fundação podemos
político para todos

Conformidade e Governança *no setor público*

Parte 4

Conformidade na Lei Geral de Proteção de Dados Pessoais

Março 2024 | São Paulo - SP

A LGPD E OS DADOS PESSOAIS

A LGPD estabelece a disciplina legal aplicável ao tratamento de dados pessoais. Compreende-se na categoria jurídica de dados pessoais as informações estabelecidas na Lei, que estão divididas em duas espécies – dados pessoais e dados pessoais sensíveis.

A LGPD busca disciplinar apenas alguns âmbitos nos quais dados pessoais são tratados. De maneira geral, a Lei se aplica a qualquer operação de tratamento realizada por pessoa natural ou jurídica, de direito público ou privado, independente do meio, do país de sua sede ou do país onde estejam localizados os dados.

Por outro lado, a LGPD não se aplica quando:

1) O tratamento dos dados pessoais seja feito por pessoa natural para fins exclusivamente particulares, sem caráter econômico.

2) O tratamento dos dados pessoais seja feito com finalidade jornalística, artística ou acadêmica, bem como para fins de segurança pública, de defesa nacional, de segurança do Estado ou para investigar e reprimir infrações criminais.

Nesse sentido, não se aplica a LGPD, por exemplo, no caso de uso de câmeras de reconhecimento facial em um determinado município, desde que a finalidade seja exclusivamente para segurança pública.

A Lei se aplica tanto nos casos em que o tratamento seja feito de forma física ou digital.

O objetivo da LGPD é proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da pessoa natural, equilibrando-os frente à inovação e à livre iniciativa.

A LGPD E A ADMINISTRAÇÃO PÚBLICA

1. O REGIME JURÍDICO DA LGPD

Quando é a Administração que realiza o tratamento dos dados pessoais, tal tratamento é realizado sob a incidência do direito administrativo, que é parte do direito público. A LGPD traz normas que são de interesse nacional, devendo ser observadas pela União, Estados, Distrito Federal e Municípios.

A liberdade de atuação da administração pública se submete ao princípio da legalidade administrativa, a legalidade própria do direito público. Isso quer dizer que administração apenas pode fazer, em matéria de uso de dados pessoais, o que a lei permite, não estando livre para fazer tudo o que ela simplesmente não proíba.

Dito de outro modo, as normas da LGPD são inderrogáveis, não podendo ser alteradas por disposições contratuais entre as partes. Trata-se, portanto, de normas submetidas ao regime de direito público.

2. A ADMINISTRAÇÃO PÚBLICA NA LGPD

Para além da necessidade de que a administração pública observe, em todo seu raio de atuação, os princípios e as normas de direito público aplicáveis (tais como os estabelecidos pelo artigo 37 da Constituição Federal de 1988), a LGPD traz um capítulo específico destinado à realização do tratamento de dados pelo setor público. Dessa forma, a Lei dispensa um tratamento distinto para as pessoas jurídicas de direito público em relação às pessoas jurídicas de direito privado, aplicando o Capítulo IV àquelas, e o Capítulo II a estas.

Acerca da incidência das regras previstas no Capítulo da LGPD direcionado ao poder público (Capítulo IV), é preciso saber que:

1) A Administração Pública Direta dos Poderes Executivo, Legislativo, Judiciário, Ministério Público e Tribunais de Contas seguem o regime do Capítulo IV;

2) A Administração Pública Indireta autárquica e fundacional, e demais controladas de direito público, também devem seguir o referido Capítulo;

3) Aos serviços notariais e de registro exercidos em caráter privado, por delegação do poder público, aplica-se o mesmo tratamento dispensado às pessoas jurídicas de direito público. Ou seja, incide sobre aqueles serviços o referido Capítulo da LGPD.

4) Às empresas públicas e as sociedades de economia mista que atuem em regime de concorrência, sujeitas ao disposto no artigo 173 da Constituição Federal, aplica-se o mesmo tratamento dispensado às pessoas jurídicas de direito privado particulares. Dessa forma, sobre essas empresas não incidem, em geral, as regras do referido Capítulo, mas sim as regras do Capítulo II.

5) As empresas públicas e as sociedades de economia mista, quando estiverem operacionalizando políticas públicas e no âmbito da execução delas, terão o mesmo tratamento dispensado aos órgãos e às entidades do Poder Público, aplicando-se a elas o Capítulo IV.

A distinção de regramento trazido pela LGPD aos órgãos e empresas da administração pública se dá, portanto, conforme o objetivo em se realizar o tratamento de dados, podendo ser feita, em termos gerais a seguinte distinção:

1) Objetivo de realizar políticas públicas: nesse caso, aplicar-se-á o Capítulo IV da LGPD.

