Mori: A mitigação de riscos de vazamento de dados pessoais

Com a recente notícia acerca do vazamento ocorrido em janeiro deste ano, apontado como o maior da história do Brasil e que envolveu mais de 223 milhões de números de CPF, nomes, datas de nascimento e gênero de cidadãos brasileiros, inclusive de pessoas já falecidas, o questionamento sobre o nível de proteção dos dados pessoais ganhou foco.

No caso em questão, muito embora o Serasa Experian tenha sido inicialmente apontado como sendo a possível fonte dos dados pessoais vazados, a empresa negou que o vazamento tenha ocorrido a partir de seu banco de dados.

Sem definições concretas sobre a origem do vazamento e com a declaração da Agência Nacional de Proteção de Dados (ANPD) de que está apurando tecnicamente as informações sobre o incidente, fato é que, em razão de vazamentos como esse, os dados pessoais estão disponíveis na rede. Trata-se de uma imensurável violação dos direitos fundamentais à privacidade e à intimidade, assegurados constitucionalmente.

A importância de se conhecer a fonte do vazamento não implica somente em responsabilização ou penalização dos responsáveis, mas principalmente na necessidade de correção de possíveis falhas, afinal, é um problema de segurança pública.

Essa situação acarreta um estado de alerta geral, na medida em que favorece o cometimento de golpes e fraudes, com potencial risco de lesão aos titulares dos dados vazados, como abertura de conta em banco e de linha de crédito com documentos falsos, entre outras práticas ilícitas. Logo, o dano já causado pelo vazamento pode ser ainda potencializado se efetivadas tais práticas.

Mas, afinal, quais são as consequências legais desses incidentes? Que medidas devem ser tomadas para evitar esse risco? Essas são algumas das principais perguntas que afligem as empresas, em especial os agentes de tratamento (controladores e operadores), considerando as responsabilidades envolvidas.

Com a edição da lei brasileira sobre proteção dos dados pessoais, a Lei nº 13.709/2018 (LGPD), que finalmente, após um período de incertezas, entrou em vigor no mês de setembro de 2020, podemos agora nos amparar em previsões legais para exigir e também cumprir com as regras de conduta que giram em torno dos dados pessoais.

A LGPD foi criada, em síntese, com o objetivo de garantir aos titulares maior nível de proteção em relação aos seus dados pessoais, exigindo dos agentes de tratamento maior controle e comprometimento com a observância dos princípios que norteiam a lei e também maior transparência e segurança em relação aos dados pessoais disponibilizados para tratamento.

Muito vem sendo discutido em relação às providências que devem ser adotadas pelos próprios titulares para evitar esses vazamentos. Contudo, ainda que os titulares possam e devam se utilizar de determinadas medidas para diminuir os riscos, é importante destacar que a responsabilidade por proteger os dados é daqueles que os recebem e realizam o tratamento, sejam entendidas públicas ou privadas.

Ainda que o tratamento dos dados pessoais seja realizado com enquadramento nas bases legais previstas, será considerado irregular se não proporcionar ao titular a segurança necessária, inclusive em razão da utilização de técnicas inadequadas ou insuficientes para conferir proteção em relação a vazamento de dados.

O ano de 2020 foi imprescindível para a consolidação da revolução digital, diante da necessidade de adaptação das estruturas corporativas em razão da pandemia da Covid-19, e também marcado negativamente pelo grande número de ataques digitais, até mesmo contra o Superior Tribunal de Justiça.

O cenário atual vivenciado no Brasil por conta desse desenvolvimento digital certamente levantou muitas discussões e incertezas sobre a intepretação da nova lei. Assim, muito se espera da atuação da ANPD, principalmente por conta da atribuição de realizar essa interpretação e regular os casos omissos, antes mesmo de passar a aplicar as sanções para os casos de violação.

De acordo com a definição da LGPD, a ANPD é o órgão da administração pública federal, integrante da Presidência da República, responsável não só por zelar pela proteção dos dados, mas também por implementar e fiscalizar o cumprimento da lei e aplicar sanções em caso de tratamento de dados realizado em descumprimento à legislação.

A LGPD prevê que em caso de infrações às normas poderão ser aplicadas pela ANPD, em face dos agentes de tratamento, sanções administrativas como a aplicação de multa correspondente a 2% do faturamento anual da empresa envolvida em vazamentos como este, limitada a R$ 50 milhões por infração, a publicização da infração, entre outras penalidades previstas em seu artigo 52.

