Opinião: LGPD: A segurança da informação é obrigação de meio

Todas as semanas são noticiadas dezenas de casos de vazamento de dados pessoais no mundo e no Brasil, envolvendo não apenas empresas privadas, mas também órgãos públicos. As principais e "*mais seguras*" agências de inteligência e investigação norte-americanas — NSA, CIA e FBI — já foram alvo da ação indesejada de hackers. Em setembro de 2019, noticiou-se um episódio de *data breach* envolvendo os dados pessoais de 98% da população equatoriana, ou seja, quase a totalidade dos

No Brasil, os exemplos mais recentes chamam muito a atenção. Em 4/11/2020, o Superior Tribunal de Justiça informou que sofreu um ataque de hackers, quando foi detectado um vírus circulando na rede de informática do tribunal. Toda a base de dados do tribunal ficou inacessível, impedindo a tramitação de milhares de processos. As sessões de julgamento foram suspensas, assim como os prazos processuais. É considerado um dos incidentes mais severos já ocorridos no país.

No primeiro turno de votação das eleições de 2020, hackers vazaram uma série de informações internas do Tribunal Superior Eleitoral para demonstrar a vulnerabilidade do sistema. Em resposta, o tribunal reafirmou a integridade do pleito e da apuração. Já neste ano, mais recentemente, noticiou-se o maior vazamento de dados pessoais ocorrido no Brasil, com a divulgação de mais de 223 milhões de números de CPF, mais do que a totalidade da população brasileira.

Sob o ponto de vista legal, uma das principais discussões do tema é definir se a segurança da informação a que estão obrigadas empresas privadas e entes públicos é uma obrigação de meio ou de resultado e, como tal, qual a responsabilidade que pode gerar aos agentes de tratamento em processos administrativos e judiciais que envolvam episódios de *data breach*.

Nesse contexto, vale lembrar que a LGPD se inspirou no Regulamento Geral de Proteção de Dados da União Europeia (GDPR, na sigla em inglês). E lá, a segurança da informação é obrigação de meio, estabelecendo que os controladores e processadores de dados pessoais serão responsabilizados pelos danos causados aos titulares dos dados se não cumprirem as obrigações impostas pelo próprio regulamento, ou se, de alguma outra forma, violarem suas disposições.

Dentre essas obrigações, encontram-se diversas medidas de segurança que devem ser rigorosamente aplicadas, compatibilizando-se com os riscos atinentes aos serviços prestados. Os agentes de tratamento de dados estão, assim, obrigados a empregar os melhores esforços na segurança da informação.

Decisões de órgãos de proteção de dados dos mais diversos países que integram a União Europeia — e que, portanto, submetem-se à aplicação do GDPR — demonstram que a não responsabilização dos agentes de tratamento de dados por eventuais episódios de *data breach* depende do atendimento integral às obrigações impostas pelo regulamento.

Perfilhando o regime adotado na Europa, entendemos que a Lei Geral de Proteção de Dados Pessoais articulou a segurança da informação como uma obrigação de meio, e não de resultado. Uma análise sistemática da Lei, e em especial dos artigos 43, incisos II e III, 44, *caput* e parágrafo único, e 46, *caput* e §§ 1º e 2º, torna clara essa percepção.

Nos termos desses artigos da lei, deve-se observar a conduta adotada pelo agente de tratamento de dados pessoais ao longo do período que antecedeu o *data breach*, para definir se possui responsabilidade sobre o ocorrido. Ou seja, os esforços prévios e contínuos envidados pelo agente são determinantes para aferir se estará obrigado a reparar eventuais danos sofridos pelos usuários que tiveram seus dados acessados de forma indevida.

Caso o agente de tratamento forneça a segurança que o titular possa esperar — considerados o modo pelo qual é feito o tratamento dos dados pessoais, os resultados e riscos que razoavelmente dele se espera, e as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado —, ainda que ocorra um acesso indevido de terceiros, defendemos que o agente não está obrigado a reparar os titulares, justamente porque cumpriu as obrigações que lhe foram impostas.

