Joelsons e Marques: Incidentes de segurança da informação

Vivemos na era do *Big Data* [1], marcada pela coleta e compartilhamento de informações, onde os dados pessoais dos indivíduos adquirem grande valor. Com a valorização dos dados pessoais, surgiu a necessidade de regulação do setor, vindo a ser editada no Brasil a chamada Lei Geral de Proteção de

018, "LGPD").

Aliada a esta tendência, a pandemia da Codiv-19 alavancou o processo de migração das relações ao ambiente virtual, em especial, diante da instituição do modelo de trabalho remoto. No entanto, ainda que as tecnologias tenham trazido consigo grandes avanços, se tornou cada vez mais frequente a ocorrência de incidentes de segurança da informação envolvendo dados pessoais.

Não é raro, atualmente, ouvir-se falar que o *site* ou plataforma de determinada empresa está fora do ar, incluindo as maiores do mercado, e até mesmo que o sistema de órgãos do governo e tribunais foi comprometido devido a um incidente de segurança da informação.

Foi pensando nisso, que a LGPD, previu a segurança dos dados como um de seus princípios norteadores (artigo 6º, inciso VII) [2], estabelecendo alguns parâmetros a serem seguidos no tratamento dos dados pessoais, de modo a evitar que incidentes de segurança da informação ocorram e, caso ocorram, sejam remediados da melhor forma.

2023 - www.conjur.com.br - Todos os direitos reservados.

Assim, é importante levar-se em consideração que a Sociedade responsável pelo tratamento de dados deve instituir um plano preventivo de segurança, que envolve, mas não se limita, a implementação de programa de governança em privacidade; a nomeação de uma encarregado de dados ("DPO"); o mapeamento e a manutenção dos registros de operações de tratamento de dados pessoais; a avaliação dos riscos, incluindo a documentação em relatórios de impacto e realização de um planejamento para mitigação e implementação de melhorias relacionadas; contratação de *cyber insurance* para cobertura dos riscos conhecidos e não passiveis de eliminação*;* a designação prévia de comitês de crise, com a definição das respectivas responsabilidades de cada agente; a investigação prévia e homologação apenas de fornecedores e prestadores de serviços que estejam adequados à lei, com assinatura de contratos ou aditivos que estabeleçam as instruções e obrigações aos operadores; a instituição de mecanismos de segurança nos sistemas, abrangendo, inclusive, as práticas de *privacy by design*, *privacy by default* e a simulação de incidentes de segurança; além da disponibilização de treinamentos, visando não só qualificar os colaboradores, mas, também, conscientizá-los.

Neste ponto, importante frisar que a Autoridade Nacional de Proteção de Dados ("ANPD") ainda poderá regulamentar a matéria, instituindo ou alterando as medidas já previstas pela LGPD.

A respeito dos mecanismos de segurança, especificamente, tem-se que, segundo lecionam Fabiano Menke e Guilherme Goulart *"a segurança que se espera não é aplicada exatamente aos dados em si, mas sim aos sistemas que os mantêm (medidas técnicas) e ao ambiente geral da instituição (medidas organizativas). Isso significa que não bastam as medidas técnicas, como o uso de firewalls, métodos criptográficos e controles de conteúdo, se elas não vierem acompanhadas de outras medidas, como treinamentos de segurança, criação de políticas de segurança da informação, inventários de ativos etc"* [3].

Nesta perspectiva, um importante parâmetro existente para a manutenção da segurança dos sistemas é a certificação ISO 27001, que tem como objeto a disponibilização de requisitos para estabelecer, implementar, manter e melhorar, continuamente, um sistema de gestão de segurança da informação. Não obstante, ainda que referidas prática sejam adotadas, é possível que incidentes de segurança da informação ocorram.

