ao grau de exposição verificado no tratamento (SOMBRA; CASTELLANO: 2019, 169)[16], levando em consideração a natureza e sensibilidade dos dados tratados; as características específicas das operações; o estado atual da tecnologia; os direitos do titular, principalmente quanto a potencial afetação de suas liberdades civis e direitos fundamentais; além da própria capacidade da organização em comprovar seu nível de aderência à legislação e a eficácia das medidas adotadas - especialmente quanto à concretização dos princípios previstos no art. 6º.

Nesse cenário, o correto mapeamento e registro das operações de tratamento (art. 37) afigura-se como um elemento imprescindível, pois é a partir do levantamento dos tipos e dos fluxos dos dados pessoais que poderão ser analisados os riscos envolvidos e corretamente implantadas as medidas de segurança necessárias para cada tipo de processo identificado, sempre de acordo com as características do tratamento e as exigências circunstancias aplicáveis à organização.

Embora a LGPD traga a informação de que a ANPD poderá vir a dispor sobre padrões técnicos mínimos para fins de aplicabilidade relacionados a aspectos de segurança, a materialização das medidas técnicas e administrativas adequadas podem ser realizadas de forma imediata, por meio da utilização de normas técnicas reconhecidas mundialmente como boas práticas sobre o assunto, como, por exemplo, as publicadas pela Associação Brasileira de Normas Técnicas.

16 IDEM

Nesse sentido, aliás, o Guia de Boas Práticas para Implementação da LGPD na Administração Pública Federal[17] traz recomendação de utilização do padrão técnico estabelecido pela ABNT, especificamente as normas ABNT NBR ISO/IEC 27001 – Tecnologia da informação — Técnicas de segurança — Sistemas de gestão da segurança da informação — Requisitos; ABNT NBR ISO/IEC 27002 – Código de Prática para controles de segurança da informação; ABNT NBR ISO/IEC 27701 Técnicas de segurança — Extensão da ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 para gestão da privacidade da informação — Requisitos e diretrizes; 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.

A título de exemplo, podem ser citadas as seguintes espécies de medidas técnicas e operacionais: políticas, em especial a de privacidade, retenção e eliminação de dados e segurança da informação; gestão de ativos; controles de acesso; segurança física dos ambientes; treinamento e capacitação; criptografia; anonimização; cópias de segurança; antivírus; firewall; segregação de redes; detectores de invasão de sistemas; ferramentas de prevenção à perda de dados; testes de vulnerabilidade; procedimentos de atualização de software; dentre outros.

Incidentes de segurança e sua comunicação

Não há na LGPD uma definição expressa sobre o que seria um incidente de segurança, restando ausente apontamento específico sobre o tema. Não obstante, a partir de uma interpretação harmônica, pode-se definir "incidente de segurança" como acontecimento inesperado ou indesejado, que seja hábil a comprometer a segurança dos dados pessoais, de modo a expô-los expor a acessos não autorizados e situ-

17 BRASIL. *Guia de Boas Práticas. Lei Geral de Proteção de Dados*. Governo Federal, Abril/2020, pp. 44/45. Disponível em: https://www.gov.br/governodigital/pt-br/governanca-de-dados/guia-lgpd.pdf. Acesso em: 1 de nov. de 2020.

ações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito (JIMENE; TAMER: 2020, 291)[18].

Nesse sentido e considerando ainda os princípios de segurança da informação, tem-se que um incidente de segurança restaria caracterizado pela ocorrência de um ou vários eventos adversos, acidentais ou ilícitos, que têm uma probabilidade significativa de comprometer as características de confidencialidade, integridade e disponibilidade dos dados pessoais tratados pela organização.

Apesar da necessidade de adoção de medidas de segurança aptas a prevenir tratamentos irregulares, como controles técnicos e organizacionais (princípio da segurança – art. 6°, VII), seu monitoramento contínuo (princípio da prevenção – art. 6°, VIII) e do dever de registrar interna e regularmente de todos os incidentes ocorridos (princípio da responsabilização e prestação de contas – art. 6, X), não haverá necessidade de notificação externa de todo e qualquer evento de segurança adverso verificado na organização, pois, nos termos da Lei, o controlador deverá realizar comunicações à Autoridade Nacional e aos titulares de dados apenas nos casos dos incidentes de segurança que possam acarretar risco ou dano relevante aos titulares (art. 48).

Com efeito, diante da possível identificação de um incidente de segurança, portanto, cabe ao controlador confirmar ou não a suspeita de sua ocorrência e avaliar a natureza, o tipo e volume de dados envolvidos e a gravidade de suas consequências, obrigatoriamente comunicando à Autoridade Nacional e aos titulares de dados sempre que se restar configurada situação de risco ou dano relevante ao titular.

Em relação ao prazo, a legislação não informa especificamente um tempo limite para efetivação da medida, apenas afirmando que a comunicação deverá ser feita em "prazo razoável" e "imediato" (art. 48,

18 JIMENE, Camilla do Vale. TAMER, Maurício Antonio. Plano de Resposta a Incidentes de Segurança de Dados Pessoais In Data Protection Officer (encarregado) / Coordenadores. OPICE BLUM, Renato. VAINZOF, Rony. MORAES, Henrique Fabretti. São Paulo: Thomson Reuters Brasil, 2020.

caput, §1º e seu inciso V), estando, portanto, atualmente o cumprimento dessa exigência estritamente vinculado a uma análise contextual da situação, de acordo com os fatos e justificativas apresentados, sendo recomendável, entretanto, que diante da ocorrência de um incidente de segurança, a comunicação seja feita o mais rápido possível, a partir de sua confirmação.

Quanto ao conteúdo, o controlador deverá fazer constar na comunicação, no mínimo, as seguintes informações (art. 48, §1º e incisos):

a) a descrição da natureza dos dados pessoais afetados;

b) as informações sobre os titulares envolvidos;

c) a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial;

d) os riscos relacionados ao incidente;

e) os motivos da demora, no caso de a comunicação não ter sido imediata; e

f) as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.

A partir da comunicação, a Autoridade Nacional, então, verificará a gravidade do incidente e poderá, caso necessário, determinar a adoção de providências para a salvaguarda dos direitos dos titulares, tais como ampla divulgação do fato em meios de comunicação e medidas para reverter ou mitigar os efeitos do incidente (art. 48, §2º e incisos).

Analisando as disposições do texto legal, algumas conclusões devem ficar claras diante da ocorrência de um incidente de segurança:

a) não é todo o evento ou incidente que exigirá a comunicação, mas apenas e tão somente os casos mais graves, isto é, aqueles em que, no contexto analisado, potencialmente possam acarretar risco ou dano relevante ao titular;

b) é irrelevante para fins de sua caracterização se o incidente de segurança decorre de situação acidental ou intencional, com a obrigação de comunicação derivando diretamente da avaliação de sua gravidade;

c) nos termos da Lei, o dever de comunicação é uma obrigação

reservada ao controlador, não vinculando diretamente os operadores de dados pessoais, pelo que a formalização de cláusula contratual específica nesse sentido, definindo o dever de notificação interpartes, mostra-se imprescindível; e

d) até que a ANPD fixe um prazo específico de comunicação, o cumprimento dessa exigência – e a própria utilização dos termos "prazo razoável" ou "imediata" -, restará vinculado à análise dos fatos e justificativas circunstanciais do caso concreto, sendo recomendável, entretanto que, confirmado o incidente, sua comunicação seja feita o mais rápido possível.

Sob outro prisma, tem-se que detectar e saber onde, como e quando ocorreu o incidente; quais suas causas; que dados foram atingidos; quantos e quais titulares foram afetados; quais evidências precisam ser coletadas e quais medidas (preventivas ou repressivas) foram ou devem ser adotadas, são questões que precisarão ser imediatamente enfrentadas para viabilizar a comunicação adequada e impedir o agravamento de situações dessa natureza.

Ademais, em qualquer caso, será necessário comprovar que foram adotadas medidas técnicas adequadas que tornem os dados pessoais afetados ininteligíveis, no âmbito e nos limites técnicos de seus serviços, para terceiros não autorizados a acessá-los (art. 48, §3º), bem como que os sistemas utilizados foram estruturados de forma a atender aos requisitos de segurança, aos padrões de boas práticas e de governança e aos princípios gerais previstos nessa Lei e às demais normas regulamentares (art. 49).

