Aspis: A observação da LGPD e o custo de um vazamento de dados

A Lei Geral de Proteção de Dados (LGPD), que passou a vigorar no Brasil em 2020, possui extrema importância no âmbito empresarial. Essa importância não se prende apenas a critérios jurídicos e de TI, mas também a governança corporativa.

Não é nenhuma novidade que empresas utilizam e tratam dados de terceiros, na grande maioria das vezes, com finalidade econômica, o que não é nenhuma ilicitude, desde que observados determinados critérios.

Dados pessoais passaram a ser uma moeda muito importante e valiosa no mercado e nas estratégias empresarias. Através de dados coletados, as empresas podem conhecer melhor o perfil e as preferências de seus clientes, elaborar publicidade mais assertiva e também obter *feedback* de suas atividades.

Muitas vezes, recebemos acesso "gratuito" a determinados produtos e conteúdos única e exclusivamente cadastrando nossos dados pessoais em determinados sites ou locais físicos.

Na verdade, de gratuito isso não tem nada. Para certo tipos de negócios, são muito mais valiosos os dados pessoais de clientes e consumidores do que um eventual pagamento de mensalidade para acessar certa plataforma ou para fazer parte de algum clube de descontos, por exemplo.

Dados pessoais possuem alto valor de mercado e seguidamente são comercializados.

A proteção desses dados não é algo novo, tanto no nosso ordenamento jurídico como também no ordenamento jurídico de outras nações.

O próprio Código de Defesa do Consumidor (CDC) já trata desse assunto desde a sua entrada em vigor, há 30 anos, através do artigo 6º, no qual aponta para a necessidade de informações adequadas e claras sobre produtos e serviços.

Do mesmo modo, o conceito de fornecedor (artigo 3º do CDC) equipara-se ao conceito amplo de agentes de tratamento (artigo 5º, incisos VI e VII, da LGPD) e o conceito de consumidor (artigo 2º do CDC) equipara-se, em sentido amplo, ao conceito de titular dos dados (artigo 5º, I da LGPD).

E ainda o artigo 43 do CDC, antecipadamente, já tratava da necessidade da segurança de dados, como se percebe do *caput* do artigo: *"O consumidor, sem prejuízo do disposto no artigo 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes".*

Importante ressaltar que *LGPD prevê mecanismos protetivos similares aos previstos no CDC*, como é o caso da inversão do ônus da prova, por exemplo.

A proteção de dados na União Europeia é regida pela GDPR, *General Data Protection Regulation* (Regulamento Geral de Proteção de Dados), que vigora desde o ano de 2016 e é equivalente à nossa LGPD.

Mencionada lei é rigorosamente observada nos países nos quais ela vigora, sendo que infrações a ela são severamente punidas.

Recente pesquisa elaborada pelo *Ponemon Institute* para a *IBM Security* [1] produziu um relatório sobre o prejuízo que pode ser causado por um vazamento de dados em empresas de diversos países. Os números assustam, mas não surpreendem.

Esse relatório se tornou uma das principais ferramentas de estudo comparativo no setor de segurança virtual, oferecendo aos gestores, aos operadores do Direito, aos líderes de TI, gerenciamento de riscos e segurança uma visão pontual dos fatores que reduzem ou aumentam o prejuízo de um vazamento de dados. Ele também oferece uma visão das tendências de vazamentos de dados, demonstrando consistências e flutuações nos prejuízos que foram analisados ao longo do tempo.

Esse estudo apontou em US$ 3,86 milhões o valor médio de prejuízo que uma empresa tem com o vazamento de dados.

De forma interessante, também concluiu que as empresas que sofreram com vazamentos de mais de um milhão de registros tiveram um prejuízo, muitas vezes, superior à média geral. Vazamentos de um milhão a dez milhões de registros custam, em média, US$ 50 milhões para as empresas, mais de 25 vezes o custo médio de US$ 3,86 milhões para vazamentos de menos de cem mil registros. Em vazamentos de mais de 50 milhões de registros, o prejuízo médio foi de US$ 392 milhões, mais de cem vezes a média.

