Pesquisa — Lei Geral de Proteção de Dados Pessoais

Gabriel Gian, 8° período

A **Lei Geral de Proteção de Dados Pessoais** (LGPD ou LGPDP), Lei nº 13.709/2018, é a legislação brasileira reguladora das atividades de tratamento de dados pessoais e que também altera os artigos 7º e 16 do Marco Civil da Internet de 23 de abril de 2014. A partir da mesma, o Brasil tornou-se parte do grupo de países que contam com uma legislação específica para o controle e regulamentação do fluxo e contenção de dados pessoais dos cidadãos em geral.

A LGPD baseia-se em legislações já existentes, como o **Regulamento Geral sobre a Proteção de Dados** (GDPR) da União Europeia, vigente desde 25 de maio de 2018 e aplicável a todos os países da União Europeia, e o **California Consumer Privacy Act of 2018** (CCPA), dos Estados Unidos da América, implementado através de uma iniciativa em âmbito estadual, no estado da Califórnia, aprovado desde 28 de junho de 2018, que fundamentam-se em direitos universais, como a **Declaração Universal dos Direitos Humanos** (DUDH), visando proteger direitos individuais como a privacidade, a inviolabilidade da intimidade, a liberdade de expressão, a autodeterminação informativa, de comunicação de opinião, a livre iniciativa, a defesa do consumidor, *et cetera*, e busca prevenir e remediar eventos como o **escândalo do Facebook e da Cambridge Analytica**, que veio à tona em 2018 e representou uma grave violação dos dados pessoais para o uso em manipulações da opinião pública para ganho político.

A lei distingue entre **dados pessoais** e **dados pessoais sensíveis**, além de prever a atuação de uma **autoridade nacional** reguladora e fazer distinção de três diferentes entes quanto à transmissão e manipulação de dados pessoais: os **titulares dos dados**, sendo *pessoas físicas* que emitem dados de natureza pessoal sigilosos ou não, que serão obtidos pelos **controladores**, sendo *entes responsáveis pela obtenção e tratamento dos dados* pelos **processadores**, que por sua vez são entes subordinados aos controladores que operam, de fato, *a partir dos dados obtidos de forma a cumprir o que é acordado* entre os titulares e os controladores, podendo possuir ou não outros entes subordinados ou subjacentes.

Os dados coletados devem seguir todas as boas práticas de tecnologia vigentes atualmente, como por exemplo:

- O uso de tecnologias presentes na suíte de protocolos **IPSec**, como o **transport layer security** (TLS);
- Armazenamento de dados de maneira segura, utilizando-se de meios como a criptografia—embora a mesma não seja citada na Lei—com algoritmos como o **RSA** e o **AES**, estratégias de **backup** e **recuperação de desastres** como o armazenamento em mídias diferentes, e, preferivelmente, apenas a quantidade de dados necessária—nem mais, nem menos—para o processamento deve ser coletada;
- Políticas de autenticação como o **OAuth** e a autenticação de múltiplos fatores (MFA);
- Políticas de controle de acesso como o **role-based access control** (RBAC) e o **controle de acesso à rede** (NAC), assim como a virtualização de ambientes;

- O uso de ferramentas de prevenção contra ameaças, como **firewalls**, softwares **antivírus**, **e-mail gateways** e **gerenciadores de eventos de segurança** (SIEMs);
- Segurança do acesso ao ambiente físico da infraestrutura de TI, como servidores e datacenters;
- **Atualizações regulares** de sistemas operacionais, firmwares e softwares;
- Medidas para a **conscientização** de todos os colaboradores no que concerne à segurança da informação como **cursos** e **treinamentos**.

O titular deve ser informado de todas essas questões de maneira clara e objetiva, e deve poder escolher ou **optar por consentir ou não** com tal coleta.

Do lado da governança, o controlador deve, como boa prática, formular um **Relatório de Impacto de Proteção de Dados**, documento onde é levantado o processo e os métodos a serem aplicados para a gestão correta dos dados coletados dos titulares. Este documento deve guiar toda a organização, dos processadores aos **encarregados** ou **data protection officers** (DPOs), até os controladores. Todavia, não é somente o controlador que deve se responsabilizar pela gestão dos dados pessoais, mas também os *titulares devem ser implicados com suas próprias responsabilidades civis*, uma vez que a má gestão dos dados pessoais (e.g. confiança de senhas e documentos a terceiros) por parte do próprio titular pode acarretar em nulidades em possíveis litígios, uma vez que o nível de acordo de cada parte deve ser seguido de acordo com o que está previsto em sua responsabilidade.

As exceções na aplicação da LGPD são os fins **jornalísticos** (e.g. reportagens) **artísticos** ou **acadêmicos** (e.g. pesquisas), assim como fins exclusivos de **segurança pública**, **defesa nacional**, **segurança do Estado**, atividades de **investigação** e **repressão de infrações penais** ou provenientes de fora do território nacional e que **não sejam objeto de comunicação**, desde que o país proporcione grau de proteção de dados pessoais **adequado ao previsto na Lei**.

Como os dados devem ser obtidos de *boa fé*, tratados e protegidos, penalizações no que concerne à proteção dos dados são isentas de dolo ou culpa, uma vez que o controlador tem a **obrigação** de adotar procedimentos que deem transparência do seu *legítimo interesse* e, ainda, a autoridade nacional poderá requisitar ao controlador o Relatório de Impacto de Proteção de Dados Pessoais. As penalidades previstas na LGPD podem ser de advertência, onde a autoridade nacional notificará com o prazo para que o controlador responda e demonstre que efetivamente está adotando as práticas corretas ou que fará as devidas correções. Ainda, pode ser de **multa de 2% sobre o faturamento anual da empresa**, não podendo exceder a **50 milhões de reais**. É possível a aplicação de **multa diária num montante de dez mil reais**, observando-se que o total não deve ultrapassar os 50 milhões de reais estabelecidos no inciso anterior.