FILIADA À FACESP ASSOCIAÇÃO COMERCIAL E EMPRESARIAL DE OSVALDO CRUZ

Lei Geral de Proteção de Dados - LGPD

FILIADA À FACESP
ASSOCIAÇÃO COMERCIAL E EMPRESARIAL DE OSVALDO CRUZ

LEI GERAL DE PROTEÇÃO DE DADOS – LGPD

Lei nº 13.709/18

No Brasil, em setembro de 2020 entrou em vigor a Lei Geral de Proteção de Dados (LGPD) que estabelece regras para uso, proteção e transparência de informações pessoais no país.

As ameaças à informação, brechas de segurança e vazamentos de dados são incidentes que ocorrem diariamente com empresas de todos os portes, podendo comprometer os dados pessoais de usuários. Além disso, caso isso se torne público, pode ainda impactar de forma negativa a reputação de uma companhia, tornando-a menos confiável e mostrando que aquela empresa não trata as informações de clientes, fornecedores e colaboradores com o devido cuidado. Além disso, a LGPD, como toda lei, traz consigo sanções e multas.

Neste trabalho, temos o objetivo de auxiliar as empresas para que conheçam o cenário no qual a LGPD foi inserida, como se adequar a nova lei e quais são os desafios para o seguimento corporativo em relação a essa nova realidade.

I - Introdução

Pensar em segurança digital, proteção de dados e privacidade passou a ser uma necessidade e uma tarefa diária, principalmente para as empresas.

Nunca se discutiu tanto a importância da proteção de dados e os cuidados com a privacidade, dois fatores que ao longo dos últimos anos se tornaram fundamentais para os processos corporativos em todo o mundo. O intuito deste documento é apresentar a LGPD de forma simples e objetiva, destacando aspectos básicos como seus princípios, atores, estruturas, impactos e,

principalmente, como as empresas podem compreender este novo processo e direcionar ações de conformidade com as novas determinações.

É importante saber que o processo de adequação das empresas não é responsabilidade apenas das equipes de Tecnologia da Informação (TI), mas também deve ser visto e tratado com todas as áreas que compõem a organização. Cada colaborador, independentemente de sua área, pode ter um papel fundamental nesse processo que se tornou necessário e urgente. A adequação exige maturidade por parte de todos os envolvidos a fim de evitar possíveis incidentes de segurança e consequências legais e de reputação.

É necessário que as empresas estejam preparadas e com seus processos voltados para a criação de canais, mecanismos e serviços seguros. Os consumidores estão cada vez mais cientes da responsabilidade que as empresas devem ter com a proteção de seus dados.

II - O que é a LGPD?

A Lei Geral de Proteção de Dados – LGPD, estabelece regras sobre coleta, armazenamento, tratamento e compartilhamento de dados pessoais, impondo mais proteção nos processos e aplicando penalidades para os casos de não cumprimento. A nova lei se aplica a qualquer pessoa, física ou jurídica (pública ou privada) que faça o tratamento de dados pessoais, destacando-se como um dos grandes marcos sobre a proteção e privacidade de dados no Brasil.

Logo, para entender a LGPD, também é fundamental compreender a interpretação da lei em relação a dados pessoais:

- Dados pessoais: são os dados que permitem a identificação direta ou indireta de uma pessoa, como RG, CPF, passaporte, carteira de habilitação, endereço, telefone, e-mail, IP e até mesmo cookies.

- Dados pessoais sensíveis: o artigo quinto da LGPD prevê que sejam considerados dados sensíveis todos aqueles que façam referência a "origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural".

Assim, a LGPD usa de direitos fundamentais de liberdade e de privacidade como parâmetro para as regras a respeito da coleta e armazenamento de dados pessoais, incluindo também o compartilhamento desse tipo de informação. Nesse contexto, existem princípios que norteiam o processo estabelecido para o tratamento de dados pessoais, de acordo com a LGPD. Logo, a empresa deve respeitar esses princípios para estar em conformidade com a lei, considerando o cuidado na forma de coleta e tratamento de dados pessoais de seus clientes. Listamos:

1. *Finalidade*: Só é possível trabalhar com dados de clientes para propósitos legítimos, específicos, explícitos e informados ao titular dos dados, sem possibilidade de tratamento posterior que seja incompatível com suas finalidades;

2. *Adequação*: O uso dos dados deve ser compatível com as finalidades informadas ao titular, de acordo com o contexto do negócio.