Nesse ponto, além de ser considerado um item de governança minimamente adequado (art. 50, §2º, I, "g"), a elaboração de um plano de resposta a incidentes de pronto emprego se mostra como uma medida de segurança absolutamente necessária, pois, sem a especificação dos procedimentos e responsabilidades, indicação clara dos canais e/ou pessoas a serem acionadas, atualização, testes e treinamento pertinentes, homologação prévia de fornecedores externos (sistemas e equipes de apoio de resposta, perícia forense computacional, etc), entre outros,

restará inviável prevenir, combater ou corrigir a ocorrência de incidentes de segurança ou mesmo identificá-los e cumprir com as exigências legais mínimas de comunicação e mitigação de seus efeitos.

Ainda sobre a necessidade de adoção de medidas preventivas/corretivas e da estruturação de um procedimento de resposta, cumpre ponderar que a demonstração de mecanismos e procedimentos internos capazes de minimizar danos, voltados ao tratamento seguro e adequado de dados – em especial diante da ocorrência de incidentes de segurança -; a implementação de política de boas práticas e governança – dentre elas a elaboração de um plano de resposta a incidentes –, bem como a pronta adoção de medidas corretivas serão parâmetros e critérios levados em consideração para aplicação ou gradação de eventual sanção (art. 52, §1°, VIII, IX e X c/c art. 50, §2°, I, "g", e art. 48, §2°, II).

Das boas práticas e da governança

Considerando que a regularidade de qualquer tratamento depende da adoção de medidas de segurança (art. 46), mas, sobretudo da fiel observância aos princípios informativos trazidos pela LGPD (art. 6°), é possível concluir que a adequação vai muito além da simples execução de ações pontuais e isoladas.

Nesse sentido, aliás, a Lei dispôs expressamente que os sistemas utilizados para tratamento de dados pessoais devem ser estruturados de forma a atender aos requisitos de segurança, aos padrões de boas práticas e de governança, aos princípios gerais previstos na LGPD, bem como às demais normas regulamentares (art. 49).

A depender da sensibilidade dos dados e da escala e volume das operações de tratamento, na prática restará inviável a algumas organizações manter um nível apropriado de conformidade ou a eficiência dos controles implementados, sem que efetivamente se comprometam com estratégias para o contínuo gerenciamento e monitoramento de seus processos, pessoas e tecnologias.

Outrossim, o reconhecimento da proteção dos dados pessoais

como um direito fundamental autônomo e implícito no texto constitucional[19], acabou por estabelecer um dever de proporcionalidade de dupla dimensão ao Estado: não intervir ou agir com excesso em relação as liberdades individuais (aspecto negativo) e, de forma reflexa, atuar no sentido de garantir que os direitos dos cidadãos (titulares) sejam concreta e suficientemente protegidos (aspecto positivo) - no caso da proteção dos dados, atuando com objetivo de evitar riscos para o cidadão em geral, por meio da adoção de medidas de proteção ou de prevenção especialmente em relação ao desenvolvimento técnico ou tecnológico.

Um completo processo de adequação demandará, portanto, a adoção de um conjunto coordenado de ações, que vão desde o diagnóstico inicial do nível de aderência à legislação, até a implementação de medidas que, não apenas objetivem o simples gerenciamento dos riscos mapeados, mas, sobretudo, integrem e disseminem a cultura de proteção de dados no cotidiano da organização, sendo a conscientização e o efetivo controle das condutas o maior desafio a ser enfrentado, pois, certamente, nenhuma atividade de conformidade, por melhor que seja, resiste à falta de apoio por parte da alta administração ou a baixa adesão dos servidores.

Nesse contexto, as boas práticas e a governança se apresentam como instrumentos capazes dar concretude aos princípios e diretrizes de proteção de dados, convertendo-os em atitudes práticas de gerenciamento, que se espalham pela estrutura da organização, alcançando os níveis estratégico, tático e operacional, e incorporam os padrões de privacidade às rotinas, durante todo o ciclo de vida dos dados.

Assim, considerados a natureza, o escopo, a finalidade, a probabilidade, a gravidade dos riscos e os benefícios relacionados ao tratamento dos dados do titular, a LGPD dispôs que os agentes de tratamento poderão formular ou aderir a regras de boas práticas e governança que, dentre outros aspectos, estabeleçam as condições de

19 STF - ADI: 6387 DF – Distrito Federal 0090566-08.2020.1.00.0000, Relator(a): Min. Rosa Weber.

organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, normas de segurança, padrões técnicos, obrigações específicas, ações educativas, mecanismos de supervisão e de mitigação de riscos (art. 50, caput e §1º).

Outrossim, como forma de dar efetividade e operacionalidade aos princípios da segurança e prevenção, a legislação ainda apresenta a possibilidade de o controlador, no contexto de suas operações e dos riscos envolvidos, implementar um programa de governança em privacidade, que, no mínimo (art. 50, §1º, I):

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

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

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

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

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

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

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

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

Destaca-se, entretanto, que quando implementado e apropriado, a organização deverá ter capacidade de demonstrar a efetividade de seu programa de governança em privacidade, em especial, a pedido da Autoridade Nacional de Proteção de Dados ou de outras entidades responsáveis por eventualmente promover o cumprimento de boas

práticas ou códigos de conduta setoriais (art. 50, §1°, II).

Cumpre mencionar ainda que, apesar de não obrigatória, a existência de um programa de governança em privacidade será levada em consideração quando da aplicação ou gradação de eventual sanção. De acordo com a LGPD, além das peculiaridades do caso concreto (contexto), a Autoridade Nacional utilizará como parâmetro ou critério de análise a demonstração da existência de mecanismos e procedimentos internos capazes de minimizar o dano, voltado ao tratamento seguro e adequado de dados, e à adoção de política de boas práticas e governança (art. 52, §1°, VIII e IX).

No caso específico dos agentes do Poder Público, restou estabelecido que a ANPD poderá solicitar a publicação de relatórios de impacto e sugerir a adoção de padrões e de boas práticas para os tratamentos de dados pessoais (art. 32).

CAPÍTULO 7 - FISCALIZAÇÃO

Noções gerais

Dita o art. 6º, X, que as atividades de tratamento de dados pessoais deverão observar, além da boa-fé e outros princípios, a responsabilização e a prestação de contas, ou seja, deverá o Poder Público demonstrar a adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

A própria LGPD criou, em seu art. 55-A, a Autoridade Nacional de Proteção de Dados (ANPD), órgão da administração pública federal, a quem compete, conforme art. 55-J, I e IV, zelar pela proteção dos dados pessoais e 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.

Compatibilização da LGPD com o regime público e as sanções aplicáveis

No que toca à fiscalização e às sanções administrativas, deve-se compatibilizar o que dispõe a referida Lei com o regime do serviço público.

Nos termos do §3º do art. 52, "o disposto nos incisos I, IV, V, VI, X, XI e XII do caput deste artigo poderá ser aplicado às entidades e aos órgãos públicos, sem prejuízo do disposto na Lei nº 8.112, de 11 de dezembro de 1990, na Lei nº 8.429, de 2 de junho de 1992, e na Lei nº 12.527, de 18 de novembro de 2011".

Dessa forma, são aplicáveis ao Poder Público 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 a que se refere a infração até a sua regularização;

d) eliminação dos dados pessoais a que se refere a infração;

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

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

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

Denota-se que os órgãos e entidades da Administração Pública não estão sujeitos às penalidades de multa simples e multa diária, previstas nos incisos II e III do art. 52. As referidas multas têm por base o faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração, o que torna impossível tal aferição junto ao Poder Público.

Dessa forma, também são inaplicáveis ao Poder Público os §§4º e 5º do art. 52, e os arts. 53 e 54, uma vez que dispõem sobre base, destinação e metodologias que orientarão o cálculo do valor-base das sanções de multa.

O art. 64, por sua vez, não afasta a proteção e, via de consequência, o viés sancionatório conferido por outros diplomas: "Os direitos e princípios expressos nesta Lei não excluem outros previstos no ordenamento jurídico pátrio relacionados à matéria ou nos tratados internacionais em que a República Federativa do Brasil seja parte."

