A IMPORTÂNCIA DA INVESTIGAÇÃO POLICIAL PARA AS INVESTIGAÇÕES INTERNAS SOBRE VAZAMENTO DE DADOS PESSOAIS NO COMPLIANCE DIGITAL CORPORATIVO

CLAUDIA DA COSTA BONARD DE CARVALHO[1]

RESUMO: O presente artigo visa demonstrar a importância da investigação policial de vazamento de dados pessoais no âmbito corporativo, como medida de boas práticas em programa de Compliance, para otimização das investigações internas e preservação da imagem da empresa, minimizando-se as consequências de um incidente de segurança.

1.Introdução

O Compliance das empresas privadas passou a enfrentar uma nova realidade com o advento da Lei 13.709/18 (Lei Geral de Proteção de Dados), a qual disciplina o tratamento de dados pessoais que circulem em meios digitais, para preservação da privacidade dos titulares de tais informações.

Embora a referida norma ainda não tenha entrado em vigor, por conta de diversas propostas de alterações de texto, a implementação dos seus ditames já está em curso nas empresas, as quais estão adaptando sua rotina operacional e as suas obrigações legais para cumprimento da LGPD, de forma a evitar sanções e prejuízos nela previstos.

Ocorre que, o cumprimento da LGPD tem sido encarado essencialmente como algo que importa somente às relações de direito privado envolvidas no tratamento de dados pessoais que circulem em sistemas corporativos.

[1] ADVOGADA CRIMINAL, GRADUADA PELA UERJ E PÓS GRADUADA EM DIREITO PENAL E PROCESSO PENAL PELA UNIVERSIDADE ESTÁCIO DE SÁ, ESPECIALIZADA EM CYBERSECURITY E COMPLIANCE, AUTORA DO LIVRO DIREITO PENAL 4.0 E DO PODCAST CYBERCRIME NEWS, INSTRUTORA DA CRIMINAL COMPLIANCE BUSINESS SCHOOL, CONTATO: CLAUDIA. CARVALHO@ADVBONARDDECARVALHO.COM.

Nesse sentido, percebe-se a ênfase em medidas administrativas de proteção de dados de âmbito interno e na inserção de novas cláusulas contratuais sobre privacidade nos negócios, para solução de eventuais situações decorrentes de vazamento de dados pessoais, como estratégias de Compliance Digital.

Cabe destacar que, de acordo com os seus pilares básicos, o Compliance envolve a análise e a mitigação de riscos, incluindo os criminais, como fraudes, crimes econômicos e etc.., o que requer investigações internas para detecção destas ocorrências no âmbito corporativo.

Assim, havendo um vazamento de dados, há que se considerar também que o mesmo poderia ter finalidades criminosas, pelo que, a investigação se torna mais complexa, necessitando-se, em muitos casos, de apoio da autoridade policial, que pode elucidar melhor outros aspectos do incidente de segurança.

Com isso, um vazamento de dados precisa ser investigado não só internamente pelas empresas, como também no âmbito policial, diante de suas graves consequências, as quais podem afetar toda a operação da empresa e sua imagem, caso determinadas medidas não sejam adotadas, como o devido registro policial do fato, em caso de incidente de segurança.

2. Vazamento de Dados Pessoais nas empresas

A atividade das empresas acarreta diversos riscos, os quais podem surgir, por exemplo, em novos negócios, no relacionamento com fornecedores ou na falta de conscientização de colaboradores no acesso aos sistemas, por conta da necessária circulação de dados pessoais que tais operações envolvem.

Assim sendo, o vazamento de dados pessoais é uma possibilidade permanente e deve ser mitigada, conforme as estratégias de Compliance Digital que forem definidas em conjunto com a alta direção das empresas.

