PROSPECTUS
ISSN 2674-8576 Gestão e Tecnologia
Projeto Interdisciplinar

VAZAMENTO DE DADOS PESSOAIS E FRAUDE DO BOLETO: UM ESTUDO DE CASO HIPOTÉTICO

LEAKAGE OF PERSONAL DATA AND BANK SLIP FRAUD: A HYPOTHETICAL CASE STUDY

Alexandra Aparecida Dias Bozzato[1], Elton Diego Souza[1], Gabriela Ribeiro Goes Teixeira[1], Guilherme Figueira[1], William Topan Verginio[1] Evandro Jose Theodoro[2], Marcia Regina Reggiolli[3]

1- Graduandos do curso de Tecnologia da Gestão da Tecnologia da Informação, Faculdade de Tecnologia de Itapira "Ogari de Castro Pacheco" (FATEC – Itapira); 2- Docente da FATEC – Itapira; 3- Coordenadora do curso de Gestão da Tecnologia da Informação, FATEC – Itapira.

Contato: evandro.theodoro@fatec.sp.gov.br

RESUMO

O boleto bancário é a segunda forma de pagamento mais utilizada no Brasil, só perde para o cartão de crédito. Esse tipo de pagamento quando fraudado pode fazer vítimas recorrentes, através de compras *on-line*, emissão de segunda via em sites ou até mesmo por correspondência. O objetivo deste estudo é analisar um caso fictício, com a ocorrência de vazamento dos dados pessoais de vários usuários, após participarem de um sorteio em um *shopping* na cidade de Lauro de Freitas – BA. Após a análise do estudo de caso, atrelada ao conhecimento de segurança da informação e principalmente ao que menciona a Lei Geral de Proteção de Dados (LGPD), de 14 de agosto de 2018, o foco é apontar as falhas cometidas por todos os envolvidos no caso e sugerir propostas de melhorias, tendo como base as sanções administrativas ditadas pela LGPD, para que desta maneira, evitar que ocorram novamente.

Palavras-chave: Vazamento de dados pessoais. LGPD. Segurança da Informação.

ABSTRACT

The bank slip is the second most used form of payment in Brazil, the first is the credit card (ARAÚJO, 2020). When it is defrauded, it can make recurring victims, through online purchases, duplicates issuance on websites or even by mail. The aim of the current study is to analyze a fictitious case study, in which the personal data of several users are leaked, after participating in a drawing in a shopping mal in the city of Lauro de Freitas – BA. After analyzing the case study linked to the knowledge of Security of Information and mainly to what the General Data Protection Law (LGPD), of August 14, 2018, mentions, the focus

is to point out the failures committed by all involved in the case and suggest proposals for improvements, based on the administrative sanctions dictated by the LGPD, so that in this way, prevent them from occurring again.

Keywords: Leakage of personal data. LGPD. Information Security.

INTRODUÇÃO

A informação é um bem de valor imensurável, um recurso que move o mundo. Trata-se de um processo de comunicação entre o emissor e o receptor de uma determinada mensagem, e, quando assimilada de forma adequada, gera conhecimento para o indivíduo e consequentemente, para a sociedade em que ele vive.

Sobre a informação, é possível afirmar que:

> A informação sintoniza o mundo, como onda ou partícula, participa da evolução e da revolução do homem em direção à sua história. Como elemento organizador, a informação referência o homem ao seu destino; mesmo antes de seu nascimento, através de sua identidade genética, e durante sua existência pela sua competência em elaborar a informação para estabelecer a sua odisseia individual no espaço e no tempo. A importância que a informação assumiu na atualidade pós-industrial recoloca para o pensamento questões sobre a sua natureza, seu conceito e os benefícios que pode trazer ao indivíduo e no seu relacionamento com o mundo em que vive (BARRETO, 1994, p. 1).

Em se tratando de um bem tão valioso quanto a informação, deve-se ter consciência de que é necessário protegê-la, fazendo o uso da segurança da informação em diversos segmentos, seja dentro de organizações, local em que muitas vezes a informação se torna um importantíssimo objeto de competitividade no mercado, quanto na vida de cada indivíduo da sociedade, cujas informações pessoais, não devem ser violadas (ARAÚJO, 2020).