É de se ressaltar, ainda, que as penalidades elencadas na LGPD são aplicadas diretamente ao órgão ou à entidade da Administração Pública, e não diretamente ao agente público autor da infração.

Assim, conforme o §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, e em legislação específica". No mesmo sentido, é o já mencionado §3º do art. 52, de modo que a LGPD pode ser aplicada em concomitância com o regime disciplinar dos servidores públicos, a Lei de Acesso à Informação e a Lei de Improbidade Administrativa.

Ficam ressalvados, portanto, os regimes jurídicos dos servidores públicos, os quais preveem penalidades específicas, como o Regime Jurídico Único dos Servidores Civis do Estado do Pará (Lei Estadual n. 5.810/1994), a Lei de Acesso à Informação (Lei Federal n. 12.527/2011) e a Lei de Improbidade Administrativa (Lei Federal n. 8.429/1992). Mantém-se assim, da mesma forma, a competência dos entes para apurar e aplicar penalidades de natureza disciplinar administrativa a seus agentes.

Extrai-se do mencionado §2º ser possível, dessa forma, a aplicação de penalidades pela LGPD, imposta pela Autoridade Nacional de Proteção de Dados, conforme art. 55-J, IV, sem prejuízo de sindicância ou processo administrativo disciplinar a ser levado a efeito pelos entes públicos.

A ANPD, no caso do Poder Público, antes de aplicar as sanções previstas nos incisos X, XI e XII do art. 52, referentes à suspensão do banco de dados, suspensão do tratamento de dados e proibição parcial ou total do tratamento de dados, deverá ouvir os respectivos órgãos e entidades com competências sancionatórias, nos termos do art. 52, §6º, II. Ademais, tais penalidades somente poderão ser aplicadas após já ter sido imposta ao menos uma das sanções de que tratam os incisos IV, V e VI do caput do art. 52 para o mesmo caso concreto.

Em qualquer dos casos, a ANPD deverá observar os critérios dispostos no §1º do art. 52, quais sejam:

a) a gravidade e a natureza das infrações e dos direitos pessoais afetados;

b) a boa-fé do infrator;

c) a vantagem auferida ou pretendida pelo infrator;

d) a condição econômica do infrator;

e) a reincidência;

f) o grau do dano;

g) a cooperação do infrator;

h) a adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano, voltados ao tratamento seguro e adequado de dados, em consonância com o disposto no inciso II do §2º do art. 48 da Lei;

i) a adoção de política de boas práticas e governança;

j) a pronta adoção de medidas corretivas; e

k) a proporcionalidade entre a gravidade da falta e a intensidade da sanção.

Em caso de vazamento de dados ou acessos não autorizados, será possível a conciliação entre o controlador e o titular dos dados, conforme autoriza o §7º do art. 52; contudo, se não houver acordo, o controlador fica sujeito às penalidades do art. 52.

Quando houver infração à LGDP em decorrência do tratamento de dados pessoais por órgãos públicos, a ANPD poderá, nos termos do art. 31, enviar informe com medidas cabíveis para fazer cessar a violação. A ANPD, ademais, poderá solicitar a agentes do Poder Público a publicação de relatórios de impacto à proteção de dados pessoais e sugerir a adoção de padrões e de boas práticas para os tratamentos de dados pessoais pelo Poder Público, consoante o art. 32.

Por fim, impende registrar que a LGPD, no que toca aos arts. 52, 53 e 54, entrará em vigor apenas a partir do dia 1º de agosto de 2021, nos termos do art. 65, I-A.

ANEXO I - QUADROS SINÓPTICOS

Quadro sinóptico 1 - Hipóteses legais de tratamento dos dados

HIPÓTESE DE TRATAMENTO DE DADOS PESSOAIS	DISPOSITIVO LEGAL (LGPD)	CONSENTIMENTO DO TITULAR?
Mediante consentimento expresso e inequívoco do titular	Art. 7º, I	SIM
Cumprimento de obrigação legal ou regulatória do controlador	Art. 7º, II	NÃO
Execução de políticas públicas a cargo do controlador	Art. 7º, IIII	NÃO
Realização de estudos por órgão de pesquisa, público ou privado	Art. 7º, IV	NÃO
Para execução ou para procedimentos preliminares relativos a contrato	Art. 7º, V	SIM, de modo específico e em cláusula contratual destacada
Exercício de direitos, seja por parte do titular, seja pelo controlador, em processo judicial, administrativo ou arbitral	Art. 7º, VI	NÃO
Para proteção da vida ou da incolumidade física do titular ou de terceiro	Art. 7º, VII	NÃO

Para a tutela da saúde do titular	Art. 7º, VIII	NÃO, se se tratar de procedimento realizado exclusivamente por profissionais da saúde, serviços de saúde ou autoridade sanitária
Para atender interesses legítimos do controlador ou de terceiro	Art. 7º, IX	NÃO, via de regra. Pode exigir consentimento expresso no caso de prevalecerem direitos e liberdades fundamentais do titular que exija a proteção
Proteção do crédito	Art. 7º, X	NÃO

Quadro sinóptico 2 - Hipóteses de tratamento de dados sensíveis

HIPÓTESE DE TRATAMENTO	DISPOSITIVO LEGAL (LGPD)	CONSENTIMENTO DO TITULAR?	OBSERVAÇÕES
Mediante consentimento expresso do titular	Art. 11, I	SIM	O consentimento precisa se dar de forma específica e destacado em cláusula própria
Cumprimento de obrigação legal ou regulatória	Art. 11, II, "a"	NÃO	
Execução de políticas públicas	Art. 11, II, "b"	NÃO	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"	NÃO	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"	NÃO	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"	NÃO	A proteção pode ser do titular ou de terceiro
Tutela da saúde	Art. 11, II, "f"	NÃO	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"	NÃO	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

Quadro sinóptico 3 - Direitos dos titulares de dados que decorrem de princípios

DIREITOS DOS TITULARES DE DADOS QUE DECORREM DE PRINCÍPIOS	PRINCÍPIO CORRESPONDENTE	DISPOSITIVO LEGAL (LGPD)
Direito ao tratamento adstrito aos propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades	Princípio da finalidade	Art. 6°, I
Direito ao tratamento adequado, compatível com as finalidades informadas ao titular, de acordo com o contexto do tratamento	Princípio da adequação	Art. 6°, II
Direito à limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento	Princípio da necessidade	Art. 6°, III
Direito à consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais	Princípio do livre acesso	Art. 6°, IV
Direito à exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade para o cumprimento da finalidade de seu tratamento	Princípio da qualidade dos dados	Art. 6°, V

Direito a 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 transparência	Art. 6°, VI
Direito à segurança dos dados, ao qual se contrapõe o dever, por parte dos agentes de tratamento, de 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 segurança	Art. 6°, VII
Direito à adequada prevenção de danos, ao qual se contrapõe o dever, por parte dos agentes de tratamento, de adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais	Princípio da prevenção	Art. 6°, VIII
Direito de não ser discriminado de forma ilícita ou abusiva	Princípio da não discriminação	Art. 6°, IX
Direito de exigir a adequada responsabilização e a prestação de contas por parte dos agentes de tratamento, ao qual se contrapõe o dever, por parte destes, de adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais	Princípio da responsabilização e prestação de contas	Art. 6°, X

Quadro sinóptico 4 - Direitos dos titulares de dados que decorrem de regras

DIREITOS DOS TITULARES QUE DECORREM DE REGRAS	DISPOSITIVO LEGAL (LGPD)
Direito de condicionar o tratamento de dados ao prévio consentimento expresso, inequívoco e informado do titular, salvo as exceções legais	Arts. 7º, I, e 8º
Direito de exigir o cumprimento de todas as obrigações de tratamento previstas na Lei, mesmo para os casos de dispensa de exigência de consentimento	Art. 7º, §6º
Direito à inversão do ônus da prova quanto ao consentimento	Art. 8º, §2º
Direito de requerer a nulidade de autorizações genéricas para o tratamento de dados pessoais	Art. 8º, §4º
Direito de requerer a nulidade do consentimento caso as informações fornecidas ao titular tenham conteúdo enganoso ou abusivo ou, ainda, não tenham sido apresentadas previamente com transparência, de forma clara e inequívoca	Art. 9º, §1º
Direito de requerer a revogação do consentimento a qualquer tempo, mediante manifestação expressa do titular, por procedimento gratuito e facilitado	Art. 8º, §5º
Direito de revogar o consentimento caso o titular discorde das alterações quanto ao tratamento de dados, seja na finalidade, forma e duração do tratamento, alteração do controlador ou compartilhamento	Arts. 8º, §6º, e 9º, §2º

