doi.org/ 10.51891/rease.v8i7.6340

A ADEQUAÇÃO E A EXECUÇÃO DA LGPD 13.709/18 EM FACE AS EMPRESAS, E SUA PROTEÇÃO DOS DADOS PESSOAIS

THE ADEQUACY AND ENFORCEMENT OF LGPD 13.709/18 AGAINST COMPANIES AND THEIR PROTECTION OF PERSONAL DATA

Italo Hérlon Gomes Bezerra[1]
Luis Felipe Carvalho Vieira[2]
Patrícia Nascimento[3]

RESUMO: A proteção dos dados pessoais foi um tema bastante recorrente em diversas discussões da atualidade, pois envolveu questões públicas e privadas, tanto em relações pessoais como em relações de mercado como no caso de clientes e empresas, que abrangeram assim várias áreas do direito. O objetivo deste trabalho foi analisar a eficiência da nova lei de proteção de dados a chamada LGPD, visando no seu funcionamento no âmbito das empresas. Com o isso foi procurado soluções para diminuir os crimes envolvendo o vazamento de dados, o presente trabalho foi feito, a partir de pesquisa bibliográfica, e documental, por meio de relatórios, artigos e notícias realizados acerca do tema, o trabalho tratou no primeiro tópico acerca da sociedade tecnológica e sua relação com a proteção de dados pessoais, no segundo tópico demonstrou as consequências negativas do avanço tecnológico para a proteção dos dados pessoais. Por fim o terceiro tópico apresentou soluções para os problemas abordados anteriormente.

Palavras-chave: LGDP. Sociedade Tecnológica. Software e Hardware. Proteção dos Dados. Falhas nos Sistema. Soluções para as Falhas.

ABSTRACT: The protection of personal data was a very recurrent topic in several current discussions, as it involved public and private issues, both in personal relationships and in market relationships as well as in the case of customers and companies, which thus covered various areas of law. The objective of this work was to analyze the efficiency of the new data protection law called LGPD, aiming at its operation in the scope of companies. With that, solutions were sought to reduce crimes involving data leakage, the present work was done, from bibliographic and documentary research, through reports, articles and news made on the subject, the work dealt with in the first topic about the technological society and its relationship with the protection of personal data, in the second topic, it demonstrated the negative consequences of technological advances for the protection of personal data. Finally, the third topic presented solutions to the problems discussed above.

Keywords: LGDP. Technological Society. Software and Hardware. Data Protection. System Failures. Solutions for Failures.

[1] Bacharelando em direito.
[2] Bacharelando em direito. E- mail: lipevieira123453482@gmail.com.
[3] Instituição: Christus Faculdade do Piauí – CHRISFAPI.

INTRODUÇÃO

Dada a criação do novo regulamento de proteção de dados, a LGPD no Brasil, assim como demais países pioneiros a tratar do assunto, tiveram de se adequar ao surgimento desse novo mundo do direito virtual.

Apesar de haver citações do tema distribuídos no nosso Código Penal brasileiro, ou adequações da lei, como por exemplo, o crime de estelionato, que em seu art.171 do CP dispõe de diversos fatores, mas dentro do nosso contexto onde o tema da segurança jurídica virtual que seria esparsa, analisando a situação hipotética, em que um cidadão que permite abrigar seus dados em uma empresa, onde ele acha que é segura e que garante a aplicação de todos os meios necessários para armazenar os dados com segurança. Um operador que viesse a realizar a captura de dados para obter vantagem própria patrimonial, responderia apenas por estelionato, mas hoje seria resguardado pela nova lei e também receberia reparações do dano como prevê o art. 42 disposto na LGPD.

Questiona-se a eficácia de programas de segurança digital adotados por empresas e a adequação à essa nova lei, onde ainda está nos seus primeiros passos no cenário nacional. E ainda se encontra um grau inversamente proporcional à grandeza das empresas, onde encontramos fragilidades na proteção dos dados, onde as maiores empresas têm menor vulnerabilidade na proteção e as pequenas empresas com maior vulnerabilidade, essas que lutam para se adequar, sendo que na maior proporção, não houve adequação a lei.

