SoftHouse INFORMÁTICA

Gestão Pública

LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

LGPD

UMA AMEAÇA AO GESTOR PÚBLICO

A APLICAÇÃO DA LGPD PARA O SETOR PÚBLICO

A Lei nº 13.709/18, mais conhecida como Lei Geral de Proteção de Dados, alterou significativamente o ambiente de segurança da informação na esfera da Administração Pública, em todos os entes federativos. Fato é que, a partir desta nova legislação, cada agente público passou a ser peça fundamental na criação de um ambiente adequado de proteção de dados pessoais no país.

Neste sentido, é preciso que todos os órgãos públicos, de cada ente federativo, se adequem aos fundamentos e princípios elencados pela LGPD, o que não é tarefa simples, vez que envolve o governo que é responsável diretamente por uma infinidade de dados pessoais dos cidadãos.

NÃO ATENDER A LGPD CONSTITUI EM CRIME DE RESPONSABILIDADE, ALÉM DE INFRAÇÃO POLÍTICO-ADMINISTRATIVA, DE ACORDO COM O DECRETO-LEI Nº 201/67.

O QUE É A LEI?

Muito noticiada nos veículos de comunicação, sobretudo nos últimos dias, a LGPD, de uma maneira bem resumida e objetiva, tem como principal missão garantir transparência na gestão de dados pessoais, regulamentando todas as condições pelas quais os mesmos devem ser tratados.

Vejamos o que preceitua o caput do art. 1º da Lei 13.709/2018:

Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Vale reforçar que esta nova legislação também garante aos cidadãos diversos direitos, dentre os quais o acesso aos seus dados pessoais, a retificação de dados incorretos e até mesmo a exclusão desde, caso seja possível. Entretanto, no âmbito da Administração Pública, estes direitos devem ser devidamente harmonizados com os ditames da Lei de Acesso à Informação – LAI, a fim de se evitar eventuais problemas judiciais.

Dado um contexto em que ocorrem, de maneira cotidiana, grandes vazamentos de dados pessoais que afetam milhões de indivíduos, não é em vão que a LGPD dispôs um Capítulo inteiro sobre as regras para o tratamento de dados pela Administração Pública. Inclusive, recentemente, houve um vazamento de grandes proporções que ainda está sendo investigado, em que foram expostos dados pessoais de mais de 223 milhões de brasileiros.

