O QUE FAZER DIANTE DE UM INCIDENTE DE SEGURANÇA EM DADOS PESSOAIS?

Vinícius Pena dos Santos*
Danyella Nunes de Souza Marques**

Há alguns anos, os ataques e mais variadas práticas ilícitas cometidas pela internet crescem considerável e constantemente. No entanto, a pandemia da Covid-19 e o consequente isolamento social que impulsionou ou propiciou que inúmeras organizações implementassem o trabalho remoto pela primeira vez possibilitaram que o fenômeno social se expandisse. Diante da nova realidade, pessoas mal-intencionadas, infelizmente, se aproveitam da maior vulnerabilidade das redes para intensificar suas atividades.

A preocupação em segurança da informação e programas de governança justificadamente também aumentaram. No entanto, mesmo com a adoção de inúmeras medidas preventivas cabíveis, é possível qualquer organização, seja ela estatal ou não, continue exposta a um incidente de segurança em dados pessoais. Como agir então?

Afinal, o que é um incidente de segurança para a LGPD?

Para fins legais, o incidente de segurança é o "o acontecimento indesejado ou inesperado que seja hábil a comprometer a segurança dos dados pessoais, de modo a expô-los a acessos não autorizados e a situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito" (JIMENE; TAMER, 2020).

Sob tal perspectiva, pode-se dizer que um plano de resposta a incidentes de segurança deve ser voltado a lidar com qualquer situação que exponha os dados pessoais às situações acima descritas e integrantes de tal conceito.

Como acontece normalmente?

Ao contrário do que o senso comum pode indicar, os incidentes de segurança da informação dentro de empresas ou organizações são corriqueiros e podem, inclusive,

chegar a centenas de milhares por dia, a depender do porte da entidade. A perda de um *pen drive*, o furto de um *notebook*, a interrupção de acesso a um sistema são situações, do ponto de vista técnico, que podem ser consideradas incidentes de segurança, uma vez que a informação corporativa estará exposta a uma ameaça.

Contudo, muitos dos casos sequer envolvem dados pessoais ou, mesmo que envolvam, não configurariam uma ocorrência que possa propiciar problemas aos titulares. Vale lembrar que a "LGPD estabeleceu em seu artigo 48 o dever do controlador de comunicar a ocorrência de incidente de segurança para a ANPD e para o titular dos dados pessoais, porém limitou àqueles que possam acarretar risco de dano ou dano relevante aos titulares" (JIMENE; TAMER, 2020).

Outros, porém, já ocorrem com todos os elementos de preocupação e gravidades para o dia a dia da empresa, por exemplo, quando esta se vê diante de uma mensagem mencionando a criptografia de todos os seus servidores, cuja liberação fica condicionada ao pagamento de um resgate em valor financeiro, normalmente em criptoativos (na maioria das vezes, em *bitcoin*).

Além das exigências trazidas pela LGPD, algumas outras normas exigem a comunicação do incidente aos respectivos órgãos competentes a depender de algumas condições, sem negar a existência de riscos reputacionais e à imagem, o que requer das empresas atuação diligente diante de um evento dessa natureza.

Resposta a um incidente de segurança da informação

O avanço tecnológico e a automatização das relações sociais naturalmente pressupõem que nenhuma empresa ou organização está imune a tais situações. Em que pese o crescente investimento em tecnologia e segurança da informação, além da ampla difusão de medidas preventivas – o mapeamento e a manutenção dos registros de operações de tratamento de dados pessoais, a designação prévia de funções e comitê de crise, a homologação de fornecedores, a contratação de *cyber insurance* e até a simulação de incidente de segurança –, um incidente pode ocorrer. Portanto, é imprescindível saber como agir diante do episódio.

Por sua gravidade, um incidente de segurança da informação, demanda a elaboração e aplicação imediata de medidas técnicas e jurídicas que visem conter os riscos legais, comerciais e reputacionais da empresa ou organização, pois "a ausência ou o atraso na resposta ao incidente não só implica a desconformidade com as normas de proteção de dados pessoais (*GDPR* e LGPD), como o tempo e a qualidade da resposta

ao incidente em segurança em dados pessoais são critérios legais a serem considerados quando da aplicação da sanção pela autoridade competente"(JIMENE; TAMER, 2020).

Mapeamento dos dados

O conjunto de medidas, céleres e eficientes, se iniciam com a identificação dos dados vinculados ao incidente. A empresa ou organização precisa analisar, cautelosa e detalhadamente, quais foram as informações envolvidas no episódio[1]: mapear se os dados compõem ou não a sua base de dados ou, no caso do controlador, se certificar de que não tenha tratado os dados pessoais de nenhuma forma.

Subsequentemente, deve verificar se os dados do incidente são ou não caracterizados como dados pessoais. Caso as informações estejam relacionadas à pessoa natural identificada ou identificável (art. 5º, I, LGPD), aplica-se a LGPD. Em caso negativo, afasta-se sua incidência.

