Opinião: Ataques cibernéticos e proteção de dados na saúde

Segundo estudos recentemente divulgados pela IBM Security, no relatório intitulado *"X-force Threat Intelligence Index"*, os setores relacionados ao fornecimento de insumos e respostas primárias à pandemia da Covid-19 — especialmente o setor de saúde — sofreram, em 2020, o dobro de ataques r.

Segundo a pesquisa, entre os principais fatores que levaram ao aumento de tais incidentes de segurança estão a infraestrutura ainda em estágio inicial de segurança cibernética de parte dos participantes do mercado, uma vez que, segundo os autores do relatório, não havia, desde o surgimento da Covid-19, uma grande preocupação geral por parte dos agentes e órgãos sanitários sobre proteção dos dados pessoais, sobretudo em comparação com outros grupos de instituições que já ocupavam palco central das preocupações relacionadas a dados (como o setor financeiro, por exemplo) [1].

Assim, a guinada global representada pela pandemia não somente alterou as perspectivas rotineiras e as concepções de trabalho e relacionamentos sociais, mas também impulsionou e colocou em evidência na sociedade setores e preocupações distintas. A busca por insumos para a produção de vacinas, a necessidade de monitoramento dos funcionários acometidos pela doença viral nas empresas, além da preocupação na diminuição dos efeitos da pandemia na economia global, representam planos de fundo objetivos que colocaram o setor de saúde, concebido de forma geral, como um dos mais visados no cenário mundial.

Tendo isso em vista, os ataques cibernéticos na área sanitária e industrial de suporte tinham de antemão grandes chances de ocorrer. O relatório demonstra que o *industrial control systems* (sistema de controle industrial) relatou um aumento de 49% das vulnerabilidades dos sistemas industriais entre os anos de 2019 e 2020. Além disso, o relatório prevê que a Europa é o continente mais afetado no espaço virtual, tendo experienciado 31% dos ataques cibernéticos relatados pela *X-force*.

Nesse contexto, é interessante pontuar que a Europa é uma das pioneiras na elaboração de legislação de proteção de dados. Já em 1995, o Parlamento Europeu aprovava o texto da Diretiva 95/46, que previa uma série de regras e requisitos para o tratamento de dados pessoais e representou grande revolução nos entendimentos sobre a matéria no mundo (em complemento a variadas iniciativas legislativas ocorridas desde 1970 no contexto europeu). Posteriormente, aprovada em 2016 e em vigor desde 2018, a União Europeia (UE) editou a *General Data Protection Regulation* (GDPR), regulamento que inspirou inúmeras outras leis a respeito do tema ao redor do mundo, inclusive no Brasil.

Ainda assim, mesmo com o influente histórico em matéria de proteção de dados da UE, contando com a presença de inúmeras autoridades nacionais dos Estados-membros que compõem o bloco, doutrinadores e legislações complementares e setoriais, o continente europeu não se vê isento de ataques, tendo sido alvo de episódios relevantes no tocante ao vazamento de dados pessoais.

Sob a perspectiva do cenário nacional, o relatório aponta que o Brasil foi o país mais atacado da América do Sul e América Central em 2020. Diferentemente da UE, o Brasil somente editou sua lei geral de proteção de dados em 2018, a Lei nº 13.709, de 14/8/2018 (LGPD), que entrou em vigor em setembro de 2020 depois de certo tumulto e controvérsias. Anteriormente, o país contava com leis setoriais em matéria de proteção de dados, como algumas das disposições previstas no Código de Defesa do Consumidor, na Lei do Sigilo Bancário, no Marco Civil da Internet e na Lei do Cadastro Positivo.

O atraso brasileiro na criação e implementação de arcabouço jurídico geral sobre proteção dos dados pessoais pode ser um dos fatores para não se ter observado no país até a edição da LGPD uma cultura nacional de preocupação com o manuseio adequado e mitigação de riscos de vazamentos de dados pessoais. Isso poderia justificar, em certa medida, a ocorrência de número relevante de ataques cibernéticos no Brasil evidenciados na pesquisa.