3. *Necessidade:* As empresas apenas devem solicitar dados de clientes que sejam estritamente necessários para alcançar as suas finalidades. É preciso fazer uma ponderação entre o que é realmente essencial para o negócio. Resumindo, os dados armazenados devem
atender ao princípio da necessidade.

4. *Livre acesso:* O cliente ou titular dos dados tem o direito de consultar, de forma simples e gratuita, todos os dados que a empresa detenha a seu respeito. Os dados devem poder ser acessados pelo usuário a qualquer momento. Além disso, o titular deve saber o que a empresa faz com os seus dados e de que forma o tratamento é realizado e por qual período.

5. *Qualidade dos dados:* É uma espécie de complemento do princípio anterior. Neste caso, o cliente deve poder atualizar, completar ou excluir dados que estejam incorretos ou sejam incompatíveis, garantindo a qualidade de seus dados. É fundamental ter atenção, exatidão, clareza e relevância dos dados nesse processo, tendo em conta a necessidade e a finalidade de seu tratamento.

6. Transparência: Trata-se do direito do cliente de ser informado e entender de forma clara e transparente como os dados serão tratados e quais os responsáveis pelo processo. Esse princípio também inclui a transparência em casos de incidentes de segurança sofridos pela empresa, como casos de vazamentos de dados. Além disso, a empresa não pode compartilhar dados pessoais com outras pessoas ou empresas sem que o titular seja informado.

7. Segurança: Os dados pessoais devem ser tratados de uma forma que garanta a devida segurança e confidencialidade, incluindo evitar o acesso a dados pessoais ou equipamentos usados para o seu tratamento ou o uso dos mesmos por pessoas não autorizadas. Essa etapa deve evitar qualquer tipo de incidente de segurança como vazamento de dados, roubo ou mesmo a distribuição das informações. O papel das empresas é buscar procedimentos, meios e tecnologias que garantam a proteção e segurança dos dados pessoais.

8. *Prevenção:* Além de toda a tecnologia e da inversão em sistemas que sejam adequados, as equipes que compõem as empresas devem ser treinadas para que o tratamento de dados ocorra de forma eficaz. Por exemplo, o ideal é

realizar a restrição de dados dentro das áreas para que nem todos os departamentos tenham acesso aos dados de clientes. O objetivo é evitar a ocorrência de danos em virtude do tratamento de dados pessoais durante o processo interno. Resumindo, as empresas devem tomar medidas antes que ocorra qualquer tipo de incidente que possa comprometer os dados pessoais de seus clientes.

9. *Não discriminação*: Um pouco fora da estrutura de sistemas, esse princípio faz referência a forma como os dados são utilizados. Ou seja, as empresas não podem utilizar esse tipo de dado como forma de discriminação ou promover qualquer tipo de abuso contra os seus titulares. A LGPD criou regras específicas para o tratamento de dados pessoais sensíveis, como os que tratam sobre origem racial ou étnica, religião, opinião política, saúde, entre outros.

10. Responsabilização e prestação de contas: Trata-se da prestação de contas tanto aos clientes como também as autoridades
sobre o que acontece na empresa em relação ao cumprimento da LGPD. É necessário demonstrar à Autoridade Nacional de Dados que os objetivos propostos foram cumpridos. Neste caso, as empresas devem ter provas e evidências de todas as medidas implementadas.

III - <u>Como implantar a LGPD?</u>

Com base nos princípios acima explicitados, podemos concluir que o objetivo básico de proteção de dados é proteger a segurança e privacidade das informações pessoais (clientes, fornecedores e colaboradores) que circulam no âmbito do seu negócio.

Quem são os atores envolvidos na LGPD:

- ANPD: Autoridade Nacional de Proteção de Dados – ANPD, possui atribuições relacionadas a fiscalização do cumprimento da LGPD;

- ✪ Titular: Proprietário dos dados pessoais que serão tratados durante todo o processo;
- ◎ Controlador: Pessoa física ou jurídica responsável por definir como os dados pessoais serão tratados em seu âmbito;
- ✵ Operador: Pessoa física ou jurídica que realiza o tratamento dos dados pessoais em nome do controlador;
- ★ Encarregado: Pessoa indicada pelo controlador para mediar a comunicação entre controlador, titular e a ANPD.