A segurança da informação, como cita Bastos e Caubit (2009) é caracterizada pela aplicação adequada de dispositivos de proteção sobre um ativo ou um conjunto de ativos visando preservar o valor que este possui para as organizações.

A aplicação destas proteções busca preservar a confidencialidade, a integridade e a disponibilidade (CID), não estando restritos somente a sistemas ou aplicativos, mas também informações armazenadas ou veiculadas em diversos meios além do eletrônico ou papel. É alcançada por um conjunto de atividades e práticas, através da elaboração de protocolos, procedimentos, políticas de Segurança da Informação, ferramentas de monitoramento e controle, entre outros (BASTOS; CAUBIT, 2009).

Atualmente, a falha na segurança da informação no mundo totalmente globalizado em que vivemos, e com novas tecnologias surgindo a cada dia, representa um grande perigo às organizações e à sociedade, que se tornam alvos vulneráveis a espionagem ou ataques de *hackers*.

Todas as ações digitalizadas, sejam elas por meio de celulares, computadores, máquinas de cartões de crédito, entre outros, são coletadas, copiadas e distribuídas para diversos bancos de dados, de empresas privadas ou até mesmo, do poder público.

Muitas vezes, essa coleta de informações acontece sem o consentimento do titular, e, mesmo quando é dada a opção de usar um serviço e ter os dados coletados ou a opção desistir de usar o serviço em questão, essa escolha é feita por meio do uso de políticas de privacidade e termos e condições praticamente ilegíveis.

Essas informações não só estão sendo coletadas com pouca ou nenhuma noção de consentimento, como frequentemente são tratadas sem qualquer responsabilidade ou transparência pública, e compartilhadas, vendidas e transmitidas a terceiros.

É neste contexto de coleta de dados e disseminação de informações, que podemos citar o escândalo ocorrido nas eleições presidenciais dos Estados Unidos no ano de 2016, envolvendo empresas multinacionais como o *Facebook* e a *Cambridge Analytica*.

O escândalo começou quando jornais de grande repercussão na TV americana, revelaram que a empresa britânica *Cambridge Analytica*, uma empresa de *marketing* cuja especialidade é analisar grandes quantidades de dados pessoais para construir estratégias supostamente mais eficazes a serem empregadas em campanhas publicitárias de várias ordens, sejam de índole meramente comercial, sejam de caráter político, obteve ilegalmente dados de cerca de 50 milhões de usuários do *Facebook.* A informação foi dada por um ex-funcionário da empresa (BBC, 2018).

Os dados, foram usados para alimentar um sistema capaz de traçar um perfil psicográfico dos americanos e usados na campanha de *Donald Trump*. O mecanismo teria permitido entender os traços comportamentais dos eleitores para oferecer-lhes propaganda política com mais chances de êxito.

A publicidade foi distribuída no *Facebook* em forma de anúncios patrocinados no *feed.* As informações foram obtidas a partir de um teste de personalidade aparentemente inofensivo, disponibilizado gratuitamente aos usuários da rede social em 2014.

Segundo o criador, o pesquisador *Aleksander Kogan*, o seu método de análise aplicado ao teste era capaz de traçar o perfil de qualquer pessoa rapidamente a partir de informações como páginas curtidas e postagens

realizadas na plataforma. O problema era que o teste obtinha dados não só de quem preenchia os formulários e aceitava as condições de uso, mas de toda a rede de contatos dos participantes, alcançando assim, milhões de pessoas (ALECRIM, 2017).

Na época antecedente às eleições, pesquisas apontavam que, além dos grupos de eleitores que já estavam decididos entre os candidatos democratas ou republicanos, havia um grande número de eleitores indecisos, e há quem diga que, através desta coleta e manipulação de dados feita pela *Cambridge Analytica*, estes eleitores tiveram suas opiniões manipuladas e foram induzidos a votar em *Trump,* fazendo assim, com que o mesmo assumisse assim o cargo de Presidente dos Estados Unidos no início de 2017.

Após este episódio, que pode ter mudado o cenário político em uma das maiores potências mundiais, os legisladores americanos criaram a Lei de Privacidade dos Consumidores da Califórnia, intitulada *California Consumer Privacy Act* (CCPA), com a intenção de devolver aos consumidores o exercício do controle sobre suas informações pessoais (TUMELERO, 2020).

