PROSPECTUS
ISSN 2674-8576 Gestão e Tecnologia
Projeto Interdisciplinar

PROPOSTA DE ADEQUAÇÃO À LGPD: UM ESTUDO DE CASO HIPOTÉTICO

LGPD ADAPTATION PROPOSAL: A HYPOTHETICAL CASE STUDY

Brendon Benegas[1], Elenilson Lima de Freitas[1], Richard Alexandre Idesti Junior[1], Thalles Ariel de Oliveira[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

A Lei Geral de Proteção de Dados (LGPD) é a legislação brasileira que regula as atividades de coleta e tratamento de dados pessoais e que estabelece um padrão de regras a serem seguidos no intuito de proteger os titulares de dados. O presente trabalho tem o objetivo de apresentar métodos de adequação à LGPD fazendo uma breve análise de um estudo de caso envolvendo tratamento de dados pessoais, vazamento de dados e a utilização maliciosa desses. Tendo como resultado uma proposta de solução do problema listando passos importantes a serem tomados a fim de evitar que problemas como o do caso estudado ocorram.

Palavras-chave: LGPD. Coleta de dados. Tratamento de dados.

ABSTRACT

The General Data Protection Law is the Brazilian legislation that regulates the activities of collection and processing of personal data and that establishes a standard of rules to be followed in order to protect data subjects. The present work aims to present methods of adaptation to the LGPD by making a brief analysis of a case study involving treatment of personal data, data leakage and the malicious use of these. Resulting in a proposal to solve the problem, listing important steps to be taken in order to prevent problems such as the case studied from occurring.

Keywords: LGPD. Data collection. Data processing.

INTRODUÇÃO

Promulgada no final de 2018, a Lei Geral de Proteção de Dados (LGPD) determina que qualquer pessoa jurídica ou física, seja um médico, advogado, comerciante ou qualquer profissão ou negócio que faz a captação de informações de pessoas, mesmo que seja o mínimo de informações tais como nome, CPF, RG, endereço etc., precisa seguir um padrão de regras que tem como base a regulamentação europeia (GDPR) (DONDA, 2019).

A lei tem a intenção de garantir proteção dos dados das pessoas físicas usando de sansões e penalidades como multas, a fim de motivar o seu cumprimento dentro das empresas (DONDA, 2019).

O presente trabalho tem como objeto de estudo métodos para adequação de empresas à LGPD. Estabelece-se, portanto, o seguinte objetivo geral: identificar os problemas contidos no estudo de caso que dizem respeito à Lei Geral de Proteção de Dados e propor formas de adequação. Como objetivos específicos, têm-se: analisar, descrever e detalhar os problemas contidos no objeto de estudo, bem como seu contexto; descrever o que pode ocorrer se os problemas não forem solucionados, consequências e impactos; descrever sugestões de melhoria.

A adequação das empresas à LGPD é obrigatória e está associada ao tema da segurança da informação, que está diretamente relacionada com a proteção de dados, tanto da organização quanto de seus clientes (MENDES; DONEDA, 2020). Essa lei traz diversos pontos positivos como por exemplo o fato de que as empresas não podem mais tratar os dados de terceiros como bem entendem, como feito anteriormente.

O presente estudo de caso envolve uma ocorrência de vazamento de dados durante uma ação de *marketing* de um *shopping center*, logo, tem-se vários atores que compõem o caso, sendo elas o *shopping*, a empresa de marketing e a vítima, e através da LGPD, será feito uma avaliação das problemáticas ocorridas durante esta ação de *marketing* que de alguma forma foram contrárias ao que diz a lei.

Segundo Branco (2018) a LGPD foi aprovada depois de quase 10 de anos de espera. A LGPD, ou Marco Civil da Internet, foi criada em 14 de agosto de 2018 e visa medidas preventivas e proativas na manutenção e privacidade dos dados de terceiros.

A LGPD entrou em vigor em maio de 2020, tornando-se uma realidade para todo o país, ela enfatiza a construção de uma política de segurança da Informação, buscando explorá-la sobre as principais normas, cujo princípio é proteger a privacidade dos cidadãos brasileiros, aplicando-se a instituições públicas e privadas (RODRIGUES, 2019).