Elaboração de *data breach score*

Em ocorrendo o vazamento de dados relacionados a pessoas naturais identificadas ou identificáveis, faz-se necessária a elaboração do chamado *data breach score*, para a apuração da gravidade dos dados envolvidos. O documento, específico e direcionado à sinalização de criticidade e gravidade do evento, permite que a organização entenda melhor os riscos aos quais está sujeita, possibilitando uma melhor compreensão do tratamento que deverá dar à comunicação com os titulares dos dados vazados e autoridades competentes.

Confecção de parecer técnico e de investigação

A partir da percepção do incidente, também é recomendável a elaboração de estudo técnico e de investigação detalhada. O desenvolvimento dos mesmos não possui como objetivo "apenas a identificação e coleta de evidências técnicas necessárias à formatação de prova sobre o incidente, mas principalmente para a extração de relatório circunstanciado que aponte eventuais falhas de segurança que permitiram ou contribuíram com a ocorrência do incidente" (JIMENE; TAMER, 2020). O documento, do ponto de vista técnico, pode direcionar as correções necessárias, fundamentais

[1] De acordo com JIMENE e TAMER (2020), caso o controlador tenha feito a coleta, mas o incidente seja relacionado à base de operador, remanesce a responsabilidade de ambos em relação ao incidente.

para que a organização evolua em relação às boas práticas de governança em privacidade.

Monitoramento na *surface web*, *deep web* e *dark web*

A pesquisa tanto na *surface web* quanto na *deep web e dark web* constitui medida importante para que a organização acompanhe a repercussão do incidente, entenda os riscos atrelados e, eventualmente, identifique algum elemento de prova importante para certificar a origem do episódio ou sua autoria.

Por meio do referido monitoramento, é possível adotar medidas para "remoção de conteúdo do ar, como por exemplo, bases de dados que foram alvo de vazamento, a fim de minimizar a exposição indevida de dados pessoais e eventual aproveitamento por terceiros para fins criminosos" (JIMENE; TAMER, 2020).

Além disso, será possível verificar se algum dado foi exposto não só para aferição da existência ou inexistência de danos, sua quantificação e mesmo identificação de algum indício adicional de investigação dos eventuais responsáveis pelo evento.

Comunicações

Ainda, é importante pensar na comunicação aos titulares dos dados envolvidos e órgãos competentes, a depender da atividade econômica desempenhada pela empresa, sua localização e de eventuais filiais, além do tipo de evento sofrido e da sensibilidade de eventuais dados.

Atualmente, existem algumas normas que exigem a comunicação obrigatória das autoridades competentes no Brasil, como a instrução nº 612/2019 da Comissão de Valores Mobiliários e a Resolução nº 4.658/2018 do Banco Central do Brasil. Além disso, caso a empresa possua dados no território da União Europeia, já que tem o livre arbítrio de escolher o local de armazenamento, deverá obedecer ao artigo 33 da *General Data Protection Regulation* (GDPR), comunicando o incidente.

Também é muito importante que se atendam às disposições normativas que versam sobre a comunicação do incidente, sob pena de aplicação de sanções em face da empresa. "Diante de incidentes que possam acarretar risco ou danos relevantes aos titulares, cumpre ao controlador comunicar à ANPD e ao titular do dado pessoal, de modo que tal situação deve também estar prevista em um plano de resposta a incidentes. Lembra-se, inclusive, que a não comunicação pode ser considerada, em si, um descumprimento à Lei, podendo resultar na aplicação das sanções administrativas

previstas em seu art. 52. Assim, em um exemplo hipotético, poderia incorrer o controlador em duas infrações à Lei em razão de um incidente só, uma pelo próprio incidente (se esse se deu por violação aos preceitos legais) e uma decorrente da não comunicação (JIMENE; TAMER, 2020).

Coleta das provas digitais e a identificação dos responsáveis pelo ilícito

Descobrir as causas do incidente e seus responsáveis, ou ao menos tentar, pode não ser uma das tarefas mais simples. No entanto, mesmo que essa tentativa não tenha êxito, fazer prova positiva da diligência da organização e da investigação realizada é providência que por si demonstra o compromisso da organização em tratar com o incidente e até minimizar eventuais e possíveis responsabilizações civis e administrativas. Afinal, "tão grave quanto o incidente em si, é a organização desprezá-lo" (JIMENE; TAMER, 2020).

Uma vez localizado algum registro eletrônico (números de *IP*, datas e horas) - por exemplo, nos servidores da organização -, é possível, com base no que dispõe a legislação vigente aplicável, especialmente o Marco Civil da Internet, ajuizar medidas cíveis em face dos provedores de aplicação, visando identificar os provedores responsáveis por fornecer o serviço de conexão à internet a determinados usuários.

As medidas judiciais podem ser úteis tanto para a responsabilização extracontratual ou contratual dos envolvidos no incidente – podem ser responsabilizados tanto os usuários responsáveis pelo incidente, como eventuais empresas parceiras da organização por descumprimento de alguma cláusula contratual, em caso de contratos entre controladores e operadores de dados pessoais em que, estes últimos, embora haja previsão contratual, falham na estruturação dos mecanismos de segurança necessários (JIMENE; TAMER, 2020) - quanto para a responsabilização criminal do usuário responsável após a apresentação de um Pedido de Instauração de Inquérito Policial.