2) Objetivo econômico, caracterizando a exploração

direta de atividade econômica pelo Estado, conforme o artigo 173 da Constituição Federal: nesse caso, aplicar-se-á o Capítulo II da LGPD.

2.1 BASE LEGAL PARA O TRATAMENTO DE DADOS PELA ADMINISTRAÇÃO PÚBLICA

As pessoas jurídicas de direito público encontram-se em uma situação especial em relação à LGPD. Por exemplo:

1) O sujeito de direito público é a União:

2) A União é organizada em ministérios, que são órgãos públicos, mas não constituem uma pessoa jurídica distinta.

3) A quem caberá a posição de controlador dos dados pessoais?

4) Resposta: o controlador será a pessoa jurídica, isto é, a União. Aplica-se, portanto, a teoria do órgão.

Nesse aspecto, a União:

1) É responsável pelas obrigações da LGPD.

2) É responsável por obrigações contratuais que envolvam proteção de dados pessoais e segurança da informação.

3) Responsabiliza-se por atos ilícitos que venham a ser praticados pelos seus órgãos ou servidores.

Aos órgãos da Administração Pública, de forma descentralizada, é que cabem as atribuições típicas de controlador. Assim, eles são responsáveis, por exemplo, pelo:

1) Tratamento compartilhado de dados;

2) Aplicação de sanções administrativas a servidores que estiverem descumprindo a lei;

3) Designação do Encarregado de forma transparente.

4) Estabelecimento de estruturas adequadas para responder a requisições de exercício de direitos por parte dos titulares de dados pessoais e a requerimentos da ANPD e outros órgãos competentes.

2.1.1 QUANDO ATUANDO NA OPERACIONALIZAÇÃO DE POLÍTICAS PÚBLICAS

O tratamento de dados pode ser realizado pela administração pública para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em

contratos, convênios ou instrumentos congêneres (art. 7o, III da LGPD).

Já em relação aos dados sensíveis, a administração pública poderá tratá-los, sem o consentimento do titular, somente quando necessário à execução de políticas públicas previstas em leis ou regulamentos (art. 11, II, "b" da LGPD).

Assim, a administração pública pode tratar dados pessoais tendo por fim interesse público e com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público, desde que:

> I. sejam informadas aos titulares de dados as hipóteses em que, no exercício de suas competências, realizam o tratamento de dados pessoais, fornecendo informações claras e atualizadas sobre a previsão legal (tanto a previsão da base legal da LGPD como a base legal específica da política pública a ser executada), a finalidade do tratamento, os procedimentos e as práticas utilizadas para a execução dessas atividades, em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos;
>
> II. seja indicado um encarregado de dados pessoais

2.1.2 QUANDO ATUANDO NA EXECUÇÃO DE ATIVIDADE ECONÔMICA

Neste caso, o Estado atua por meio de empresas públicas e empresas de economia mista, assumindo o regime jurídico de direito privado. No que diz respeito à aplicação da LGPD, as bases legais para o tratamento de dados nesses casos são as mesmas que aquelas estabelecidas para os agentes privados. As estatais que atuam em regime de concorrência, por exemplo, seguem essa regra.

3. GOVERNANÇA EM PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS

No que diz respeito à governança em privacidade e proteção de dados prevista no art. 50 da LGPD, os mecanismos estão, nesse caso, voltados a garantir, por um lado, a devida forma regular de realização do tratamento de dados pessoais, pautada pelos princípios constitucionais e legais, com destaque para os estabelecidos pela LGPD.

A governança no setor público deve considerar a necessidade de construção de uma nova cultura ética em relação a dados pessoais, realizada por padrões comportamentais exigíveis a todos os agentes públicos, dando, assim, eficácia e confiabilidade aos órgãos públicos, bem como legitimidade para o exercício de sua finalidade quando do tratamento de dados pessoais.