Este estudo, portanto, traz como tema delimitado “A adequação e a execução da LGPD em face as empresas e sua proteção dos dados pessoais.” Demonstrando a necessidade de que as empresas estejam conformes em face à lei geral de proteção de dados para assim ter um ciclo contínuo de ajustes e busque a segurança digital continuadamente, assegurando assim a proteção dos dados de clientes, colaboradores e parceiros contra vazamentos, pois esses dados cada vez mais tornam-se vulneráveis e valiosos, razão da qual seja se faz necessidade da constante inovação tecnológica defensiva, assim como a inovação jurídica para proteção legal.

Ainda buscou-se apontar as fraquezas que os sistemas de segurança podem apresentar, uma vez que quanto mais se aplicam softwares e táticas de proteção, encontram-se cada vez mais, mais brechas. Em 2020, quando a lei ainda estava em estado de vacância,

foram descobertas aproximadamente 19 mil novas vulnerabilidades. Pois como mencionado o processo de evolução é constante, diário. Ao passo que cada vez mais se busca a proteção, o outro lado também evolui em seus cybers attacks. Portando a busca deve ser constante, seja na evolução dos softwares assim como na legislação fazendo assim, com que a LGPD se torne primordial para a melhor proteção dos dados digitais que cada empresa carrega e deve se manter segura.

Com o avanço tecnológico, os dados armazenados se tornaram um ativo intangível de importância, uma vez que estamos cada vez mais conectados, as informações pessoais tornam-se de valor ímpar para as empresas, onde a segurança e confidencialidade geram alto valor pela carga informacional. Desta forma surgiu a problemática: Como as empresas se adequam ao avanço legal da proteção de dados?

Assim sendo temos como objetivo primário: Analisar como as empresas buscam a adequação à lei e como buscam solucionar e se proteger contra-ataques de hackers e vazamentos de dados e como objetivos secundários: Analisar como as empresas buscam o adequação à lei e como buscam solucionar e se proteger contra ataques de hackers e vazamentos de dados. Analisar sobretudo a eficácia na aplicação da nova legislação, esboçar a necessidade da proteção de dados, pois com o avanço tecnológico, se tornaram um ativo intangível de importância.

Este trabalho está pautado na investigação e análise do tema proposto , o que o torna uma pesquisa qualitativa , pois seu foco é analisar e apresentar uma melhor estruturação e relação que o profissional tem com sua empresa, onde segundo Castro (2005) o responsável de um tratamento de dados, deve dar a conhecer ao titular dos dados a realização do tratamento que lhe respeite, indicando, nomeadamente, seus fins, categorias de dados tratados, período de conservação dos dados, eventuais comunicações dos mesmos, assim como sua confidencialidade, e necessidade de autorização prévia para utilização ou eliminação destes, buscando sempre o melhor para o mesmo, e propondo melhorias positivas que podem ser feitas nos sistemas de segurança dos dados.

O estudo consiste em um trabalho descritivo de revisão bibliográfica, foi utilizado livros, artigos, reportagens; especialmente RODOTÀ (2008); BURCH (2018); SOPRANA (2018); SILVA (2005); SILVEIRA (2017); VALENTE (2018), bem como legislação pertinente.

1.1 Justificativa

Com o avanço da tecnologia, a proteção dos dados se tornou profundamente necessária. Onde num mundo cada vez mais digitalizado as operações financeiras, dados pessoais, dados de empresas e sociedades ficaram altamente vulneráveis no meio cibernético. Dessa forma tornando a proteção desta inescusável. Além do mais, com a crise do Covid- 19 muitas empresas adotaram e continuaram a modalidade de trabalho a distância, tornando a proteção de dados ainda mais essencial.

Pois como mencionado o processo de evolução é constante, diário. Ao passo que cada vez mais se busca a proteção, o outro lado também evolui em seus cyber attacks. Portando a busca deve ser constante, seja na evolução dos softwares assim como na legislação fazendo assim, com que a LGPD se torne primordial para a melhor proteção dos dados digitais que cada empresa carrega e deve se manter segura.