Direito de acesso facilitado ao tratamento de dados, cujas informações devem ser disponibilizadas de forma clara, adequada e ostensiva acerca de (entre outras): finalidade específica do tratamento; forma e duração do tratamento, observados os segredos comercial e industrial; identificação do controlador; informações de contato do controlador; informações acerca do uso compartilhado de dados pelo controlador; finalidade, responsabilidades dos agentes que realizarão o tratamento e direitos do titular, com menção explícita aos direitos contidos no art. 18	Art. 9º
Direito de ser informado sobre aspectos essenciais do tratamento de dados, com destaque específico sobre o teor das alterações supervenientes no tratamento	Art. 8º, §6º
Direito de ser informado, com destaque, sempre que o tratamento de dados pessoais for condição para o fornecimento de produto ou de serviço, ou, ainda, para o exercício de direito, o que se estende à informação sobre os meios pelos quais o titular poderá exercer seus direitos	Art. 9º, §3º
Direito de ser informado sobre a utilização dos dados pela Administração Pública para os fins autorizados pela Lei e para a realização de estudos por órgão de pesquisa	Art. 7º, III e IV, c/c art. 7º, §1º
Direito de que o tratamento de dados pessoais cujo acesso é público esteja adstrito à finalidade, à boa-fé e ao interesse público que justificaram sua disponibilização	Art. 7º, §3º
Direito de condicionar o compartilhamento de dados por determinado controlador que já obteve consentimento a novo e específico consentimento. No caso da Administração Pública Federal, em que o tratamento é embasado nas hipóteses de dispensa de consentimento original, o compartilhamento demandará uma nova justificativa de tratamento	Art. 7º, §5º

Direito de ter o tratamento de dados limitado ao estritamente necessário para a finalidade pretendida quando o tratamento for baseado no legítimo interesse do controlador	Art. 10, §1º
Direito à transparência do tratamento de dados baseado no legítimo interesse do controlador	Art. 10, §2º
Direito à anonimização dos dados pessoais sensíveis, sempre que possível, na realização de estudos por órgão de pesquisa	Art. 11, II, "c"
Direito de ter a devida publicidade em relação às hipóteses de dispensa de consentimento para: tratamento de dados sensíveis no cumprimento de obrigação legal ou regulatória pelo controlador; ou tratamento compartilhado de dados necessários à execução, pela Administração Pública, de políticas públicas previstas em leis ou regulamentos	Art. 11, §2º
Direito de impedir a comunicação ou o uso compartilhado entre controladores de dados pessoais sensíveis referentes à saúde, com o objetivo de obter vantagem econômica (exceto nos casos de portabilidade de dados quando consentido pelo titular)	Art. 11, §4º
Direito de que os dados pessoais sensíveis utilizados em estudos de saúde pública sejam tratados exclusivamente dentro do órgão de pesquisa e estritamente para a finalidade de realização de estudos e pesquisas e mantidos em ambiente controlado e seguro, conforme práticas de segurança previstas em regulamento específico e que incluam, sempre que possível, a anonimização ou pseudonimização dos dados, bem como considerem os devidos padrões éticos relacionados a estudos e pesquisas	Art. 13
Direito de não ter dados pessoais revelados na divulgação dos resultados ou de qualquer excerto do estudo ou da pesquisa sobre saúde pública	Art. 13, §1º
Direito de não ter dados pessoais utilizados em pesquisa sobre saúde pública transferidos a terceiros pelo órgão de pesquisa	Art. 13, §2º

Direito ao término do tratamento, quando verificado que: (i) a finalidade foi alcançada ou que os dados deixaram de ser necessários ou pertinentes ao alcance da finalidade específica almejada; (ii) houve o fim do período de tratamento; (iii) houve comunicação do titular, inclusive no exercício de seu direito de revogação do consentimento, conforme disposto no §5º do art. 8º da Lei e resguardado o interesse público; ou (iv) por determinação da autoridade nacional, quando houver violação ao disposto na Lei	Art. 15
Direito à eliminação ou ao apagamento dos dados, no âmbito e nos limites técnicos das atividades, sendo autorizada a conservação somente nas exceções legais	Art. 16

Quadro sinóptico 5 - Tratamento de dados pessoais pelo Poder Público

HIPÓTESE AUTORIZADORA	PUBLICIDADE	ENCARREGADO	CONSENTIMENTO DO TITULAR?
Atendimento de finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público	SIM, como regra. O Poder Público deverá publicar, preferencialmente, em seus sítios eletrônicos informações sobre o tratamento de dados pessoais, inclusive de dados sensíveis, de forma clara e atualizada, detalhando a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução desses tratamentos	SIM. Deve ser nomeado um encarregado, que será a figura responsável pela operação de tratamento de dados na Administração. A identidade e informações de contato do encarregado (por exemplo: horário de atendimento, localização, telefone e e-mail específico para orientação e dúvidas) terão de ser divulgadas pela Administração, preferencialmente em seus sítios eletrônicos	NÃO

Quadro sinóptico 6 - Regime de atuação das estatais

REGIME DAS ESTATAIS	TRATAMENTO DADO PELA LGPD	CONSENTIMENTO DO TITULAR?
Exploradora de atividade econômica	Aplicação do mesmo regime das pessoas jurídicas de direito privado	SIM
Prestadora de serviços públicos ou operacionalizando política pública	Aplicação do regime aplicável aos órgãos e entidades do Poder Público	NÃO

ANEXO II - PROPOSTA DE ROTEIRO DE ADEQUAÇÃO E ETAPAS DE IMPLEMENTAÇÃO DO PROGRAMA DE GOVERNANÇA EM PRIVACIDADE

1) Etapa de Planejamento e Construção

• Estabelecer um comitê multidisciplinar e nomear o encarregado em proteção de dados pessoais para o órgão/entidade, o qual deve contar com uma estrutura administrativa proporcional e compatível a complexidade de suas atribuições;

• Levantar as leis e regulamentações de privacidade e proteção de dados e outras normas setoriais aplicáveis, além de reunir a documentação interna relacionada à matéria (políticas, instruções, contratos, convênios, termos e outros instrumentos congêneres);

• Realizar avaliação do grau de maturidade do órgão/entidade em relação à cultura de proteção de dados e do nível de aderência à legislação;

• Analisar como os requisitos de conformidade afetam órgão/entidade e alinhar as expectativas com a alta administração, a fim de priorizar as ações mais críticas, de acordo com seu valor estratégico, os setores/núcleos mais afetados e os recursos disponíveis;

• Identificar os fluxos e os tipos de dados pessoais tratados pelo órgão/entidade, mapeando seus ciclos de vida, desde a coleta até a eliminação, estruturando um inventário de dados e o respectivo registro das operações de tratamento;

• Elaborar uma matriz de riscos considerando a estrutura, a escala e o volume dos tratamentos, a importância e sensibilidade dos dados tratados, os direitos dos titulares e a probabilidade e o impacto de eventos negativos relacionados à privacidade e proteção de dados pessoais para o órgão/entidade;

• Desenhar o programa de governança em privacidade orientado ao risco, a ser aprovado pela alta administração e implementado por meio de um plano de adequação, com etapas, atividades, entregáveis e cronograma definidos; e

• Apresentar o plano de adequação aos servidores/empregados públicos, esclarecendo as exigências de conformidade estabelecidas na legislação, os papeis e responsabilidades e a necessidade de apoio e engajamento de todos para a efetividade do programa.

