LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD) E SETOR PÚBLICO

Um guia da Lei 13.709/2018, voltado para os órgãos e entidades públicas

ITS

Sumário

Apresentação

Muito se tem falado sobre a nova Lei Geral de Proteção de Dados Pessoais (LGPD), Lei 13.709/18, na perspectiva empresarial privada. Contudo, um de seus pontos mais relevantes é sua aplicação às práticas de tratamento de dados no âmbito do setor público. Primeiro porque o setor público, em seus diversos poderes (Executivo, Legislativo e Judiciário) e entes federativos (União, Estados, Distrito Federal e Municípios), valem-se do tratamento de dados pessoais dos cidadãos, não apenas para a elaboração e execução de políticas públicas, mas também para o oferecimento dos mais diversos serviços. O uso da tecnologia da informação e das técnicas de tratamento de dados tem sido cada vez mais explorado pela administração pública como importante instrumento para a gestão pública, sendo importantes exemplos os programas de Governo Eletrônico (eGOV) – iniciado em 2000 – e as experiências com as chamadas cidades inteligentes. Esse motivo, por si só, já justificaria uma atenção especial para o tratamento de dados pessoais na perspectiva do setor público, mas a relevância não para por aí.

A transparência dos dados em mãos do Poder Público, por sua vez, é princípio constitucional que foi regulamentado no Brasil pela LAI - Lei de Acesso à Informação (Lei nº 12.527 de 2011) e tem um dos seus limites na vedação ao fornecimento de dados pessoais pelo Poder Público. A composição entre os princípios da proteção da privacidade (e dos dados pessoais) e da transparência é tema que perpassa a regulamentação referente aos dois assuntos, que são, portanto, interligados e com delimitações que são objeto de debate.

Tal delimitação se afigura como necessária em diversos sistemas jurídicos. Na União Europeia, por exemplo, o Grupo de Trabalho do Artigo 29 (WP29), em seu parecer sobre os dados abertos e a reutilização de informações do setor público, destacou que o objetivo de se assegurar acesso à informação gerida por órgãos públicos é garantir transparência e controle sobre esses mesmos órgãos. Ou seja, antes de qualquer outra coisa, "os objetivos primários de direitos de acesso à informação têm a ver com a salvaguarda da transparência dos agentes públicos,

com o reforço dos controles democráticos", mas essa transparência tem que ser efetivada em consonância com os direitos fundamentais de privacidade e proteção de dados, e é justamente esse objetivo por trás do disposto no Artigo 31 da LAI, que visa a garantir esse equilibro de interesses, como analisaremos neste documento.

Considerando que no Brasil foi recentemente aprovada a Lei nº 13.709/18 (LGPD), que tem como fim precípuo assegurar a proteção de dados pessoais das pessoais naturais, e que tanto a proteção da privacidade quanto a transparência são direitos fundamentais previstos constitucionalmente, cabe, portanto, ao gestor público a tarefa de verificar de que forma deve-se orientar a interpretação dos princípios em questão de forma a proteger o cidadão na integralidade do projeto constitucional.

Destaque-se que a LGPD, dedicou todo um capítulo (IV) ao tratamento de dados pessoais pelo Poder Público, e foi exatamente neste capítulo que buscou estabelecer um equilíbrio entre acesso à informação nas mãos da administração pública e a proteção dos dados pessoais dos cidadãos, fazendo expressas menções à LAI.

O presente documento visa a contribuir com essa difícil tarefa do gestor público, através da apresentação de algumas linhas interpretativas sobre os dispositivos LGPD na perspectiva da aplicação pelo setor público. Existem várias regras criadas especificamente para o setor, como as relativas a compartilhamento de dados pessoais, transparência e bases autorizativas dos tratamentos de dados pessoais exclusivas para órgãos e entidades públicas. Além disso, algumas peculiaridades, como a previsão de diferentes sanções a depender do regime concorrencial ou não da entidade pública, fato de relevante importância para empresas públicas e sociedades de economia mista, que ora atuam como entidades privadas, ora como gestores ou executores de políticas públicas.

Todas essas questões serão abordadas com mais clareza ao longo do guia, a fim de possibilitar a real adaptação à LGPD e promover mais conhecimento sobre o tema. Tivemos o cuidado, também, de apresentar alguns exemplos práticos que

as novas regras impactariam, assim como listamos, ao final, algumas reações de órgãos e entidades públicas à aprovação da LGPD e à necessidade de adequação a este novo marco normativo.

A conformidade à LGPD vai depender de uma mudança cultural, e essa mudança deve vir logo. A Administração Pública, em suas mais diversas esferas, tem todos os meios para servir de exemplo.

Este documento não tem o objetivo de esgotar o tema ou de substituir a necessária análise que os distintos órgãos e entidades públicas deverão realizar com relação aos tratamentos de dados pessoais que conduzem e às distintas bases de dados sob sua gestão, mas pretende servir como um ponto de partida para esse exercício e um instrumento de conscientização quanto à necessidade de mudança, não apenas cultural, mas efetivamente de gestão e governança dos dados pessoais.

Esperamos que lhes seja útil!

INSTITUTO DE TECNOLOGIA E SOCIEDADE - ITS

A LGPD (Lei Geral de Proteção de Dados Pessoais)

Lei Federal n. 13.709/2018

A crescente utilização de dados pessoais e a sua importância para os mais variados aspectos de nossas vidas refletem, hoje, em um aumento da atividade normativa destinada a especificar qual estatuto jurídico deve seguir o tratamento desses dados. Não à toa, mais de 100 (cem) países ao redor do mundo já adotaram uma lei geral para regular o tratamento de dados pessoais em diferentes setores.