2 REFERENCIAL TEORICO

O uso da tecnologia em uma sociedade foi de uma complexa demanda, dessa forma, foi necessário analisar como a lei se adequou junto à sociedade tecnológica e como as empresas estiveram tornando esses dispositivos eficazes de maneira segura que não trouxesse malefícios, tanto para a empresa, como para o titular de uma obrigação.

> O resultado do surgimento da internet e suas diversas ramificações é a globalização foi uma mudança significativa na forma em que se vive a sociedade e toda estrutura social teve que se alinhar a essas mudanças incluindo o próprio sistema: governo, empresas e os próprios cidadãos que o movimentam, conforme afirmou o sociólogo CASTELLS (2003, p. 225)

A Galáxia Internet é um novo ambiente de comunicação. Como a comunicação é a essência da atividade humana, todos os domínios da vida social estão sendo modificados pelos usos disseminados da Internet, como este livro documentou. Uma nova forma social, a sociedade de rede, está se construindo em torno do planeta, embora sob uma diversidade de formas e com consideráveis diferenças em suas consequências para a vida das pessoas.

Essa nova realidade trazida pelo advento da internet trouxe consigo seus malefícios e por conta disso foi preciso estar sempre atento as singularidades desse novo formato, no qual se encontrou um universo de informações e interações tecnológicas, sendo assim foi

necessário criar a existência de uma legislação que protegesse os indivíduos do perigo da internet, no que se referiu a segurança dos seus dados pessoais.

2.1 A LGPD aplicada na nova sociedade tecnológica

A LGPD no Brasil foi apenas uma das variadas regras que foram sendo estabelecidas no mundo todo para a proteção de dados pessoais e privacidade dos indivíduos online, princípios e critérios legalmente aceitos foram fundamentais para organizar esse universo que ainda dispõe de pouca transparência e segurança. Sendo assim, o objetivo dessa norma foi para proteger os dados pessoais de fornecedores, clientes de empresas, cadastros que foram armazenados em empresas ou em seus provedores de internet, para que nenhum dos dados fossem roubados ou transferidos para outrem sem nenhum consentimento ou autorização do titular.

> Foi bastante difícil de crer que grandes empresas como o, WhatsApp, a Apple, entre outras, que investiram milhares de dólares, para uma programação de alta tecnologia para a segurança dos dados pessoais, foram vítimas de invasões e roubo de informações pessoais. Sendo assim o cidadão precisou estar ciente de qualquer situação onde seus dados pessoais possam ser divulgados e a empresa oferecendo o serviço, precisa garantir essa segurança no tratamento de dados e está interação já foi previamente acertada e regulamentada, como destacou (CASTRO, 2005, p. 230)

[...] esta deve ser determinada – deve ser conhecida antes do início do tratamento -, explícita – o que exclui o tratamento de dados para fins não claramente determinados ou vagos, ou o seu desconhecimento por parte do titular dos dados-, e legítima – não podendo ser contrária à lei, designadamente atendendo à competência ou à bondade do interesse que demonstre ter o responsável pelo tratamento na sua realização.

Dito isso ficou evidente a importância de uma legislação voltada somente para a proteção de dados, pois foram diversos os problemas que o vazamento ou o uso indevido de dados poderia acarretar a uma pessoa ou à uma empresa.

2.1.1 Compartilhamento e proteção de dados pessoais

A finalidade da LGPD (Lei Geral de Proteção de Dados) foi criada para a proteção dos direitos fundamentais de liberdade e a segurança à privacidade dos indivíduos brasileiros ou residente no país. O artigo 5° da lei 13.709/18 discorreu sobre o dado pessoal, que é todo dado de reconhecimento de um indivíduo, diante de uma breve distinção: são os dados

sensíveis, que são dados de cunho privado, que destinaram questões biológicas e psicológicas de determinado indivíduo.