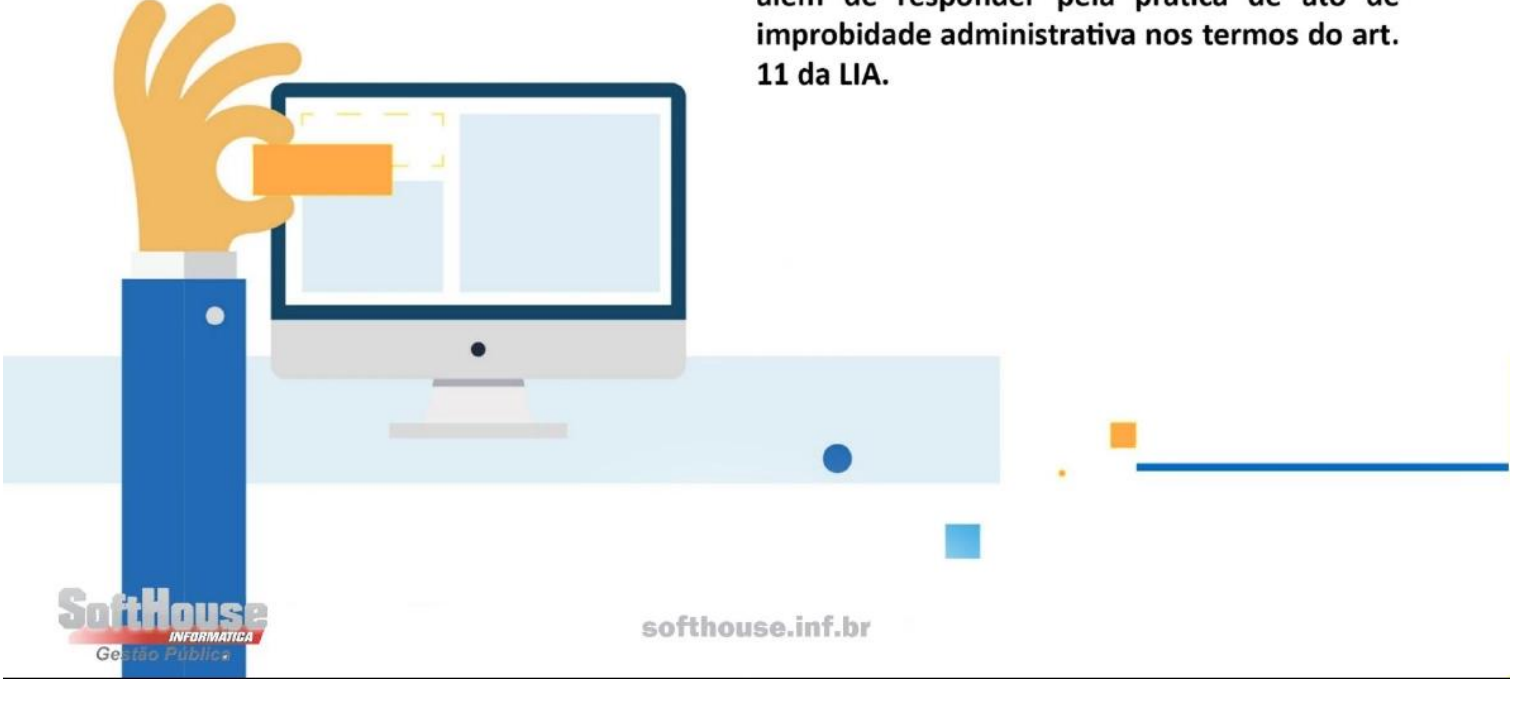
Neste sentido, é interessante verificar o art. 52 da LGPD, que regula de forma específica as sanções que poderão ser aplicadas pela Autoridade Nacional de Proteção de Dados Pessoais (ANPD). A norma é expressa, em seu §3º do art. 52, no sentido de que estas sanções poderão ser aplicadas às entidades e aos órgãos públicos, sem prejuízo do disposto na Lei nº 8.112/90, na Lei nº 8.429/92, e na Lei nº 12.527/11.

Ou seja, há referência expressa ao Estatuto do Servidor Público Federal, à Lei de Acesso à Informação (LAI) e à Lei de Improbidade Administrativa (LIA), sendo certo de que a responsabilidade pela violação aos ditames da LGPD ecoa para além das suas previsões sancionatórias específicas.

Vale lembrar que os atos de improbidade administrativa são divididos em atos que gerem enriquecimento ilícito ao agente ou a terceiro a ele relacionado (art. 9º da LIA), atos que gerem prejuízo ao erário (art. 10 da LIA) e atos que atentarem contra os princípios da Administração Pública (art. 11 da LIA).

Para ilustrar melhor as situações que podem gerar este tipo de problema, vejamos o exemplo de um servidor público da Secretaria de Saúde de um pequeno município que, buscando atingir a pessoa com a qual tenha criado inimizade no último pleito eleitoral ocorrido na cidade, torne público um dado pessoal sensível a ela pertencente, objetivando atingir a sua honra perante os cidadãos daquela região.

Deste modo, o servidor público age em violação clara e manifesta à Lei Geral de Proteção de Dados, gerando à Prefeitura Municipal dever de responder perante a ANPD. Entretanto, perante a própria Prefeitura, este agente público deverá responder a um procedimento administrativo, além de responder pela prática de ato de improbidade administrativa nos termos do art. 11 da LIA.



Ainda, caso o vitimado pela conduta do servidor público ingresse em juízo contra a Prefeitura, obtendo êxito na demanda, a conduta do agente violador passará a causar um efetivo e concreto dano ao Erário municipal, podendo o servidor passar a ser enquadrado como infrator do artigo 10 da LIA.

Outrossim, partindo-se da mesma situação do exemplo disposto, pode-se imaginar que esse mesmo servidor público, apossado dos dados pessoais sensíveis armazenados nos sistemas da Secretaria, decida vendê-los para pessoa que, posteriormente, os utilizará para a aplicação de golpes criminosos. Haverá, pois, conduta prevista art. 9º da LIA, vez que ele receberia uma vantagem patrimonial indevida originada de uma violação da LGPD.

