OS IMPACTOS DA LGPD E O COMPLIANCE NAS INSTITUIÇÕES CONTROLADORAS DE DADOS SENSÍVEIS

Fernanda Alves de Souza Silva[1], Guilherme Laureano[2], Renato Violin[3]

[1] Discente do Curso Superior de Tecnologia em Análise e Desenvolvimento de Sistemas / fernanda.silva114@fatec.sp.gov.br
[2] Discente do Curso Superior de Tecnologia em Análise e Desenvolvimento de Sistemas / guilherme.laureano@fatec.sp.gov.br
[3] Docente do Curso Superior de Tecnologia em Análise e Desenvolvimento de Sistemas / renato.violin2@fatec.sp.gov.br

RESUMO

Se antes da pandemia vivíamos em um mundo conectado, o salto digital que ocorreu nos últimos dois anos acelerou todas as estimativas sobre a produção e troca de dados cibernéticos. O avanço da tecnologia e a digitalização dos processos, dos mais simples aos mais complexos, projetam a certeza da necessidade da aplicação de metodologias de segurança cada vez mais rígidas e concisas. Com o ingresso progressivo das informações pessoais e sensíveis dos indivíduos na internet, cresce o peso da importância das informações e a necessidade de torná-las privadas e disponíveis apenas ao portador, tratadas por uma empresa intermediária seguindo os parâmetros da LGPD e supervisionada por um agente de segurança (DPO). A partir destes princípios este artigo analisará o processo sintético do percorrer das informações sensíveis desde à autorização do proprietário, a segurança das informações e suas ramificações até o destino onde a informação digital deverá ser conservada sob a tutela da instituição e/ou do usuário.

Palavras-chave: digital, LGPD, DPO, segurança, privacidade, proteção de dados.

Abstract

If before the pandemic we lived in a connected world, the digital leap that took place over the past two years has accelerated all estimates of production and exchange of cyber data. The advancement of technology and the digitization of processes, from the simplest to the most complex, project the certainty of the need to apply increasingly strict and concise security methodologies. With the progressive entry of personal and confidential information of individuals on the internet, the importance of information grows and the need to make it private and available only to the holder, managed by an intermediary company following the parameters of the LGPD and supervised by a security agent (DPO) grows. Based on these principles, this article will analyze the synthetic process of passing sensitive information from the owner's authorization, the information security, and its consequences to the destination where the digital information must be kept under the supervision of the institution and/or the user.

Keywords: digital, LGPD, DPO, security, privacy, data protection.

1 INTRODUÇÃO

Publicada em 14 de agosto de 2018 e instaurada, após muitos estudos e discussões, no ano de 2021, a nova Lei Geral de Proteção de Dados veio ao Brasil como mais uma ferramenta de suporte ao internauta visando a garantia de proteção dos direitos fundamentais de liberdade e a padronização da manipulação das informações de um indivíduo. A lei representa um marco histórico na regulamentação sobre o tratamento de dados pessoais no país, tanto em meios físicos quanto em plataformas digitais.

Com o objetivo de mitigar o uso indevido e abusivo de dados, a lei é responsável por aprofundar a regulamentação das questões relativas ao uso de dados pessoais no ambiente virtual. O conceito de dados pessoais é representado pelo Art. 5 da Lei 13709/18 que considera dado pessoal como a informação relacionada a pessoa natural identificada ou identificável. Esse dado corresponde a um atributo humano, o artigo também traz outros conceitos correlatos a própria lei, como o dado pessoal sensível, ou seja, dados relacionados a aspectos íntimos do cidadão, como opinião política, filiação religiosa, vida sexual e dados biométricos por isso demandam uma proteção maior, que poderia acarretar algum tipo de discriminação ou preconceito.

Os Impacto da LGPD, são relevantes tanto no aspecto da proteção dos dados pessoais quanto para a atividade empresarial. Pois impacta diretamente na relação e comunicação com os clientes, na coleta e análise de dados pessoais, na rotina dos colaboradores da empresa e consequentemente nos custos. Sendo assim se torna de extrema importância a construção de políticas de segurança de dados de forma clara e concisa, para garantir a compreensão e confiança do cliente. Além de investimentos em uma base de dados segura, imune de possíveis violações. Com é fundamental disseminar os princípios básicos da lei e manter seu corpo de colaboradores atualizados sobre o que a lei exige. Optando por custos com a adequação à lei de proteção de dados ao invés de multas e penalidades de descumprimento da lei.