A seguir, os pontos principais que estão presentes na política de privacidade e suas descrições abaixo, conforme previsto no Artigo 5º, redação dada pela Lei nº 13.853, de 2019 (BRASIL, 2019):

- **Dado pessoal**

São todos os dados de informação que estão relacionadas a uma pessoa.

Art. 5º, I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;

- **Dado pessoal sensível**

É o tipo de dados que permite revelar informações pessoais sobre a pessoa e dessa forma podendo gerar atos discriminatórios.

Art. 5º, II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

- **Dados anônimos**

Todas as informações que não possuí vínculo direto com o seu titular.

Art. 5º, III - dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;

- **Banco de dados**

Art. 5º, IV - banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico;

- **Titular**

Art. 5º, V - titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;

- **Controlador**

O controlador está encarregado de tomar decisões sobre o processo que irá tratar os dados pessoais.

Art. 5º, VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais.

- **Operador**

O controlador tem o papel de realizar o tratamento das informações em nome do controlador.

Art. 5º, VII - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.

- **Encarregado**

É a ponte de troca de informações entre o controlador, os titulares e a autoridade nacional da produção de dados (ANTD).

Art. 5º, VIII - encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD).

- **Agente de tratamento**

Os agentes de tratamento são compostos pelo Controlador, operador e encarregado.

Art. 5º, IX - agentes de tratamento: o controlador e o operador.

DESCRIÇAO DO PROBLEMA

O caso estudado envolve um *shopping center* da capital baiana, uma empresa de *marketing* e uma residente da cidade de Freitas Bahia, J.M.N., engenheira, de 38 anos, que começou a receber diversas ligações telefônicas e mensagens em suas redes sociais, oferecendo-lhe produtos e serviços do qual ela não conhecia, cartões de créditos não solicitados por ela, além de um boleto se passando por uma cobrança emitida pela escola que a filha dela frequenta, boleto esse que a engenheira pagou acreditando ser autêntico.

Ao receber uma notificação da escola informando que a mensalidade do mês não tinha sido paga, J.M.N. percebeu que foi vítima de um golpe e decidiu acionar o PROCON, que a informou que problemas parecidos estavam ocorrendo com diversas outras pessoas, devido a um vazamento de dados pessoais ocorrido em uma empresa de *marketing* contratada pelo *shopping* que ela havia fornecido diversos dados para participar de uma promoção e poder concorrer a um carro, após fazer uma compra no valor acima de R$ 350,00.

Na promoção em que J.M.N. participou, foi utilizado um sistema de inteligência artificial desenvolvido pela própria empresa de *marketing* para coletar diversos dados pessoais dos consumidores, sendo algum desses: endereço, RG, CPF, sua foto tirada na hora e sua idade, sendo solicitado até mesmo que respondesse se estava trabalhando, seus gostos pessoais, seu perfil no *Facebook*, no *Linkedln*, se era casada, se tinha filhos, a idade deles, a escola em que eles estudavam, se morava de aluguel ou tinha casa própria, se tinha cachorro ou gato, se usava óculos e diversos outros dados sem deixar os titulares cientes do motivo de estar os coletando.

Ao ser questionado pelo acontecimento, o representante do *shopping* afirmou que os infortúnios ocorridos eram de responsabilidade da empresa

contratada na campanha, enquanto a empresa de *marketing* alegou ter sofrido ataque de um *hacker* que roubou tais informações, lesando também a mesma que teve seus dados estratégicos vazados, o que repercutiu em grandes prejuízos à empresa.

O ocorrido resultou em responsáveis não nomeados, problemas não resolvidos e diversas pessoas físicas e jurídicas prejudicadas

DIAGNÓSTICO DO PROBLEMA

As fragilidades detectadas nesse estudo de caso por parte do *shopping* foram: não se informar corretamente se a empresa contratada trataria os dados sensíveis dos clientes de forma correta e responsável; não se responsabilizar pelos dados coletados dos clientes. Já, por parte da empresa contratada pelo *shopping* foram: coletar dados que não possuem relação com o sorteio realizado; coletar muitos dados sensíveis; falta de processos de segurança da informação bem elaborados.

