Por Jacopo Angelozzi (*)

Os ataques cibernéticos que têm acontecido durante a pandemia ilustram o quão vulneráveis até mesmo empresas bem preparadas podem ser a tais ameaças. Aqui no Brasil, o setor de saúde teve que lidar com alguns transtornos após os sistemas de informações de grandes hospitais serem atacados por hackers. A escolha do alvo se deve pelo rico conjunto de informações de pacientes que essas organizações possuem e por tratar-se de informações sensíveis que poderiam prejudicar dramaticamente o titular em caso que sua confidencialidade for comprometida por um vazamento. Afinal, hoje em dia os dados se transformaram em uma moeda de troca bastante valiosa.

A capacidade de usar as informações de forma analítica possibilitou uma evolução tecnológica e social que trouxe muitos benefícios para a sociedade, mas também pode ser um risco altamente prejudicial para a realidade de organizações e indivíduos. É pela existência desta ameaça que a nova Lei de Proteção de Dados (LGPD) busca estabelecer uma regulamentação para captação e uso de dados no Brasil, no tocante à pessoa física.

Com o projeto de conversão da MP 959/2020 aprovado pelo Congresso e agora dependendo de sanção do Presidente, a LGPD entrará em vigor nos próximos dias. Ainda que tenha sido alterada, definindo-se que as penalidades serão aplicadas somente em agosto de 2021, as empresas que violarem a lei estarão sujeitas às sanções como advertências, bloqueios ou suspensões dos serviços, além de multas que poderão atingir o valor máximo de R$ 50 milhões por infração ou a 2% do faturamento da organização. Isso sem se falar no risco reputacional ao qual a empresa ficará exposta.

Muitos incidentes são resultados de erro humano e podem ser mitigados por treinamentos de conscientização da equipe, bem como suporte especializado para realização de gerenciamento de risco. Mas mesmo com todo o cuidado, as chances de se violar a lei existe.

Um exemplo de ameaça é representado pelo grande número de dispositivos móveis que se conectam a redes corporativas criando uma circulação/fluxo enorme de informações. Uma gestão da conectividade móvel que não se preocupa com as devidas medidas de proteção dos acessos remotos, (como VPN e MFA) pode ser facilmente explorada por pessoas mal-intencionadas que queiram acessar os ativos de uma organização.

De acordo com o relatório **Risk Barometer 2020**, os incidentes cibernéticos ocupam o 1º lugar global como o risco comercial mais preocupante. As consequências deste tipo de incidente podem ameaçar a continuidade dos negócios, pois podem acarretar perdas relevantes e imediatas, as quais exigirão recursos financeiros que a empresa não havia provisionado ou sequer previsto.

Diante disso, empresas buscam a contratação de coberturas do seguro contra riscos cibernéticos que cobrem despesas relacionadas a terceiros. Como exemplo, temos as despesas legais e de investigações forenses associadas ao momento imediatamente sucessivo ao ataque, quando é necessário entender a entidade do vazamento, quais informações confidenciais foram indevidamente acessadas. Nesta fase do incidente de segurança, podem entrar em consideração, em determinadas hipóteses, também custos de extorsão cibernética, como de *ransomware*. Além disso, o seguro protege financeiramente em caso de perda de lucro devido ao tempo de inatividade causado pelo incidente cibernético e em caso de sanções impostas por alguns órgãos reguladores, sempre de acordo com os termos da apólice contratada.

A nova lei cria um verdadeiro empoderamento para os titulares dos dados: os direitos sobre o tratamento das informações pessoais se traduzem em obrigações de proteção e transparência para todas as entidades que operam com esses ativos intangíveis. Esse cenário ajuda a entender a necessidade de direcionar a oportuna atenção para prevenir e mitigar todos os possíveis riscos de violar tais direitos. Em caso de ocorrência de um incidente cibernético, a LGPD prevê ainda que uma empresa deve tomar as medidas exigidas pela lei como notificar seus clientes, fornecedores, parceiros ou funcionários sobre uma violação de privacidade. Isso, logicamente, pode aumentar a possibilidade de ter que responder a eventuais ações judiciais por danos.

Com tudo isso, fica claro que a LGPD permitirá maior segurança nas relações entre pessoas físicas

e jurídicas, no que se refere ao tratamento dos dados pessoais, garantindo os respectivos direitos individuais. No entanto, é fundamental que as empresas busquem alternativas estratégicas para mitigar o máximo possível esses riscos e ameaças realizando uma gestão de dados consciente que vai resultar em um desenvolvimento sustentável não somente do próprio negócio, mas também do ambiente econômico como um todo.

(*) **Jacopo Angelozzi**, subscritor sênior de Linhas Financeiras América Latina da Allianz Global Corporate & Specialty (AGCS).