Vazamento de dados: uma preocupação da Lei Geral de Proteção de Dados

Vitor Morais de Andrade e Lygia Maria M. Molina Henrique

Atualmente, notícias sobre vazamento de dados e penalizações às empresas com consequências gravosas têm sido corriqueiras no noticiário

Atualmente, notícias sobre vazamento de dados e penalizações às empresas com consequências gravosas têm sido corriqueiras no noticiário e os exemplos abaixo elucidam esta realidade.

- A empresa Altaba, formada pela venda da Yahoo à Verizon, foi condenada nos Estados Unidos à multa de U$ 35.000.000,00, em razão da Yahoo não ter comunicado o vazamento de dados de ao menos 500 milhões de usuários ainda em 2014[1], além disso, o referido vazamento gerará indenização estimada em 50 milhões de dólares para cerca de 200 milhões de pessoas, vítimas do vazamento. A comunicação somente ocorreu em 2016;
- O Banco Inter, réu em Ação Civil Pública proposta pelo Ministério Público do Distrito Federal, por vazar dados pessoais de cerca de 19 mil correntistas, realizou acordo extrajudicial em que arcará com R$ 1.500.000,00 em danos morais destinados a órgãos públicos, que combatem crimes cibernéticos e instituições de caridade[2]. O MPDFT havia entendido que o Banco não teria tomado os cuidados necessários para garantir a segurança dos dados pessoais de seus clientes e não clientes, além disso, inicialmente, o Inter negou o vazamento e se recusou a prestar informações;
- A UBER, por sua vez, em outubro de 2016 teve dados vazados de 57 milhões de usuários e motoristas em todo o mundo. A empresa demorou um ano para comunicar a respeito do incidente e esta postura já lhe custou um acordo com o governo dos Estados Unidos em U$ 500.000.000,00 e R$ 4,5 milhões a autoridades de proteção de dados da Holanda e Reino Unido[3]. No Brasil, a UBER é investigada pelo Ministério Público do Distrito Federal e Territórios (MPDFT) a respeito do mesmo vazamento;
- O Google, recentemente, recebeu multa de 50 milhões de euros por violação a dados pessoais de Autoridade de proteção de dados francesa, com base no GDPR. A Autoridade entendeu que o Google não divulga em seu site com clareza e transparência como as informações dos usuários são utilizadas, por exemplo, informações sobre o processamento de dados não estavam próximas das informações sobre armazenamento de dados pessoais, exigindo que o titular buscasse exaustivamente por tais considerações. Além disso, algumas caixas de texto para coleta de consentimento expresso do usuário já vinham preenchidas, de modo a macular esta base legal para tratamento de dados pessoais[4];
- A Senacon (Secretaria Nacional do Consumidor), do Ministério da Justiça e Segurança Pública, instaurou em face do Google Brasil processo administrativo, diante de uma denúncia do Ministério Público Federal do Piauí. O que motivou a instauração do processo foram indícios de análise do conteúdo dos e-mails pessoais, enviados pelo Gmail, sem consentimento expresso do usuário[5].

Todos estes casos poderiam ter tido um desfecho distinto se a postura das empresas tivesse sido outra frente a ocorrência do incidente, conforme podemos averiguar na análise abaixo embasada pela LGPD:

Empresa	Suposta Violação de Dados/Incidente de segurança	Atuação da Autoridade	Conduta Esperada/Fundamento da LGPD
Altaba	Demora em 2 anos para comunicar vazamento de dados pessoais de 500 milhões de usuários	Sanção de U$ 35.000.000,00	A comunicação do incidente à autoridade competente em prazo razoável (art.48, da LGPD), entendido peloGDPR como 72 horas (considerando 85)
Banco Inter	Vazamento de dados pessoais de 19 mil correntistas; Negativa em prestar informações sobre o ocorrido às autoridades.	Propositura de Ação Civil Pública; e, Acordo extrajudicial de R$ 1.500.000,00 a título de danos morais.	Adoção de medidas de segurança adequada para a proteção dos dados pessoais de acessos não autorizados (art.6º, VII e VIII – princípio da segurança e da prevenção, arts.46 e ss); e, Comunicação da autoridade em prazo razoável (art.48, da LGPD).
UBER	Demora em um ano para comunicar vazamento de dados pessoais de 57 milhões de usuários	Autoridade Americana – sanção de U$ 500.000.000,00; Autoridades da Holanda e Reino Unido – sanções somadas em R$ 4,5 milhões; MPDFT – instauração de investigação.	A comunicação do incidente à autoridade competente em prazo razoável (art.48, da LGPD), entendido pelo GDPR como 72 horas (considerando 85)
Google	Não divulgação com clareza e transparênciade como os dados dos usuários são utilizados; Caixas de texto de consentimento já preenchidas.	50 milhões de Euros	Atendimento ao princípio da transparência - garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos

			comercial e industrial (art.6º, VI); Coletar consentimento consistente em manifestação livre, informada e inequívoca (art.5º, XII, art.7º, I, art.8º). Caixas de texto preenchidas antecipadamente não revelam consentimento, não revelam manifestação de vontade do titular.
Google Brasil	Acesso não autorizado a conteúdo de e-mail; tratamento de dados sem consentimento expresso (conduta investigada).	Processo administrativo em curso	Solicitação de consentimento livre, informado, inequívoco e referente à finalidade específica, antes de eventual acesso (art.5º, XII, art.7º, I, art.8º).