Assim, a proteção de dados e mais amplamente, segurança da informação, abrange todos os controles administrativos, lógicos e técnicos, necessários para proteger informações.

No que concerne ao ciclo de vida de dados pessoais (informações pessoais que transitam desde a coleta até o descarte), ou seja, todo o período em que os dados pessoais do titular são armazenados na empresa. Temos as seguintes fases:

1ª Fase. Coleta: forma pela qual os dados são coletados pela empresa;

2ª Fase. Processamento: etapa relacionada às maneiras como os dados são utilizados pela empresa;

3ª Fase. Compartilhamento: com quem as informações são compartilhadas;

4ª Fase. Armazenamento: cuidados com o armazenamento dos dados pessoais;

5ª Fase. Descarte: "quando", "como" e "por que" os dados são descartados.

Nesse aspecto deve ser desenvolvida e implementada uma estrutura para gerenciar segurança da informação dentro da empresa, onde podemos citar como pontos cruciais:

A) *Confidencialidade e privacidade*: Previne o acesso, uso, revelação, leitura, inspeção ou registro não autorizado de dados.

B) *Integridade*: Previne a modificação inadequada ou não autorizada de dados.

C) *Disponibilidade*: Garante que usuários autorizados tenham acesso confiável e pontual aos dados, e previne a interrupção ou destruição de dados não autorizados.

Para proteger a confidencialidade de dados, usando uma abordagem baseada em risco, a empresa pode implementar controles apropriados para abordar vulnerabilidades e atingir um nível aceitável de risco aos dados contra ameaças específicas. Quanto maior o risco para os dados, maior devem ser as medidas que devem ser implementadas. Nessa linha de trabalho, apresentamos a seguinte opção de gestão:

1. *Avaliação de riscos*: Definir circunstâncias ou eventos adversos naturais e/ou de origem humana, o impacto potencial ou consequências e a probabilidade e frequência de ocorrência.

2. *Tratamento de riscos*: Determinar quais proteções e/ou controles estão ausentes ou fracos em um ativo, tornando, portanto uma ameaça potencialmente mais prejudicial, cara, provável ou frequente. Implementar políticas, controles e/ou outras medidas para reduzir o impacto ou probabilidade de uma ameaça específica contra um ativo específico.

Uma avaliação de riscos de segurança de dados envolve i*dentificar suas operações de processamento de dados (determinar como e onde os dados são usados)*: Os dados dentro de uma organização têm diferentes perfis de risco, não apenas baseado no conteúdo dos dados, mas também devido à maneira que os dados são usados dentro da empresa. Portanto, é importante entender como os dados são processados dentro do seu negócio ao iniciar o processo de avaliação de riscos. Por exemplo:

- ✓ Recursos humanos com gestão de folha de pagamento de funcionários, recrutamento e retenção, registros de treinamento, ações disciplinares e avaliações de desempenho;
- ✓ Gestão de clientes, marketing e fornecedores com informações do cliente, ordens de compra e venda, faturas, listas de e-mail, dados de marketing e propaganda e contratos do vendedor.

Assim para cada operação de processamento de dados, considere o seguinte:

- Quais dados pessoais estão sendo processados?
- Qual é o propósito do processo?
- Onde o processamento ocorre?
- Quem é responsável pelo processo?
- Quem tem acesso aos dados?

O treinamento de consciência de segurança para todos os seus funcionários é necessário para garantir que seus funcionários não sejam o elo mais fraco quando se trata de proteção de dados na sua empresa. Seus funcionários precisam saber mais do que apenas as políticas de segurança e procedimentos da empresa. Eles também precisam entender porque eles são necessários. Isso significa investir em educação e consciência de segurança, que, frequentemente, é a única medida mais eficiente de segurança que você pode implementar.

Ao trabalhar com sua equipe, você pode levantar consciência dos problemas. Eduque todos que usam seus sistemas, incluindo executivos, fornecedores e parceiros. E lembre-se de que violações de políticas de segurança devem ter consequências. A falha em aplicar políticas enfraquece todo o esforço de segurança. As responsabilidades individuais precisam ser claramente definidas e entendidas: todos precisam saber seu papel.