Tais exemplos demonstram a importância da realização de procedimentos de adequação à LGPD, a fim de evitar problemas jurídicos e fiscalizações. Entretanto, situação ainda mais complexa e que deve gerar ainda mais problemas aos gestores públicos se dá no compartilhamento de dados pessoais com entidades privadas, ocasiões estas em que o Poder Público deverá fazer especial atenção aos artigos 26 e 27 da LGPD.

Isto porque a legislação permite a transferência de dados pessoais a agentes privados apenas em situações específicas, o que pode gerar uma celeuma de problemas aos administradores públicos, que deverão realizar a adequação deste tipo de transferência com os agentes privados que contratarem.

Portanto, os gestores públicos devem estar atentos a estas especificidades contidas na LGPD, tendo em vista que negar a execução de lei federal, sem dar o motivo da recusa ou da impossibilidade, constitui, em tese, crime de responsabilidade tipificado pelo art. 1º, inciso XIV do Decreto-Lei nº 201/67. A omissão em praticar atos expressamente previstos em Lei também constitui infração político-administrativa prevista no art. 4º, inciso VII da mesma norma.

Além do controle ordinário realizado pelas corregedorias, tribunais de contas e pela Ministério Público, a legislação prevê também um controle estrito da ANPD sobre os órgãos da Administração Pública. Um exemplo disso é a obrigação de que os contratos e convênios que preveem a transferência de dados pessoais para agentes privados sejam necessariamente compartilhados com a Autoridade (art. 26, §2º da LGPD).

A ANPD poderá também solicitar todas as informações sobre o tratamento, enviar informes com as medidas cabíveis, e até mesmo solicitar a publicação do Relatório de Impacto à Proteção de Dados Pessoais (RIPD) pelo Poder Público.

Assim, para estarem adequados à legislação, os órgãos públicos terão que seguir os seguintes passos:

1. Diagnóstico: uma espécie de raio-x inicial do órgão público, em que será tirada uma "fotografia" da situação atual no que tange o compliance com a LGPD para a elaboração de uma matriz de risco e de um plano de ação;

2. Mapeamento de processos e de dados: identificação e validação de todos os processos realizados e dados tratados pelo órgão público, a fim de identificar possíveis riscos no que tange o compliance com a LGPD, além de contemplar todo o ciclo de vida de todos os dados pessoais utilizados.

3. Adequação de contratos administrativos: elaboração e avaliação de contratos, convênios e outros instrumentos similares, prevendo cláusulas relacionadas com a LGPD, principalmente no que tange à transferência de dados pessoais a agentes privados.

4. Adequação da base legal de todos os dados pessoais: cada dado pessoal tratado pela Administração Pública deve necessitar de respaldo legal em uma das bases de tratamento elencadas pela LGPD.

5. Políticas: devem ser elaboradas e implementadas políticas internas da Administração Pública relativas à proteção de dados pessoais, através da edição de circulares, ofícios ou outros documentos internos.

6. Treinamentos: a equipe de servidores públicos e demais funcionários devem ser devidamente treinados sobre a LGPD e seus impactos no cotidiano do órgão público.

7. Relatório de Impacto à Proteção de Dados Pessoais: deve ser elaborado este relatório previsto em lei, o qual descreve como é realizada a gestão de riscos pelo órgão público no que diz respeito à LGPD.

8. Nomeação de um Encarregado pela Proteção de Dados Pessoais (DPO): deve ser nomeado um DPO, conforme o disposto no art. 41 da LGPD.

Ainda, há de se considerar a contratação de uma consultoria especializada no assunto para auxiliar o gestor público a tomar as melhores decisões sobre as medidas de adequação à LGPD no órgão público.

Sugere-se também que sejam realizados debates para a criação de políticas públicas que digam respeito à privacidade e à proteção de dados pessoais naquela esfera federativa, discutindo-se de forma mais geral iniciativas que integrem governo digital, privacidade e transparência da Administração Pública.

SoftHouse
INFORMÁTICA
Gestão Pública

E-MAIL: LGPD@SOFTHOUSE.INF.BR
SITE: SOFTHOUSE.INF.BR