Nesse contexto, o setor de saúde presencia atualmente dupla necessidade de preocupação com proteção de dados pessoais: seja para cumprir a LGPD, seja para se proteger da maior exposição potencializada pela pandemia da Covid-19. Não à toa, a LGPD, seguindo a tendência representada pelo GDPR, classificou, em seu artigo 5º, inciso II, os dados referentes à saúde como um tipo específico de dados pessoais sensíveis, indicando a preocupação especial com esse tipo de dado pessoal. Como consequência, o tratamento de dados pessoais de saúde deve se respaldar em rol de bases legais mais restritivo (previsto no artigo 11, em comparação com o artigo 7º), além de exigir maior cuidado e preocupações adicionais na implementação dos demais requisitos exigidos pela lei.

Uma das preocupações que levaram legisladores a incluir dados de saúde entre os dados pessoais sensíveis consiste na possibilidade de discriminação negativa e abusiva, gerando predileções e exclusões indevidas baseadas em condições de saúde, por exemplo, nas relações de trabalho e nas relações sociais de forma geral.

Considerando o panorama acima, a Confederação Nacional de Saúde (CNSaúde) trouxe a público, no último dia 12 de março, o Código de Conduta dos Prestadores de Serviços de Saúde. Trata-se de um guia para auxiliar na observância à LGPD e construir boas práticas de forma geral no setor. Apresentado à Autoridade Nacional de Proteção de Dados (ANPD), o documento foi preparado pela Agência Nacional de Saúde (ANS) em conjunto com órgãos sanitários, hospitais, farmácias e doutrinadores em matéria de proteção de dados.

O código é um marco a ser seguido, verdadeira demonstração da possibilidade erigida pelo *caput* do artigo 50 da LGPD: *"Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança"*, regras essas que poderão ser reconhecidas e divulgadas pela ANPD (artigo 50, §3º, LGPD).

Nesse sentido, considerando que a CNSaúde é uma entidade sindical que representa os estabelecimentos de serviços de saúde no Brasil, o código estabelece diretrizes específicas, para além da norma geral consubstanciada na LGPD, para seguimento por todos os agentes do setor sanitário no tratamento de dados pessoais.

Além de uma primeira parte introdutória, que estabelece o panorama legislativo e alguns pressupostos teóricos da LGPD e da regulamentação setorial no setor de saúde, o código disciplina temas importantes para os participantes desse mercado, como, por exemplo: 1) ciclo de vida dos dados no setor de saúde; 2) âmbito de aplicação dos termos *"prestadores privados de serviço de saúde"*; 3) protocolo de atendimento; 4) definição de controlador/operador no tratamento de dados cadastrais, prontuários médicos e exames laboratoriais; 5) protocolo de compartilhamento; 6) compartilhamento de dados pessoais entre estabelecimentos de saúde; e 7) confluência entre as regulamentações do setor de saúde e de proteção de dados e a ação conjunta de suas respectivas agências reguladoras. Não há previsão de sanções específicas em caso de descumprimento do código.

Diante do exposto, o código representa importante iniciativa setorial que vem em momento bastante propício, diante da exposição do segmento de saúde a partir da pandemia da Covid-19. Além disso, a medida pode abrir caminho para outras de mesma natureza em outros setores, o que estimula e auxilia a aplicação efetiva, técnica e menos dolorosa da LGPD. Se entre os grandes desafios da LGPD estão a expectativa em servir de proteção contra incidentes de segurança e a previsão de normas gerais de difícil aplicação homogênea a diferentes mercados, guias setoriais, como o código, podem representar uma solução interessante e adequada.

[1] Nick Rossmann, líder de Inteligência de Ameaças Globais da IBM Security X-Force, comenta que: "Basicamente, a pandemia reformulou o que agora é considerado uma infraestrutura crítica e os invasores perceberam isso. Muitas organizações tiveram que ir pela primeira vez para a linha de frente em esforços de ajuda, seja para apoiar a pesquisa sobre Covid-19, dar suporte às cadeias de abastecimento de alimentos e vacinas ou produzir equipamentos de proteção individual. A vitimologia dos atacantes ia mudando conforme os acontecimentos relacionados à Covid-19 se desenrolavam, indicando mais uma vez a adaptabilidade, engenhosidade e persistência dos adversários do ciberespaço." Disponível em: https://www.ibm.com/blogs/ibm-comunica/ibm-security-ataques-ciberneticos/.

Date Created
10/04/2021