Considerando este cenário, a Lei Geral de Proteção de Dados Pessoais (lei 13.709/18 - LGPD), além de trazer a necessidade de as empresas ajustarem os seus bancos de dados às bases legais para tratamento (art.11), igualmente revela preocupação com a segurança e integridade da informação em relação ao tratamento de dados, exigindo que o controlador[6], em caso de incidente de segurança que o controlador e diante de um incidente com potencial de risco ou lesivo aos titulares de dados, comunique estes e a autoridade nacional a respeito (art.48, da LGPD).

A referida comunicação, conforme exigência legal, deve ser realizada em prazo razoável e deverá conter, no mínimo, as seguintes informações: (i) natureza dos dados pessoais afetados; (ii) informações sobre os titulares envolvidos; (iii) indicação de medidas mitigadoras e de segurança utilizadas para a proteção dos dados; (iv) os riscos envolvidos no acidente; e caso a comunicação não seja imediata, (v) as razões da demora.

Ocorre que a LGPD não define o que seria considerado um "incidente de segurança" e também não traz delimitações do que seria um incidente com potencial de risco, tendo deixado tais parâmetros para a Autoridade de Proteção de Dados Pessoais (ANPD), recém-criada pela medida provisória 869/18.

Enquanto a ANPD não regulamenta estas lacunas, o Regulamento Geral Europeu de Proteção de Dados Pessoais (GDPR) se mostra como uma direção interpretativa que não pode ser ignorada, principalmente, pela semelhança da lei brasileira com este texto.
O GDPR, diferentemente da LGPD, define **"violação de dados pessoais"** (incidente de segurança), como:

"(...) uma violação da segurança que provoque, de modo acidental ou ilícito, a destruição, a perda, a alteração, a divulgação ou o acesso, não autorizados, a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento (...)".

A violação de dados pessoais é assunto tratado por este Regulamento em seus considerandos 83, 85/88 e artigos 33 e 34. O considerando 83 traz o exemplo da cifragem como medida a atenuar riscos; o considerando 85 exemplifica os tipos de danos que a violação de dados pessoais poderia causar - perda de controle sobre os seus dados pessoais, a limitação dos seus direitos, a discriminação, o roubo ou usurpação da identidade, perdas financeiras, a inversão não autorizada da pseudonimização, danos para a reputação, a perda de confidencialidade de dados pessoais protegidos por sigilo profissional ou qualquer outra desvantagem econômica ou social significativa das pessoas físicas – este considerando ainda estipula o prazo de 72 horas para a comunicação do ocorrido à autoridade respectiva.

Os artigos 33 e 34, respectivamente, tratam da notificação à autoridade e da notificação ao titular de dados pessoais. A fim de dar cumprimento à LGPD a empresa pode, ainda, como medida de "Boa Prática" e educativa, criar regras coorporativas referentes à segurança da informação e incidente de segurança, como bem destaca o art.50[7], deste Diploma.

Até então, no Brasil, a fiscalização dos incidentes de segurança tem sido realizada pelo Comitê de Proteção dos Dados Pessoais do Ministério Público do Distrito Federal, justamente, em razão da demora na criação da ANPD. Este Comitê editou, inclusive, um formulário de Comunicação de Incidente[8], sendo certo que já há casos sob investigação por meio de Inquérito Civil e Procedimento Preparatório.

Assim, medidas preventivas e regras coorporativas sobre segurança da informação, manutenção da integridade dos dados e procedimento padrão para casos de incidentes são ferramentas que não podem faltar a um Programa Empresarial de *Compliance* com a LGPD.

---

1 Altaba, ex-Yahoo, é multada por vazamento de dados de usuários e Yahoo propõe US$ 50 milhões para indenizar vítimas do maior vazamento de dados da história

2 Banco Inter fecha acordo e pagará R$ 1,5 milhão por vazamento de dados

3Vazamento de dados rende mais R$ 4,5 milhões em multas contra Uber

4França multa Google em US$ 57 milhões por falta de proteção de dados de usuários

5 MJ instaura processo contra Google Brasil por violação de privacidade

6 "Pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais".

7 "Art. 50. Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, **as normas de segurança, os padrões técnicos**, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os **mecanismos internos de supervisão e de mitigação de riscos** e outros aspectos relacionados ao tratamento de dados pessoais".

8 http://www.mpdft.mp.br/portal/index.php/conhecampdft-menu/nucleos-e-grupos/comissao-de-protecao-dos-dados-pessoais/comunicacao-de-incidente-de-seguranca?view=form

---

*__Vitor Morais de Andrade__ é mestre e doutor em Direito pela PUC/SP e advogado do __LTSA Advogados__.

*__Lygia Maria M. Molina Henrique__ é graduada e mestre em Direito pela PUC/SP e advogada do __LTSA Advogados__.