A LGPD e o vazamento de dados pessoais na empresa: o que fazer e como agir para minimizar danos?

A Lei Geral de Proteção de Dados (Lei nº 13.709/2018), em vigor desde setembro de 2020, impõe importantes direitos aos titulares de dados pessoais, bem como deveres aos agentes de tratamento que, nas suas atividades, manipulem dados pessoais.

Segundo o relatório "Prejuízo de um vazamento de dados", realizado pelo Ponemon Institute em parceria com IBM Security, o prejuízo total médio de um vazamento de dados aumentou 10% desde 2014, sendo o tempo médio para detectar e conter um vazamento de dados é de 280 dias e 315 dias quando for por um ataque mal-intencionado.

Nesse cenário, a responsabilidade para com a segurança da informação, já prevista em guidelines, normas e melhores práticas antes da LGPD, foi reforçada com os regulamentos que protegem dados pessoais, merecendo cada vez mais atenção.

São exemplos de importantes normas relacionadas à segurança da informação:

– a norma ABNT ISO/IEC NBR 27001:2013 que estabelece requisitos para o sistema de gestão da segurança da informação (SGSI);

– a norma ABNT ISO/IEC NBR 27002:2013, que prevê controles de segurança da informação e, recentemente, receberam a extensão dos requisitos e diretrizes específicos para controladores e operadores, trazidos pela norma ABNT ISO/IEC NBR 27701:2020, que dispõe acerca do Sistema de Gestão da Privacidade da Informação (SGPI).

Deste modo, a segurança da informação, destinada à proteção das dimensões envolvendo confidencialidade, integridade, disponibilidade e demais atributos da informação, também considera as especificidades envolvendo dados pessoais, razão pela qual a proteção da informação abrange não apenas dados corporativos ou classificados com críticos e confidenciais, mas também, dados ligados à pessoas naturais.

A segurança da informação é elevada ao *status* de um princípio na LGPD, envolvendo a utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas, relacionadas à destruição, perda, alteração, comunicação ou difusão.

Do mesmo modo, estabelece a LGPD que um tratamento de dados irregular não é somente aquele que não observa a legislação, mas, principalmente, aquele que não fornece a segurança que dele se pode esperar, considerando padrões e práticas aplicáveis à época do tratamento.

Nesta linha, agentes de tratamento responderão por danos decorrentes da violação de segurança quando não adotarem medidas físicas, técnicas e organizativas aptas a proteger dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

Assim, se antes, controladores e operadores poderiam assumir o risco de omitir uma vulnerabilidade explorada ou um incidente que envolvesse dados pessoais, em um cenário de normas de proteção de dados e maior conscientização, a omissão ou a descoberta por outras fontes pode ser catastrófica ao negócio.

Se o incidente envolve riscos aos titulares de dados, procedimentos ágeis devem ser executados em um processo claro,

definido e testado previamente, com colaboradores responsáveis, conscientes de seu papel para a estrutura de governança de dados da organização e capacitados tecnicamente para conter um incidente de segurança.