Nesse sentido, a LGPD traz balizas a serem observadas pela administração pública para a realização dos processos de tratamento de dados pessoais

que estejam sob responsabilidade do órgão ou entidade. A LGPD estabelece a necessidade de estruturação de uma governança em privacidade; seus requisitos gerais são:

1) Atender aos requisitos de segurança no tratamento de dados pessoais;

2) Atender aos padrões de boas práticas e de governança;

3) Atender aos fundamentos previstos na LGPD. São eles:

a. O respeito à privacidade. Fundamento que vai ao encontro ao previsto na própria Constituição Federal, segundo a qual o Poder Público não pode violar a privacidade de indivíduos, exceto nas hipóteses legais legalmente admitidas.

b. A autodeterminação informativa. Pretende conferir ao titular a possibilidade de acompanhar o que é realizado com seus dados.

c. A liberdade de expressão, de informação, de comunicação e de opinião e a inviolabilidade da intimidade, da honra e da imagem. Estes fundamentos, em conjunto, são fundamentais para o exercício da personalidade e para a autodeterminação dos seres humanos.

d. O desenvolvimento econômico e tecnológico e a inovação e a livre iniciativa, a livre concorrência e a defesa do consumidor. Fundamentos originados a partir do art. 170 da Constituição Federal.

e. Os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais. O que se poderia extrair de tais fundamentos seria a intenção da LGPD em evitar o monitoramento excessivo e indevido por parte do Poder Público.

É possível que os controladores possam formular as regras de boas práticas e de governança, individualmente ou por meio de associações, estabelecendo assim os parâmetros para um setor específico. Nessas regras de boas práticas é possível definir:

1) As condições de organização;

2) O regime de funcionamento;

3) Os procedimentos, incluindo reclamações e petições de titulares;

4) As normas de segurança;

5) Os padrões técnicos;

6) As obrigações específicas para os diversos envolvidos no tratamento

7) As ações educativas;

8) Os mecanismos internos de supervisão e de mitigação de riscos; e

9) Outros aspectos relacionados ao tratamento de dados pessoais.

Deve ser levado em consideração, para a elaboração das regras de boas práticas que tratem dos aspectos acima elencados tendo em vista o tratamento de dados, a natureza, o escopo, a finalidade e a probabilidade e a gravidade dos riscos e dos benefícios decorrentes de tratamento de dados do titular. Logo, dependendo do setor específico da administração pública (em especial no caso de estatais), é possível estabelecer tais regras de boas práticas para que o setor, como um todo, possa segui-las.

3.1. O PROGRAMA DE GOVERNANÇA EM PRIVACIDADE

A LGPD também destaca a importância de os controladores e operadores estruturarem um programa de governança em privacidade, também conhecido no mercado como "programa de compliance digital".

Ao realizar o tratamento de dados, o controlador deve ter em conta a estrutura, a escala e o volume das operações, uma vez que tais elementos estão relacionados ao nível de risco de sua operação. Portanto, existem atividades de políticas públicas que vão exigir um tratamento em larga escala de dados pessoais, o que vai requerer maior preocupação de todos no referido processo.

Imprescindível também que tenha atenção especial à categoria dos dados pessoais, a qual pode impactar na gravidade dos danos ao seu titular em casos de incidentes de segurança. Além disso, os tipos de titulares (vulneráveis, crianças, idosos, por exemplo) também podem impactar na criticidade do tratamento.

Tudo isso considerado, deve-se implementar programa de governança que, no mínimo:

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

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

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

d) estabeleça políticas e salvaguardas adequadas com base em processo de avaliação

sistemática de impactos e riscos à privacidade;

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

f) esteja integrado à 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;

É importante que o programa de governança em privacidade traga evidências de sua efetividade sempre que seja apropriado, e, conforme dispõe a LGPD, especialmente quando seja solicitado pela autoridade nacional (ANPD), ou mesmo por outra autoridade que seja responsável por promover o cumprimento de boas práticas ou códigos de conduta.

Além disso, é necessário que as regras de governança em privacidade sejam sempre publicadas de forma a que os servidores da instituição tomem pleno conhecimento delas, as quais devem também sempre ser objeto de monitoramento, avaliação e atualização.

3.2. O ENCARREGADO DE DADOS NO CONTEXTO DA GOVERNANÇA EM PRIVACIDADE

Cada órgão público deverá nomear um Encarregado (também conhecido como data protection officer – DPO) para atuar como ponto de contato entre titulares dos dados pessoais, o controlador e ANPD. O ente da administração pública deverá, para isso, disponibilizar de forma pública o contato e a identificação do Encarregado, em preferência no website próprio da instituição a que ele pertença.

A função de encarregado costuma ser exercida pelas pastas ligadas à integridade ou à transparência, como as controladorias gerais, vinculada à função na pessoa do controlador-geral, de maneira a evitar o acúmulo com as áreas responsáveis pela tecnologia da informação. O acúmulo não é proibido por lei, embora possa gerar sobrecarga de funções ou então conflito de interesses (já que o responsável teria que fiscalizar a si mesmo quanto ao cumprimento da LGPD). Na Instrução Normativa SGD/ME nº 117, de 19 de novembro de 2020, o Governo Federal optou por vedar essa cumulação (art. 1º, § 1º, II).