Uma lei geral de proteção de dados pode ser definida, em termos gerais, como um marco regulatório que estabelece direitos e garantias para o cidadão em relação aos seus dados pessoais, independente de quem ou de que forma estes sejam tratados.

A ideia de "proteção" visa a assegurar que o cidadão tenha a seu dispor meios para exercer efetivo controle sobre seus dados e, também, que todo o ecossistema em torno do tratamento de dados pessoais tenha contrapesos e incentivos para que danos ao cidadãos sejam evitados. Isto sem, contudo, impedir a inovação a partir do tratamento de tais dados, elemento fundamental da sociedade da informação.

A Lei nº 13.709/18, que é a Lei Geral de Proteção de Dados do Brasil, ou, simplesmente, "LGPD", tem exatamente esse escopo: aplica-se aos setores público e privado e tenta estabelecer um equilíbrio entre a proteção dos dados dos cidadãos e, no caso do setor público, a utilização desses dados para a elaboração e execução de políticas públicas e a correta prestação de serviços públicos.

Por fim, vale ressaltar que a LGPD foi publicada em 14 de agosto de 2018 e entra em vigor em 16 de agosto de 2020. Relevante nesse contexto é ainda a Medida Provisória 869/2018 ("MP"), ainda não convertida em lei e em discussão no Congresso Nacional. No âmbito da MP, algumas mudanças foram propostas[1], de forma que alterações podem acabar ocorrendo na Lei.

A quem a LGPD se aplica no setor público?

(Artigo 3º)

_Qualquer órgão ou entidade pública
_Empresas públicas e sociedades de economia mista

O que está de fora?

(Artigo 4º)

_Casos de tratamentos de dados realizados para:
fins exclusivamente: jornalísticos e artísticos; acadêmicos;
fins exclusivos de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais.

_Casos de tratamentos de dados provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado à LGPD.

[1] Para acompanhar a tramitação da MP, ver <https://www.congressonacional.leg.br/materias/medidas-provisorias/-/mpv/135062> e <https://legis.senado.leg.br/comissoes/comissao;jsessionid=EE7BD8446F47748F1400625D871C856F?0&codcol=2238>. Acesso em 03 de maio de 2019.

Caso de tratamentos de dados para fins exclusivos de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais

Apesar de não estarem dentro do escopo da LGPD e, portanto, não sujeitos às disposições sobre proteção de dados por ela trazidas, a própria LGPD estabelece algumas limitações ao tratamento de dados para essas finalidades, todas elas contidas nos parágrafos do seu Artigo 4º, que são:

_*Esses tratamentos de dados serão regidos por legislação específica, que deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular previstos nesta Lei;*

_*Só será admitido o tratamento de dados para tais finalidade por pessoa jurídica de direito privado em procedimentos sob a tutela de pessoa jurídica de direito público, sendo certo que os dados pessoais constantes de bancos de dados constituídos para tais finalidades não poderão ser tratados em sua totalidade por pessoas jurídicas de direito privado, exceção feita às controladas pelo Poder Público.*

Principais Definições

(Artigo 5º)

/Titular

É a pessoa natural a quem se referem os dados pessoais que são objeto de tratamento. Titular será o contribuinte, servidor ou empregado público, gestor público, pessoa física com a qual o órgão ou entidade pública possui alguma relação contratual.

/Controlador

Pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais. No setor público será o órgão público, entidade pública, empresa pública ou sociedade de economia mista que toma as decisões a respeito do tratamento de dados pessoais. Por exemplo, a Receita Federal, em relação às bases de dados que gere. O órgão público que mantém um banco de dados de seus servidores ou empregados públicos também se enquadraria nesta definição.

/Operador

Pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador. Por exemplo, o SERPRO (Serviço Federal de Processamento de Dados) ou a DATAPREV (Empresa de Tecnologia e Informações da Previdência Social) atuam como operadores quando processam dados pessoais em nome de outros órgãos ou entidades públicas.

/Encarregado

Pessoa indicada pelo controlador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados.

A Autoridade Nacional poderá estabelecer normas complementares sobre a definição e as atribuições do encarregado, inclusive hipóteses de dispensa da necessidade de sua indicação, conforme a natureza e o porte da entidade ou o volume de operações de tratamento de dados.

/Uso compartilhado de dados

Comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados.

/Órgãos de pesquisa

Órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no País, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico. Universidades Públicas e entidades de pesquisa pública, como a Fundação Oswaldo Cruz, se enquadram nesta definição.

Princípios da LGPD

(Artigo 6º)

A LGPD estabeleceu diferentes princípios norteadores do tratamento de dados pessoais. Esses princípios reforçam o fato de que a nova lei busca modificar completamente a cultura e a tutela jurídica de dados pessoais na era da informação.

/Livre Acesso e Transparência
Os titulares podem consultar gratuita e facilmente seus dados.

/Finalidade
O tratamento dos dados devem ter propósitos legítimos, específicos, explícitos e informados.

/Adequação
O tratamento dos dados deve ser compatível com as finalidades.

/Necessidade
Apenas os dados mínimos necessários à atividade devem ser tratados. Eles devem ser pertinentes, proporcionais e não excessivos.

/Qualidade de dados
Dados devem ser exatos, claros e adequados, de acordo com a finalidade.

/Segurança e Prevenção
Devem ser utilizadas medidas técnicas e administrativas para prevenir acidentes (como vazamentos de dados ou invasão por hackers).

/Responsabilização e Prestação de Contas
A efetividade dessas medidas técnicas e administrativas deve ser demonstrada.

/Não Discriminação
É vedado o tratamento de dados para fins discriminatórios ilícitos ou abusivos.

