Lei Geral de Proteção de Dados terá eficácia plena no Brasil já no próximo ano. Especialista analisa os principais pontos para a adequação do mundo corporativo à nova realidade sobre dados pessoais

Proteger a privacidade não é uma preocupação nova quando se trata do mundo digital. O Brasil deu ao tema uma legislação ampla com o Marco Civil da Internet sancionado há cinco anos. O documento, que foi elaborado em 2009 e passou por um longo processo de apreciação do Congresso Nacional e de consultas públicas, é uma espécie de Constituição para a internet no país e determina os direitos dos usuários, além de definir regras para as empresas que atuam no território nacional online.

Mas foi desde agosto do ano passado que o Brasil passou a fazer parte do grupo de países que possuem dispositivo legal específico sobre proteção de dados. A LGPD (Lei Geral de Proteção de Dados) é a versão brasileira do General Data Protection Regulation, mais difundido pela sigla GDPR. Assim como a GDPR direciona as obrigações das empresas que trabalham com dados pessoais dos residentes nos países membros da União Europeia e da Área Econômica Europeia, a LGPD determina as atividades das empresas que lidam com os dados privados daqueles que residem no Brasil.

Para o mundo corporativo, a LGPD traz importantes definições, sobretudo, após aprovação no início de junho da Medida Provisória (MP) n°869/2018 que recria a Autoridade Nacional de Proteção de Dados (ANPD). A MP do Congresso Nacional foi convertida em lei e altera a LGPD para dispor, além do tratamento de dados pessoais no âmbito do direto público, das atividades de proteção de dados também no setor privado.

“É como se fosse um recado mais direto do Poder Legislativo para a inciativa privada. Ou seja, para que as empresas que ainda não começaram a se adequar à LGPD preocupem-se com as determinações da lei que tem eficácia plena prevista já para o próximo ano”, opina Sandro Souza, responsável pela área de IT Services da consultoria GRC Solutions.

Com a ANPD, as empresas passam a ter um órgão público específico para direcionar a aplicação da nova realidade no tratamento de dados. O descumprimento da LGPD, sujeitará as empresas a multas que podem chegar a 2% do faturamento (ou até R$ 50 milhões) da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil. Já com base na GDPR, a multa é de 2% ou 4% e pode atingir 20 milhões (de euros).

“Será necessário uma adequação estrutural das corporações que atuam no Brasil na relação com clientes e parceiros empresariais. Esse processo de adaptação inclui treinamentos relacionados a conscientização e regras mais efetivas”, explica Souza. “A legislação prevê que, em casos de contratação de terceiros – como empresas de desenvolvimento de software – para o processamento de dados pessoais, a companhia precisa estabelecer em contrato cláusulas específicas sobre a proteção da privacidade de clientes”, completa.

Nesse caminho de adequação, segundo Souza, algumas questões são fundamentais para estabelecer a conformidade das empresas com as novas regras. “É fundamental que as empresas se planejem para identificar e classificar dados para realização de inventário e avaliação de impacto sobre a proteção de dados, por meio do que chamamos de AIPD ou Privacy Impact Assessment (PIA)”, explica.

O especialista da consultoria ressalta que nesse processo também é indispensável para qualquer empresa um suporte jurídico atuante. “Soma-se a isso, a necessidade de metodicamente rever contratos e acordos de confidencialidade; o entendimento da relação empresa x titulares dos dados e a consequente disponibilidade de mecanismos eficazes para atender eventuais solicitações desses titulares, como por exemplo a exclusão e retificação de dados”, complementa Souza.

Destaques sobre a regulação e a lei de proteção de dados

De acordo com Sandro Souza, tanto a GDPR, quanto a LGPD trazem de forma clara e ampla a definição do que vem a ser o processamento de dados pessoais. “Qualquer operação realizada com dados pessoais de modo automatizado ou não automatizado”, aponta ele. Souza destaca que essa descrição mais direta – bem como a adequada significação do que são e quais os tipos de dados pessoais – tem grande importância no processo de estruturação da cultura de proteção de dados nas empresas.

A regulação europeia e a lei brasileira classificam, por exemplo, os dados pessoais em diretos, indiretos e sensíveis. São considerados diretos os dados que podem ser associados a um indivíduo sem a necessidade de informações complementares. O DNA é um exemplo de dado pessoal direto. Já os endereços de IP dos computadores são considerados dados indiretos, pois não podem ser atribuídos a um indivíduo sem a devida complementação informacional.

Dados considerados sensíveis recebem, geralmente, proibição de tratamento na GDPR e na LGPD pois entram numa categoria especial de dados pessoais. Com base nos regramentos, são sensíveis os dados que revelam origem étnica ou racial, opiniões políticas, crenças religiosas e convicções filosóficas, dados relativos à vida sexual e a saúde do indivíduo, dentre outras especificações.

“Mas é permitido o tratamento de dados pessoais sensíveis, sob forma de exceção, se houver, por exemplo, consentimento explícito, obrigação legal e para defesa jurídica, interesse público, fins estatísticos ou se os dados já foram tornados públicos pelo próprio titular”, pontua Souza, que também informa: “É importante entender algumas diferenças entre a GDPR e a equivalente brasileira. Na LGPD há casos específicos em que os dados podem ser tratados sem o consentimento do titular. Um desses casos trata-se da garantia de prevenção à fraudes e segurança do titular nos processos de identificação e autenticação de cadastro em sistemas eletrônicos”.

A LGPD e a GDPR também dispõem sobre a minimização para o tratamento de dados pessoais de forma a limitar à uma necessidade e finalidade pertinentes, levando em consideração os princípios da proporcionalidade e subsidiariedade, ou seja, quando esgotadas outras possibilidades. Além disso, discorrem sobre procedimentos de notificação às autoridades competentes em casos de violação da segurança de dados pessoais.

Ainda de acordo com Sandro Souza, dois conceitos relacionados aos serviços de TI se destacam quando o assunto é adequação à nova regulamentação: “Privacidade por padrão e privacidade por design. O primeiro é mais focado nos sistemas existentes e está ligado aos controles e à segurança. O segundo, na construção dos sistemas com esforços prioritários direcionados à proteção da privacidade dos usuários desde o início e antes do desenvolvimento”, explana Souza. “Ambos necessitam de monitoramento e testes periódicos para avaliar os níveis de segurança”, conclui.

Fonte: **GRC Solutions**, em 17.06.2019.