

## Fernando Santiago: Lei de dados muda atuação de empresas

Finalmente sancionada (em 14 de agosto de 2018), a nova Lei Geral de Proteção de Dados Pessoais brasileira (LGPD) afeta profundamente o modo de funcionamento de todas as empresas brasileiras. Não a lógica comercial, mas a de gestão das informações. Trata-se de um verdadeiro “tsunami” para as companhias que terão, a partir da promulgação e publicação de lei em comento, 18 meses para se adaptar a uma realidade que, para a maior parte delas, lhes é totalmente estranha. Isso sem falar nos órgãos e entidades da Administração Pública, cujo modelo de gestão das informações pessoais é, salvo raríssimas exceções, muito aquém do que seria considerado “mediocre”.

Com efeito, para a maior parte das empresas e órgãos públicos brasileiros, os dados pessoais são vistos e tratados como um elemento de cunho quase “burocrático”, para não dizer banal. As informações sobre os empregados (nome, endereço, férias, salário, auxílios diversos, licenças médicas etc.) são geridas pelo RH com o auxílio de softwares pouco ou nada complexo, segundo o caso. Os contatos dos clientes (ou cidadãos) são tratados artesanalmente, normalmente para fins de envio de faturas, e-mails ou cobranças, e o histórico das compras efetivadas arquivados para fins de garantia dos produtos adquiridos.

A partir da entrada em vigor da LGPD, essa forma de gestão tende a tornar-se uma lembrança dos velhos tempos ou relatos (cases) figurando nos livros de administração.

Efetivamente, a era da informação deu origem a um fenômeno recente de produção e intercâmbio de dados em escala nunca visto na história da humanidade. Várias empresas criaram novos modelos de negócios utilizando esse “ativo”, e acumularam enorme quantidade de capital, poder e influência em tempo recorde (o Google foi criado em 1998, o Facebook em 2004). Em contrapartida, houve um movimento gradual de tomada de consciência da necessidade de se proteger esse ativo (dados pessoais) contra o seu uso indevido ou não autorizado. A Europa é, sem dúvida, onde o tema encontra-se mais maduro, regido atualmente pelo Regulamento Geral de Proteção de Dados Pessoais (GDPR).

No Brasil, a entrada em vigor da LGPD pretende criar um quadro normativo moderno, amplamente inspirado pelo Regulamento Europeu. Trata-se, entre outros objetivos, de colocar o país dentre o seleto rol de países ou organismos internacionais que proporcionem grau de proteção de dados pessoais adequado.

Assim, foram criadas uma série de obrigações para as empresas acerca da coleta, do uso e das garantias de integridade dos dados pessoais a serem observadas, sob pena de pesadas sanções. Da mesma forma, a referida lei atribuiu direitos aos titulares dos dados pessoais que podem ser exercidos contra quaisquer empresas ou entidades públicas que detenham tais informações. Nesse sentido, se os dados pessoais se tornaram indubitavelmente um precioso ativo, eles podem dar origem, se mal administrados, a um importante passivo para aqueles que os detêm.

Segue abaixo, a título ilustrativo, um resumo de alguns pontos e novidades trazidas pela nova lei de proteção de dados pessoais:

Aplicação territorial. Submetem-se à LGPD as empresas ou entidades públicas que efetuem o tratamento

---

de dados pessoais no Brasil, que colem dados no Brasil, ou que ofercem bens ou servic?os no territ?rio nacional.

### **Cinco principais princ?pios a serem observados no tratamento dos dados**

- Finalidade: os dados devem ser tratados para os fins espec?ficos informados ao titular, sem possibilidade de tratamento posterior de forma incompat?vel.
- Necessidade (ou minimiza?o): s? devem ser coletados dados pertinentes, proporcionais e na?o excessivos em relac?a?o a?s finalidades pretendidas.
- Livre acesso: os titulares dos dados devem poder consultar gratuitamente a forma e a durac?a?o do tratamento dos seus dados.
- Seguranc?a: os agentes de tratamento dos dados tem obriga?o de adotar medidas para proteger os dados pessoais de acessos na?o autorizados e de situac?o?es acidentais ou ili?citas de destruic?a?o, perda, alterac?a?o, comunicac?a?o ou difus?o.
- Responsabilizac?a?o e prestac?a?o de contas: os agentes de tratamento dos dados devem demonstrar a adoc?a?o de medidas eficazes e capazes de comprovar o cumprimento das normas de protec?a?o de dados pessoais.

### **O consentimento para o tratamento dos dados pessoais**

O consentimento passa a ser a melhor forma para legitimar o tratamento dos dados pessoais. Ele deve ser expl?cito e, quando solicitado no meio de um contrato comportando outros elementos, deve constar de uma cl?usula separada. O consentimento pode ser revogado a qualquer momento pelo titular dos dados. Outros motivos tamb?m legitimam o tratamento dos dados pessoais (ex: Cumprimento de obrigac?a?o legal ou regulato?ria, execuc?a?o de contrato do qual seja parte o titular, estudos por o?rg?o de pesquisa, dentre outros).

### **Principais direitos dos titulares dos dados**

- Direito de acesso e correc?a?o de dados incompletos, inexatos ou desatualizados.
- Direito ? anonimiza?o dos seus dados, bloqueio ou eliminac?a?o de dados desnecess?rios, excessivos ou tratados em desconformidade com o disposto na Lei.
- Direito ? portabilidade dos dados a outro fornecedor de servic?o ou produto (ex: bancos, visando facilitar a abertura de contas correntes, ou seguradoras etc.).
- Direito ? eliminac?a?o dos dados pessoais tratados com o consentimento do titular.
- Direito ? informac?a?o das entidades pu?blicas e privadas com as quais houve uso compartilhado de dados.
- Direito ? revogac?a?o do consentimento.

### **Transfer?ncia internacional de dados**

---

A transferência internacional de dados pessoais só é permitida para países que proporcionem grau de proteção de dados pessoais adequado ao previsto na Lei, ou quando houver comprovadas garantias de cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados previstos no mesmo texto normativo.

### **Sanções em caso de descumprimento da lei**

- Advertência com prazo para adoção de medidas corretivas.
- Multa simples, de até 2% do faturamento da empresa, grupo ou conglomerado no Brasil, limitada a R\$ 50 milhões por infração.
- Multa diária, observado o limite total de R\$ 50 milhões.
- Publicização da infração.
- Bloqueio dos dados pessoais a que se refere a infração até a sua regularização.
- Eliminação dos dados pessoais a que se refere a infração.

Como visto, há uma revolução silenciosa em curso. As empresas devem iniciar um processo de adaptação desde já visando evitar dissabores, exposição pública, pesadas multas ou até mesmo o aumento dos gastos com processos judiciais, posto que os direitos dos titulares dos dados podem ser exercidos perante o órgão regulador que deve ser criado (a criação prevista no projeto original foi vetado pelo presidente Temer) mas também perante os órgãos de defesa do consumidor ou judiciário. As empresas despreparadas serão talvez as protagonistas involuntárias de uma nova onda de corrida aos Procons.

### **Date Created**

20/08/2018