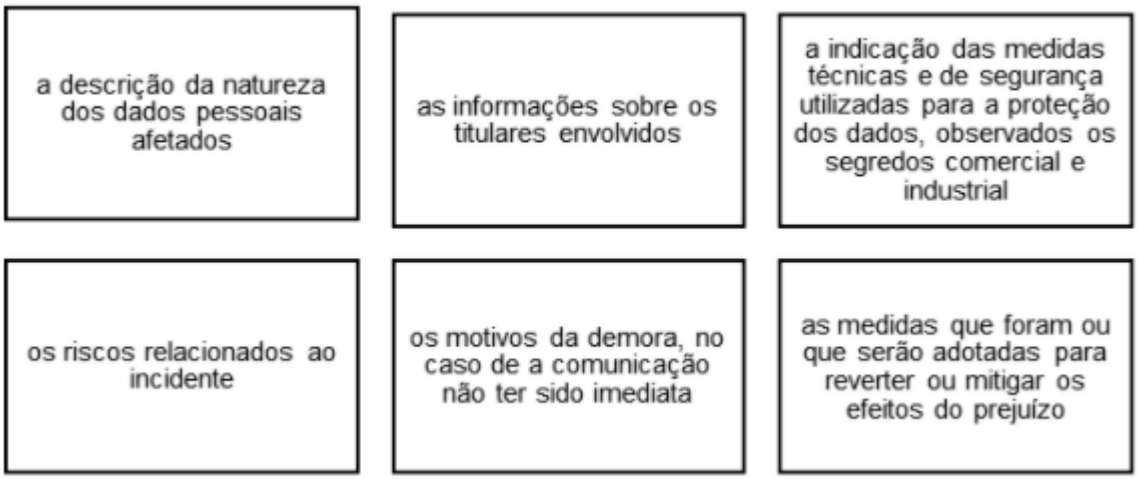
Se minha empresa teve dados pessoais vazados, o que é preciso fazer?

De início, cumpre esclarecer que, após a confirmação, conforme o art. 48 da LGPD, o controlador deverá comunicar à Autoridade Nacional de Proteção de Dados (ANPD) e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.

Em tese, se não envolve risco ou dano relevante aos titulares, a comunicação não seria necessária. Recomenda-se que esta avaliação seja feita por consultoria e perícia forense digital independente em conjunto com o time interno, capaz de compreender a dimensão do ataque, vulnerabilidade explorada, medidas preventivas ou reativas acionadas e, então, ponderar pelo risco ou não aos titulares.

Nesse cenário, o DPO (*Data Protection Officer*) assume papel consultivo, pois a autonomia e independência são inerentes a sua função, zelando pelo melhor interesse do titular de dados e, como canal de comunicação, ser o elo entre a empresa, os titulares de dados e a Autoridade Nacional de Proteção de Dados (ANPD).

Por sua vez, caso o ataque ou vazamento de dados proporcione risco ou dano relevante aos titulares, a comunicação à ANPD e aos titulares de dados ou clientes deverá conter, no mínimo:



Resta evidente que, se a empresa não estabelecer um processo claro para resposta a incidentes, terá dificuldades de tomar a decisão sobre incidentes com dados pessoais, sobre comunicar ou não, bem como em levantar as informações detalhadas do ocorrido, sobretudo se a exploração se deu em ambiente de um operador ou controlador conjunto.

Nessas situações, poderá ocorrer a aplicação de penalidades, inclusive multas, lembrando que, no juízo de gravidade do incidente, será avaliada eventual comprovação de que foram adotadas medidas técnicas adequadas que tornem os dados pessoais afetados ininteligíveis, com o intuito de terceiros não autorizados acessá-los.

Nesse contexto, vale destacar que a perícia digital em questões envolvendo dados pessoais pode contribuir no processo de resposta a incidentes, não só para coleta de evidências e manutenção da cadeia de custódia, mas para identificar a extensão dos danos e se envolvem dados pessoais, apurando o possível *modus operandi* e a autoria.

Assim, é preciso compreender que um Sistema de Gestão de Proteção de Dados compõe-se de uma série de processos, práticas e ações para que a empresa demonstre conformidade com normas e práticas de proteção de dados, inclusive no atendimento do princípio da responsabilização e prestação de contas (art. 6º, X).

A gestão de incidentes de segurança da informação é diretriz prevista na ABNT ISO/IEC NBR 27002 e que agora é atualizada com diretrizes adicionais na seção 6.13 da ABNT ISO/IEC NBR 27701. Além disso, há a norma ABNT ISO/IEC NBR 27.035 que é específica para resposta a incidentes e a norma ABNT ISO/IEC NBR 29.151 que estabelece objetivos de controle, controles e diretrizes para a implementação de controles, a fim de atender aos requisitos identificados por uma avaliação de risco e impacto relacionada à proteção de informações pessoalmente identificáveis.