Precedentes judiciais proferidos antes da LGPD confirmam essa opinião. Para o Tribunal de Justiça do Rio de Janeiro no julgamento da Apelação nº 0024968-52.2013.8.19.0061, "*(…) nenhum sistema informatizado é imune a esse tipo de invasão. O que o administrador de rede deve promover é o cuidado necessário com o uso de tecnologias que visem dificultar tais invasões, visto que a complexidade e alcance das fraudes cibernéticas andam sempre à frente da especialização tecnológica dos sistemas de segurança de rede, o que é demonstrado pelas constantes notícias de descoberta de novas fraudes e invasões, inclusive em grandes corporações. Assim, para que ficasse caracterizada a responsabilidade do Estado, seria necessário demonstrar sua negligência quanto aos aspectos de proteção de rede. Todavia, não há prova nos autos de que o Estado negligenciou a ponto de facilitar a invasão de seu sistema*".

Nesse mesmo sentido, o Superior Tribunal de Justiça reconheceu no julgamento do Recurso Especial 1.398.985/MG que não há sistemas infalíveis e, por isso mesmo, "*(…) também não significa que se deva exigir um processo de cadastramento imune a falhas. A mente criminosa é astuta e invariavelmente encontra meios de contornar até mesmo os mais modernos sistemas de segurança. O que se espera dos provedores é a implementação de cuidados mínimos, consentâneos com seu porte financeiro e seu know-how tecnológico — a ser avaliado casuisticamente, em cada processo — de sorte a proporcionar aos seus usuários um ambiente de navegação saudável e razoavelmente seguro*".

Se o agente de tratamento de dados atua em conformidade com a LGPD, empregando os melhores esforços na segurança da informação, adotando medidas eficazes e necessárias para a proteção dos dados pessoais armazenados, eventual vazamento de dados não se configura, *per se*, uma falha na prestação de seus serviços.

Interessante notar um diálogo entre esse racional e a teoria do risco do desenvolvimento, que resguarda o fornecedor contra eventuais danos causados aos consumidores, considerando que, à época da introdução de determinado produto ou serviço no mercado, não havia como impedir, técnica ou cientificamente, determinado resultado a partir da utilização daquele produto/serviço.

Responsabilizar o agente de tratamento por eventual episódio de *data breach* — ainda que tenha envidado todos os esforços e empregado todas as medidas que estavam a seu alcance — seria contrário aos interesses dos próprios titulares, e, em verdade, da sociedade como um todo. Isso porque, temendo responsabilização decorrente de eventual falha sobre a qual, à época, não se tinha conhecimento, os agentes de tratamento de dados seriam desestimulados a criar novos serviços e tecnologias.

Por se tratar de uma obrigação de meio, a análise de seu cumprimento deve se dar com base no conjunto fático-probatório a partir do qual se poderá verificar se foi ou não fornecida a segurança necessária pelo agente, consideradas as circunstâncias relevantes indicadas nos incisos I, II e III do artigo 44 da LGPD.

Dado o teor genérico do artigo 46, §1º, da LGPD, enquanto a Autoridade Nacional de Proteção de Dados (ANPD) não dispuser sobre os padrões de segurança para cada atividade, essa análise será subjetiva, o que significa que ficará a critério de cada órgão ou magistrado definir quais padrões técnicos mínimos são esperados de cada agente de tratamento na proteção dos dados dos titulares contra acessos indevidos de terceiros.

Logo, apesar da segurança da informação ser uma obrigação de meio, os agentes de proteção terão, em casos de incidentes de segurança com vazamento de dados pessoais, a árdua tarefa de demonstrar que não houve qualquer violação aos dispositivos da LGPD, porquanto forneceram a segurança que deles era esperada, empregando todos os esforços que estavam ao seu alcance para evitar que os dados de seus usuários fossem indevidamente acessados.

Date Created
02/06/2021