IV - <u>Conclusão</u>

Os processos e ferramentas que podem ser utilizadas para a adequação à LGPD, variam de acordo com a forma de trabalho e o porte da empresa. Algumas já podem contar com procedimentos e tecnologias de proteção e necessitem apenas de alguma adequação e outras podem não ter noção nenhuma sobre como ou o porquê utilizar esses procedimentos, por isso, é importante buscar auxílio de profissionais que detenham conhecimento e experiência na área. LEMBRE-SE: A fiscalização terá inicio em agosto/2021.

Algumas perguntas e respostas que sua empresa precisa saber para atender a LGPD.

Embora não haja uma lista universal aplicável, algumas dúvidas surgem com mais frequência do que outras. E essas perguntas e respostas sobre a LGPD buscam dar um discernimento básico sobre essa nova legislação.

1 - O que é a LGPD na prática?

A LGPD tem como objetivo proteger a privacidade de consumidores e regulamentar a troca de informações entre Pessoas Físicas e Pessoas Jurídicas (empresas). Criada em 2018, a LGPD entrou em vigor em 2020 e as sanções começarão a ser aplicadas a partir de agosto/2021.

2 - Quais dados são protegidos pela LGPD?

O foco da LGPD é a proteção de dados pessoais e dados sensíveis, que possam identificar ou revelar características do indivíduo, definidos no artigo 5° da lei. São exemplos de dados pessoais para a LGPD:

- *Nome ou apelido*
- *RG*

- *CPF*

Os dados abaixo são considerados dados pessoais para a LGPD quando vinculados com algum dos dados acima:

- *E-mail*
- *Endereço*
- *Dados de localização*
- *Endereço de IP*
- *Cookies*
- *Identificador de publicidade do telefone*

São considerados dados sensíveis para a LGPD:

- *Religião*
- *Etnia*
- *Sexo*
- *Posicionamento político*
- *Orientação sexual*
- *Dados comerciais e bancários*
- *Filiação sindical*
- *Dados genéticos e biométricos*
- *Dados relacionados à saúde*

3 - Qual o impacto nas empresas? E para os usuários?

Para as empresas, o impacto é relevante, uma vez que a lei exige a aplicabilidade e aprimoramento de controles de segurança no tratamento de dados pessoais. Isso ajudará a fortalecer os setores de inteligência em segurança da informação, tanto no setor privado quanto público. Já os titulares dos dados passarão a ter melhor controle, autonomia sobre seus dados pessoais e segurança ao repassá-los para fazer cadastros.

4 - A quem se aplica a LGPD?

A LGPD se aplica a empresas sediadas no Brasil, que oferecem produtos e serviços ao mercado brasileiro ou que coletam e tratam dados de pessoas que estejam no país.

5 - Qual o risco envolvido no tratamento indevido dos dados?

Os principais riscos são o reputacional e o financeiro, pois o tratamento indevido e não seguro de dados pessoais, pode acarretar, por exemplo, em uma exposição indevida de dados pessoais de clientes ou de colaboradores acarretando multas e indenizações.

6 - Qual a penalidade para uma empresa que descumpra a LGPD?

Varia de advertência a multas que vão até 2% do faturamento.

7 - Que medidas devem ser tomadas para nos adaptarmos à LGPD?

Sugerimos:

- *Mapeamento dos processos que utilizam dados pessoais e o saneamento de dados não essenciais;*
- *Aprimoramento dos controles de segurança e proteção dos locais onde são tratados os dados pessoais;*
- *Divulgação e aculturamento de colaboradores e parceiros com relação aos cuidados no tratamento de dados pessoais.*

8 - Quem pode acessar os dados pessoais de sua empresa? Existem diferentes níveis de acesso para diferentes posições?

O fato de você, como controlador ou processador, ter o direito de processar os dados não significa que todos os seus funcionários possam acessá-los, devem ser apenas as pessoas cuja obrigação funcional dentro da sua empresa exige que tenham essa necessidade. Lembre-se ainda de especificar que tipo de

dados eles podem acessar (por exemplo, dados do cliente, dados relativos ao emprego) e o que eles podem fazer com os dados. Algumas pessoas precisarão ter acesso total, incluindo o direito de inserir, modificar ou apagar os dados, enquanto para outras apenas o direito de visualizar os dados será suficiente.

RECOMENDAMOS BUSCAR AUXÍLIO DE PROFISSIONAIS QUE DETENHAM CONHECIMENTO SOBRE A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS – LGPD.

Fonte:
Claudio Roberto Tonol
OAB/SP 167.063