O conceito de dado pessoal sensível ou não, deixa claro a importância da proteção desses dados, sendo direitos fundamentais dos cidadãos muitas vezes relacionados a liberdade, intimidade, e a privacidade por isso a lei se torna fundamental e o motivo de sua criação. O Art. 1° da LGPD deixa claro esse objetivo, “Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural” (BRASIL, 2018).

Com isto, várias empresas operadoras – assim denominadas pela nova Lei - preparadas ou não, adquiriram a necessidade da adaptação das suas ferramentas para com as controladoras, ou clientes, sob o acompanhamento de um encarregado de Dados responsável pela supervisão das conformidades das novas atitudes a serem tomadas.

O escopo deste artigo é a análise macro da adaptação e metodologias aplicadas a segurança dos dados em instituições controladoras de dados pessoais e sensíveis, além de destacar os principais pontos da lei, informando e esclarecendo a todos que lidam com o tratamento de dados pessoais, a respeito da LGPD e seus impactos. Assim poderemos adequar seus processos internos para desenvolver um ambiente em compliance com a lei.

2 REFERENCIAL TEÓRICO

A nova Lei Geral de Proteção de Dados cuida dos diretos dos titulares dos dados e do comprimento dos deveres das empresas na forma de tratar, armazenar e manipular os dados, onde é aplicada a toda pessoa física ou jurídica de direito público ou privado, não importando a localização de suas bases de dados, desde que a coleta ou o tratamento seja realizado em território brasileiro. Não se aplicando a tratamento de dados realizados por pessoas naturais, para fins particulares sem fins econômicos ou para fins que envolvam a segurança nacional (Brasil,2018).

Com isso é de extrema importância o investimento das empresas em segurança da informação nos setores de TI, evitando problemas futuros como vazamento de dados ou até mesmo ações de má conduta das próprias empresas que muitas vezes

fornecem ou vendem os dados de seus clientes sem seu consentimento, acarretando em multas que podem ser de 2% do faturamento da empresa, limitado a R$52 milhões ou multa diária que pode ser estipulada até que a falha seja corrigida em R$10 à 50 mil ao mês.

3 METODOLOGIA

Metodologia é a definição de como fazer a coleta de dados de uma pesquisa e como fazer a análise desses dados para solucionar o problema do tema escolhido. Por meio dela é que devem ser definidos os instrumentos e fontes para a coleta de dados (Severino, 2002, p 32).

Este artigo possui como metodologia pesquisas bibliográficas e exploratórias. A pesquisa bibliográfica resume-se em consultas nas bases públicas da Constituição Federal, livros, artigos, documentos, entre outros que auxiliem na elaboração desta análise. Como metodologia exploratória, análises de mercado e seus posicionamentos públicos para a melhor compreensão dos impactos e levantamento de informações da concepção do objeto da segurança dos dados e a análise da Lei Federal n^{0}13.709 para compreender as funções e obrigações dos agentes da LGPD.

4 RESULTADOS E DISCUSSÃO

Boas práticas de segurança de dados são recomendadas há mais de 20 anos, porém como não era uma exigência, mas apenas uma recomendação, poucas empresas faziam uso dessas recomendações, afinal isso envolve custos com pessoal, tecnologia e treinamento (POHLMANN, 2020).

Para compreendermos o objeto a ser analisando, dados são composições de informações codificadas, que permitem ser processadas eletronicamente, classificados como distintos e objetivos, quantificáveis e qualificáveis, pessoais e/ou sensíveis onde independentes não conduzem informação alguma (Le Cadic,1996).

Quanto às informações, estas dependem de significados, atribuições e compreensões dos dados. Segundo Capurro e Hjorland (2007) não há uma definição

única, podendo assim ser de caráter polissêmico e que as informações dependem das necessidades interpretativas e habilidades do indivíduo. Esclarecidas as diferenças, passaremos a analisar o percurso de uma informação sensível em uma instituição.

Informações e dados correlatos são gerados a cada momento e aplicados as suas devidas finalidades deixando a empresa alinhada com seu core business, negócio principal ou ainda atividade principal que a *empresa* desempenha.