Como se sabe, as penalidades previstas na LGPD somente poderão ser aplicadas a partir de 1º de agosto deste ano, conforme estabeleceu a Lei nº 14.010/2020.

Vale destacar, entretanto, que as sanções previstas são administrativas e não obstam a aplicação de sanções civis ou penais, ou mesmo de outras sanções administrativas, uma vez que a existência e atuação da ANPD não prejudica ou interfere na competência de órgãos como o Procon e o Ministério Público. Assim, nada impede que venha a ser arbitrado, por exemplo, valor de indenização por danos causados a terceiros, inclusive maior que a multa aplicada pela ANPD.

Em recente aparição, o presidente da ANPD declarou que inicialmente o foco de atuação do órgão será a educação e não a aplicação das sanções administrativas, que seriam pouco eficientes, eis que as multas acabariam sendo repassadas pelas empresas aos seus clientes.

Um ponto essencial a ser considerado para afastar as possíveis penalidades decorrentes da violação da LGPD, o que inclui a despreocupação com a correção de possíveis vulnerabilidades, é a ação preventiva. Sobretudo porque a dosimetria da sanção, que ocorrerá de acordo com cada casa concreto, considerará os critérios indicados no §1º do artigo 52, entre os quais cabe destacar a gravidade da infração e a adoção reiterada de mecanismos e procedimentos internos capazes de minimizar o dano causado.

Em consonância com o artigo 44 da LGPD será considerado irregular o tratamento de dados pessoais que deixar de observar a legislação ou que não fornecer ao titular a segurança que ele pode esperar, consideradas, dentre outras circunstâncias relevantes, *"as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado"*.

Como indicado, a LGPD dispõe que as técnicas de tratamento seriam aquelas disponíveis à época. Trata-se de um detalhe significante o legislador utilizar na redação da lei as palavras "disponíveis" ao invés de "existentes", visto que são completamente distintas. O fato de existir, por exemplo, um sistema de segurança extremamente eficiente em outro país e ainda não comercializado para outros países, não o torna disponível aos controladores brasileiros. E ainda que *"o sistema passe a ser comercializado no Brasil, mas pelo valor de 50 milhões de dólares a licença. Isso faz com que o sistema esteja 'disponível' para os controladores brasileiros? Entendemos que não. A palavra 'disponíveis' precisa levar em consideração a possibilidade ou não de o controlador ter acesso a determinado sistema, não o simples fato de ele existir ou ser comercializado fora dos padrões econômicos do controlador sob análise"* [1].

Não obstante, a lei não atrela a segurança exclusivamente à adoção de medidas técnicas. Em linha com que estabelece o princípio da segurança, elencado na LGPD, os agentes de tratamento deverão utilizar-se de *"medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão"*.

Em resumo, para garantir a efetiva proteção dos dados pessoais não basta a utilização de medidas técnicas, sendo imprescindível também a adoção de medidas de ordem administrativa.

Um exemplo bem claro e que retrata essa necessidade é o de uma empresa hipotética que adota medidas técnicas adequadas a cumprir satisfatoriamente com os objetivos de confidencialidade, integridade e disponibilidade. Suponha-se que cada empregado dessa empresa tenha sua própria credencial que, a depender do cargo hierárquico, possibilite diferentes graus de autorização de acesso. Todavia, por mera comodidade no dia a dia, os empregados optam por compartilhar as credenciais entre sim, enganando o sistema de segurança da empresa. Por meio desse exemplo é possível demonstrar que ainda que exista um sistema de segurança, se este não for operado com regras que técnicas e administrativa que possibilitem regularizar o tratamento de dados, a iniciativa acaba frustrada [2].

As medidas a serem adotadas não dizem respeito apenas à segurança de informação. Até mesmo porque nem todo vazamento decorre de violação do sistema de segurança, assim como nem todo tratamento incide sobre os dados pessoais *online*/digitais mas também *offline*/físicos, sendo possível, portanto, a causa decorrente de culpa ou dolo dos próprios colaboradores.

Convém destacar que *"quanto às medidas administrativas, os dispositivos trazidos pela lei demandarão um esforço coletivo de todos os atores envolvidos e implicarão a criação de novas rotinas de trabalho, de procedimentos de segurança de informação e aumento dos mecanismos de transparência e governança. A cultura de proteção aos dados pessoais precisará ser cada vez mais difundida, em especial entre aqueles que prestem serviços para agentes de tratamento"* [3].