Dados pessoais de clientes foi o tipo de registro mais frequentemente comprometido e o que mais causou prejuízo nos vazamentos de dados das organizações.

Segundo a pesquisa, 80% das organizações afetadas declararam que os dados dos clientes foram comprometidos durante o vazamento, muito mais do que qualquer outro tipo de registro (registro de funcionários, fornecedores, dados bancários etc).

Pelos cálculos elaborados pelos pesquisadores, enquanto o prejuízo *médio por registro perdido ou roubado* foi de US$ 146 em todos os vazamentos de dados, os que contêm informações de identificação pessoal do cliente custam às empresas US$ 150 *por registro comprometido*.

Destaca-se ainda que uma em cada cinco empresas (19%) que sofreram com vazamentos de dados decorrentes de ataques *hackers* foi invadida como consequência de credenciais de funcionários roubadas ou comprometidas, aumentando o prejuízo total médio de um vazamento para essas empresas em quase US$ 1 milhão, para US$ 4,77 milhões.

No geral, ataques *hackers* foram apontados como a causa principal mais frequente (52% dos vazamentos no estudo) em comparação com erro humano (23%) ou falhas no sistema (25%).

Ademais, além das credenciais roubadas ou comprometidas, os servidores em nuvem mal configurados foram relacionados como o vetor de ameaças inicial mais frequente nos vazamentos causados por ataques *hackers* em 19%.

Como decorrência dos vazamentos causados por configurações incorretas da nuvem, o prejuízo médio de um vazamento aumentou em mais de meio milhão de dólares, para US$ 4,41 milhões.

Na questão temporal, em média, as empresas que participaram do estudo precisaram de 207 dias para identificar e 73 dias para conter um vazamento de dados em um tempo médio de 280 dias.

No setor da saúde o ciclo de vida de um vazamento chegou, em média, a 329 dias, e no setor financeiro foi de 233 dias (96 dias mais curto).

Conforme verificado no estudo, a implantação total da automação da segurança ajudou as empresas a reduzir o ciclo de vida de um vazamento em 74 dias em comparação com as empresas sem automação da segurança (de 308 para 234 dias).

E agora um ponto importantíssimo, a preparação para a resposta a incidentes (RI), ou seja estar adaptados às regras de proteção de dados, foi o fator que mais reduziu o prejuízo das empresas.

O prejuízo total médio de um vazamento de dados nas empresas com uma equipe preparada para as respostas a incidentes e que também testaram um plano de RI, usando exercícios ou simulações, foi de US$ 3,29 milhões, em comparação com US$ 5,29 milhões nas empresas sem equipe de RI e que não tenham praticados testes de RI, uma diferença de US$ 2 milhões.

Pelas conclusões a que esse estudo da *IBM Security* chegou, é possível verificar o quão grave pode se tornar um vazamento de dados. E, do mesmo modo, percebe-se o quanto são relevantes as adequações das empresas à LGPD, bem como o preparo e o treino de sua equipe.

Como já dito no início deste artigo, adequar-se à LGPD é uma questão de governança corporativa, que pode impactar diretamente nos resultados das empresas.

Abster-se de adotar as medidas preconizadas pela LGPD, ou não atualizar o plano preventivo de respostas a incidentes, passou a ser uma falha na gestão da empresa que pode resultar em enormes prejuízos financeiros, além do prejuízo reputacional.

Portanto, deverá o empresariado observar as regras da LGPD como uma forma de segurança de seu próprio negócio.

É sabido que muitas empresas estão postergando a adequação à LGPD devido ao seu considerável custo.

Estamos em um momento de pandemia, no qual a receita de empresas de diversos seguimentos diminuiu significativamente. Porém, postergar demasiadamente essa adaptação, ou ao menos deixar de demonstrar a intenção de se adaptar a LGPD, pode significar uma perda muito maior no futuro. Hoje especialistas entendem que adequar-se à LGPD pode ser considerado um dos melhores investimentos que uma empresa pode fazer.

[1] Disponível em https://www.bibliotecadeseguranca.com.br/wp-content/uploads/2021/01/relatorio-sobre-o-prejuizo-de-um-vazamento-de-dados.pdf.

Date Created
01/09/2021