Adalberto Júnior: Descumprimento da LGPD e o setor de saúde

25/02/2023

As sanções administrativas, previstas pela Lei Geral de Proteção de Dados (LGPD), começaram a valer a partir do dia 1º de agosto de 2021, embora ainda não tenha sido aplicada nenhuma sanção até o momento. Durante o ano de 2022, a Autoridade Nacional de Proteção de Dados (ANPD) iniciou o processo de regulamentação das sanções e poderá aplicar sanções retroativas por violações que tenham sido praticadas desde agosto de 2021, podendo ser aprovado ainda no mês de fevereiro de 2023, passando para a fase de fiscalização e aplicação das multas.

A aplicação retroativa fica restrita às infrações que eventualmente forem cometidas após a vigência dos artigos 52, 53 e 54 da LGPD, já que não há possibilidade de aplicação de sanções por infrações ocorridas antes disso. Outro ponto relevante a ser destacado é que não é apenas a ANPD que poderá realizar a fiscalização do cumprimento da legislação. Outros órgãos, como o Ministério Público, Senacon e o Poder Judiciário também devem atuar no caso de serem acionados diretamente pelos titulares.

Olhando para o cenário internacional e tomando como parâmetro o Regulamento Geral de Proteção de Dados (RGPD), desde a sua entrada em vigência na União Europeia, em 25 de maio de 2018, já foram aplicadas pouco mais de 900 sanções, com valor que ultrapassa 1,3 bilhões de euros e o setor de saúde é um dos mais afetados. O maior grupo de multas está relacionado a medidas técnicas e organizacionais insuficientes, isto é, falta de segurança de dados. Somente nesta área foram aplicadas 21 multas, num total de cerca de 8,9 milhões de euros ou mais de 90% do valor total das multas no setor da saúde.

No Brasil, em 2021, um hospital foi condenado a pagar uma indenização para uma paciente por conta de falhas de segurança na guarda dos prontuários médicos. Em resumo, de acordo com o processo, houve uma invasão aos sistemas do hospital, possibilitando que uma pessoa não autorizada tivesse acesso a informações que deveriam ser mantidas em sigilo e, com isso, conseguiu convencer familiares da paciente a realizar um depósito no valor de R$ 3.000 para a realização de supostos procedimentos médicos não cobertos pelo serviço contratado. Ao final da

ação, o hospital foi condenado ao pagamento de uma indenização por danos morais e em restituir o valor pago ao golpista pela família da paciente.

Contudo, mais preocupante do que os valores que são pagos em multas e indenizações, o dano reputacional e à imagem é algo que poderá conduzir o titular a procurar outra empresa para se relacionar por quebra de confiança. E para evitar as punições, o segredo é apenas um: estar em conformidade com a legislação e preparado para atender às demandas e solicitações que chegarem, sejam dos titulares ou dos órgãos de fiscalização.

É importante entender o ciclo de vida dos dados pessoais, apontar as finalidades pela qual ocorre cada uma das operações de tratamento e definir as bases legais que justificam e autorizam as atividades. Além disso, avaliar os compartilhamentos e as medidas de segurança que são adotadas para proteger a confidencialidade, integridade e disponibilidade das informações também é altamente recomendável.

No setor da saúde, por lidar com dados sensíveis, os cuidados devem ser redobrados pelos agentes de tratamento. Além disso, em razão da volumetria de dados pessoais e dados pessoais sensíveis que são manipulados no dia a dia em clínicas, consultórios, laboratórios e hospitais, os riscos podem ser muito altos e precisam ser tratados de acordo com a urgência e nível de criticidade. Isso porque, conforme previsão da LGPD, no caso de algum dano (patrimonial ou moral) ao titular, o agente de tratamento fica obrigado a reparar.

Daí vem a necessidade de se estabelecer um Programa de Governança em Proteção de Dados, que possa trazer segurança para as atividades de tratamento que são realizadas, garantindo um nível adequado de conformidade com a legislação como um todo (e não apenas com a LGPD), permitindo que os agentes de tratamento realizem suas operações e possam estar preparados para atender aos titulares, órgãos de fiscalização e também para agirem em casos de incidentes de segurança.

