Por Maria da Gloria Faria (*)

Não se ignora que nesses dois anos de pandemia da Covid-19 o vazamento de dados e as ações de hackers, que já vinham em crescimento acelerado mundo afora, sofreram um aumento exponencial no Brasil. Somos recordistas de tentativas de ataques, bem e ou não tão bem, sucedidos.

Dezembro de 2021 ficou marcado por dois graves episódios que colocam em xeque a proteção de dados entre nós. São eles o vazamento de **160 mil chaves Pix** de clientes de uma empresa gestora de Cartões Pré-Pagos, e a invasão hacker que atingiu a Rede Nacional de Dados de Saúde (RNDS).

Vazamento de chaves Pix

Com uma carteira de 5 milhões de clientes, o vazamento das chaves Pix teria decorrido de “falhas pontuais” nos sistemas da intermediadora de pagamentos, entre os dias 3 e 5 de dezembro e expôs dados de 159.603 clientes pessoas físicas.

Com a **Lei Geral de Proteção de Dados (LGPD)**, Lei nº 13.709/2018 em pleno vigor desde 1º de agosto de 2021, e conforme previsto em seus artigos **52**, **53** e **54** a empresa gestora de Cartões Pré-Pagos poderá receber sanções que vão desde uma **advertência** com prazo para adoção de medidas corretivas, **até multas de R$50 milhões**.

A **Secretaria Nacional do Consumidor (Senacon)**, órgão do Ministério da Justiça, abriu uma investigação preliminar para apurar informações e obter confirmação de fatos que possam levar à instauração de um processo administrativo. Dentre outras providências, encaminhou ofícios ao **Banco Central (BC)** e à **Autoridade Nacional de Proteção de Dados (ANPD)**, esta última, a entidade competente para aplicar as multas e sanções administrativas previstas na LGPD.

Art. 55-K. A aplicação das sanções previstas nesta Lei compete **exclusivamente** à ANPD, e suas competências prevalecerão, no que se refere à proteção de dados pessoais, sobre as competências correlatas de outras entidades ou órgãos da administração pública.

Vale ressaltar que a aplicação das sanções previstas na LGPD não substitui a aplicação de outras sanções administrativas previstas no **Código do Consumidor**, Lei nº 8.078 de 11 de setembro de 1990, e em legislação específica.

Ainda que, realmente, os dados expostos sejam os cadastrais, como informado pelo Banco Central, sem que deles constem dados sensíveis como senhas, movimentações ou saldos financeiros, que permitiriam movimentação de recursos ou acesso às contas, permanece o risco de serem utilizados para estelionato digital. Nessa nova modalidade de golpe o criminoso, de posse dos dados pessoais, se faz passar por um funcionário do banco para tentar obter as credenciais de senha do usuário.

Rede Nacional de Dados de Saúde (RNDS)

Um ataque hacker pelo “Lapsus$ Group”, que assumiu a autoria no próprio site do MS e deixou a mensagem “Nos contate caso queiram o retorno dos dados”, conseguiu tirar do ar um enorme número de dados e informações. Ficaram inoperantes vários sistemas como o de monitoramento da Covid – 19, o e-SUS Notifica e o SIVEP – Gripe e o SI-PNI que reúnem, respectivamente, informação sobre casos leves de Covid-19, internação por síndrome respiratória aguda grave (incluindo influenza e Covid-19) e vacinação.

Também atingido, o ConecteSUS ficou sem a funcionalidade para a emissão do Certificado Nacional de Vacinação Covid-19 e da Carteira Nacional de Vacinação Digital, deixando em falta um grande contingente de pessoas que necessitaram desses certificados, no período.

A falta de informação clara por um período de mais de um mês, em pleno recrudescimento da pandemia com a transmissão comunitária de uma variante do Sars- CoV-2, mais infecciosa, a Ômicron, provocou grande impacto no planejamento e estratégias de monitoramento de internações, ocupação de leitos, insuficiência de testes nas unidades de atenção primária, gerando longas filas para atendimento. E não foi só a saúde pública que sofreu com a privação dos dados capturados, também a saúde suplementar foi atingida com efeitos diretos e indiretos.

Consta do GUIA DE ELABORAÇÃO DE TERMO DE USO E POLÍTICA DE PRIVACIDADE PARA SERVIÇOS PÚBLICOS às fls. 27:

“A Administração Pública, no papel de custodiante das informações pessoais dos usuários, deve cumprir todas as legislações inerentes ao uso correto dos dados pessoais do cidadão de forma a preservar a privacidade dos dados utilizados na plataforma”.

E às fls. 24:

“Cabe também a Administração Pública implementar controles de segurança para proteção dos dados pessoais dos titulares”.

Estatísticas públicas são essenciais. Essenciais também são o cuidado e os investimentos em tecnologia, sistemas confiáveis, manutenção criteriosa, pessoal capacitado e políticas adequadas de privacidade, segurança da informação e *compliance* que o setor público deve priorizar, sobretudo em áreas sensíveis como a da saúde.

Sem dúvida alguma a LGPD é indutora de boas práticas no tratamento de dados pessoais e a ANPD possui competência e mecanismos para cercear e punir aqueles que não observarem os dispositivos da lei.

Entretanto, mais que tudo, se faz necessária uma mudança cultural. O investimento em sistemas e no material humano deve ser continuado e constantemente atualizado, visto que grande parte dos vazamentos ocorre por falha humana.

É importante assinalar que a LGPD prevê que os titulares dos dados possam buscar seus direitos por ação judicial.

Art. 22. A defesa dos interesses e dos direitos dos titulares de dados poderá ser exercida em juízo, individual ou coletivamente, na forma do disposto na legislação pertinente, acerca dos instrumentos de tutela individual e coletiva.

Portanto, caso o titular venha a sofrer danos patrimoniais ou morais, em decorrência direta ou indireta, de vazamento dos seus dados pessoais, sensíveis ou não, ele poderá buscar judicialmente o ressarcimento e/ou indenização de seus prejuízos, por meio de ação judicial.

(*) **Maria da Gloria Faria** é advogada, sócia administradora de Motta & Faria Advocacia, Conselheira do IAP – Instituto Ação pala Paz, Conselheira e Presidente do GNT de Novas Tecnologias da AIDA Brasil, Organizadora e articulista da Revista Jurídica de Seguros - RJS.