É possível, ainda, que os órgãos tenham pontos focais especializados nos tipos de tratamento da política pública respectiva, como uma espécie de "embaixadores", e que possam interagir com o encarregado centralizado.

Pode-se, ademais, considerar a criação, como órgão auxiliar do Encarregado, de um comitê de privacidade, de caráter colegiado, que congregue diversos setores da Administração Pública. Tal colegialidade permitiria que toda a Administração se envolvesse nos debate sobre medidas voltadas ao aprimoramento de providências no atendimento à LGPD.

No geral, os elementos que devem orientar a estrutura para que o encarregado exerça suas funções, bem como quais são as qualidades e competências pessoais que deve possuir, envolvem conhecimento jurídico, de segurança da informação, de governança de dados e de acesso à informação no setor público. Ademais, o Encarregado deve receber treinamento contínuo para aperfeiçoamento e atualização em relação aos temas de privacidade e proteção de dados.

3.3. A INTEROPERABILIDADE E ESTRUTURAÇÃO DOS DADOS TRATADOS PELO PODER PÚBLICO

A LGPD prevê em seu art. 25, que integra o Capítulo IV, que os dados pessoais deverão ser mantidos em formato interoperável e estruturado para o uso compartilhado, visando a execução de políticas públicas, a prestação de serviços públicos, a descentralização da atividade pública e a disseminação e acesso das informações pelo público em geral.

O conceito de "formato interoperável e estruturado para o uso compartilhado" é melhor compreendido ao se analisar o contexto da evolução tecnológica do setor público.

O Poder Público possui uma enorme estrutura caracterizada pelo atraso tecnológico, salvo raras exceções.

Isso ocorre em razão de:

1) Limitação de orçamentos;

2) Alternância de gestões e consequente descontinuidade de projetos estruturantes;

3) Priorização de gastos na contratação de pessoas em detrimento do investimento em tecnologia da informação;

4) Ausência de alinhamento estratégico entre órgãos de um mesmo setor;

5) Priorização heterogênea de investimentos em tecnologia da informação entre órgãos públicos.

Tudo isso prejudica - para não dizer que inviabiliza - a execução de políticas públicas, a eficiente prestação de serviços, a descentralização da atividade pública, a disseminação e o acesso de informações pelo público em geral.

Para lidar com esse problema do fluxo informacional na Administração Pública, a solução tecnológica preconizada pela LGPD é a interoperabilidade e a

estruturação dos dados.

3.3.1. A INTEROPERABILIDADE

Trata a interoperabilidade da capacidade de diversos sistemas e organizações trabalharem em conjunto, garantindo às pessoas, organizações e sistemas computacionais que interajam para trocar informações de maneira eficaz e eficiente.

A interoperabilidade é premissa de um governo moderno baseado em sistemas que trabalhem nas diversas esferas. Ao promover a interoperabilidade, a LGPD prescreve que o dado deve ser tratável por qualquer sistema e deve ser transitável pela web.

Para isso, é necessário que os dados estejam em padrão aberto e que os sistemas que vão trabalhá-lo estejam aptos a fazê-lo, independentemente do fato de também adotarem a concepção de código aberto.

Ressalta-se que a natureza do dado (dado pessoal ou dado pessoal sensível, ou até mesmo dado que não seja pessoal) e conceito é diferente da forma em que ele se apresenta. A LGPD, neste contexto, determina que os dados pessoais devem ser armazenados em formato de arquivo não proprietário, cuja especificação esteja documentada publicamente, seja de livre conhecimento e implementação e livre de patentes ou qualquer outra restrição legal quanto à sua utilização.

Isso não significa dizer, porém, que os dados pessoais e dados pessoais sensíveis dos cidadãos podem ser acessados por qualquer pessoa. Isso estaria em total desacordo com as demais disposições da LGPD.

Como exemplos de arquivos em formato aberto, pode-se citar:

1) Para documentos: PDF, TXT, HTML;

2) Para arquivos em áudio: OGC e FLAC;

3) Para imagens: PNG e SVG.

Já o dado armazenado em formato fechado ou proprietário é, por exemplo, um documento de texto, de um determinado órgão público, que seja codificado em formato que somente o sistema daquele órgão consiga interpretá-lo, sem possibilidade de que outro o faça.