Por parte da vítima também pode-se citar alguns problemas como: o fornecimento de dados pessoais sem se importar com o que vão fazer com eles; ignorar vazamento de dado e a falta de conscientização da importância dos seus dados.

Após a análise e detecção dos problemas envolvidos na ação de *marketing* do *shopping* e que culminou com o vazamento de dados da cliente deve-se destacar as seguinte vulnerabilidades envolvidas: a falta de conscientização por parte dos clientes a respeito da importância dos seus dados pessoais, que permitiu que suas informações fossem obtidas pela empresa; a falta de rigorosidade no processo de contratação, o qual permitiu que o *shopping* contratasse uma empresa negligente com a segurança dos dados dos clientes; negligência por parte da empresa de *marketing* em relação a segurança de dados, que permitiu que houvesse uma brecha a ser aproveitada pelos invasores. Se a cliente não tivesse ignorado os sinais, como o recebimento de um cartão de crédito o qual não foi requisitado, ela poderia ter identificado o vazamento dos seus dados mais cedo. Caso esses problemas não venham a ser corrigidos eles podem vir a acontecer novamente e tanto o *shopping* quanto a empresa de *marketing* podem ser penalizadas pela Autoridade Nacional de Proteção de Dados (ANPD).

PROPOSIÇÃO DE SOLUÇÃO

Após as considerações elencadas no diagnóstico do problema, define-se algumas propostas de solução para a problemática e que foram divididas em seis categorias para que as empresas do caso estudado possam estudar a viabilidade e a adequação a legislação, no caso a LGPD, tendo-se por base o estudo e argumentos dos seguinte autores e Donda (2020), Miragem (2019), Carvalho e colaboradores (2019), Garcia e colaboradores (2019) e Rapôso e colaboradores (2019).

A primeira etapa importante para o processo de adequação à nova lei é a criação e um comitê especializado, formado por profissionais das diversas áreas da empresa que serão afetadas. O propósito desse comitê é garantir que a empresa opere dentro dos princípios legais e atenda aos requisitos da lei avaliando os riscos e definindo os códigos de conduta.

O oficial de proteção de dados, ou DPO na sigla em inglês para *Data Protection Officer*, é o profissional responsável pelas questões referentes a proteção de dados dentro da empresa; além de liderar o comitê e organizar as ações de proteção de dados, ele auxilia a empresa a adaptar seus processos de forma a ter um foco mais na segurança dos dados tanto da organização quanto dos clientes.

O mapeamento de dados é o processo de adaptação mais importante e complexo da LGPD, sendo primeiramente necessário saber onde estão localizados os dados para aplicarmos o tratamento correto e estabelecer quais serão os mecanismos de proteção que serão utilizados. Este processo é essencial para entender de fato o ciclo de vida dos dados dentro da organização. Nesse primeiro momento é necessário mapear onde estão as informações. No estudo de caso podem ser utilizados alguns *softwares* para auxiliar a identificar onde estão as informações e classificá-las, pois no cenário real o controle sobre a informação é muito distribuído.

Para adequar-se às regulamentações e adotar padrões de segurança da informação pode-se contratar profissionais especializados ou até mesmo recorrer ao suporte de empresas de consultoria da área.

Deve-se identificar quais tipos de dados sensíveis estão sendo coletados e reavaliar a real necessidade da coleta dessas informações, valendo destacar que após realizado o mapeamento do ciclo de vida dos dados, o processo de identificação de vulnerabilidades fica mais fácil. A realização de controle e monitoramentos dos acessos e do tratamento dos dados é de considerável importância.

Os três pilares da segurança da informação - integridade, disponibilidade e confidencialidade - envolvem diretamente o tema de possíveis desastres, pois

este assunto engloba riscos de perda de informação, e como especificado no artigo 46, precisamos adotar medidas de segurança para possíveis desastres.

É necessário identificar quais os ativos com maior valor para o negócio e quais têm maior risco de serem comprometidos em caso de um desastre. É comum que a maioria dos sistemas de recuperação contra desastre utilize tecnologias de *backup*.

É sempre importante validar se os *backups* que foram feitos estão funcionando corretamente caso seja necessário recuperá-los. Existem outras tecnologias de segurança, como replicação ou redundância de *software/hardware*. É importante sempre garantir a confidencialidade, disponibilidade e integridade dessas informações.