Frise-se que, recente pesquisa da KROLL[2] identificou alto índice de fraudes praticadas mediante vazamento de dados (39%), que podem ser causados por invasão de sistemas por terceiros ou por atividade estranha praticada com a participação de colaboradores

Logo, as investigações internas devem ser conduzidas com análise de sistemas e de relatório de impacto de incidente de segurança da informação, onde possa ser apurado onde está localizado o vazamento de dados pessoais, com verificação de logins e de níveis de acesso autorizados a determinados funcionários, bem como detecção de malwares instalados clandestinamente e demais providências a serem tomadas.

Ao lado disso, também existe a necessidade de verificar que obrigações legais possam surgir do vazamento de dados pessoais, bem como realizar as devidas comunicações que sejam necessárias, como imprensa, clientes, funcionários e fornecedores, para que o fato fique devidamente esclarecido, conforme a posição oficial da empresa.

Tais atitudes são fundamentais na averiguação sobre o incidente de segurança da informação, mas não bastam para que sua verificação seja satisfatória para todos os envolvidos.

3- O papel da atividade policial na investigação de vazamento de dados

As investigações internas sobre vazamento de dados vão priorizar sempre a localização de vulnerabilidades dentro de seus sistemas, ou seja, a dimensão do dano que possa ter sido causado (comprometimento da autenticidade, disponibilidade ou confidencialidade de dados) e o agente causador (malware, falhas de atualização de programas e etc.,) bem como a implantação imediata de medidas de contenção do vazamento.

Ocorre que, em qualquer situação, há a imprescindível atuação humana, seja na obtenção de acesso ilegal aos sistemas, por técnicas de engenharia

[2] KROLL. Disponível em: < https://www.kroll.com/en/insights/publications/global-fraud-and-risk-report-2019>. Acesso em 20.07.2020.

social sobre colaboradores, ou na invasão de sistemas por disseminação de softwares que vão rastrear indevidamente a rede corporativa.

Com isso, há, evidentemente conduta criminosa, ou seja, tanto na invasão de sistemas (artigo 154-A do CP)[3], seja na prática de diversos delitos, mediante o uso de informações pessoais vazadas.

Não bastasse isso, a elucidação do fato pode ter desdobramentos fora do sistema da empresa, com o envolvimento de pessoas que estejam em outro país ou servidores de fora do perímetro de segurança corporativo.

Neste contexto, a investigação policial do fato se torna relevante, por permitir a averiguação da situação fora dos limites dos sistemas corporativos, facilitando a identificação de pessoas envolvidas e até mesmo a ligação do fato com quadrilhas cibernéticas já conhecidas e atuantes sobre sistemas de empresas do mesmo ramo de negócio.

Assim, o registro policial do fato pode demonstrar, de forma inequívoca, o empenho e a intenção da empresa em elucidar verdadeiramente o vazamento de dados, sem que haja suspeitas de acobertamento de fraudes internas, para que seus responsáveis sejam logo identificados e o fato não se repita.

Além disso, a investigação policial pode contar com recursos tecnológicos não disponíveis nas empresas, como perícias cibernéticas específicas, cujos resultados otimizariam bastante o andamento das investigações internas.

Vale lembrar ainda que o relato na delegacia poderá ser enviado a clientes, para que possam ter maiores detalhes do que ocorreu, o que pode impedir a aplicação de multas contratuais, por eventual interrupção de serviço, considerando-se o fato como força maior ou caso fortuito, afastando-se alegações de falta de segurança suficiente no tratamento de dados, de acordo com a situação.

---

[3] Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita:

4- O desenvolvimento da investigação interna de vazamento de dados com apoio da autoridade policial

Uma investigação interna eficaz de vazamento de dados requer a colheita de relevantes evidências digitais, as quais demonstrem a anatomia do vazamento de dados, bem como detectem também os rastros eletrônicos deixados pelo envolvido na situação.

Frise-se que, ao contrário das investigações padrão, que se iniciam por uma acusação lançada contra determinada pessoa, via canal de denúncias da empresa, agora parte-se do fato para alcançar-se depois o provável responsável por ele, sendo esta, a maior dificuldade, justamente pela anonimização daqueles que agem ilicitamente na internet.