"Como parte do processo de gestão de incidentes de segurança da informação global, convém que a organização estabeleça responsabilidades e procedimentos para identificação e registros de violações de DP. Adicionalmente, convém que a organização estabeleça responsabilidades e procedimentos relativos à notificação para as partes envolvidas nas violações de DP (incluindo o tempo de tais notificações e à divulgação para as autoridades, levando em conta a regulamentação e/ou legislação aplicadas" (ABNT, 2019, p.28)".

Vale notar que, como parte dos processos de gestão de incidentes, é muito importante que a empresa defina papéis e responsabilidades, além de procedimentos para identificação e registro de violações de dados pessoais, mantendo inclusive procedimentos para notificação das partes envolvidas e divulgação às autoridades, além do desenvolvimento de uma análise crítica dos sistemas de Tecnologia da Informação e Comunicação (TIC).

A violação a dados poderá ter ocorrido em um operador de dados pessoais, um contratado, terceirizado, prestador de TI etc. Nestes casos, é fundamental que o controlador estabeleça, também, de forma preventiva, cláusulas contratuais que disciplinam como o operador irá fornecer informações necessárias ao controlador para que este possa cumprir com suas obrigações e prazos diante de um incidente constatado.

Em todos os casos, a resposta adequada ao incidente, coleta de evidências e a perícia digital são essenciais, sobretudo para se evitar responsabilizações, considerando que, conforme disposto na LGPD, os agentes de tratamento não serão responsabilizados quando provarem, por exemplo, que os dados vazados não pertencem à empresa, não houve violação à legislação, ou quando provarem que os danos decorreram de culpa exclusiva do titular, como nos casos em que o titular é enganado por fraudador, que captura seus dados pessoais e credenciais de acesso ou mesmo senhas bancárias e dados de cartão de crédito. São questões que a perícia técnica, interna ou externa, poderá identificar e detalhar nas apurações.

Respostas a incidentes: orientações basilares

Em síntese, ao tratarmos de respostas a incidentes que exponham dados pessoais de clientes, temos que ter em mente as seguintes orientações:

1. Mantenha um processo/plano claro para lidar com incidentes, considerando a LGPD e regulamentos de privacidade em vigor, definindo papéis e responsabilidades dos atores envolvidos;
2. Certifique-se que os agentes de tratamento assinaram cláusulas contratuais específicas se comprometendo com a segurança dos dados e a colaboração quando da ocorrência de incidentes;
3. Realize a simulação de incidentes de segurança, ao menos uma vez ao ano, para verificar a maturidade do processo, a velocidade da resposta, gestores envolvidos, preservação das evidências e se demais tarefas são corretamente executadas. Com o teste do seu plano de resposta a incidentes será possível otimizar a capacidade de conter, mitigar e restabelecer os sistemas de forma ágil e eficaz;
4. Invista em programas de governança, gerenciamento de riscos e conformidade;
5. Incentive terceiros, colaboradores e usuários a

notificarem qualquer suspeita pelos canais apropriados. Divulgue, ostensivamente, os canais apropriados;

6. Nesta linha, mantenha um ponto de contato online para que as pessoas possam notificar a suspeita de incidentes de segurança da informação ou com dados pessoais. Um exemplo interessante é o site da Apple, que disponibiliza uma página para que pessoas possam denunciar possíveis vulnerabilidades *"Se você acredita que tenha descoberto uma vulnerabilidade de segurança ou privacidade em um produto Apple, relate-o para nós."* (https://support.apple.com/pt-br/HT201220). Na página existe um procedimento claro para relato das vulnerabilidades e como a Apple trata a questão internamente. Desenvolva algo neste sentido. Muitas empresas não possuem canais, o que encoraja pessoas a encaminharem a descoberta de uma vulnerabilidade para outras empresas, como imprensa, associações de defesa de titulares de dados e terceiros. Tenha em mente que é sempre bom que você saiba primeiro de um problema com seus sistemas.
7. Realize testes de intrusão (*pentests*) constantemente, teste também a eficácia de mecanismos de pseudonimização e anonimização, e mantenha abertos contatos e canais para notificações de vulnerabilidades por pesquisadores e profissionais;
8. Em casos de incidentes, realize uma perícia ou auditoria digital nos ambientes para identificar a extensão do dano e o comprometimento a dados pessoais, bem como se é o caso de comunicação a titulares e ANPD ou não. DPOs e Comitês de Proteção de Dados podem se embasar nestes documentos para a correta tomada de decisões. Se os *datasets* foram publicados na Internet, realize uma perícia comparativa, para apurar se efetivamente vieram de seus sistemas ou não e a possível autoria.
9. Se a violação se deu em terceiros ou operadores, faça valer o contrato ou acordo de processamento de dados, e requeira todas as informações e evidências (caso já não