A pandemia do coronavírus fez com que houvesse uma alta na procura por atendimentos médicos e diariamente foram divulgadas informações sobre o número de novos contaminados, total de vacinados, registro de óbitos e indicação dos que foram curados. O compartilhamento destas informações consta no item 43, do Anexo da Portaria nº 204/2016, do Ministério da Saúde, que estabelece os critérios e lista de doenças que devem ser comunicadas

compulsoriamente com os órgãos de saúde pública.

O volume de informações divulgadas e o registro em um banco de dados unificado atraiu hackers que realizaram ataque aos servidores do DataSUS e gerou o comprometimento de informações de saúde de milhões de brasileiros, causando instabilidade no aplicativo ConecteSUS, que reúne registros da vacinação contra o coronavírus. Após a identificação das falhas que permitiram o acesso indevido, houve a necessidade de reparos por parte do Ministério da Saúde, para reforçar o nível de segurança e recuperar os registros do aplicativo.

Esse ataque acendeu o alerta para o setor da saúde, fazendo com que inúmeras instituições que ainda não haviam iniciado seus programas de governança, começassem a se movimentar para adequar suas atividades. Pelo que se percebe do cenário atual, somente com a elaboração e implementação de um programa de governança em proteção de dados aderente, com a revisão das medidas de segurança para garantir o sigilo das informações que estejam sob guarda e responsabilidade das instituições e reforço das boas práticas para gerar engajamento e aculturamento interno, é possível demonstrar um nível seguro de conformidade.

Por lidar com dados pessoais sensíveis, que podem gerar um nível de exposição extremamente elevado aos titulares, as instituições de saúde precisam se manter vigilantes quanto às regras de proteção de dados e segurança da informação, vez que se encontram como alvo principal dos ciberataques. As empresas ligadas ao setor de saúde estão entre as mais visadas para ataques cibernéticos, superando o setor de varejo que foi altamente afetado nos últimos anos.

Os cibercriminosos sabem que os ataques que envolvem dados de pacientes podem afetar a continuidade dos atendimentos médicos e, em razão disso, caso não haja um backup atualizado e medidas de segurança capazes de garantir a confidencialidade, integridade e disponibilidade dos dados pessoais, numa tentativa de ransomware, por exemplo, há uma possibilidade de cobrarem valores elevados para o resgate de tais informações.

Pesquisa divulgada pela Check Point Research (CPR), referente ao terceiro trimestre de 2022, mostra que a saúde é o setor mais atingido por ataques cibernéticos no Brasil, sendo que uma em cada 42 organizações foi afetada por um ransomware. Em média, as organizações foram atacadas 1.484 vezes semanalmente, um aumento de 37% comparado ao período do terceiro trimestre de 2021. Para proteger suas informações, é importante que as empresas do setor de saúde implementem medidas de segurança cibernética rigorosas.

Isso inclui a realização de treinamentos de segurança para todos os funcionários, a instalação de software de segurança atualizado em todos os dispositivos e a criação de políticas rigorosas de senhas, controle de acessos e gestão de ativos. Além disso, é importante monitorar constantemente as atividades de rede e contar com uma equipe de segurança cibernética para monitorar as ameaças e responder rapidamente a qualquer incidente. Em conjunto com o Data Protection Officer (DPO), esses profissionais têm o conhecimento e a habilidade para proteger as informações sensíveis e garantir a continuidade dos negócios.

Estar atento às novidades tecnológicas e implementar as medidas adequadas obviamente que não é garantia de que a empresa não sofrerá um incidente, assim como a adoção de boas práticas. Porém, a boa-fé do agente de tratamento é um critério atenuante no caso de aplicação

de sanções pela autoridade.

Fonte: https://conjur.jumps.com.br/2023-fev-25/adalberto-junior-descumprimento-lgpd-setor-saude/