2) Etapa de Implementação

• Elaborar um código de conduta e ética que, além de definir princípios, fundamentos, diretrizes e responsabilidades para todo o órgão/entidade – servidores/empregados públicos e terceiros -, também demonstre ser a proteção de dados um valor institucional fundamental;

• Criar ou revisar a política de privacidade do órgão/entidade, com os respectivos aviso e termos de uso, e desenvolver o conjunto de políticas internas – específicas e complementares - necessárias à adequação dos procedimentos administrativos, definição de padrões de comportamento, proibições e fixação dos controles de conformidade e segurança;

• Implementar as medidas e controles de segurança necessários ao gerenciamento e mitigação dos riscos identificados nas operações de tratamento de dados pessoais, de acordo as prioridades definidas pela alta administração;

• Adequar processos, procedimentos e documentos, realizando as análises jurídico-administrativas pertinentes, de acordo com as políticas, medidas e controles de privacidade e segurança estabelecidos;

• Realizar diligências e determinar providências de adequação em relação aos servidores/empregados públicos e terceiros, providenciando a consequente aditivação de seus contratos e adotando o devido dever de cuidado em relação às operações de tratamento realizadas em nome do órgão/entidade;

• Adotar mecanismos de transparência (ativa e passiva) e garantir o exercício dos direitos dos titulares, utilizando a ouvidoria como o canal de comunicação adequado ao recebimento dos requerimentos, operacionalização dos atendimentos e estruturação das respostas;

• Apresentar as novas políticas, sistemas, procedimentos, medidas de segurança e controles aos servidores/empregados públicos e ter-

ceiros, assim como promover eventos e ações para disseminar a cultura de privacidade, conscientizando a todos sobre a importância e responsabilidades relacionadas à proteção de dados no órgão/entidade;

• Realizar treinamentos e capacitação (periódicos) de servidores/empregados públicos e terceiros, de acordo com a complexidade das suas atividades e as especificidades das operações de tratamento de dados pessoais que realizam;

• Promover a cultura de privacidade e adotar ações para incorporar a proteção de dados ao cotidiano do órgão/entidade, visando a garantir a segurança adequada aos dados pessoais desde a concepção e por padrão, durante todo o ciclo de vida do processo, sistema, projeto, serviço ou produto; e

• Incorporar a gestão de riscos aos processos do órgão/entidade e, mediante avaliação, elaborar os Relatórios de Impacto à Proteção de Dados Pessoais (RIPD), quando necessário.

3) Etapa de Monitoramento e Revisão

• Manter e atualizar os registros formais de todas as etapas, atividades e procedimentos relacionados à implementação e execução do programa de governança em privacidade, em especial os que comprovem os marcos de conformidade e a documentação obrigatória ou necessária à regular prestação de contas;

• Estabelecer um plano de resposta a incidentes de pronto emprego, com procedimentos e responsabilidades predefinidos, que seja atualizado, testado e treinado constantemente, e indique claramente os canais e/ou pessoas a serem acionadas, eventual utilização de seguro (se existente) e/ou a possibilidade de contratação de serviços técnicos especializados de terceiros, os quais já devem estar previamente cadastrados para atuação imediata quando necessário;

• Criar indicadores de performance (métricas), de clara compreensão e reprodução, para avaliação de resultados, encaminhamento de relatórios à alta administração e demonstração da efetividade do programa de governança em privacidade;

• Estruturar procedimentos e atividades de monitoramento e a au-

ditoria, interna e externa, aptos a, de forma contínua e sistemática, avaliar indicadores, identificar lacunas ou inconformidades, bem como acompanhar mudanças legislativas, dos objetivos do órgão/entidade ou decorrentes do uso de novas tecnologias; e

• Atualizar, corrigir e aperfeiçoar as medidas de adequação e governança, a partir dos indicadores, inconformidades, vulnerabilidades ou incidentes detectados, colocando em prática as lições aprendidas e promovendo ações de revisão e melhorias permanentes, de forma a prevenir falhas futuras ou superar fragilidades do programa.

ANEXO III - PERGUNTAS E RESPOSTAS SOBRE A LGPD

Perguntas e Respostas sobre a LGPD

1) Que pessoas devem observar a Lei Geral de Proteção de Dados?

A Lei Federal n. 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados – LGPD), dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural, devendo ser observadas pela União, Estados, Distrito Federal e Municípios, ou seja, ela regula o tratamento de dados pessoais feito por pessoa jurídica de direito público ou privado, abrangendo secretarias, autarquias, fundações, empresas públicas e sociedades de economia mista. Ela alcança todos os entes da Administração Pública direta e indireta.

2) A Lei Geral de Proteção de Dados se aplica apenas a dados armazenados em meios digitais?

Não. Os dispositivos da LGPD se aplicam tanto a dados armazenados em meios digitais, quanto a dados armazenados em meios físicos.

3) O que o legislador espera de você?

Ao aplicar os dispositivos da LGPD, o legislador quer que você: respeite a privacidade; a autodeterminação informativa; a liberdade de expressão, de informação, de comunicação e de opinião; a inviolabilidade da intimidade, da honra e da imagem; o desenvolvimento econômico e tecnológico e a inovação; a livre iniciativa, a livre concorrência e a defesa do consumidor; e os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

4) O que é autodeterminação informativa?

É saber quais dados pessoais estão sendo coletados e qual a finalidade.

5) A Lei Geral de Proteção de Dados deve ser observada em que atividades?

A LGPD aplica-se a qualquer operação de tratamento: realizada no território nacional; que tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; ou que tenham sido coletados no território nacional, considerando-se coletados no território nacional os dados pessoais cujo titular nele se encontre no momento da coleta.

6) A Lei Geral de Proteção de Dados se aplica em casos de segurança pública, segurança do Estado ou atividades de investigação e repressão de infrações penais?

Essa Lei não se aplica ao tratamento de dados pessoais realizado para fins exclusivos de: segurança pública; segurança do Estado; ou atividades de investigação e repressão de infrações penais, sendo vedado, nestas hipóteses, o tratamento dos dados por pessoa de direito privado, 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. Em tempo, o tratamento de dados pessoais para estes fins será objeto de legislação específica.

7) O que é dado pessoal?

É toda informação relacionada à pessoa natural identificada ou identificável.

8) O que é dado pessoal sensível?

É toda informação que se refere à 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 relacionado a uma pessoa natural.

9) O que é dado anonimizado?

É o dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento, ou seja, o dado que, submetido a técnicas próprias, não possa ser levado a identificar uma pessoa.

10) O que é banco de dados?

É o conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico.

11) Quem é titular?

É a pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.

12) Quem é controlador?

É a pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais. Em tempo, a própria entidade controladora poderá realizar o tratamento dos dados.

13) Quem é operador?

É a pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador. É possível que o operador e o controlador sejam pessoas diferentes (se, por exemplo, uma pessoa jurídica armazena dados a pedido de uma autarquia, a autarquia será controladora e a pessoa jurídica será operadora).

14) Quem é 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).

15) O que é tratamento?

É 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.

16) O que é anonimização?

É a utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo.

17) O que é consentimento?

É a manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada.

18) O que é bloqueio?

É a suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados.

19) O que é eliminação?

É a exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado.

20) O que é transferência internacional de dados?

É a transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o autorifaf seja membro.

21) O que é uso compartilhado de dados?

É a 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.

22) O que é relatório de impacto à proteção de dados pessoais?

É a 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.

23) O que é órgão de pesquisa?

É o 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.

24) O que é Autoridade Nacional de Proteção de Dados?

É o órgão da Administração Pública responsável por zelar, implementar e fiscalizar o cumprimento da LGPD em todo o território nacional. Suas competências e estrutura regimental constam da LGPD e do Decreto Federal n. 10.474, de 26 de agosto de 2020.

25) Quais os princípios gerais que devem ser seguidos nas atividades de tratamento de dados?

Toda atividade de tratamento de dados pessoais deverá observar a boa-fé e, também, os seguintes princípios: finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segu-

rança, prevenção, não discriminação, responsabilização e prestação de contas.

26) O que é o princípio da finalidade?

É a realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades.

27) O que é o princípio da adequação?

É a compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento.

28) O que é o princípio da necessidade?

É a 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.

29) O que é o princípio do livre acesso?

É a 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.

30) O que é o princípio da qualidade dos dados?

É a garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento.

31) O que é o princípio da transparência?

É a garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial.

32) O que é o princípio da segurança?