Suprimidos pela nova LGPD a emissão e armazenagem de conteúdo desnecessários, que ocorria com frequência no período anterior a Lei onde as empresas muitas vezes coletavam as informações dos consumidores sem o seu consentimento e só depois é que decidiam o que fariam com elas.

Para combater possíveis violação de dados, é necessário pensar que o cibercrime evolui em paralelo com as soluções tecnológicas que possibilita vivermos em mundo cada vez mais conectado. Com esta rotina identificamos as possíveis rotas de saída das informações, onde podemos identificar indícios de vazamentos de dados e aplicar ações corretivas.

Como controladora destas informações, as instituições adquirem a tarefa de assegurar a confidencialidade com adaptações físicas e lógicas de seus sistemas de comunicação e informação, como a hipótese da implantação de firewalls físicos controladores dos fluxos de pacotes da rede interna, a identificação dos terminais emissores de informações para o ambiente externo da Instituição e a criação de políticas de tratamentos e armazenamento de dados nos data centers das empresas, prevenindo possíveis vazamentos e outros problemas relacionados à segurança da informação.

Segundo Paludetto e Barbieri (2019), no mundo todo, empresas sofrem com o crescente aumento de ameaça à segurança e confidencialidade dos dados. A implantação de ferramentas operadoras, aquelas que manipulam as informações e dão significado a Instituição controladora, terceirizadas ou próprias, preferencialmente de alta confiabilidade e disponibilidade para àquelas fornecidas por empresas especializadas em dados sensíveis, e devidamente documentadas e codificadas para àquelas próprias da Instituição controladora, é de suma importância para o início do tratamento das informações.

No dia 23/11 no Jornal Globo do Rio de Janeiro, pudemos acompanhar a informação com o título "*Proteção de Dados:* " A união estima arrecadar pelo menos 20 bilhões em multas nos primeiros doze meses de vigência da lei de proteção de dados pessoais''. Com a possibilidade de sofrer punições severas, pode-se concluir que uma das maiores preocupações das empresas está em como proteger os dados coletados. Nesse processo de conformidade torna-se essencial que estas conheçam os agentes e a importância no ciclo de vida da informação em seu meio.

Art. 5º Para os fins desta Lei, considera-se:

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;

Tratamento de dados inclui toda operação realizada com dados pessoais como 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 (DONDA, 2020, p18).

Entende-se que as informações devem ser claras aos proprietários e tratadas pela ferramenta operadora de maneiras que apenas aqueles que necessitem o acesso possam tê-la, em termos técnicos estes dados devem ser criptografados e protegidos de possíveis invasores.

Muitas preocupações das empresas em relação a proteção de dados no ano de 2020-2021 foram pontuadas pelas empresas, visto que o perímetro destas foram abertos para o home office, se tornando necessária a proteção desses usuários remotamente, tornando mais vulnerável seus dados. Período marcado pela despreparação a tais ferramentas de proteção, orçamentos necessários e falta de pessoas qualificadas na área de segurança da informação.