A realização de auditorias é essencial para garantir a Segurança da Informação e possibilita a documentação e registro das operações, conforme requer o artigo 37. A implantação de *softwares* de auditoria facilita o processo de documentação por possibilitar a classificação e automação dos relatórios.

Em casos de incidentes de segurança o artigo 48 define que o operador dos dados deve notificar a autoridade nacional e esses relatórios são essenciais para o detalhamento adequado da situação.

CONCLUSÃO

A sociedade ainda não tem consciência dos potenciais benefícios e riscos do processo de digitalização em curso no Brasil e no mundo.

Muitos consumidores aceitam os termos de negócios *on-line* sem terem lidos, permitindo que empresas continuem com a coleta de dados, que nem sempre tem relação com o produto ofertado.

É necessário que as legislações acompanhem os avanços tecnológicos na mesma velocidade em que o uso de bens e serviços cresce no mundo globalizado. Por esse motivo, o estudo de caso desenvolvido apresenta o modelo de regulamentações sobre tratamento de dados pessoais tendo em vista a garantia dos direitos fundamentais para a proteção da dignidade humana.

No entanto, há um longo caminho para que as disposições da LGPD possam de fato proteger os dados pessoais e a segurança de seus titulares. Isso porque algumas questões relevantes sobre as formas de cumprimento à LGPD carecem de regulamentações a respeito das suas sanções.

O Brasil está implementando um novo marco regulatório e estabelecendo uma mudança cultural no âmbito da proteção de dados, com isso espera se proporcionar meios mais claros e eficazes para as pessoas zelarem pelas

informações que lhe dizem respeito. Diferente do que vem acontecendo em outros países, pois apenas estão reformando ou atualizando seus modelos nacionais existentes.

Afinal, a proteção do consumidor e do direito fundamental à privacidade encontram amparo no princípio fundamental da dignidade da pessoa humana, de modo que o indivíduo não pode ser tratado como uma coisa ou objeto, cujos dados possam ser tratados sem o devido respeito às normas vigentes.

REFERÊNCIAS

BRANCO, S. **As Hipóteses de Aplicação da LGPD e as Definições Legais**. In: MULHOLLAND, C. (org.). A LGPD e o Novo Marco Normativo no Brasil São Paulo. Série Pautas em Direto. Porto Alegre: Arquipélago Editorial, 2018 (*e-book*).

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.

CARVALHO, L.; OLIVEIRA, J. CAPPELLI, C.; MAJER, V. Desafios de transparência pela Lei Geral de Proteção de Dados Pessoas. **Anais do VII Workshop de Transparência em Sistemas (WTRANS)**, XXXIX Congresso da Sociedade Brasileira de Computação, Belém, Pará, 2019.

DONDA, D. **Guia Prático de Implementação da LGPD:** tudo o que sua empresa precisa saber para estar em conformidade. São Paulo: Labrador, 2020.

GARCIA, L. R.; AGUILERA-FERNANDES, E.; GONÇALVES, R. A. M.; PEREIRA-BARRETO, M. R. **Lei Geral de Proteção de Dados Pessoais.** São Paulo: Editora Edgard Blücher Ltda., 2019.

MENDES, L. S.; DONEDA, D. Reflexões iniciais sobre a nova Lei Geral de Proteção de Dados. **Revista de Direito do Consumidor**, v. 120, ano 27, p. 469-483, 2020.

MIRAGEM, B. A Lei Geral de Proteção de Dados (Lei 13.709/2018) e o direito do consumidor. **Revista dos Tribunais Online**, v. 1009, p. 1-35, 2019.

RAPÔSO, C. F. L.; LIMA, H. M.; OLIVEIRA JUNIOR, W. F.; SILVA, P. A. F.; BARROS, E. E. S. LGPD - Lei Geral de Proteção de Dados Pessoais em tecnologia da informação: revisão sistemática. **Revista de Administração do Cesmac**, v. 4, p. 58-67, 2019.

RODRIGUES, T. F. Análise do sistema de segurança da informação da empresa NDD. **Repositórios de relatórios** - Engenharia de Produção, n. 1, 2019.

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