3.3.1.1. SOFTWARE DE CÓDIGO ABERTO E SOFTWARE DE CÓDIGO FECHADO

O sistema computacional ou software é construído em dada linguagem, resultado da compilação de seu código-fonte. O software cujo código-fonte é acessível a qualquer pessoa com conhecimento técnico para que o execute, copie e redistribua, modifique ou o estude é considerado software livre, de código aberto ou aderente à Licença Pública Geral (General Public Licence - GPL);

Por outro lado, se o código fonte não é acessível ou passível de distribuição

ou alteração, por se tratar de obra protegida pelo direito de propriedade intelectual previsto pela Lei 9.609/1998 (Lei do Software), diz-se que o software é de padrão tecnológico fechado ou proprietário. Ressalta-se que ser de padrão tecnológico aberto ou fechado não significa, em qualquer dos dois casos, que o software seja gratuito.

Esses conceitos são fundamentais para se compreender que a imposição legal de interoperabilidade de dados não implica na obrigatoriedade de toda a Administração Pública adotar o software livre (de código aberto), construído em linguagens abertas de programação, ou ainda que deva adotar o mesmo sistema para o tratamento de dados (sistema único).

Os dados devem ser acessíveis e passíveis de leitura pelos diversos sistemas computacionais e esses devem ter a capacidade de acessá-los e tratá-los, independentemente do padrão adotado na sua construção.

3.3.1.2. COMO IMPLEMENTAR A INTEROPERABILIDADE

Feitos os esclarecimentos iniciais, como implementar a interoperabilidade?

O compartilhamento de dados pode ser feito de diversas formas, como:

1) Pela disponibilização de arquivos de texto, imagem, áudio, vídeo ou planilhas eletrônicas para download;

2) Pela disponibilização de um portal dotado de ferramenta de consulta à base de dados;

3) Pela utilização de software ETL, que é um software que proporciona a integração de sistemas por meio da troca de arquivos, extraindo um conjunto de dados de uma aplicação de origem, reestruturando-a para o formato do sistema de destino (transformação) e realizando o carregamento desse pacote de dados para tratamento por esse sistema;

4) Pelo desenvolvimento de uma API, que é uma interface de comunicação entre sistemas que utiliza grande diversidade de protocolos e permite que um sistema utilize, em larga escala, funcionalidade do outro sem a necessidade de implementá-las em seu próprio código;

5) Por um webservice, que é uma espécie limitada de API em que a interação entre sistemas é padronizada e disponibilizada para acesso via web;

Por um lado, o webservice trabalha exclusivamente sob a lógica computacional de requisição e resposta, sendo mais limitado que uma API convencional. Por outro lado, o webservice permite a interação do sistema com diversas aplicações

externas que atendam ao seu padrão.

Por meio das três últimas abordagens (ETL, API e webservice), é possível realizar a integração de sistemas, ou seja, a criação de um canal em que softwares troquem informações diretamente entre si.

No Poder Executivo Federal, o Padrão de Interoperabilidade do Governo Eletrônico é o e-PING;

No Poder Judiciário nacional e órgãos de Justiça, como o Ministério Público, Polícia Civil e Defensoria Pública, adota-se, obrigatoriamente, o Modelo Nacional de Interoperabilidade – MNI. Trata-se de um modelo de interoperabilidade baseado em webservices, estabelecido pela Resolução Conjunto 3/2013 do Conselho Nacional de Justiça e do Conselho Nacional do Ministério Público.

O intercâmbio e tratamento de dados está disponível a qualquer outra instituição pública que venha a aderir ao MNI, sem necessidade alguma de abandono de seus sistemas de origem, em franca postura de bom emprego dos recursos públicos.

3.3.2. DADOS ESTRUTURADOS

São dados formatados, normalmente organizados em tabelas, com linhas e colunas sendo, por isso, facilmente processados por um sistema gerenciador de bancos de dados, passíveis de serem obtidos por máquinas, quantificados, transferíveis e tratáveis.

A estruturação de dados se insere no contexto do modelo de interoperabilidade, condizente com a ideia de que os dados devem estar organizados para serem acessados com eficiência.

Em conclusão, a LGPD determina que os dados pessoais e dados pessoais sensíveis sejam armazenados de forma estruturada e em formato aberto (interoperável), de modo a permitir seu consumo por outros órgãos ou entes públicos, possibilitando a execução de políticas públicas, a prestação de serviços públicos, a descentralização da atividade pública, a disseminação e o acesso das informações pelo público em geral.