tenha sido informado), para que possa notificar as autoridades e os titulares de dados (se for o caso). Requeira informações sobre a investigação e elementos já identificados pelo operador, em detalhes;

10. Em todos os casos, preserve as evidências adequadamente, considerando melhores práticas, incluindo ABNT ISO/IEC NBR 27037. Lembre-se que medidas de resposta adequadas podem significar a demonstração do comprometimento da organização e evitar mais danos e responsabilizações.

O que deve conter em um processo de resposta a incidentes de segurança da informação?

Como visto até aqui, sem um processo de resposta a incidentes prévio e definido empresas terão problemas com incidentes envolvendo dados. Um processo de resposta a incidentes de segurança da informação visa documentar os passos a serem seguidos quando do incidente e precisa conter, no mínimo:

– A equipe de resposta a incidentes: a declaração das pessoas responsáveis pela área na empresa que irá avaliar a situação, discutir as medidas a serem adotadas e produzir os relatórios necessários;

– Quem será a primeira pessoa a ser comunicada quando do incidente de segurança;

– Procedimentos a serem adotados antes, durante e após o incidente de segurança;

– Medidas adotadas pelo DPO para comunicar os titulares e a ANPD, além dos requisitos da comunicação;

– Elaboração de relatórios e documentos que demonstrem a adoção de medidas para evitar o incidente de segurança e, se houver, o que foi feito;

– Procedimentos de simulação de incidentes de segurança para verificar os riscos e mitigá-los.

– Aprendizado com o incidente de segurança da informação.

Considere, para estruturação de um processo de resposta a incidentes, as disposições da diretriz 6.13.1.5 da norma ISO 27701.

E caso tenha encontrado falhas ou vulnerabilidades em sistemas de empresas e que expõem dados pessoais?

Pode ser (aliás, quase sempre acontece), no entanto, que quem descobriu a vulnerabilidade não foi o controlador, mas um terceiro, pesquisador, analista, hacker, pessoa física, outra empresa etc. Muitas dúvidas surgem neste caso, sobretudo no que diz respeito a qual metodologia seguir.

Infelizmente, muitas empresas, informadas por terceiros de que são vulneráveis, acabam por processar criminalmente o notificante, o que incentiva que estes não a notifiquem e acabem dando destinação diversa ao encontrado, até mesmo encaminhando para a mídia.

Em tempos de LGPD, não serão incomuns as notificações à imprensa de vazamento de dados, sobretudo quando controladores não possuem canal de notificação ou ignoram avisos e mensagens

de pessoas (quando as trata como criminosas). Os danos para as empresas serão imensos, pois como esta será vista quando uma vulnerabilidade, que expõe dados pessoais, é descoberta antes pela mídia ou terceiros?