2.2 Consequências do vazamento de dados

As possíveis falhas com o vazamento de dados foram ocasionadas de diversas maneiras, como por exemplo: ataques cibernéticos, hackers, funcionários mal-intencionados, perda de notebooks ou laptops, dispositivos roubados, além de falhas nas programações de programas de proteção. Grandes empresas também foram vítimas de situações como essa, como no caso do Facebook que já foi exposto várias vezes e por isso é um dos principais problemas pois não lida com os dados pessoais dos seus usuários com o devido zelo.

Em relação à falta de transparência do funcionamento da empresa, Tim Wu alertou (BURCH, 2018). Há um número abusivo de aplicativos e que buscam por dados pessoais muito mais do que se pensa. Um dos maiores problemas é que o Facebook deu a impressão que se podia controlar a própria privacidade, definindo suas configurações de certas maneiras – porém, essas configurações não alteraram nada. Elas se tratavam de falsos botões. (Tradução nossa).

Um exemplo dos vazamentos de dados que mais ocorreu no Brasil foi quando ocorre um acidente entre os colaboradores de uma empresa, quando um colaborador costumava esquecer pastas confidenciais decodificadas no computador e um colega de trabalho que estava usando o computador, olhou e leu os arquivos confidenciais sem a devida permissão, o colega acessou os dados por engano, mesmo que não houve o compartilhamento de dados, mesmo assim os dados ainda foram violados por um terceiro que sem permissão visualizou os dados que eram para ser protegidos.

Outro caso que ocorreu o vazamento de dados, foi de um funcionário mal-intencionado, o que quer dizer é que o indivíduo acessou e compartilhou os dados alheios para prejudicar uma pessoa ou até mesmo a empresa, mesmo que esse indivíduo tenha autorização legítima para a utilização dos dados, o mesmo usou de má-fé e a sua intenção foi usar informações de forma escusa.

Quando o dispositivo é roubado, a vítima pode ter deixado o dispositivo decodificado ou desbloqueado, ocasionando que um terceiro possa ter acesso a todas as informações nele contido. Já no caso de hackers, o ou os autores usam vetores de ataques para derrubar

sistemas de programação que protegem os dados, lhes dando acesso aos dados que eram criptografados, fazendo com que os mesmos roubassem informações pessoais de uma rede ou de um indivíduo. Então cada ataque tem suas particularidades, que varia conforme cada indivíduo e cada grau de sua violação.

Para evitar os crimes relacionados ao vazamento de dados foi necessário utilizar novas estratégias de defesa, como ocorreu com a questão do consentimento dos titulares que antigamente os aplicativos não pediam autorização, e agora são obrigados a pedir. Para garantir de fato esse direito tem-se que os antigos contratos de "adesão" não são mais aceitos (SOPRANA, 2018).

Nessa toada (SOPRANA, 2018) fala sobre a mudança prática para os cidadãos é: os novos modelos de contratos agora deverão vir com opt-in, um botão que expressa a vontade ou não de o usuário em aceitar fornecer seu dado. Opções pré-marcadas em termos de uso ou em questionários eletrônicos não servirão mais como consentimento.

2.3 Soluções para as falhas

As soluções para as possíveis falhas vieram na adequação da empresa com a nova lei de proteção aos dados, junto de algumas ferramentas que podiam facilitar essa adequação, como: plano de segurança da informação, senhas complexas e autenticação multifator (MFA), proteção dos endpoints, segurança física dos data centers, classificação dos dados, sistemas anti-hackers, funcionários de boa-fé, e funcionários honestos de boa índole.

Para o plano de segurança e informação, foi implementado de uma maneira efetiva e aderente em que a empresa tivesse uma política interna formal totalmente definitiva as ações e responsabilidades dos agentes que se tratavam das informações e dos dados pessoais. A organização foi para estabelecer regas claras e objetivas para criação de um ambiente de adequação a lei geral de proteção de dados.

Para senhas e complexas e autenticação multifator, os usuários normalmente costumavam usar senhas fracas para acessar suas contas corporativas pois, colocando senhas complexas faziam com que os usuários a esqueçam, colocando em risco toda a rede de organização, e fazendo com que os dados fossem ser hackeados ou vazados por qualquer usuário com mais facilidade. Então a solução foi usar senhas mais complexas com maior dificuldade, além de usar autenticação de dois fatores, com essa medida foi possível evitar ataques brutais e dificultou e limita ou as invasões.

