Por Milena Monticelli Wydra (*)

A Lei Geral de Proteção de Dados Pessoais (LGPDP), Lei nº 13.709/2018, que entrará em vigor em agosto de 2020, determina como os dados dos cidadãos - denominados usuários, podem ser coletados e tratados, prevê punições para transgressões e tem, como objetivo, estimular o desenvolvimento sustentável da economia e dos negócios.

Outros regulamentos similares pelo mundo são o *General Data Protection Regulation* (**GDPR**) na União Europeia e, nos Estados Unidos, o ***California Consumer Privacy Act of 2018*** (CCPA).

A lei geral de proteção de dados representa um avanço importante, colocando o Brasil ao lado de outros diversos países que já possuem tratamento definido sobre o tema. A nova legislação reforça a importância da boa-fé no tratamento dos dados pessoais, exigindo-se razoabilidade e transparência no seu tratamento, procurando penalizar excessos e abusos, através da definição da responsabilidade dos detentores dos dados e do dever de indenizar.

A disciplina da proteção de dados pessoais tem como fundamentos: (i) o respeito à privacidade; (ii) a autodeterminação informativa; (iii) a liberdade de expressão, de informação, de comunicação e de opinião; (iv) inviolabilidade da intimidade, da honra e da imagem; (v) o desenvolvimento econômico e tecnológico e a inovação; (vi) a livre iniciativa, a livre concorrência e a defesa do consumidor; e (vii) os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

Mas quem são os destinatários desta nova Lei?

A maioria das empresas brasileiras, (de pequeno, médio ou grande porte), que armazene e trate dados, não-digitais e/ou digitais, de clientes, funcionários e/ou terceiros, para exercer suas atividades, além de organizações públicas e privadas que obtenham e tratem dados pessoais de usuários, em território nacional, visando desenvolver e exercer suas atividades – com fins econômicos.

O que é tratamento de dados pessoais?

Toda operação que se utilize de informações de usuários, sejam eles clientes/fornecedores/trabalhadores e outros, como matéria-prima, como as que se referem à coleta, produção, recepção, classificação, utilização, acesso, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

Da importância e forma do consentimento do titular – usuário

Organizações públicas e privadas só poderão coletar dados pessoais se tiverem consentimento do titular, o chamado usuário. A solicitação deverá ser feita de maneira clara para que o usuário saiba, exatamente, o que vai ser coletado, para quais fins e, igualmente, se haverá compartilhamento de seus dados. Quando houver envolvimento de menores de idade, os dados somente poderão ser tratados com o consentimento dos pais ou responsáveis legais.

O consentimento deverá ser fornecido por escrito, em cláusula destacada, ou por qualquer outro ato que demonstre a vontade expressa do titular dos dados. Não se admite o consentimento implícito. O consentimento será sempre considerado uma autorização temporária, podendo ser revogado a qualquer momento pelo titular, o que deve ser garantido a ocorrer, por procedimento gratuito e facilitado por parte da empresa.

Se houver mudança de finalidade ou repasse de dados a terceiros, um novo consentimento deverá ser solicitado. O usuário poderá, sempre que desejar, revogar a sua autorização, bem como, pedir acesso, exclusão, portabilidade, complementação ou correção dos seus dados.

Dados Sensíveis

Há uma categoria classificada como “dados sensíveis”. Ela diz respeito às informações como crenças religiosas, posicionamentos políticos, características físicas, condições de saúde e vida sexual. O uso desses dados será mais restritivo, sendo a atenção especial no sentido de se evitar o uso para fins discriminatórios. Também será necessário garantir que tais dados serão devidamente protegidos.

Da aplicação da Lei em território nacional ou fora dele

A nova lei será aplicada às operações de tratamento de dados realizados no Brasil ou em outro país, desde que a coleta de dados ocorra em território brasileiro.

Se necessário, a empresa poderá transferir os dados para uma filial ou sede estrangeira, com a condição de que o país de destino também tenha leis abrangentes de proteção de dados ou possa garantir mecanismos de tratamento equivalentes aos que são exigidos no Brasil.

Punições

Em caso de vazamento de dados, esse fato deverá ser comunicado às autoridades competentes, para que tomem as medidas civis e criminais necessárias.

A punição pelo descumprimento da lei geral de proteção de dados vai depender da gravidade da situação, partindo de advertências até multa equivalente a 2% (dois por cento) do seu faturamento, limitada ao valor máximo de R$ 50.000.000,00 (cinquenta milhões de reais).

Todas as sanções serão precedidas de um procedimento administrativo que garanta a ampla defesa do suposto infrator. As sanções serão aplicadas considerando as particularidades de cada caso, com parâmetros e critérios próprios.

O Controlador e o Operador de dados

Tanto a iniciativa privada quanto os órgãos públicos deverão indicar um responsável pelo tratamento dos dados dentro da organização. Eventuais solicitações ou comunicações referentes a dados pessoais serão tratados prioritariamente com essa pessoa.