Para pessoas e pesquisadores que encontram vulnerabilidades e exposição de dados pessoais em plataformas, algumas recomendações:

1. Registre a vulnerabilidade com metadados, documentando como é explorada, e quais os riscos. Se for algo exposto (sem necessidade de exploração, disponível ou facilmente acessível), também documente e sendo o caso registre uma ata notarial. Demonstre sempre a finalidade de contribuir e não de explorar a falha e que não avançou na cópia dos dados, adulteração ou exclusão de dados pessoais;
2. Evite fazer *dump,* copiar ou disponibilizar os dados pessoais e demonstre isso claramente em sua notificação. Avalie como demonstrar a vulnerabilidade de modo menos invasivo possível.
3. Não é recomendável condicionar o fornecimento de "maiores detalhes da vulnerabilidade" à contratação de serviços de correção da mesma. Este fato pode ser mal interpretado pela empresa/controlador, que poderá iniciar um processo judicial ou criminal.
4. Busque os canais oficiais de notificação, e sempre dê ciência a uma testemunha sobre a descoberta da vulnerabilidade e sua finalidade na pesquisa.
5. Caso seja ignorado, pode ser que a empresa queira "acobertar" o vazamento, prejudicando cidadãos e titulares. Neste caso, considere encaminhar a questão à ANPD e às autoridades de aplicação de Lei.
6. Caso não tenha sido ignorado e a empresa esteja tratando a notificação, é importante observar como lidará com o incidente e se efetivamente irá fazer os comunicados aos titulares e autoridade. Acompanhe de perto e diante de

omissões, considere comunicar a ANPD ou autoridades competentes.

Infelizmente, apesar de todas as medidas de proteção dos pesquisadores, nunca saberemos como o controlador poderá reagir a um comunicado de vulnerabilidade e vazamento de dados pessoais que trata..

Inúmeros casos ocorrem onde pesquisadores foram considerados infratores, pelo fato de dar-lhes ciência de uma vulnerabilidade, com uma simples prova, mesmo sem terem comercializado ou disponibilizado dados, mesmo sem pedirem nada em troca. Alguns pesquisadores, inclusive, registram Boletim de Ocorrência ou iniciam o processo de notificação assistidos por advogados especialistas em direito digital, antes de informarem e notificarem a falha, como uma tentativa de se protegerem de processos reflexos e interpretações errôneas.

Conclusões

Não negligencie. Todas as empresas estão sujeitas a ataques e incidentes que exponham dados pessoais. Por isso, um Sistema de Gestão da Privacidade da Informação implantado e mantido atualizado e efetivo pode cooperar para que a empresa reduza ou mitigue os riscos de eventual incidente de segurança, adotando controles e medidas técnicas e administrativas preventivas.

Do mesmo modo, um processo claro de resposta a incidentes envolvendo dados pessoais, como visto, não só demonstra *compliance*, mas, poderá, em casos concretos, minimizar os riscos de danos aos controladores e, principalmente, aos titulares de dados.

Foram vazados dados da sua empresa? Aja corretamente e evite multas e responsabilidades:

A CyberExperts atua na adequação de negócios e empresas à

LGPD, bem como na perícia em dados e resposta a incidentes envolvendo vazamento de dados pessoais e auditorias de conformidade, atuando desde a investigação do incidente ao relacionamento com titulares de dados e Autoridades. Fale conosco. Acesse: www.cyberexperts.com.br.

Sobre o autor:

José Antonio Milagre (https://app.exeed.pro/holder/badge/55319) Data Protection Officer (DPO) EXIN. Pesquisador em direito e dados do Núcleo de Estudos em Web Semântica e Análise de Dados da USP (Universidade de São Paulo). Mestre e Doutorando em Ciência da Informação pela UNESP. Pós Graduado em Gestão de Tecnologia da Informação. Advogado com atuação em Direito Digital. Perito Judicial em Informática e Proteção de Dados. Presidente da Comissão de Direito Digital da Regional da Vila Prudente da OAB/SP. Autor de dois livros pela Editora Saraiva (Marco Civil da Internet: Comentários a Lei 12.975/2014 e Manual de Crimes Informáticos).

Colaboradora: Laura Secfém Rodrigues. Pós-graduanda em Direito, Tecnologia e Inovação com ênfase em proteção de dados, no Instituto New Law. Graduada em Direito pela Instituição Toledo de Ensino (ITE).