Afinal, o que são dados?

A LGPD traz três categorias e diferentes níveis de proteção.

/Dado pessoal

A LGPD classifica como dado pessoal qualquer informação relacionada a pessoa natural identificada ou identificável.

Atenção! Pessoa natural não é apenas o contribuinte, mas também o servidor e o empregado público, pessoas físicas com as quais a administração pública se relaciona, e até mesmo os gestores públicos e demais representantes do povo com mandato eletivo.

Isso significa que um grande número de identificadores constituem o dado pessoal, como o nome, o CPF, RG, informações sobre localização e assinaturas online. Em resumo, praticamente toda informação coletada sobre uma pessoa será um dado pessoal.

/Dado pessoal sensível

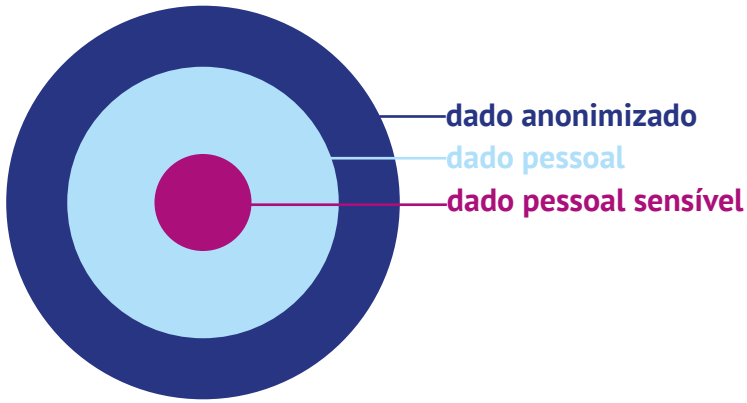
A LGPD definiu como dado pessoal sensível aquele dado pessoal "sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico" de uma pessoa natural.

Dados relacionados a políticas direcionadas a minorias, por exemplo a LGBTS, seguramente envolverão o tratamento de dados sensíveis. Na mesma linha, os sistemas de identificação biométrica, como aquele adotado pelo TSE (Tribunal Superior Eleitoral) para fins de votação eletrônica. O tratamento desses dados atrai um regime de proteção ainda mais restritivo.

/Dado anonimizado

Quando existe um dado que não é capaz de identificar o seu titular, utilizando os meios técnicos razoáveis e disponíveis na ocasião do seu tratamento, ele é chamado de dado anonimizado.

O dado anonimizado não será considerado dado pessoal para os fins da LGPD, salvo quando o processo de anonimização ao qual foi submetido for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido.



Quais os requisitos para que a Administração Pública possa tratar os dados pessoais (não sensíveis)?

(Artigo 7º)

_Mediante o consentimento do titular

O consentimento é uma manifestação livre, informada e inequívoca que autoriza o tratamento de dados pessoais para uma finalidade determinada. Autorizações genéricas serão nulas. Não é admitido um consentimento implícito. Esse consentimento, diferente das demais bases legais autorizativas do tratamento de dados pessoais, pode ser revogado a qualquer momento.

_Ou quando estiver presente alguma das seguintes situações:

> Cumprimento de obrigação legal ou regulatória pelo controlador.

> 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.

> Para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais. Nessa hipótese se enquadra, por exemplo, a pesquisa realizada por universidade públicas e, também, por institutos de pesquisa públicos, como a Fundação Oswaldo Cruz.

> Quando é necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados. É o caso, por exemplo, de contratos celebrados pela administração pública com fornecedores de produtos ou serviços, assim como concessões de serviços públicos e de uso de bens públicos, contratos de parcerias público-privadas e outros instrumentos contratuais da Administração Pública.

> Para o exercício regular de direitos em processo judicial, administrativo ou arbitral. Essa hipótese se aplicaria, por exemplo, ao tratamento de dados pessoais de servidores ou empregados públicos para fins de defesa dos interesses da administração pública em processos judiciais ou mesmo administrativos, o mesmo valendo para o tratamento de dados pessoais de contribuintes nas mesmas hipóteses.

> Para a proteção da vida ou da incolumidade física do titular ou de terceiro. O tratamento de dados pessoais no âmbito da atuação da Defesa Civil, com vistas a proteger a vida e a incolumidade física do titular ou de terceiros se enquadraria nessa hipótese.

> Para a tutela da saúde, em procedimento a ser realizado por profissionais da área da saúde ou por entidades sanitárias. Hospitais públicos e demais entidades sanitárias públicas estão autorizadas a tratar dados dos respectivos pacientes, sem seu consentimento, para fins de tutela da saúde.

> Quando é necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

> Para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

E os sensíveis?

(Artigo 11)

_Mediante o consentimento do titular

O consentimento é uma manifestação livre, informada e inequívoca que autoriza o tratamento de dados pessoais para uma finalidade determinada. Autorizações genéricas serão nulas. Não é admitido um consentimento implícito. Esse consentimento, diferente das demais bases legais autorizativas do tratamento de dados pessoais, pode ser revogado a qualquer momento. O consentimento para o tratamento de dados sensíveis precisa, ainda, ser dado de forma específica e destacada, para finalidades determinadas.

_Sem o consentimento do titular, nas hipóteses em que for indispensável para:

> Cumprimento de obrigação legal ou regulatória pelo controlador.

> Tratamento compartilhado de dados necessários à execução, pela Administração Pública, de políticas públicas previstas em leis e regulamentos. Percebe-se aqui uma diferença se comparadas às hipóteses de tratamento de dados pessoais não sensíveis, vez que foram excluídos os casos de políticas públicas respaldadas em contratos, convênios ou instrumentos congêneres.