3. METODOLOGIA

Este trabalho está pautado na investigação e análise do tema proposto, o que o torna uma pesquisa qualitativa com uma abordagem bibliográfica, pois seu foco é analisar e apresentar uma melhor estruturação e relação que o profissional tem com sua empresa com sua adequação legal, no que se refere aos dados pessoais dos clientes no qual os estes não poderão ser compartilhados por nenhuma pessoa sem autorização explicita. Assim sendo não poderá ocorrer tratamentos de dados que poderão ser utilizados ou eliminados, mas com devida autorização do titular, buscando sempre o melhor para o mesmo e propondo melhorias positivas que podem ser feitas nos sistemas de segurança dos dados.

> A pesquisa bibliográfica é habilidade fundamental nos cursos de graduação, uma vez que constitui o primeiro passo para todas as atividades acadêmicas. Uma pesquisa de laboratório ou de campo implica, necessariamente, a pesquisa bibliográfica preliminar. (ANDRADE, 2010, p. 25).

O estudo consiste em um trabalho descritivo de revisão bibliográfica, foi utilizado livros, artigos, reportagens, ou seja, pode-se usar desta ferramenta como um meio para responder, questionar, avaliar, sobre os temas relacionados ao presente trabalho.

CONSIDERAÇÕES FINAIS

O presente artigo discorreu sobre o processo os conceitos e os objetivos traçados no trabalho em questão sobre normas de proteção de dados pessoais. Da concepção do direito à privacidade, do desenvolvimento e da implementação das normas de proteção de dados pessoais para que as empresas tragam novas melhorias para os indivíduos que usam seus dados na internet. Possuindo assim, fundamento constitucional e assumem a feição de um direito fundamental, com novos programas mais seguros sobre o uso de dados pessoais Sob a égide da LGPD, foi possível revelar os esforços e o grande desafio contemporâneo para assegurar, ao fim, o exercício de soberania do indivíduo, a sua personalidade, a sua privacidade e a sua autodeterminação informativa.

Na atual sociedade da informação sites e aplicativos, com, com garantias mais convictas de que seus dados não vazarão. Assim sendo, ao tratamos sobre a denominada Vigilância Líquida, verifica-se alta produção e processamento de dados pessoais, alimentado por rápida transmissão de dados transfronteiriços que não parecem encontrar obstáculos apesar das distâncias físicas. Alcançando assim um novo patamar alcançou-se um novo patamar

REFERÊNCIAS

ANDRADE, M. M. **Introdução à metodologia do trabalho científico: elaboração de trabalhos na graduação**. São Paulo, SP: Atlas, 2010.

BURCH, Sean. **Facebook Is „Rotten,"Privacy Is Its „Kryptonite,"Says Ex-FTC Advisor:** Social network's business model is at odds with protecting its users, according to one expert. 2018. Disponível em:. Acesso em: 15 jun. 2021.

RODOTÀ, Stefano. **A vida na sociedade da vigilância - a privacidade hoje**. Rio de Janeiro: Renovar, 2008. Tradução de: Danilo Doneda, Luciana Cabral Doneda.

SILVA, José Afonso da. **Curso de Direito Constitucional Positivo**. 24. ed. São Paulo: Malheiros, 2005.

SILVEIRA, Sergio Amadeu da. **Tudo sobre tod@s: Redes digitais, privacidade e venda de dados pessoais**. São Paulo: Edições Sesc, 2017.

SOPRANA, Paula. **O que é a GDPR, a lei de proteção de dados europeia, e por que ela importa.** 2018. Disponível em: . Acesso em: 15 jun. 2018.

VALENTE, Jonas**. Privacidade em perspectivas:** Promovendo a privacidade e a proteção de dados pela tecnologia: Privacy by Design e Privacy Enhancing-Technologies. Organizadores: Sergio Branco e Chiara de Teffé. Rio de Janeiro: Lumen Juris, 2018.