Então a partir destes eventos, foi criada no Brasil, a Lei nº 13.709 a Lei Geral de Proteção de Dados (LGPD) baseada na lei americana de 14 de agosto de 2018 (BRASIL, 2019).

A LGPD trata da proteção dos dados pessoais dos indivíduos em qualquer relação que envolva o tratamento de informações classificadas como dados pessoais, tanto de pessoa física quanto de pessoa jurídica. Se trata de uma Lei extremamente técnica, a qual reúne uma série de itens de controle para assegurar o cumprimento das garantias previstas, cujo lastro se funda na proteção dos direitos humanos.

A aplicação da LGPD se faz importante no estudo de caso, objeto de discussão deste artigo, pois se trata do vazamento de dados pessoais ocorrido após várias pessoas participarem de um sorteio num shopping localizado na cidade de Lauro de Freitas - BA, onde, a empresa responsável pela coleta dos dados pessoais dos participantes do sorteio, alegam ter sofrido um ataque *Hacker*. O vazamento dos dados resultou em diversos golpes, dentre eles, o envio de um boleto falso em nome da escola da filha de um dos participantes.

DESCRIÇAO DO PROBLEMA

Trata-se de um estudo de caso fictício, cuja personagem, denominada J.M.N., residente em Lauro de Freitas - BA, 38 anos de idade, casada, engenheira química e doutorando do Programa de Pós-Graduação da Universidade Federal da Bahia foi vítima de um golpe. J.M.N. começou a receber diversas mensagens

em redes sociais e ligações telefônicas lhe oferecendo produtos e serviços, além de cartões de créditos não solicitados.

Após algum tempo, J.M.N. recebeu um boleto bancário referente a mensalidade da escola de sua filha de 8 anos, e o pagou. Dias depois, recebeu uma ligação da escola referindo que havia um débito referente ao mês de junho, mesmo mês do boleto que ela havia recebido e pago. Analisando os fatos, J.M.N. chegou à conclusão de que havia recebido um boleto falso.

Ao procurar o PROCON, um funcionário da entidade a informou que várias pessoas relataram o mesmo problema e que, houve um vazamento de dados pessoais em uma empresa de *marketing* contratada por um *shopping* da capital Baiana. J.M.N. se recordou de ter participado do sorteio e preenchido um formulário em um *totem* de autoatendimento, desenvolvido por uma empresa de *marketing* contratada pelo *shopping*.

O formulário, além de exigir uma foto da nota fiscal com valor acima de R$350,00, continha inúmeras informações como: endereço, RG, CPF, uma foto tirada na hora, idade, gostos pessoais, perfil do *Facebook, LInkedin,* se era casada, tinha filhos, idade dos filhos, escola onde eles estudavam, se morava de aluguel ou tinha casa própria, se tinha animal de estimação, se usava óculos, se estava trabalhando, entre outros.

Após o preenchimento de todas estas questões, as informações eram gravadas em um sistema e J.M.N., assim como outros clientes que participaram do tal sorteio, receberam um bilhete com um número para concorrer ao prêmio.

Devido ao vazamento dos dados, a reputação do *shopping* foi abalada nas redes sociais, e quando questionado, o mesmo colocou a culpa na empresa de *marketing* contratada para realizar o sorteio. Já a empresa de *marketing* alegou que um *hacker* invadiu o sistema, roubando as informações pessoais dos participantes do sorteio, assim como dados da empresa, alegando que a mesma também fora lesada.

DIAGNÓSTICO DO PROBLEMA

Inúmeros fatores foram cruciais para que tanto J.M.N., quanto tantos outros clientes participantes do sorteio, fossem vítimas de golpes onerosos.

De início, observou-se que, houve uma falha altamente comprometedora por parte do *shopping*.

Este, por ser responsável pela contratação de uma empresa que realizaria um sorteio para seus clientes, dentro de suas dependências, deveria ter verificado a idoneidade da empresa em questão, assim como, se a mesma havia implantado

em seu sistema todas as técnicas necessárias para garantir a segurança das informações nele contidas.

Houve falha também por parte da vítima, J.M.N., que, por sua vez, preencheu todas as informações solicitadas pelo formulário, informações estas que são extremamente desnecessárias para a realização de um simples sorteio. J.M.N. deveria ter questionado o porquê da necessidade de se preencher tantas questões irrelevantes ou até mesmo, deixar de preencher o formulário. Afinal de contas, não estava claro a finalidade dos dados fornecidos.