> Para realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais. Nessa hipótese se enquadra, por exemplo, a pesquisa realizada por universidade públicas e, também, por institutos de pesquisa públicos, como a Fundação Oswaldo Cruz.

> O exercício regular de direitos em processo judicial, administrativo ou arbitral. Essa hipótese se aplicaria, por exemplo, ao tratamento de dados pessoais de servidores ou empregados públicos para fins de defesa dos interesses da administração pública em processos judiciais ou mesmo administrativos, o mes-

mo valendo para o tratamento de dados pessoais de contribuintes nas mesmas hipóteses.

> Para a proteção da vida ou da incolumidade física do titular ou de terceiro. O tratamento de dados pessoais sensíveis no âmbito da atuação da Defesa Civil, com vistas a proteger a vida e a incolumidade física do titular ou de terceiros se enquadraria nessa hipótese.

> Para a tutela da saúde, em procedimento a ser realizado por profissionais da área da saúde ou por entidades sanitárias. Assim, hospitais públicos e demais entidades sanitárias públicas estão autorizadas a tratar dados pessoais sensíveis dos respectivos pacientes, sem seu consentimento, para fins de tutela da saúde.

> Garantia da prevenção à fraude e da segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no Artigo 9º da LGPD e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais. Um exemplo que se enquadra perfeitamente nessa hipótese é o sistema de identificação biométrica implementado pelo TSE (Tribunal Superior Eleitoral) para a votação na urna eletrônica.

DISPENSA DE CONSENTIMENTO E PUBLICIDADE DO TRATAMENTO DE DADOS

No caso de tratamento de dados para cumprimento de obrigação legal ou regulatória pelo controlador ou para tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos por órgãos e entidades públicas, será dada publicidade à referida dispensa de consentimento, nos termos do inciso I do caput do Artigo 23 da LGPD.

Tratamento de dados pessoais por órgãos de pesquisa

(Artigo 13)

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 pseudoanonimização dos dados, bem como considerem os devidos padrões éticos relacionados a estudos e pesquisas.

A LGPD também trouxe outras regras protetivas para a hipótese:

> Divulgação dos resultados ou excertos do estudo ou pesquisa não poderá revelar dados pessoais.

> O órgão de pesquisa será responsável pela segurança da informação e não poderá – em hipótese alguma – transferir os dados a terceiros.

> O acesso aos dados pessoais pelos órgãos de pesquisa para fins de realização de estudos em saúde pública será objeto de regulamentação por parte da autoridade nacional e das autoridades da área de saúde e sanitárias, no âmbito de suas competências.

Direitos dos titulares dos dados

(Artigo 18)

_O titular tem o direito de:

> Confirmar a existência de tratamento (Informação);
> Acessar os dados;
> Correção de seus dados (incompletos, inexatos ou desatualizados);
> Anonimização, bloqueio ou eliminação de dados (desnecessários, excessivos ou em desconformidade com a Lei);
> Portabilidade dos dados;
> Eliminação dos dados pessoais tratados com o consentimento do titular (exceto Artigo 16);
> Informação sobre entidades com as quais os dados foram compartilhados;
> Informação sobre a possibilidade de não fornecer consentimento e consequências;
> Revogação do consentimento.

Registro de Processamento de Dados Pessoais

(Artigo 37)

Os órgãos e entidades públicas, empresas públicas e sociedades de economia mista que se enquadrem nas definições de controlador ou operador deverão criar e manter um registro das operações de tratamento de dados que realizarem.

Encarregado pelo Tratamento de Dados Pessoais

(Artigo 41)

O órgão ou entidade pública, empresa pública ou sociedade de economia mista, quando atuar na qualidade de controlador, deverá indicar encarregado pelo tratamento de dados pessoais.

A identidade e as informações de contato do encarregado deverão ser divulgadas publicamente, de forma clara e objetiva, preferencialmente no sítio eletrônico do controlador.

Atividades do encarregado

> Aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;

> Receber comunicações da autoridade nacional e adotar providências;

> Orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais;

> Executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.

A Autoridade Nacional poderá estabelecer normas complementares sobre a definição e as atribuições do encarregado, inclusive hipóteses de dispensa da necessidade de sua indicação, conforme a natureza e o porte da entidade ou o volume de operações de tratamento de dados.

Porém, até que sejam definidas tais regras pela Autoridade, todos os órgãos públicos, entidades públicas, empresas públicas e sociedades de economia mista que atuarem como controladores terão que nomear um encarregado pelo tratamento de dados pessoais.

Notificações de Incidentes de Segurança

(Artigo 48)

O que é um incidente de segurança?

A LGPD não define incidente de segurança. O CERT.br (Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil), mantido pelo Comitê Gestor da Internet no Brasil (CGI.br), grupo responsável por receber, analisar e responder a incidentes de segurança em computadores, envolvendo redes conectadas à Internet brasileira, define incidente de segurança como "qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança de sistemas de computação ou de redes de computadores".

Pelo que consta do caput do Artigo 46 da LGPD, apenas os incidentes de segurança que importarem em "acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito" deverão ser notificados.

Comunicação sobre a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares

Esse é um tema de fundamental importância para o setor público, já que diversos órgãos e entidades públicas, assim como empresas públicas e sociedades de economia mista, em todas as esferas de governo e da federação, tratam dados pessoais tanto de contribuintes como de servidores e empregados públicos, sendo que muitos desses dados se enquadram na definição de dado pessoal sensível. Portanto, o estabelecimento de uma política clara sobre o que fazer quando da ocorrência de incidentes de segurança é de vital importância.