Lavratura de Boletim de Ocorrência ou elaboração de Pedido de Instauração de Inquérito Policial, como medida de *compliance* e prova positiva para as empresas

Registrar uma ocorrência, visando à lavratura de um Boletim de Ocorrência ou, após a realização das medidas elencadas acima, apresentar um Pedido de Instauração de Inquérito Policial visam à mesma consequência jurídica para a organização e perante

a sociedade: a instauração de um procedimento investigatório preliminar, o Inquérito Policial. A diferença entre a adoção de uma ou outra estratégia está no lapso temporal que os pedidos poderão ser apresentados.

No primeiro caso, pode-se lavrar a ocorrência nos primeiros dias após a identificação do incidente, já que constitui uma comunicação prévia e sem maiores subsídios técnicos, apenas e tendo como grande objetivo posicionar a empresa como vítima do evento.

No segundo, contudo, caso haja identificação de registros eletrônicos, por exemplo, é aconselhável apresentar o pedido após o ajuizamento da ação civil de quebra de sigilo. Isso porque, em que pesem os pedidos que constem na ação possam ser realizados pela Autoridade Policial competente, entraves administrativos de toda ordem podem prejudicar a efetividade das medidas adotadas.

Independente da providência adotada, ambas são medidas e circunstâncias que, pela própria natureza, devem tramitar em sigilo. No entanto, sempre há chance, ainda que remota, do caso ganhar alguma repercussão além da organização. Ainda, os crimes em potencial, por circunstâncias legais, muito dificilmente resultarão na realização de prisões cautelares ou definitivas dos envolvidos.

No entanto, a comunicação dos fatos à Autoridade Policial competente é uma possibilidade a ser cogitada porque:

(i) há a concreta possibilidade de identificação de outros elementos de prova a indicar a prática dos crimes esperados;

(ii) caso algum procedimento administrativo seja instaurado visando apurar os fatos, a comunicação nesse sentido demonstra o que a empresa fez para apurar os fatos, o quão diligente se demonstrou e pode mitigar riscos reputacionais e jurídicos;

(iii) é prova positiva de alta relevância para a empresa, que visa concretizar as melhores práticas de governança e *compliance* adotadas;

(iv) a experiência prática em casos semelhantes tem demonstrado que a atuação das empresas na persecução criminal tem resultados didáticos e de conformidade claros interna e externamente, que resulta na diminuição de riscos de segurança de todas as ordens; e

(v) além de ser medida de conclusão importante de todos os esforços e investimentos dedicados ao incidente.

Relatório de providências adotadas e revisão do Programas de Governança em Privacidade

Também é válido incluir entre as providências a elaboração de um relatório circunstanciado que detalhe os resultados identificados, a fim de que a empresa adote as medidas necessárias para a prevenção de novos episódios envolvendo vulnerabilidades tecnológicas. Esse documento tem como objetivos:

(i) permitir que o incidente e as providências adotadas fiquem registrados. Com isso, poderá a organização demonstrar, sobretudo para a fiscalização administrativa ou de procedimento extrajudicial (inquérito civil público) ou judicial (coletivo ou individual do titular do dado pessoal) que respondeu ao incidente em prazo razoável;

(ii) gerar um documento para a organização no sentido de viabilizar, futuramente, que essa consiga avaliar os episódios que teve no passado e traçar uma linha evolutiva ou gráfica em direção aos altos níveis de maturidade em privacidade ou, se não for o caso, para que a organização identifique as possíveis causas de estagnação ou queda nos patamares de privacidade. Essas linhas históricas documentadas também serão importantes como provas positivas no caso de fiscalização, mencionado acima; e

(iii) a documentação do incidente e das providências adotadas permite e facilita, no caso de apuração de falhas, que o programa de privacidade seja revisado e alterado, se for o caso (JIMENE; TAMER, 2020).

Conclusão

A ampla difusão tecnológica e a impossibilidade de proteger em sua completude um sistema informático ou determinada rede fazem com que incidentes de segurança em dados pessoais sejam cada vez mais frequentes. Contudo, mais do que realizar a maior quantidade de medidas preventivas para evitar sua ocorrência, é necessário traçar um plano de contenção a seus riscos. Um plano eficiente e organizado deve estabelecer os papeis e responsabilidades de cada sujeito, dispor as medidas que deverão ser executadas e de forma coordenada. Apenas dessa forma é possível diminuir os impactos, retificar a crise e reparar eventuais vulnerabilidades, de modo que dificulte a ocorrência de outros incidentes no futuro.

Referência bibliográfica

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.

*** *Vinícius Pena dos Santos*** *é graduado em Direito pela Universidade Presbiteriana Mackenzie (2019) é advogado do escritório Opice Blum, Bruno, Abrusio e Vainzof Advogados Associados.*

**** *Danyella Nunes de Souza Marques é*** *graduanda em Direito pela Universidade Presbiteriana Mackenzie é estagiária do escritório Opice Blum, Bruno, Abrusio e Vainzof Advogados Associados.*