Assim, a Sociedade que mantiver um plano preventivo consolidado, sairá na frente, visto que 1) poderá demonstrar à ANPD e outros órgãos regulatórios sua preocupação com a segurança dos dados pessoais e que continuamente adota medidas visando resguardar seus usuários; 2) em posse dos seus processos mapeados, conseguirá ter uma noção maior dos dados pessoais que foram comprometidos e o risco que o incidente pode oferecer aos titulares; e 3) já tendo estabelecidas as funções dos comitês de crise e seus respectivos agentes, poderá iniciar imediatamente o plano de contingência.

2023 - www.conjur.com.br - Todos os direitos reservados.

De qualquer forma, ocorrendo um incidente de segurança da informação, a Sociedade precisará pôr em prática planos de contenção, erradicação e restauração do ambiente, que demandam a elaboração e aplicação imediata de medidas técnicas e jurídicas que visem conter os riscos legais, comerciais e reputacionais da sociedade. Para tanto, a sociedade precisará do auxílio de um time interdisciplinar, que envolve a atuação de setores estratégicos da própria instituição, como diretoria, DPO e a área de TI, especialistas na seara de gestão de crise, perícia informática e/ou especialistas da plataforma e sistemas comprometidos, além de uma equipe jurídica especializada.

Assim, após o incidente ser contido, a Sociedade precisará analisar de forma cautelosa e detalhada quais foram as informações envolvidas no episódio, de modo a identificar a natureza e o volume dos dados comprometidos.

Verificando que os dados comprometidos tratam-se de dados pessoais, a Sociedade precisará fazer um estudo chamado *Data Breach Score*, de modo a apurar a gravidade e o risco oferecido aos titulares com o incidente de segurança. Para tanto, poderá ser utilizada a metodologia da *European Union Agency for Network* and Information Security (Enisa) [4] para avaliação da gravidade das violações de dados pessoais, enquanto a ANPD não disponibilizar recomendações próprias para o Brasil.

A partir desse estudo, será avaliada a necessidade de comunicação dos titulares, ANPD e demais órgãos regulatórios como Procon, Senacom, CVM e Bacen acerca do incidente de segurança. Isso porque, conforme a própria LGPD estabelece, apenas, os incidentes de segurança relevantes devem ser comunicados (artigo 48), no prazo recomendado pela ANPD de até dois dias úteis contados a partir da data do conhecimento do evento.

Paralelamente a este estudo, deverão ser adotadas medidas para preservação das evidências do incidente, através de mecanismos como a ata notarial [5] e o *blockchain* [6], realizando-se, inclusive, uma cópia do ambiente comprometido, de modo que este possa ser restabelecido e, ao mesmo tempo, permita-se a condução das investigações para a identificação dos agentes causadores do incidente e consequente responsabilização destes.

Tratando sobre as investigações, é importante que se mantenha um monitoramento tanto na *surface web* quanto na *deep web e dark web*, para que a Sociedade acompanhe a repercussão do incidente. Em aditivo, é recomendável a elaboração de um estudo técnico e de investigação detalhada do incidente, de modo que referido documento sirva não só para as investigações, mas, também, para que a Sociedade identifique eventuais falhas de segurança existentes e possa corrigi-las [7]. Por fim, é valioso avaliar-se a necessidade de lavratura de boletim de ocorrência ou elaboração de pedido de instauração de inquérito policial, como medida de *compliance* e prova positiva para as Sociedades, que também servem como mecanismos de contribuição para as investigações.

Referidas recomendações não são um rol fechado de medidas básicas a serem adotadas pelas Sociedades, mesmo porque, as práticas costumam ser alteradas ao longo dos tempos, mas são parâmetros importantes a serem seguidos pelas Sociedades, capazes de prevenir, mitigar e remediar os riscos a que se submete cada organização [8].

2023 - www.conjur.com.br - Todos os direitos reservados.

Por fim, sublinha-se que a transformação na postura do mercado, que está atento às Sociedades que sofrem incidentes de segurança e não conseguem obter respostas efetivas e adequadas, tampouco demonstrar minimamente sua aderência a programas de governança em privacidade, constitui também uma chave importante para que todos os *players* compreendam a importância de tais medidas e invistam atenção e recursos necessários para adequação à LGPD.