Basicamente, o incidente deve ser comunicado à Autoridade Nacional e ao titular dos dados, pelo órgão público, entidade pública, empresa pública ou sociedade de economia mista que desempenhar o papel de controlador, sempre que o incidente de segurança "possa acarretar risco ou dano relevante aos titulares".

Prazo razoável

A ser definido pela Autoridade Nacional. Na legislação europeia que trata do mesmo tema ("General Data Protection Regulation – GDPR") o prazo definido foi de 72 horas.

Conteúdo

O conteúdo da notificação deve abarcar:

> Descrição da natureza dos dados pessoais afetados;
> Informações sobre os titulares envolvidos;
> Indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados;
> Riscos relacionados ao incidente;
> Motivos da demora, no caso de a comunicação não ter sido imediata; e
> Medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.

Outras providências

A Autoridade Nacional (dependendo da gravidade do incidente) pode determinar a adoção de outras providências, tais como:
i) ampla divulgação do fato em meios de comunicação
ii) medidas para reverter ou mitigar os efeitos do incidente.

Serviços notariais e de registro

(Artigo 23, §§ 4º e 5º)

Os serviços notariais e de registro exercidos em caráter privado, por delegação do Poder Público, terão o mesmo tratamento dispensado às pessoas jurídicas de direito público.

Os órgãos notariais e de registro devem fornecer acesso aos dados por meio eletrônico para a Administração Pública.

Estruturação dos dados

(Artigo 25)

Os dados deverão ser mantidos em formato interoperável e estruturado para o uso compartilhado, com vistas à execução de políticas públicas, à prestação de serviços públicos, à descentralização da atividade pública e à disseminação e ao acesso das informações pelo público em geral.

Regras específicas de tratamento de dados para o setor público

(Artigo 23)

Finalidade e interesse público

O tratamento de dados pessoais pelas pessoas jurídicas de direito público referidas no parágrafo único do Artigo 1º da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação), deverá ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público, desde que:

> Sejam informadas as hipóteses em que, no exercício de suas competências, realizam o tratamento de dados pessoais, fornecendo informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos;

> Seja indicado um encarregado quando realizarem operações de tratamento de dados pessoais.

Prazos

Os prazos e procedimentos para exercício dos direitos do titular perante o Poder Público observarão o disposto em legislação específica, em especial as disposições constantes da Lei nº 9.507, de 12 de novembro de 1997 (Lei do Habeas Data), da Lei nº 9.784, de 29 de janeiro de 1999 (Lei Geral do Processo Administrativo), e da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação).

Publicidade

A autoridade nacional poderá dispor sobre as formas de publicidade das operações de tratamento pelo Poder Público.

O disposto na LGPD não dispensa as pessoas jurídicas de instituir as autoridades de que trata a Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação).

Empresas públicas e sociedades de economia mista

(Artigo 24)

O que devemos saber?

As empresas públicas e as sociedades de economia mista que atuam em regime de concorrência, sujeitas ao disposto no Artigo 173 da Constituição Federal, terão o mesmo tratamento dispensado às pessoas jurídicas de direito privado particulares.

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.

Por exemplo, um banco público no tratamento de dados pessoais de seus correntistas terá o mesmo tratamento de um banco privado. Porém, quando este banco público estiver operacionalizando políticas públicas e no âmbito da execução

delas, terá o mesmo tratamento dedicado pela LGPD aos órgãos e às entidades do Poder Público.

Será o caso da Caixa Econômica Federal em algumas situações. Quando ela atuar como um banco, tratando dados de seus correntistas para, por exemplo, oferecimento de um financiamento, ela deverá seguir as regras aplicáveis ao setor privado. Por outro lado, quando ela tratar dados pessoais no âmbito do FGTS, do Programa de Integração Social (PIS) ou do Seguro-Desemprego, ela deverá observar as regras aplicáveis ao setor público.

Compartilhamento de dados no âmbito da Administração Pública

(Artigo 26)

O uso compartilhado de dados pessoais pelo Poder Público deve:

> Atender a finalidades específicas de execução de políticas públicas e atribuição legal pelos órgãos e pelas entidades públicas;

> Respeitar os princípios de proteção de dados pessoais elencados no Artigo 6º da LGPD.

Uma hipótese de uso compartilhado de dados no âmbito da Administração Pública é aquela regulada pela Portaria da Receita Federal no Brasil nº 1.384, de 09 de setembro de 2016.

Transferência Internacional de Dados

(Artigo 33)

A LGPD estabeleceu hipóteses taxativas em que a transferência internacional de dados é permitida. Veja abaixo:

> Países + Organizações Internacionais com grau adequado de proteção (Artigo 33, I)

> Frente a cláusulas contratuais específicas, cláusulas-padrão, normas corporativas globais, selos, certificados e códigos de conduta (Artigo 33, II)

> Quando for necessária para a cooperação jurídica internacional entre órgãos públicos de inteligência, de investigação e de persecução, de acordo com os instrumentos de direito internacional (Artigo 33, III)

> Quando for necessária para a proteção da vida ou da incolumidade física do titular ou de terceiro (Artigo 33, IV)

> Quando a Autoridade Nacional autorizar (Artigo 33, V)

> Quando resultar em compromisso assumido em acordo de cooperação internacional (Artigo 33, VI)

> Consentimento específico e em destaque para a transferência de dados (Artigo 33, VII)

> Quando o titular tiver fornecido o seu consentimento específico e em destaque para a transferência, com informação prévia sobre o caráter internacional da operação, distinguindo claramente esta de outras finalidades (Artigo 33, VIII)

> Quando for necessária para o cumprimento de obrigação legal ou regulatória pelo controlador; para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados (Artigo 33, IX)

Órgãos públicos da Administração Direta e autarquias e fundações públicas de direito público.