Isso reflete a necessidade de aplicação das regras de *compliance*, visando a alterar a cultura dos colaboradores, para fins de assegurar a observância das novas regras legalmente exigidas. Isso corresponde ao incentivo ao desenvolvimento da cultura da privacidade e da proteção de dados pessoais.

A nova lei requer medidas preventivas para evitar a violação dos direitos fundamentais à privacidade e intimidade dos titulares dos dados pessoais. Afinal, *"quando a lei afirma que considerações sobre dados pessoais e sua proteção devem existir desde a concepção de produtos e serviços, ela dá um sinal para que empresas e governos não releguem as preocupações sobre proteção de dados apenas para depois de ocorridos episódios de sua violação"* [4].

Foi justamente com essa pretensão que a LGPD direcionou uma seção para tratar de boas práticas e governança, por reconhecer como significativa a implementação do que ela intitulou ser o "programa de governança em privacidade". Não se trata de uma imposição da lei, mas, sim, de uma possibilidade imputada aos agentes de tratamento e que só traz consequências positivas, em especial considerando-se que a adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano decorrente da infração da lei será um item a ser considerado como atenuante no momento de eventual imposição de sanções administrativas (artigo 52, §1º, VIII).

Para tanto, é inafastável a necessidade de as organizações públicas e privadas estabelecerem procedimentos corporativos para que os seus colaboradores sigam as orientações apresentadas em seus códigos de conduta/boas práticas e políticas internas. Isso porque somente poderá ser exigido dos colaboradores o cumprimento das orientações que tenham sido repassadas de forma suficientemente completa e clara.

É indispensável garantir internamente a difusão das regras a serem seguidas, por meio da adoção de mecanismos de *compliance* e implementação de boas práticas no tratamento dos dados pessoais, de modo a garantir a fixação de controles internos e, via de consequência, a prevenção de condutas em desacordo com os comandos da legislação.

Ainda no que diz respeito à importância do programa de *compliance* para a satisfatória adequação à LGPD, especialmente em caráter preventivo, pertinente ressaltar que, para assegurar a efetividade do programa de *compliance*, é necessária a sua contínua avaliação, com a análise dos riscos e realização de treinamentos visando a orientação sobre a relevância dos cuidados necessários ao tratamento dos dados pessoais. A instituição deve *"investir em um programa de capacitação constante, de forma a manter todos atualizados quanto a alterações feitas em procedimentos e políticas, como para reforçar as premissas da LGPD, minimizando o risco de falhas por desconhecimento ou não compreensão do tema"* [5].

Ainda é desconhecido como será acompanhado o processo de adequação das organizações às novas regras impostas.

Apesar de ter sido finalmente constituída, a ANPD ainda não publicou nenhuma das regulamentações previstas em lei. Essas regulamentações, bem como as orientações em relação aos pontos duvidosos e obscuros da lei, serão cruciais para estabelecer a segurança jurídica, tanto para os titulares dos dados pessoais quanto para as organizações. Essa segurança, por sua vez, será vital para garantir os investimentos e a geração de negócios no Brasil.

No final do mês de janeiro, a ANPD apresentou a agenda regulatória para o biênio 2021-2022, que basicamente corresponde a um cronograma com as ações planejadas, com a definição das prioridades em três fases que reúnem dez temas, incluindo regulamento próprio sobre as sanções administrativas e metodologias que orientarão o cálculo do valor-base das sanções de multa. Os itens dessa agenda regulatória serão considerados na elaboração das diretrizes da Política Nacional de Proteção de Dados Pessoais e da Privacidade pela ANPD.

A expectativa é de que finalmente estejamos trilhando rumo à obtenção de maior amparo e informações. Ainda assim, as organizações brasileiras devem, desde já, executar mecanismos de adequação, conforme aqui apontado, e não ficar estagnadas aguardando o integral e perfeito funcionamento da ANPD para somente então começarem a corre atrás da adequação.

[1] COTS, Márcio e OLIVEIRA, Ricardo. *Lei Geral* de *Proteção* de *Dados* Pessoais *Comentada*. 2. ed. São Paulo: RT, 2019, p. 181.

[2] COTS, Márcio; OLIVEIRA, Ricardo. Op. cit, p. 186.

[3] TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coord.). Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro. São Paulo: RT, 2019, p. 435.

[4] Op. cit., p. 440.

[5] XAVIER, Fábio Correa. Ações para adequação à LGPD pela administração pública. In: Comentários à Lei Geral de Proteção de Dados Pessoais – LGPD [livro eletrônico]. Ribeirão Preto/SP: Migalhas, 2021, p. 14-15.

Date Created
11/02/2021