Quanto à responsabilidade, a Lei estabelece que tanto o controlador, quanto o operador dos dados, poderão ser responsabilizados, caso causem dano patrimonial, moral, individual ou coletivo, durante o exercício de atividade de tratamento de dados pessoais. Responderão, igualmente, acerca de incidentes de segurança da informação e/ou o uso indevido e não autorizado dos dados, ou pela não conformidade com a disposição legal.

Ressalte-se, aqui, a chamada responsabilidade objetiva dos operadores de dados em caso de danos causados aos titulares dos dados. Por isto, a comprovação de que o tratamento de dados é efetuado de forma eficaz e segundo os parâmetros da LGPD é imprescindível.

Tem-se, por definição legal:

Controlador: É a pessoa que tem competência para tomar decisões referentes ao tratamento de dados pessoais. Essa pessoa pode ser natural ou jurídica, de direito público ou privado; e

Operador: É a pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador. Este deve ser o responsável dentro da instituição pela supervisão do cumprimento das regras previstas na lei e orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais.

A responsabilidade do Operador, aquele que pratica o tratamento de dados em nome e a mando do

Controlador, pode ser limitada às suas obrigações contratuais e de segurança da informação, caso não viole as regras que lhe são impostas pela LGPD.

Há exceções, porém, quanto ao uso e tratamento de dados dos usuários

As regras acima não se aplicam para dados pessoais tratados para fins acadêmicos, artísticos ou jornalísticos, bem como, àqueles que envolvem segurança pública, defesa nacional, proteção da vida e políticas governamentais, que serão abordados por legislação própria.

Exemplos de situações alcançadas pela nova legislação em empresas/entidades

Em casos de terceirização de atividades/serviços, empresas costumam solicitar às prestadoras de serviços documentos comprobatórios de cumprimento das obrigações trabalhistas, os quais, via de regra, possuem dados pessoais dos trabalhadores terceirizados. Esses dados também devem ser protegidos e fazer parte de Código de Conduta e serem objeto de cláusulas contratuais próprias, adequadas à nova lei.

Imperioso, portanto, a revisão e adequação das políticas das empresas, seja quanto às regras internas e/ou em relação a terceiros, bem como contratos, procedimentos e demais atividades que envolvam ou possam envolver tratamento de dados pessoais (tanto de clientes quanto de empregados) conforme os princípios estabelecidos na LGPD.

Demonstrar e registrar a efetiva adoção de medidas de adequação de tratamento de dados, em registros próprios, por escrito, independentemente do tamanho da base de dados existente é ato da ordem do dia.

Recomenda-se, assim, a elaboração ou revisão por parte das empresas, de suas políticas internas, definindo de forma bastante clara os setores que poderão ter acesso a dados de candidatos, empregados, clientes, fornecedores e terceiros, bem como, a forma de utilização de tais informações, inclusive, estabelecendo penalidades contratuais em Código de Conduta, para o caso de uso indevido de dados, tais como o envio a e-mails particulares ou empregados e terceiros sem autorização de acesso aos dados. Há que se ter, também, políticas próprias relacionadas não somente à forma de coleta, mas, também, sobre a atualização e a forma de acesso dos dados pelos empregados e terceiros prestadores de serviços.

Neste sentido, os setores Jurídico, Compliance, IT e RH tem papel fundamental neste processo. É importante que o IT reestruture as políticas e os acordos de confidencialidade, com apoio do Jurídico.

Além da conscientização de todos sobre a importância dos termos da nova legislação, com a identificação de potenciais falhas em ***Compliance***, a organização deve se certificar sobre quais são as informações dos seus próprios funcionários e identificar a sua forma de armazenamento, para que sejam devidamente protegidos durante a permanência do trabalhador na entidade.

A sugestão para começar é:

Mapear onde, quando e como são coletados e tratados os dados pessoais de clientes, fornecedores e colaboradores (usuários), avaliando o local de armazenamento dos dados e qual seu o nível de proteção, como senhas e criptografia; entender, assim, o risco em que se encontra a empresa/entidade, priorizando as ações corretivas necessárias.

Obviamente, as empresas devem buscar consultoria jurídica especializada para que, em conjunto com os profissionais de IT – segurança da informação, possam proceder com a obrigatória avaliação e diagnóstico de cada setor da empresa/entidade.

Com o diagnóstico, a empresa/entidade deverá decidir se é caso de implantar, se o caso, uma nova estrutura na empresa ou, ainda, de elaboração de plano de mudanças focado na adequação da

mesma para que esteja em conformidade com a nova legislação.

Por fim, recomenda-se a criação/adequação de políticas e procedimentos internos, tais como, mas não se limitando a: Código de Conduta, revisão contratual geral, bem como, que se firme parcerias com prestadores de serviços técnicos e de assessoria jurídica, para que a resposta a ser dada a eventuais incidentes seja feita de modo a atender os requisitos previstos na LGPD, protegendo a companhia/entidade/empresa.

As empresas precisam se adequar à legislação o quanto antes e compreender que, se antever à futura regulamentação é, também, um investimento e uma grande vantagem competitiva no mercado.

(*) **Milena Monticelli Wydra** é Advogada sócia na Wydra Advogados Associados.

Fonte: **IBDEE**, em 03.04.2019.