O parágrafo único do Artigo 33 estabeleceu regra específica para as pessoas jurídicas de direito público dispostas no parágrafo único do Artigo 1º da Lei de Acesso à Informação (Lei 12.527/2008). Elas poderão, no âmbito de suas competências legais, e responsáveis, no âmbito de suas atividades, requerer à Autoridade Nacional a avaliação do nível de proteção a dados pessoais conferido por país ou organismo internacional.

Compartilhamento de dados na nuvem.

O simples uso de um serviço de armazenamento de dados em um servidor na nuvem pode ensejar uma transferência internacional de dados. Assim, é importante que haja uma revisão de todos os serviços informáticos utilizados, a fim de evitar uma transferência internacional de dados em desconformidade com o que prevê a LGPD, ensejando a aplicação de sanções por parte da Autoridade Nacional.

Transferência de dados a entidades privadas

(Artigo 26)

Regra geral

É vedada a transferência de dados pessoais para entidades privadas.

Exceções

> Execução descentralizada de atividade pública que exija a transferência, exclusivamente para esse fim específico e determinado, observado o disposto na LAI;

> Se for indicado um encarregado para as operações de tratamento de dados pessoais;

> Quando houver previsão legal ou a transferência for respaldada em contratos, convênios ou instrumentos congêneres (que deverão ser comunicados à autoridade nacional);

> Para a prevenção de fraudes e irregularidades, ou proteger e resguardar a segurança e a integridade do titular dos dados;

> Nos casos em que os dados forem acessíveis publicamente.

Comunicação e uso compartilhado de dados com entidades privadas

(Artigos 27 a 30)

Regra geral

A comunicação e uso compartilhado de dados com entidades privadas, por pessoas jurídicas de direito público, dependerá do consentimento do titular.

Exceções

> Hipóteses de dispensa de consentimento previstas na LGPD;

> Nos casos de uso compartilhado de dados;

> Exceções constantes do § 1º do Artigo 26 da LGPD (conforme item anterior).

Competências da Autoridade Nacional no tema

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

> Também poderá estabelecer normas complementares para as atividades de comunicação e de uso compartilhado de dados pessoais.

Responsabilidades

(Artigos 31, 42, 43)

Da Administração Pública

Quando houver infração à LGPD em decorrência do tratamento de dados pessoais por órgãos públicos, a Autoridade Nacional poderá enviar informe com medidas cabíveis para fazer cessar a violação.

A Autoridade Nacional 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.

Dos Agentes de Tratamento (Responsabilidade Civil)

O controlador ou o operador (inclusive os órgãos e entidades públicos, empresas públicas e sociedades de economia mista) – responde por dano em razão do exercício de atividade de tratamento de dados pessoais (em violação à legislação de proteção de dados pessoais, inclusive por não adoção de medidas técnicas de segurança).

O operador responde solidariamente pelos danos causados quando:
> Descumprir as obrigações da legislação de proteção de dados;
> Não tiver seguido as instruções lícitas do controlador.

Inversão do ônus da prova

A possibilidade existe em favor do titular e a critério do juiz, em redação similar ao Artigo 6º, VIII do Código de Defesa do Consumidor.

Excludentes de responsabilidade

Não realização do tratamento que é lhe atribuído;
Não existência de violação à legislação de proteção de dados;
Culpa exclusiva do titular dos dados ou de terceiro.

Tratamento de dados irregular

Ocorrerá quando a legislação não for observada ou quando não for fornecida a segurança esperada pelo titular. Nesse caso, há que se verificar o modo pelo qual é realizado, resultado e riscos que dele se esperam, técnicas de tratamento disponíveis à época.

Relações de consumo

(Artigos 45)

No caso de violação do direito do titular no âmbito das relações de consumo, serão aplicadas as normas sobre responsabilidade civil estabelecidas no Código de Defesa do Consumidor (CDC).

Essas regras são aplicáveis apenas às empresas públicas e sociedades de economia mista, quando atuam em regime de concorrência no âmbito de uma relação de consumo.

Boas práticas e governança

(Artigo 50)

Os controladores e operadores pelo tratamento de dados pessoais, no âmbito de suas competências, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais.

O desenvolvimento de uma política de governança de dados precedida de um mapeamento de dados realizados é uma medida recomendável a ser implementada pelo setor público.

Consequências por não agir de acordo com a lei

(Artigo 52)

O Artigo 52 da LGPD impôs sanções administrativas aplicáveis, pela Autoridade Nacional, aos agentes de tratamento de dados. No caso específico de entidades e órgãos públicos, são excluídas as possibilidades de multa simples e multa diária, nos termos do parágrafo 3º do Artigo 52. Entre os riscos, podemos destacar:

Advertência
Com indicação de prazo para adoção de medidas corretivas.

Publicização da infração
Apenas após confirmada a ocorrência.

Reputação
O impacto não são apenas sanções administrativas. Também pode afastar outras entidades que busquem parcerias pelo risco de serem impactados.

Bloqueio
Até a regularização da situação, os dados pessoais são bloqueados.

Eliminação
Confirmada a infração, os dados pessoais a ela relacionados serão eliminados.

Adaptação dos bancos de dados em funcionamento

(Artigo 63)

A Autoridade Nacional estabelecerá normas sobre a adequação progressiva de bancos de dados constituídos até a data de entrada em vigor desta Lei, consideradas a complexidade das operações de tratamento e a natureza dos dados. Independentemente do que (e até que) a Autoridade Nacional disponha sobre esse tema, é recomendado que o setor público já adote medidas para sua adequação à LGPD.