É a utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão.

33) O que é o princípio da prevenção?

É a adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais.

34) O que é o princípio da não discriminação?

É a impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos.

35) O que é o princípio da responsabilização e prestação de contas?

É a demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

36) O tratamento de dados pessoais sensíveis pode ser realizado em quais condições?

O tratamento de dados pessoais sensíveis somente poderá ocorrer com consentimento do titular ou seu responsável legal, de forma destacada e para finalidades específicas.

Sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para: a) cumprimento de obrigação legal ou regulatória pelo controlador; b) pela Administração Pública, de políticas públicas previstas em leis ou regulamentos; c) estudos por órgão de pesquisa; d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral; e) proteção da vida; f) tutela da saúde; e g) garantia da prevenção à fraude e à segurança do titular.

37) Quem é o setor público de acordo com a LGPD?

O denominado setor público, para fins de aplicação da LGPD, é composto pelos órgãos integrantes da Administração dos Poderes Executivo, Legislativo, incluindo as Cortes de Contas, Judiciário e Ministério Público, assim como pelas autarquias, fundações públicas, empresas públicas, sociedades de economia mista e demais entidades controladas, direta ou indiretamente, pela União, Estados, Distrito Federal a Municípios, nos termos do que prevê o parágrafo único do art. 1º da Lei Federal n. 12.527/2011 (LAI).

Merece, porém, especial atenção o enquadramento de empresas públicas, sociedades de economia mista e demais entidades controladas no conceito de setor público para fins da LGPD, pois, a depender da atividade que desempenharem ao tratar dados pessoais, deverão transitar entre os capítulos II e IV da LGPD, ou seja, é a finalidade a que está vinculado determinado tratamento de dado pessoal – se em regime concorrencial ou se para a execução de políticas públicas - que determinará se a entidade deve atender aos requisitos exigidos na LGPD para o setor privado ou para o setor público.

Portanto, ao ser verificado, no caso concreto, a necessidade de tratar dados pessoais, a entidade que compõe a Administração indireta cuja personalidade jurídica seja de direito privado, especialmente as empresas públicas e sociedades de economia mista, deverão identificar sob qual condição atuam, já que as consequências de atuar em regime concorrencial ou para atendimento de política pública são diversas, desde os requisitos a serem atendidos até as consequências por eventual descumprimento da Lei.

Por fim, a LGPD efetuou a equiparação com o setor público dos serviços notariais e de registro exercidos por delegação, os quais receberam o mesmo tratamento dispensado aos entes públicos quando realizarem o tratamento de dados pessoais.

38) Quando o setor público pode tratar dados pessoais?

Para a execução de políticas públicas previstas em leis, decretos, portarias do órgão ou da entidade, em contratos administrativos, acor-

dos de parceria, termos de cooperação, termos de ajustamento de conduta, convênios ou instrumentos jurídicos congêneres ou para o atendimento de finalidade pública, na persecução do interesse público e com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público.

Verifica-se, assim, que a execução de políticas públicas é indubitavelmente a principal justificativa para que o setor público realize qualquer tipo de tratamento de dados, já que é inerente à existência do Estado a formulação e implementação de políticas públicas em benefício dos cidadãos.

39) Quais as obrigações que o Poder Público assume ao realizar o tratamento de dados pessoais?

Ainda que voltado à execução de política pública, a Administração, ao realizar o tratamento de dados pessoais, deverá efetuar o correto enquadramento da situação fática em uma das hipóteses autorizadoras listadas no art. 7º da LGPD.

O ato de tratamento deve ser motivado e voltado para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades.

Atendendo-se ao princípio da transparência, exige a LGPD que o Poder Público divulgue, preferencialmente em seus sítios eletrônicos, informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas, no exercício de suas competências, voltadas para o tratamento de dados pessoais.

Também é dever da Administração indicar um servidor que exercerá a função de encarregado, conforme preconiza o inciso III do art. 23 da LGPD.

Por fim, embora sendo exceção no setor público, há casos em que o consentimento do titular dos dados precisará ser colhido e considerado. É o que ocorre por exemplo nos tratamentos de dados de crianças e adolescentes.

40) Sempre que o Poder Público efetuar o tratamento de dados pessoais deverá informar o titular do dado?

Não. De acordo com a LGPD, não há necessidade de consentimento do titular ou de garantir publicidade à referida dispensa de consentimento, conforme preconiza o inciso I do art. 23 da LGPD nos casos em que o tratamento de dados pessoais voltar-se para: a) realização de estudos por órgão de pesquisa; 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 e) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos.

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

No exercício de suas competências legais, o órgão ou entidade poderá, por meio de portaria da autoridade superior, discriminar as hipóteses autorizadoras, a finalidade, os procedimentos e as práticas que serão utilizadas para o tratamento de dados pessoais. O citado ato administrativo deverá ser amplamente divulgado no âmbito interno e ainda publicado pela Administração preferencialmente em seus sítios eletrônicos.

É importante, ainda, que no bojo de convênios, contratos administrativos, termos de cooperação técnica, acordos de parceria, termos de outorga e demais instrumentos jurídicos utilizados pelo Poder Público, conste cláusula expressa a respeito da possibilidade de tratamento de dados pessoais eventualmente coletados, devendo, nesse caso, ser observadas todas as regras previstas na LGPD.

42) Como ficam os dados pessoais que estão publicamente disponíveis após o advento da LGPD?

Dados pessoais que estejam publicamente disponíveis devem ser analisados de acordo com a base legal existente para essa disponibilização. Assim, por exemplo, no caso das remunerações de servidores públicos expostas no Portal da Transparência, impõe a Lei de Acesso à Informação que tais dados devem ser expostos, para fins de controle da sociedade.

Todavia, embora estejam públicos, esses dados devem ser protegidos, visto que não poderão ser utilizados para qualquer outra finalidade que não aquela prevista na LAI, não podendo um terceiro captá-los para fazer listas de fornecimento de crédito ou, então, a Administração Pública cedê-los para que terceiros os utilizem para qualquer fim.

43) Como diferenciar a aplicação da LGPD da LAI (Lei de Aceso à Informação)?

O acesso à informação, contida em registros ou documentos, produzidos ou acumulados por órgãos públicos ou entidades da Administração Pública indireta, é de interesse coletivo, sendo regido pela LAI. Isso significa, por exemplo, que qualquer pessoa poderá ter acesso, para fins de controle da atividade administrativa do Estado, a processos licitatórios, contratos administrativos, prestações de contas e demais documentos, salvo os considerados sigilosos segundo a Lei.

O mote central do acesso à informação na esfera da Administração Pública perante a LAI é o princípio constitucional da publicidade.

No tocante à LGPD, o acesso à informação é amparado pelo princípio do acesso livre por interesse particular, ou seja, apenas o titular dos dados pessoais tem direito a requerer, em regra.

Desse modo, o agente público, diante de uma solicitação de acesso à informação pelo particular, deve verificar qual o teor do acesso, se pessoal ou coletivo, pois a depender do requerimento poderá ser aplicada a LAI ou a LGPD ou até mesmo as duas legislações.

44) É necessário registrar as operações sobre o tratamento de dados pessoais?

A Lei obriga que o controlador e o operador mantenham registro das operações relativas ao tratamento de dados pessoais que realizarem, principalmente quando baseado no legítimo interesse (art. 37). Esses registros são importantes para demonstrar o cumprimento da Lei e em caso de apuração de responsabilidade. Por outro lado, a Lei prevê a possibilidade de a Autoridade Nacional determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, inclusive quanto aos dados sensíveis, de acordo com o previsto no art. 38. Veja-se que o art. 10, §3º, indica que o relatório poderá ser solicitado quando o tratamento tiver como fundamento o interesse legítimo. O parágrafo único do art. 38 já estabelece um regramento quanto às exigências mínimas desse documento, como: a) descrição dos tipos de dados coletados; b) metodologia utilizada para a coleta e para a garantia da segurança das informações; e c) análise do controlador em relação a medidas, salvaguardas e mecanismos de mitigação de riscos.

45) A instauração de processo fiscalizatório pela ANPD impede, suspende ou, de alguma forma, influencia a apuração funcional na esfera administrativa?