J.M.N. deveria também ter dado mais importância a quantidade de ligações, mensagens em redes sociais e até mesmo cartões de créditos não solicitados que vinha recebendo desde então. Da mesma forma como deveria ter checado o destinatário do pagamento do boleto bancário em nome da escola de sua filha, se era o mesmo que estava habituada a realizar os pagamentos ou não.

A empresa de *marketing*, contratada para realizar o sorteio, alegou ter sofrido um ataque de um *hacker*, e que devido a isso, também foi lesada. Porém, em momento algum, a empresa procurou denunciar o ataque às autoridades responsáveis, como também não provou sua boa-fé ao permitir que o sistema usado para a realização do sorteio coletasse tantas informações desnecessárias dos participantes.

PROPOSIÇÃO DE SOLUÇÃO

Por se tratar de vazamento de dados pessoais, poderiam ser adotadas sanções contidas na LGPD (BRASIL, 2019). Para entender melhor como alinhar os acontecimentos, com o que determina a Lei, deve-se considerar algumas informações contidas no Art. 5º do Capítulo I da LGPD e compará-las com os fatos descritos no estudo de caso. São elas:

I- Dado pessoal: informação relacionada a pessoa natural identificada ou identificável;

IV- Banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico;

V- Titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;

VI- Controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;

VII- Operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;

X- Tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

Considera-se que, os dados pessoais, são as informações fornecidas por J.M.N. no momento em que ela preencheu o formulário solicitado para participar do sorteio; O banco de dados, é o local onde todas estas informações colhidas foram armazenadas, dentro de um sistema sob domínio da empresa de *marketing*; O titular em questão é a vítima, J.M.N.

O controlador e operador, são pessoas tecnicamente capacitadas que controlam e operam o sistema de informações usado pela empresa de *marketing* para realizar o sorteio; Por fim, o tratamento é toda a operação realizada pela empresa de *marketing* e por seus colaboradores, os quais tinham acesso aos dados fornecidos por J.M.N.

A forma como ocorreu o tratamento dos dados é de extrema importância, para isso, devemos analisar os termos do Art. 6º da LGPD. Cabe ao tratamento dos dados pessoais os seguintes princípios:

I - Finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;

II - Adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;

III - Necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;

IV - Livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;

V - Qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;

VI - 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;

VII - Segurança: utilização 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;

VIII - Prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;

IX - Não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;

X - Responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

Diante do exposto, podemos observar que, na coleta de dados pessoais dos clientes participantes do sorteio, a finalidade foi exposta – sorteio de um carro – porém, a necessidade não está de acordo com os termos da lei.

Haja vista que, não foram coletados apenas dados estritamente necessários para que fosse realizado o sorteio, e sim, foram solicitados dados descabidos como, se a pessoa usava óculos, se tinha filhos, se os mesmos estudavam em escola particular, animais de estimação entre outros. Não foi exposto aos clientes, ou seja, titulares dos dados, o livre acesso, qualidade dos dados e transparência dos mesmos.

Quanto à segurança, prevenção e responsabilização e prestação de contas, podemos afirmar claramente de que não houve nenhuma atitude por parte das empresas envolvidas.

Segundo consta na Seção III do capítulo VI da LGPD, controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo, ou seja, é de responsabilidade da empresa de *marketing*, coletora dos dados, a reparação dos danos causados às vítimas.

Segundo a empresa, os dados foram violados por um *hacker*, porém, conforme consta no parágrafo segundo do Art. 48 da LGPD, o controlador, responsável pelo tratamento dos dados, deveria ter informado às autoridades e aos titulares acerca do vazamento de seus dados mencionando ao menos:

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;

VI - As medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.

Caso as autoridades competentes tivessem sido informadas, poderiam tomar medidas como meio de mitigar ou até mesmo reverter os efeitos do incidente, assim como, avaliar quais medidas foram adotadas pela empresa para evitar que terceiros possam ter acesso às informações.

Pode-se citar como ter um sistema estruturado que realiza o tratamento das informações de forma a atender todos os requisitos de segurança e padrões de boas práticas previstos em lei e em normas regulamentares.