Recomendações

Veja o que fazer para adequar sua atividade à LGPD

> Compreender em qual medida a LGPD se aplica ao(s) tratamentos de dados que realiza;

> Identificar qual(is) base(s) legal(is) se aplica(m) ao(s) tratamento(s) de dados que realizam;

> Rever os processos internos de tratamentos de dados com vistas à adequação à LGPD;

> Revisar as políticas de privacidade (ou criá-las se não possuírem);

> Estabelecer uma política de segurança da informação com regras claras relacionadas a incidentes de segurança, especialmente no que toca ao cumprimento dos requisitos de notificação à ANPD;

> Treinar o pessoal envolvido no tratamento de dados pessoais;

> Nomear um Encarregado pelo Tratamento de Dados Pessoais;

> Criar e implementar o Registro das operações de tratamento de dados pessoais;

> Revisar contratos, convênios e outros instrumentos que impliquem no tratamento de dados pessoais, assim como eventuais contratos e outros instrumentos que regulem o relacionamento com eventuais operadores de tratamentos de dados pessoais em nome do controlador;

> Estabelecer uma política clara de governança dos dados pessoais dentro do órgão ou entidade pública.

Exemplos de iniciativas de órgãos e entidades públicos

Algumas entidades públicas já começaram a se preparar para se adequar à LGPD. Veja abaixo alguns exemplos.

Em âmbito federal

/SERPRO (Serviço Federal de Processamento de Dados)

Em setembro de 2018, a SERPRO (Serviço Federal de Processamento de Dados), empresa pública vinculada ao Ministério da Fazenda, divulgou "Declaração de conformidade com os princípios de proteção de dados pessoais". Confira trecho:

1.0 FINALIDADE

O Serviço Federal de Processamento de Dados – Serpro, empresa pública vinculada ao Ministério da Fazenda, considerando:
I. os fundamentos da Lei no 13.709, de 14 de agosto de 2018, que dispõe sobre a proteção de dados pessoais:
a) o respeito à privacidade,
b) a autodeterminação informativa,
c) a liberdade de expressão, de informação, de comunicação e de opinião,
d) a inviolabilidade da intimidade, da honra e da imagem,
e) o desenvolvimento econômico e tecnológico e a inovação,
f) a livre iniciativa, a livre concorrência e a defesa do consumidor, e
g) os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais;

4.0 PRINCÍPIOS DA PROTEÇÃO DE DADOS PESSOAIS
(Explica a conformidade a cada um dos princípios da LGPD)

5.0 CONFORMIDADE E GOVERNANÇA

5.1 Conformidade legal
O Serpro se declara:
I. em conformidade com a lei vigente e comprometido com a garantia de futura conformidade com o teor da Lei no 13.709, de 14 de agosto de 2018, quando de sua entrada em vigor; e
II. aderente aos princípios supracitados e estabelece como escopo prioritário atingir a referida conformidade o mais cedo possível em relação à entrada da Lei em vigor.

/Conselho Nacional de Justiça (CNJ)

Em 21 de outubro de 2018, o CNJ editou a Resolução Nº 269, instituindo regras sobre a gerência de dados pessoais de candidatos a cargos públicos, mediante concurso público, do Poder Judiciário. A Resolução considerou a LGPD e resolveu que:

Art. 1º Ficam instituídas regras para a gerência de dados pessoais de candidatos a cargos públicos, mediante concurso público, do Poder Judiciário.

Art. 2º Em todos os concursos públicos do Poder Judiciário, os tribunais divulgarão apenas o nome completo e o número de inscrição dos concorrentes à(s) vaga(s) pública(s).
§ 1º A relação dos candidatos deverá ser organizada de acordo com o tipo de concorrência do concurso.
§ 2º Os tribunais deverão utilizar a tecnologia no follow ou ferramenta similar para inibir a atuação de buscadores de informação nas páginas eletrônicas em que constarem dados pessoais dos candidatos.

Art. 3º Após a vigência do concurso, os dados pessoais publicados devem ser excluídos das páginas eletrônicas abertas ao público de competência dos tribunais.
§ 1º A exclusão poderá ser feita imediatamente após o encerramento do concurso, incluindo todas as suas fases e recursos, caso haja abertura de novo certame.
§ 2º Sem prejuízo do caput deste artigo, os tribunais poderão manter o registro de todo o andamento do concurso público em página eletrônica, por prazo no interesse da Administração.

Art. 4º O atendimento aos dispostos nos artigos precedentes não impede o acesso aos dados pessoais pelas entidades constitucional e legalmente autorizadas.

/Comissão de Valores Mobiliários (CVM)

A CVM publicou uma Minuta de alteração da Instrução CVM nº 505/2011 e convocou a Audiência Pública SDM 05/2018, ambas tratando sobre dados pessoais.

A minuta dispõe novos artigos relacionados a segurança das informações. O Artigo 5-A da Minuta traz o cadastro dos clientes e requisitos mínimos de auditoria para garantir que o rastreamento das inclusões, alterações e exclusões de dados sejam suficientemente identificáveis. O Artigo 35-E traz regras de tratamento e controle como aquelas exigidas pela LGPD.

/Tribunal Regional Eleitoral de Santa Catarina (TRESC)

O TRESC, em 18 de setembro de 2018, editou a Resolução TRESC n. 7.989/2018, dispondo sobre a Ouvidoria Regional Eleitoral de Santa Catarina. A Resolução menciona expressamente a necessidade de observância à LGPD. Veja abaixo trechos:

Art. 4º A Ouvidoria do Tribunal Regional Eleitoral de Santa Catarina tem por missão servir de canal de comunicação direta entre o cidadão e a Justiça Eleitoral catarinense, com vistas a receber manifestações do usuário, orientar, transmitir informações e colaborar no aprimoramento das atividades desenvolvidas pelo Tribunal.