[1] GOODMAN, Marc. *Future Crimes*: Tudo está conectado, todos somos vulneráveis e o que podemos fazer sobre isso. São Paulo: HSM Editora, 2015. p. 91 – 92.

[2] CARVALHO, Angelo Prata de. O papel da estratégia de segurança da informação nos mecanismos de compliance de dados: em busca de uma abordagem integrada. In CUEVA, Ricardo Villas Bôas. FRAZÃO, Ana. (coord.) Compliance e política de proteção de dados. São Paulo: Thomson Reuters Brasil, 2021. (*E-book*).

[3] MENKE, Fabiano; GOULART, Guilherme. Segurança da informação e vazamento de dados. In: MENDES, Laura Schertel et al. (coord.) Tratado de proteção de dados pessoais. Rio de Janeiro: Forense, 2021. (*E-book*).

[4] *European Union Agency for Network and Information Security*. December 20, 2013. Disponível em: https://www.enisa.europa.eu/publications/dbn-severity. Acesso em: 14 abr. 2022.

[5] *"Trata-se de documento público, lavrado por tabelião de notas, nos termos do artigo 7º, III da Lei Federal 8.935/1994, que tem a finalidade de constatar a existência ou o estado de coisas, pessoas e outros objetos, com a presunção de verdade típica dos documentos públicos. Nela, o tabelião descreve os fatos que presencia, tanto no recinto interno como em local externo à serventia, ou ainda, em ambiente virtual, atribuindo fé pública àquilo que constatar. Atualmente, com o desenvolvimento da tecnologia, grande parte das relações sociais, negociações comerciais, ou mesmo interações com o Estado, se estabelecem por meio eletrônico. Nesse contexto, vê-se renovada a importância da ata notarial".* (WAMBIER, Luiz Rodrigues; WAMBIER, Tereza Arruda Alvim (Coords.). Provas. Temas Essenciais do Novo CPC: análise das principais alterações do Sistema Processual Civil Brasileiro. São Paulo: Revista dos Tribunais, 2016. p. 227).

[6] *"O blockchain, é descrito como um 'livro-razão distribuído', um protocolo seguro no qual uma rede de computadores verifica de forma coletiva uma transação antes de registrá-la e aprová-la. A tecnologia que sustenta o blockchain cria confiança, permitindo que pessoas que não o conheçam (e, portanto, não têm nenhuma base subjacente de confiança) colaborem sem ter de passar por uma autoridade central neutra —*

2023 - www.conjur.com.br - Todos os direitos reservados.

ou seja, um depositário ou livro contábil central. Em essência, o blockchain é um livro contábil compartilhável, programável, criptograficamente seguro e, portanto, confiável; ele não é controlado por nenhum usuário único, mas pode ser inspecionado por todos". (SCHWAB, Klaus. *A quarta revolução industrial*. São Paulo: Edipro, 2018. p. 28-29).

[7] JIMENE, Camilla do Vale. TAMER, Maurício Antonio. Plano de Resposta a Incidentes de Segurança de Dados Pessoais In OPICE BLUM, Renato. VAINZOF, Rony. MORAES, Henrique Fabretti. Data Protection Officer (encarregado) (coords.), São Paulo: Thomson Reuters Brasil, 2020. (*E-book*).

[8] CARVALHO, Angelo Prata de. O papel da estratégia de segurança da informação nos mecanismos de compliance de dados: em busca de uma abordagem integrada. In CUEVA, Ricardo Villas Bôas. FRAZÃO, Ana. (coord.) Compliance e política de proteção de dados. São Paulo: Thomson Reuters Brasil, 2021. (*E-book).*

Date Created
09/05/2022

2023 - www.conjur.com.br - Todos os direitos reservados.