4. OS PILARES DE UM PROGRAMA DE GOVERNANÇA EM PRIVACIDADE

A estruturação de um programa de governança deve ser feita a partir de determinados eixos de sustentação. De uma adequada organização desses eixos resultará a força e efetividade do programa de governança em privacidade. É possível utilizar como pilares aqueles definidos pela própria Controladoria-Geral da União para programas de integridade, os quais se aplicam de maneira pertinente ao programa de governança em privacidade. Os pilares fundamentais são:

1) Comprometimento e apoio da alta administração: este princípio trata da necessidade de que a alta administração da empresa esteja comprometida com a cultura

organizacional em privacidade. Para isso, é necessário que o tema seja pautado periodicamente pela alta administração, a qual deve fomentá-lo tanto pela alocação suficiente de recursos, pela preocupação de dar efetividade e autonomia ao departamento responsável, bem como dando o próprio exemplo pessoal de bom uso de dados pessoais.

2) Instância responsável: este pilar diz respeito à necessidade de que seja indicado um Encarregado. Além do já tratado acima, é importante destacar alguns elementos:

a. Imparcialidade, autonomia e independência: trata-se de elementos fundamentais para a boa gestão pelo encarregado, uma vez que não é possível a execução e devido monitoramento do programa na ausência desses requisitos.

b. Disponibilidade de recursos: é imprescindível que o encarregado possua recursos suficientes, humanos e materiais, considerando, para o setor público, os critérios administrativos e orçamentários aplicáveis.

c. O acesso direto à alta administração: O encarregado deve ter facilitado seu acesso aos órgãos da alta administração. No caso da administração pública, isso diz respeito à necessidade de acesso ao alto escalão do Poder Executivo, quando seja necessário.

3) Análise de perfil e riscos: o programa deve estar adaptado à realidade do contexto no qual seja implementado, de acordo com os riscos envolvidos nos processos de tratamento de dados pessoais. Isso demanda que sejam detectados os riscos que estão implicados em todas as atividades realizadas e elaborados procedimentos de controles e monitoramento, observando a necessidade de sua revisão e atualização periódica.

A análise deve ser feita sobretudo acerca do risco de incidentes em relação a dados pessoais, que podem abranger desde o vazamento de dados, fraudes à proteção da privacidade dos dados e outras formas de violações que possam resultar em prejuízos aos titulares de dados.

4) Regras e instrumentos: este pilar está bastante relacionado ao anterior. É a partir da detecção e análise dos riscos e da elaboração de um perfil de riscos que se deve elaborar grande parte da estrutura normativa do programa, já que esta deve estar condizente com a realidade concreta da empresa.

Assim o perfil de riscos deve informar a elaboração e atualização das políticas, procedimentos, dos mecanismos

de prevenção e mitigação de riscos e danos, das formas de reporte de irregularidades, entre outros itens que são relevantes para o programa. Também poderão ser desenvolvidas ou inseridas ferramentas de auxílio na gestão do programa.

5) Monitoramento contínuo: este pilar aponta para a necessidade de que todo o programa seja sempre aperfeiçoado. Dessa forma, são de enorme importância a adoção de mecanismos adequados de monitoramento dos próprios procedimentos e políticas por meio de indicadores de desempenho. Uma boa escolha é a aplicação do ciclo PDCA para auxiliar no ciclo de melhoria contínua do programa.

5. LGPD E AS AUTORIDADES SANCIONADORAS

5.1. NATUREZA DAS SANÇÕES

A LGPD, na Seção I do Capítulo VIII, que abrange os artigos 52, 53 e 54, estabelece a disciplina sancionatória aplicável ao âmbito da proteção e tratamento de dados pessoais.

A disciplina sancionatória, nesse caso, inscreve-se, conforme o próprio título da referida Seção ("Das Sanções Administrativas") no âmbito das sanções administrativas, ao qual se aplica o regime jurídico público de direito administrativo, mais propriamente, do direito administrativo sancionatório.

As sanções de natureza jurídica administrativa diferem-se de outras espécies sancionatórias. A distinção não se dá necessariamente por alguma diferença na qualidade material do ilícito ou da irregularidade que se busca reprimir, mas na sua qualificação normativa e, sobretudo, na disciplina jurídica que rege esse tipo de sanção.

Dessa forma, pode-se apontar as duas características centrais que qualificam esse tipo de sanção como sendo uma sanção de natureza administrativa:

1) Ser aplicada por uma autoridade administrativa no exercício de sua função;

2) Estar submetida ao regime jurídico de direito administrativo sancionador.

5.2. COMPETÊNCIA SANCIONATÓRIA

Possui competência sancionatória a autoridade a qual é atribuída o poder-dever de aplicar as sanções aos que violarem as normas cuja fiscalização esteja sob sua responsabilidade.