Art. 5º A Ouvidoria poderá se organizar em forma de sistemas ou redes, com a finalidade de:
I – articular as atividades das ouvidorias públicas;
II – garantir o controle social dos usuários sobre a prestação de serviços públicos;
III – assegurar o acesso do usuário de serviços públicos aos instrumentos de participação na gestão e defesa dos direitos;
IV – promover a efetiva interlocução entre usuário de serviços públicos e os órgãos e entidades da administração pública.

Art. 6º Compete à Ouvidoria:
I – promover e atuar diretamente na defesa dos direitos dos usuários de serviços públicos, nos termos da Lei n. 13.460/2017;
II – receber, analisar, processar e responder as manifestações encaminhadas por usuários ou reencaminhadas por demais ouvidorias, órgãos ou entidades;
III – manter e garantir, a pedido, sempre que a circunstância exigir, o sigilo dos dados do usuário nas reclamações, denúncias, sugestões, elogios e solicitações de providências ou de informações, nos termos da Lei n. 13.709, de 14.08.2018

Art. 18. A Ouvidoria assegurará ao usuário a proteção de sua identidade e demais atributos de identificação, nos termos da Lei n. 13.709, de 14.08.2018.
Parágrafo único. A preservação da identidade do manifestante dar-se-á com a proteção do nome, endereço e demais dados de qualificação dos manifestantes que serão documentados separadamente, aos quais serão dispensados o tratamento previsto no caput.

Em âmbito estadual

/Estado de São Paulo – Secretaria da Educação do Estado de São Paulo

Em 09 de novembro de 2018, foi editada a Resolução SE 61, estabelecendo critérios e procedimentos para a divulgação de dados públicos e pessoais pela Secretaria da Educação. Da iniciativa voltada para essa atividade específica, destacamos os trechos:

Artigo 3º: São vedados a coleta, o armazenamento e o tratamento de dados e informações pessoais, especialmente as sensíveis, definidos no artigo 5º, I e II da Lei Federal 13.709, de 14-08-2018, salvo os absolutamente indispensáveis à execução dos deveres e atribuições da Secretaria da Educação.

Artigo 4º: As informações e os dados de caráter sensível serão coletados, transferidos ou disponibilizados, mediante autorização expressa dos seus titulares, educandos, pais ou responsáveis, salvo as hipóteses previstas no artigo 11 da Lei Federal 13.709, de 14-08-2018.

Em âmbito municipal

/Município do Rio de Janeiro – Controladoria Geral do Município

Em 03 de dezembro de 2018, a Controladoria Geral do Município (CGM) instituiu, através da Resolução "P" CGM nº 68, um grupo de Trabalho para estudar os impactos da LGPD e sugerir adequações necessárias frente à nova Lei. Confira-se:

Art. 1º Instituir Grupo de Trabalho para, no prazo de 120 dias, apresentar a Controladora-Geral:
I - levantamento dos impactos da Lei nº 13.709/2018 nos serviços prestados pela CGM Rio e nos documentos e produtos emitidos, incluindo aqueles referentes a resultados de trabalhos finalísticos;
II - proposta de adequações necessárias aos serviços, documentos e produtos, em virtude da Lei

/Município do Rio de Janeiro – Secretaria Municipal de Transportes

Em 28 de agosto de 2018, a Secretaria Municipal de Transportes da cidade do Rio de Janeiro (SMTR) editou a Resolução nº 3014/SMTR, estabelecendo o controle das gratuidades nos transportes públicos municipais por meio do método de identificação biométrica.

Apesar de se tratar de medida que gerou opiniões diversas sobre a necessidade de utilizar a biometria para tal conferência, e seus possíveis problemas de operacionalização, a Resolução faz menção expressa à LGPD. Abaixo, veja trechos da Resolução:

Art. 2º O controle das gratuidades e dos benefícios tarifários valer-se-á dos meios tecnologicamente adequados, custeados pelos concessionários, permissionários e autorizatários dos serviços de transporte público de passageiros, para garantir o seu exercício legitimo.

§ 2º É vedada a divulgação de qualquer forma dos dados biométricos pelas concessionárias, que respeitará os direitos fundamentais de liberdade e privacidade, a inviolabilidade da intimidade e o livre desenvolvimento da personalidade da pessoa natural, conforme a Lei Federal 13.709 de 14 de agosto de 2018.

ITS RIO

A missão do Instituto de Tecnologia e Sociedade (ITS) é assegurar que o Brasil e o Sul Global respondam de maneira criativa e apropriada às oportunidades fornecidas pela tecnologia na era digital, e que seus potenciais benefícios sejam amplamente compartilhados pela sociedade.

Por meio de pesquisa e de parcerias com outras instituições, o ITS Rio analisa as dimensões legais, sociais, econômicas e culturais da tecnologia e promove melhores práticas de regulação que protejam a privacidade, a liberdade de expressão e o acesso ao conhecimento. O instituto também oferece educação em formatos inovadores, treinamentos e oportunidades de desenvolvimento para indivíduos e instituições sobre as promessas e desafios da tecnologia. Por último, o ITS Rio objetiva fortalecer a voz do Brasil, da América Latina e do Sul Global em debates sobre tecnologias, Internet e regulação.

Encontre-nos nas mídias sociais

2019
itsrio.org
R. da Assembléia, 10, 40º andar, sala 4011 - Centro, RJ


ITS