Assim como J.M.N., as vítimas titulares que tiveram seus dados vazados e consequentemente foram lesadas financeiramente, devem acionar a Autoridade Nacional de Proteção de Dados (ANPD), para que, juntamente à justiça, apliquem as sanções administrativas previstas em lei, que vão desde advertência, a multas milionárias, suspensão temporária do banco de dados a que se refere a infração, bloqueio dos dados pessoais ao que se refere a infração, dentre outros.

CONCLUSÃO

Diante da análise do estudo de caso, podemos concluir que, a Segurança da Informação é fundamental atualmente, pois estamos vivendo uma era altamente tecnológica, onde grande parte da população tem acesso a milhões de informações o tempo todo.

Devemos ter muito cuidado ao fornecer dados pessoais sem ter conhecimento da destinação destes dados e procurar sempre ficarmos informados/atualizados quanto a nossos direitos e deveres sobre tais informações, ficando atento também quando algo acabar lesando-o, seja de forma financeira, moral, ética ou de qualquer outra maneira.

A Lei Geral de Proteção de Dados veio justamente para impedir que fraudes como a estudada aconteçam, afinal se possuirmos uma lei que respalda os usuários quanto ao uso de seus dados pessoais é de extrema importância, pois todos os órgãos sejam eles compostos por pessoas físicas ou jurídicas, tem a obrigação de explanar aos usuários, consumidores e fornecedores de dados pessoais, o armazenamento, a finalidade e principalmente o tratamento dos dados fornecidos.

Isso gera uma segurança maior ao proprietário dos dados, a LGPD assegura a ele inclusive a retirada de seus dados a qualquer momento, de qualquer lugar.

Além da importância dos órgãos fiscalizadores e responsáveis por assegurar o que a LGPD determina, e da readequação das empresas que detém dados pessoais.

REFERÊNCIAS

ALECRIM, E. A controvérsia dos 50 milhões de perfis do Facebook manipulados pela Cambridge Analytica. **Tecnoblog**. 2017. Disponível em: < https://tecnoblog.net/236612/facebook-cambridge-analytica-dados/. Acesso em: 23 de out. de 2020.

ARAÚJO. F. Cinco dicas para se proteger de um boleto falso. **SERASA**. 2020. Disponível em: <https://www.serasa.com.br/ensina/seu-cpf-protegido/boleto-falso/> Acesso em: 12 de nov. 2020.

BARRETO, A. A. A questão da informação. **São Paulo em Perspectiva**, São Paulo, v. 8, n. 4, p. 3-8, 1994.

BASTOS, A.; CAUBIT, R. **ISO 27001 e 27002** - Uma Visão Prática. Porto Alegre, RS: Módulo Education Center, 2009. 257p.

BOLETO FRAUDADO: de quem é a responsabilidade? **Cobre Facil**. 27 de jul. de 2020. Disponível em: https://www.cobrefacil.com.br/blog/responsabilidade-boleto-fraudado. Acesso em: 30 de nov. de 2020.

BBC NEWS. Entenda o escândalo de uso politico de dados que derrubou o valor do Facebook e o colocou na mira das autoridades. G1. 20 de mar. de 2018. Disponível em: < https://g1.globo.com/economia/tecnologia/noticia/entenda-o-escandalo-de-uso-politico-de-dados-que-derrubou-valor-do-facebook-e-o-colocou-na-mira-de-autoridades.ghtml>. Acesso em: 21 de out. de 2020.

BRASIL. **Lei Geral de Proteção de Dados Pessoais (LGPD)**. Lei nº 13.709, de 14 de Agosto 2018. Redação dada pela Lei no 13.853, de 2019. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 16 Out. 2020.

LYRA, M. R. **Governança da Segurança da Informação.** 1. ed. Brasilia. 2015. ISBN: 978-85-920264-1-7

PINHEIRO, P. P. **Proteção de Dados Pessoais:** Comentários à Lei n. 13.709/2018 – LGPD. 2. ed. Saraiva Educação, 2020. ISBN 9788553613403.

TUMELERO, T. Mais abrangente, Lei de Proteção de Dados da Califórnia entra em vigor. **NSC Total.** 10 de jan. de 2020. Disponível em: < https://www.nsctotal.com.br/noticias/mais-abrangente-lei-de-protecao-de-dados-da-california-entra-em-vigor>. Acesso em: 05 de nov. de 2020.

Os autores declararam não haver qualquer potencial conflito de interesses referente a este artigo.