No caso da LGPD, a autoridade administrativa responsável, tanto pela regulamentação infralegal de matéria atinente ao tratamento de dados pessoais, quanto pela supervisão do cumprimento da lei e das normas infralegais pertinentes e, também, pela

aplicação das sanções administrativas, é a Autoridade Nacional de Proteção de Dados (ANPD).

A ANPD é uma autarquia de natureza especial, dotada de autonomia técnica e decisória, com patrimônio próprio e com sede e foro no Distrito Federal. Tal agência possui competência exclusiva para a aplicação das sanções administrativas estabelecidas na Lei, sendo que suas competências prevalecem sobre as competências correlatas de outras entidades ou órgãos da administração pública, no que diga respeito à proteção de dados pessoais.

Submetem-se ao poder sancionatório da ANPD os agentes de tratamentos, ou seja, os controladores e operadores de dados pessoais.

5.3. SANÇÕES DA LGPD

As sanções previstas na LGPD são:

1) Advertência;

2) Multa, diária ou simples, podendo esta última corresponder a até 2% do faturamento, com limite de R$ 50 milhões;

3) Publicização da infração após devidamente apurada e confirmada sua ocorrência;

4) Bloqueio dos dados pessoais a que se refere a infração até sua regularização;

5) Eliminação dos dados pessoais a que se refere a infração.

6) 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;

7) Proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados.

A aplicação de tais sanções demanda a observância ao contraditório e ao exercício da ampla defesa. Além disso, as sanções devem ser aplicadas de forma gradativa, isoladas ou cumuladas, tendo em vista as peculiaridades do caso concreto e considerando:

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

2) a boa-fé do infrator;

3) a vantagem auferida ou pretendida pelo infrator;

4) a condição econômica do infrator;

5) a reincidência;

6) o grau do dano;

7) a cooperação do infrator;

8) a adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano, voltados ao tratamento seguro e adequado de dados

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

10) a pronta adoção de medidas corretivas; e

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

Conforme se observa, um adequado programa de governança em privacidade impacta positivamente no aspecto sancionatório da LGPD, ou seja, a adoção de mecanismos de redução de danos causados por incidentes de segurança, bem como de políticas de boas práticas e governança, conforme os itens 8 e 9 acima apontados, reduzem a gravidade da medida sancionatória adotada.

6. RESPONSABILIZAÇÃO NO ÂMBITO DA LGPD

A responsabilidade civil, de modo geral, pode ser objetiva ou subjetiva.

No regime da responsabilidade civil objetiva, basta haver o nexo causal (a relação de causa e efeito) entre a ação e o dano sofrido. Não há necessidade de comprovação de dolo (intenção) ou culpa (negligência, imperícia, imprudência) por parte do causador do dano. Basta que seja causado o dano e quem o causou responde civilmente, devendo, portanto, efetuar sua reparação.

Já no regime da responsabilidade subjetiva, a imputação da responsabilidade exige a comprovação do dolo ou culpa. Assim, é necessário demonstrar que o causador do dano queria causá-lo, ou, então, atuou de forma negligente, imprudente ou sem a perícia necessária no exercício de determinado ato, resultando daí a obrigação de reparar o dano causado a alguém.

Aqueles que defendem a aplicação da responsabilidade subjetiva o fazem em razão da LGPD regular boas práticas e medidas de adequação aos agentes de tratamento. Assim, se a responsabilização for objetiva, ou seja, independente de dolo ou culpa, de que adiantaria o agente agir de forma diligente, investindo diversos recursos na adequação, se ele for responder por danos da mesma forma que os agentes omissos ou negligentes?

Há aqueles que defendem aos controladores e operadores de dados algo próximo da responsabilidade objetiva, em razão do fato da LGPD determinar o dever de indenizar diante da ocorrência de dano, embora preveja, neste caso, três excludentes de responsabilidade, se o agente de tratamento for capaz de provar:

I - que não realizou o tratamento de dados pessoais que lhe é atribuído;

II - que, embora tenha realizado o tratamento de dados pessoais que lhe é atribuído, não houve violação à legislação de proteção de dados; ou

III - que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiro.

Como regra geral, em se tratando de dano causado não por uma ação do Poder Público, mas por uma omissão, sua responsabilidade será subjetiva. Entretanto, em se tratando da LGPD, isso não ocorre, uma vez que esta Lei determina a necessidade de que o agente de tratamento se utilize 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", bem como a adoção de "medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais", sendo, ainda, preciso que comprove a utilização de tais medidas.