Diante disso, o apoio policial será fundamental na apuração do caso, auxiliando na identificação do envolvido e suas possíveis intenções delituosas, bem como verificação das consequências do ato praticado.

Logo, é importante que um advogado especialista em cybercrime auxilie na triagem dos elementos que apoiem a investigação interna, como e-mails suspeitos trocados entre determinados funcionários do setor do vazamento, cujo perfil deverá ser analisado pelo referido profissional no contexto da situação, auxiliando-se no direcionamento do conteúdo das entrevistas destes colaboradores pela equipe de investigação interna.

Além disso, será sugerida a possibilidade de divulgação ou não de determinados documentos sigilosos na investigação (contratos, notas fiscais e etc.), conforme o risco envolvido, evitando-se a ocorrência de outros crimes relacionados ao caso (ex: pirataria de protótipos ainda não lançados, insider trading e etc.).

Tais informações e outras serão encaminhadas pelo advogado especialista em cybercrime à autoridade policial, que determinará diligências relevantes, de acordo com a situação, como a perícia de documentos eletrônico contendo dados pessoais vazados, constatando sua eventual adulteração, bem como o rastreamento do endereço ID do computador de onde o arquivo foi criado

e identificação do provedor de internet do equipamento, que será intimado para fornecer dados do usuário do seu serviço.

Todas estas providências permitirão o levantamento de novos dados que sejam comparados com os elementos coligidos internamente na empresa, tais como as respostas das entrevistas com funcionários suspeitos do setor que sofreu o vazamento, o que viabilizará a sua conclusão mais segura.

5- A comunicação oficial do vazamento de dados como política de boas práticas de Compliance

No entanto, apesar das vantagens do apoio da investigação policial nas investigações internas de vazamento de dados pessoais, muitas empresas ainda preferem manter o incidente de segurança na esfera interna, sem realizar qualquer comunicação às autoridades, ao argumento de que, assim agindo, estariam preservando sua reputação, pela não divulgação oficial do vazamento de dados em sede policial.

Ora, qualquer tentativa de esconder um vazamento de dados pessoais, justamente por receio de dano à imagem da empresa será equivocada, tendo em vista que uma empresa que encobre irregularidades no seu funcionamento estará, primeiramente, atentando contra os princípios de conformidade e integridade do Compliance, como a transparência na sua gestão.

Não bastasse isso, tal atitude estará ainda em desacordo com a LGPD, que preconiza também que os incidentes de segurança sobre o tratamento de dados devem ser informados imediatamente ao titular dos dados, de acordo com o artigo 48 da referida norma:

> Art. 48. O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.
>
> § 1º A comunicação será feita em prazo razoável, conforme definido pela autoridade nacional, e deverá mencionar, no mínimo:
>
> I - a descrição da natureza dos dados pessoais afetados;
>
> II - as informações sobre os titulares envolvidos;

> III - a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial;
>
> IV - os riscos relacionados ao incidente;
>
> V - os motivos da demora, no caso de a comunicação não ter sido imediata; e
>
> VI - as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.

Agora, imagine-se, então, uma empresa que tenta esconder, de todas as formas, um vazamento de dados, o qual acabasse “sendo vazado” para a imprensa!

Tal atitude trará maiores danos reputacionais corporativos, tendo em vista que a empresa poderá ser vista como pessoa jurídica que não trata com seriedade tais assuntos ou ainda gerar desconfiança sobre seus dirigentes, ao argumento de que poderiam ter algum interesse em esconder os fatos, o que seria ainda mais grave, caso houvesse ainda a prática de delitos.

6-Conclusões

Vemos, desta forma, que a investigação policial pode elucidar casos graves de vazamento de dados pessoais, bem como irá preservar contratos e a reputação da empresa vítima, o que fortalecerá sua imagem e a de seus dirigentes, dentro do programa de Compliance.