Não. O poder disciplinar da Administração Pública é independente e desvinculado da fiscalização realizada pela ANPD. Eventual condenação em uma esfera não vincula ou prejudica outra. Apesar disso, a ANPD, antes de aplicar as penalidades referentes à suspensão do banco de dados, suspensão do tratamento de dados e proibição parcial ou total do tratamento de dados, deverá ouvir os respectivos órgãos e entidades com competências sancionatórias.

46) A ANPD pode aplicar penas diretamente a agentes públicos com base na LGPD?

Não há previsão expressa nesse sentido. Os agentes públicos paraenses, pessoalmente, estão sujeitos ao Regime Jurídico Único dos Servidores Civis do Estado do Pará (Lei Estadual n. 5.810/1994), à Lei

de Acesso à Informação (Lei Federal n. 12.527/2011) e à Lei de Improbidade Administrativa (Lei Federal n. 8.429/1992). Nesse sentido, a ANPD, para aplicar as penalidades referentes à suspensão do banco de dados, suspensão do tratamento de dados e proibição parcial ou total do tratamento de dados, deverá ouvir os respectivos órgãos e entidades com competências sancionatórias, a fim de considerá-las para efeito de dosimetria da sanção.

ANEXO IV - MODELOS

Cláusulas Contratuais para Proteção de Dados Pessoais (Aditivo)

TERMO ADITIVO

CLÁUSULA PRIMEIRA - DO OBJETO:

1.1. Estabelecer regra de proteção de dados pessoais no Contrato n. XXX, celebrado com XXX para a prestação de serviços de XXX.

CLÁUSULA SEGUNDA - DA ESPECIFICAÇÃO DO OBJETO:

2.1. Incluir na Cláusula XXX - DAS OBRIGAÇÕES E RESPONSABILIDADES DA CONTRATADA (adequar conforme a nomenclatura da cláusula) o seguinte item:

XX Da Proteção de Dados Pessoais

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

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

b) o tratamento seja limitado às atividades necessárias ao atingimento das finalidades de execução do contrato e do serviço contratado, utilizando-os, quando seja o caso, em cumprimento de obrigação legal ou regulatória, no exercício regular de direito, por determinação judicial ou por requisição da ANPD;

c) em caso de necessidade de coleta de dados pessoais indispensáveis à própria prestação do serviço, esta será realizada mediante prévia aprovação do ESTADO DO PARÁ, responsabilizando-se a CONTRATADA por obter o consentimento dos titulares (salvo nos casos em que opere outra hipótese legal de tratamento). Os dados assim coletados só poderão ser utilizados na execução dos serviços especificados neste contrato, e em hipótese alguma poderão ser compartilhados ou utilizados para outros fins;

c.1) eventualmente, as partes podem ajustar que o ESTADO DO PARÁ será responsável por obter o consentimento dos titulares, observadas as demais condicionantes da alínea 'c' acima;

d) os sistemas que servirão de base para armazenamento dos dados pessoais coletados, seguem um conjunto de premissas, políticas e especificações técnicas que regulamentam a utilização da tecnologia de informação e comunicação no ESTADO DO PARÁ;

e) os dados obtidos em razão desse contrato serão armazenados em um banco de dados seguro, com garantia de registro das transações realizadas na aplicação de acesso (log) e adequado controle de acesso baseado em função (role based access control) e com transparente identificação do perfil dos credenciados, tudo estabelecido como forma de garantir inclusive a rastreabilidade de cada transação e a franca apuração, a qualquer momento, de desvios e falhas, vedado o compartilhamento desses dados com terceiros;

f) encerrada a vigência do contrato ou não havendo mais necessidade de utilização dos dados pessoais, sejam eles sensíveis ou não, a CONTRATADA interromperá o tratamento dos dados pessoais disponibilizados pelo CONTRATANTE e, em no máximo trinta dias, sob instruções e na medida do determinado pelo ESTADO DO PARÁ, eliminará completamente os Dados Pessoais e todas as cópias porventura existentes (seja em formato digital ou físico), salvo quando a CONTRATADA tenha que manter os dados para cumprimento de obrigação legal ou outra hipótese da Lei Federal n. 13.709/2018.

XX.2. A CONTRATADA dará conhecimento formal aos seus em-

pregados das obrigações e condições acordadas nesta subcláusula, inclusive no tocante à Política de Privacidade do ESTADO DO PARÁ, cujos princípios deverão ser aplicados à coleta e tratamento dos dados pessoais de que trata a presente cláusula.

XX.3. O eventual acesso, pela CONTRATADA, às bases de dados que contenham ou possam conter dados pessoais implicará para a CONTRATADA e para seus prepostos – devida e formalmente instruídos nesse sentido – o mais absoluto dever de sigilo, no curso do presente contrato e pelo prazo de até 10 anos contados de seu termo final.

XX.4. A CONTRATADA cooperará com o ESTADO DO PARÁ no cumprimento das obrigações referentes ao exercício dos direitos dos titulares previstos na Lei Federal n. 13.709/2018 e nas Leis e Regulamentos de Proteção de Dados em vigor e também no atendimento de requisições e determinações do Poder Judiciário, Ministério Público e órgãos de controle administrativo.

XX.5. A CONTRATADA deverá informar imediatamente ao ESTADO DO PARÁ quando receber uma solicitação de um titular de dados, a respeito dos seus dados pessoais e abster-se de responder qualquer solicitação em relação aos dados pessoais do solicitante, exceto nas instruções documentadas do ESTADO DO PARÁ ou conforme exigido pela Lei Federal n. 13.709/2018 e Leis e Regulamentos de Proteção de Dados em vigor.

XX.6. O "Encarregado" da CONTRATADA manterá contato formal com o Encarregado do ESTADO DO PARÁ, no prazo de até vinte e quatro horas da ocorrência de qualquer incidente que implique violação ou risco de violação de dados pessoais, para que este possa adotar as providências devidas, na hipótese de questionamento das autoridades competentes.

XX.7. A critério do Encarregado do ESTADO DO PARÁ, a CONTRATADA poderá ser provocada a colaborar na elaboração do relatório de impacto, conforme a sensibilidade e o risco inerente dos serviços objeto deste contrato, no tocante a dados pessoais.

XX.8. Eventuais responsabilidades das partes, serão apuradas con-

forme estabelecido neste contrato e também de acordo com o que dispõe a Seção III,

Capítulo VI, da Lei Federal n. 13.709/2018.

CLÁUSULA TERCEIRA – DAS DISPOSIÇÕES FINAIS:

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

Termo de compromisso de confidencialidade de informações e proteção de dados pessoais e sensíveis

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

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

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

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

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

c) Técnicas, design, especificações, desenhos, cópias, modelos, flu-

xogramas, croquis, fotografias, software, mídias, contratos, acordos ou instrumentos similares, processos, tabelas, projetos, nomes de servidores, agentes políticos ou empregados públicos, resultados de pesquisas, dados orçamentários e/ou financeiros, dentre outros.

IV. Tenho conhecimento ainda da Lei Federal n. 13.709/2018;

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

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

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

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

IX. Reconheço que meus dados pessoais utilizados para acesso aos sistemas disponibilizados pelo ESTADO DO PARÁ serão conservados durante o tempo em que estiver vigente a relação contratual com o ente público ao qual estou vinculado e, após esta finalizar, durante os períodos de retenção de dados legalmente exigíveis, de forma estritamente necessária, tais como, mas não se limitando, pelos prazos prescricionais para ajuizamento de ação penal ou civil, assim como para o exercício do direito de defesa em processo judicial de qualquer natureza ou para outra finalidade por período não excessivo adotado pelo ESTADO DO PARÁ, garantida a transparência, confidencialidade,

integridade e disponibilidade das minhas informações pessoais, bem como o exercício dos direitos previstos na Lei Federal n. 13.709/2018 na vigência da relação contratual, assim como após o término da referida relação.

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

Belém, XX de XXX de 2021.