REFERÊNCIAS

AMARAL, Luiz Fernando de Camargo Prudente do. Desafios da LGPD em relação à implementação pelo Poder Público. In: OPICE BLUM, Renato (org.). Proteção de Dados: Desafios e soluções na adequação à lei. Rio de Janeiro: Forense, 2020. cap. 7, p. 77-92.

BECKER, Daniel; ALBERNAZ, Carolina; BRÍGIDO, João Pedro. LGPD e reequilíbrio econômico-financeiro dos contratos de concessão de serviços públicos: Às vezes, é preciso alterar a ordem das coisas para que elas retornem ao seu equilíbrio original. Jota, 7 jul. 2019. Disponível em: https://www.jota.info/opiniao-e-analise/colunas/regulacao-e-novas-tecnologias/lgpd-e-reequilibrio-economico-financeiro-dos-contratos-de-concessao-de-servicos-publicos-07072019#sdfootnote5anc. Acesso em: 6 jan. 2021.

BRASIL. Governo Digital. Governança de Dados. Disponível em: https://www.gov.br/governodigital/pt-br/governanca-de-dados. Acesso em: 26 nov. 2022.

CARVALHO, André Castro; CONTI, José Maurício; BLUM, Rita Peixoto Ferreira. Aplicação da LGPD ao Setor Público: Aspectos Relevantes. In: MONACO, Gustavo Ferraz de Campos; MARTINS, Amanda Cunha e Mello Smith; CAMARGO, Solano de (org.). Lei Geral de Proteção de Dados: Ensaios e Controvérsias da Lei 13.709/18. 1. ed. São Paulo: Quartier Latin, 2020. cap. VII, p. 109-125.

Escola Nacional de Administração Pública – ENAP. Governança de dados: gestão inteligente de dados. Brasília, 2019.

TASSO, Fernando Antonio. Do Tratamento de Dados Pessoais pelo Poder Público. In: MALDONADO, Viviane Nóbrega; OPICE BLUM, Renato (coord.). LGPD: Lei Geral de Proteção de Dados Comentada. 1. ed. São Paulo: Thomson Reuters Brasil, 2019. cap. IV, p. 245-285.

BIOGRAFIA

André Castro Carvalho

Bacharel (2007), Mestre (2010) e Doutor (2013) pela Faculdade de Direito da Universidade de São Paulo, tendo sua tese de doutorado recebido o Prêmio CAPES de Tese 2014 na área do Direito. Realizou estudos de pós-doutorado como visiting researcher no Massachusetts Institute of Technology - MIT (2016), sendo bolsista do Programa Estratégico - DRI (Estágio Pós-Doutoral) da CAPES, e concluiu o Programa de Pós-Doutorado realizado no Departamento de Direito Econômico, Financeiro e Tributário da Faculdade de Direito da Universidade de São Paulo (2018). Foi bacharelando (incompleto) em Economia pela Faculdade de Economia, Administração e Contabilidade - FEA da Universidade de São Paulo, tendo iniciado os estudos em 2011 e interrompido em 2012. Foi visiting researcher na Karl Franzens Universität Graz, na Áustria (2013), pelo Coimbra Group Scholarship Programme for Young Professors and Researchers from Latin America, e visiting scholar and professor na Nankai University (Tianjin) e JiLin University (Changchun), ambas na China (2012-2013), durante o período de doutorado. Possui certificação em treinamento corporativo em AML/CTF para uma instituição financeira emitido pela International Compliance Association - ICA em conjunto com a Manchester Business School (2014-2015), e é certificado em AML pela ACAMS (2019). É professor na pós-graduação no Ibmec-SP; professor regular na educação executiva em Compliance e no curso de LL.M do Insper; professor do MBA ESG/Exame e do MBA em Data Science da Trevisan Escola de Negócios. Também atua (ou atuou) como professor convidado em outros programas de extensão e de pós-graduação de diversas instituições de ensino, como PUC-SP, FIA, FIPE, FEA-USP, FD-RP, UFSCar, Unifor, EPM, ESA-DF, ABBC Educacional, Instituto Brasileiro de Ciências Bancárias - INFI e Associação Brasileira de Câmbio (ABRACAM). Foi professor de graduação de Direito Administrativo da Faculdade de Direito de São Bernardo do Campo (2011-2013), de Direito Econômico da Universidade Ibirapuera (2014) e de Direito Financeiro da Faculdade Autônoma de Direito - FADISP (2010).

Rua Fernandes Moreira, 507, Chácara Santo Antônio, São Paulo | @fundacaopodemos | fundacaopodemos.org.br