_____

Relatório de Impacto à Proteção de Dados Pessoais - RIPD

1. IDENTIFICAÇÃO DOS AGENTES DE TRATAMENTO E DO ENCARREGADO

CONTROLADOR	
OPERADOR	
ENCARREGADO	
E-MAIL ENCARREGADO	TELEFONE ENCARREGADO

2. NECESSIDADE DE ELABORAR O RELATÓRIO
3. DESCRIÇÃO DO TRATAMENTO
3.1 NATUREZA DO TRATAMENTO
3.2 ESCOPO DO TRATAMENTO
3.3 CONTEXTO DO TRATAMENTO
3.4 FINALIDADE DO TRATAMENTO
4. PARTES INTERESSADAS CONSULTADAS
5. NECESSIDADE E PROPORCIONALIDADE
6. IDENTIFICAÇÃO E AVALIAÇÃO DE RISCOS

ID	RISCO REFERENTE AO TRATAMENTO DE DADOS PESSOAIS	P1	I2	NÍVEL DE RISCO (P X I)3

Legenda: P - Probabilidade; I - Impacto.

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

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

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

7. MEDIDAS PARA TRATAR OS RISCOS

RISCO	MEDIDA(S)	EFEITO SOBRE O RISCO[1]	RISCO RESIDUAL[2]	MEDIDA(S) APROVADA(S)3	
			P	I	(P X I)

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

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

2. Risco residual é o risco que ainda permanece mesmo após a aplicação de medidas para tratá-lo.

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

8. APROVAÇÃO

RESPONSÁVEL PELA ELABORAÇÃO DO RELATÓRIO DE IMPACTO	ENCARREGADO
_____ <Nome do responsável> Matrícula: xxxxx <Local>, <dia> de <mês> de <ano>	_____ <Nome do responsável> Matrícula: xxxxx <Local>, <dia> de <mês> de <ano>
AUTORIDADE REPRESENTANTE DO CONTROLADOR	AUTORIDADE REPRESENTANTE DO OPERADOR
_____ <Nome do responsável> Matrícula: xxxxx <Local>, <dia> de <mês> de <ano>	_____ <Nome do responsável> Matrícula: xxxxx <Local>, <dia> de <mês> de <ano>

REFERÊNCIAS

Bibliografia

BIONI, Bruno Ricardo. Proteção de dados pessoais: A função e os limites do consentimento. 2ª Ed., 2ª Reimp., Rio de Janeiro: Forense, 2020.

BRASIL. Comitê Central de Governança de Dados (Coletivo). Guia de boas práticas. Lei Geral de Proteção de Dados. Brasília/DF, 2020, disponível em: https://www.gov.br/governodigital/pt-br/governanca-de-dados/guia-lgpd.pdf, Acesso em: 1 de nov. de 2020.

DONEDA, Danilo. Da privacidade a proteção de dados pessoais. 2. Ed., São Paulo: Revista dos Tribunais, 2019.

GOLA, Peter; KLUG, Christoph; KÖRFFER, Barbara; SCHOMERUS, Rudolf. BDSG, Bundesdatenschutzgesetz: Kommentar. 12. Aufl. München: Verlag C.H. Beck oHG, 2015.

JIMENE, Camilla do Vale. TAMER, Maurício Antonio. Plano de Resposta a Incidentes de Segurança de Dados Pessoais In Data Protection Officer (encarregado) / Coordenadores. OPICE BLUM, Renato. VAINZOF, Rony. MORAES, Henrique Fabretti. São Paulo: Thomson Reuters Brasil, 2020.

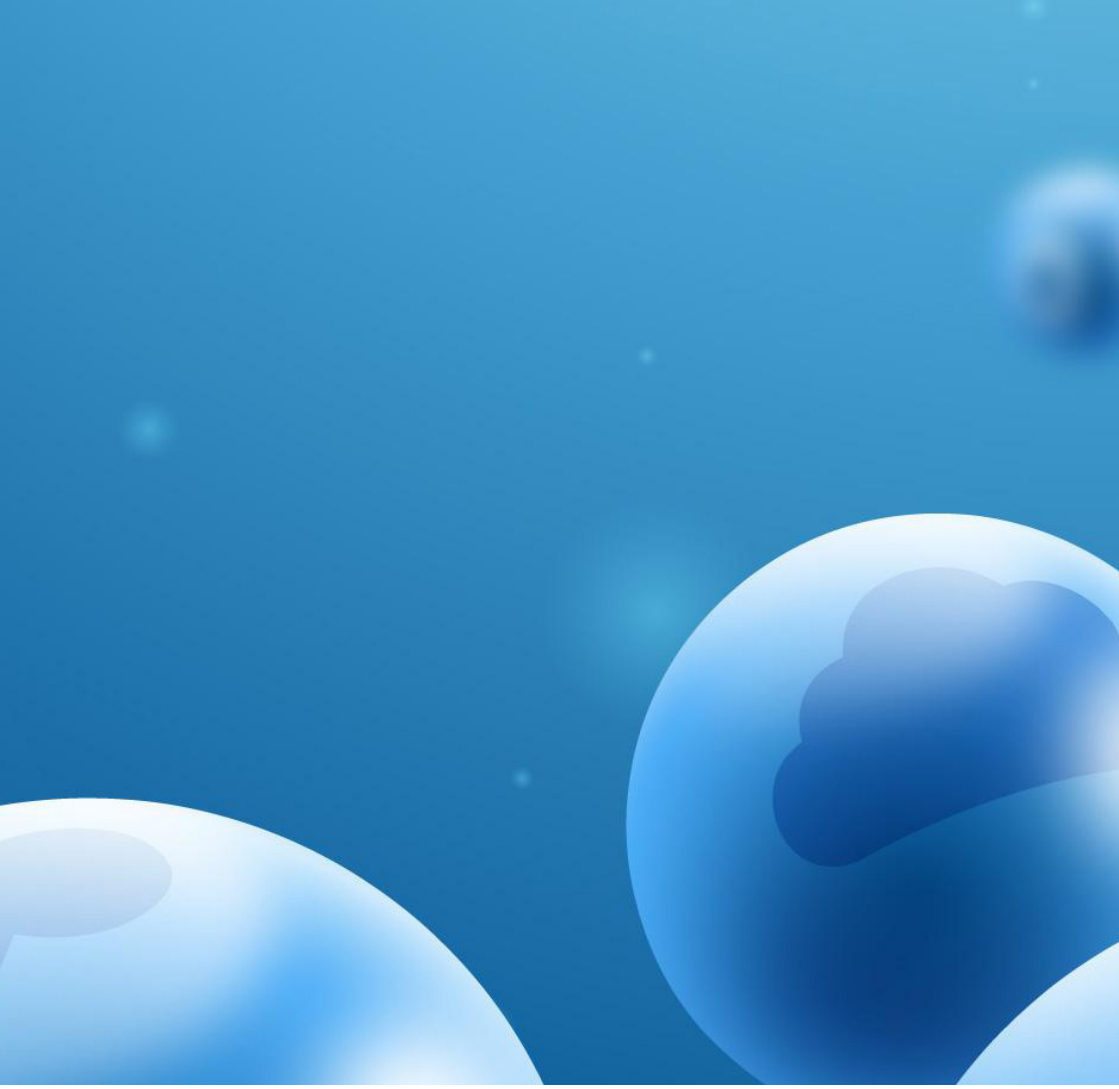
LEVY, Pierre. O que é o virtual? 2. Ed., São Paulo: Editora 34, 2011.

MULHOLLAND, Caitlin (Org). A LGPD e o novo marco normativo no Brasil. Porto Alegre: Arquipélago, 2020.

SOMBRA, Thiago Luís, CASTELLANO, Ana Carolina Heringer. Plano de Resposta a Incidentes de Segurança: reagindo rápido e de forma efetiva, in Revista do Advogado, in Proteção de dados: desafios e soluções na adequação à lei / Organizador OPICE BLUM, Renato. 2019 v. 39 n. 144 nov. pp. 168-173.

Matéria de Jornal

ADWALLADR, Carole; GRAHAM-HARRISON, Emma. How Cambridge Analytica turned Facebook 'likes' into a lucrative political tool. Matéria para o The Guardian. Publicada em 17.03.2018. Disponível em: https://www.theguardian.com/technology/2018/mar/17/facebook-cambridge-analytica-kogan-data-algorithm. Acesso em: 1 de nov. de 2020.



PGE
PROCURADORIA-GERAL
DO ESTADO DO PARÁ

GOVERNO DO
PARÁ
POR TODO O PARÁ