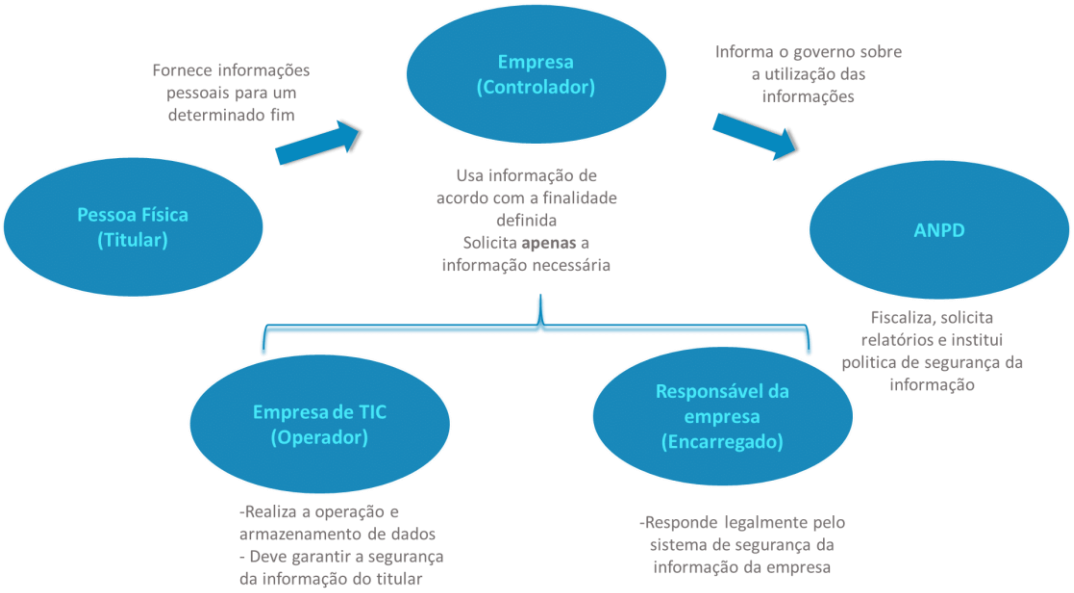
Uma das táticas muito usadas pelos hackers é o *ransomware*, software feito para invadir e sequestrar os dados, bloqueando o acesso dos usuários e/ou obtendo informações sensíveis possivelmente usadas para extorquir a vítima através de pagamento por criptomoeda, moeda digital não rastreável, para assim devolver o acesso a empresa ou a não exposição da pessoa física. A exposição do usuário e o vazamento de informações sensíveis não se trata apenas de um erro é sim de uma cadeia de eventos e escolhas executivas e operacionais no dia a dia, que podem criar essa janela de exposição

Podemos citar como exemplo a Sociedade Brasileira de Informática em Saúde (SBIS) que certifica as Instituições operadoras em diversos aspectos como meios de segurança e confiabilidade, classificando os sistemas de informação em hardware, software, banco de dados, redes, procedimentos e pessoas. Sendo referência em certificações para ERP's da área da saúde, a SBIS orienta e capacita profissionais da área da tecnologia sobre os padrões e atualizações do mercado de serviços de saúde, área que vem se adaptando constantemente as mudanças e exigências da lei n. 13709/18.

As políticas internas de operações das ferramentas de tratamentos de dados bem como padrões tecnológicos devem caminhar em conformidade na Instituição com o intuito de evitar ramificações não consentidas. A elaboração de uma comissão interna de gerenciamento da tecnologia é um passo essencial para se iniciar e entender a semântica entre o proprietário das informações e as posteriores etapas que sua interação com a Instituição venha a ocorrer.

4.1 Exemplo de Ilustrações

Figura 1 – Relação entre os agentes da LGPD



Fonte – Reprodução (Templum - https://certificacaoiso.com.br/lgpd/)

5 CONSIDERAÇÕES FINAIS

A discussão sobre o tratamento das informações não é nova, a LGPD trouxe a certeza da aplicação de uma metódica ferramenta de segurança para a correta disseminação das informações entre as plataformas de comunicação, tendo como chave-mestre de acesso e circulação o consentimento da pessoa de direitos.

Sobretudo, o setor de desenvolvimento sofrerá com a constante evolução dos dados físicos para os meios eletrônicos onde a codificação, aplicação de padrões de segurança nas bases de dados e códigos fonte, descentralizações e gatilhos antifraude farão parte do pacote básico das novas ferramentas do mercado e serão obrigatoriedade naquelas já em ambiente de produção.

“Vale para todas as empresas, independentemente do porte. Desde o pipoqueiro até uma startup, todos precisam, no mínimo, ter a certeza de quais dados

colhem e ter uma justificativa sobre a necessidade dos dados para o negócio", explica Diego Almeida, encarregado de proteção de dados do Sebrae Nacional - chamado de DPO (Data Protection Officer).

Assim como já acontece com a GDPR (Regulamentação Geral de Proteção de Dados) na Europa agora as empresas brasileiras terão que se atentar às novas responsabilidades ao coletarem e armazenarem dados de seus colaboradores e clientes, em concordância com a LGPD, caso contrário a instituição estará sujeita a sanções que passarão a poderem ser aplicadas pela ANPD *(Agência Nacional de Proteção de Dados)*.

Com isso, os negócios estão correndo contra o tempo para adequação para a nova legislação, a fim de evitar punições. Assim, abre-se um leque de possibilidades para os profissionais da área**,** o cargo de DPO passa a ser uma posição obrigatória em toda e qualquer empresa que lide com dados pessoais.

Por fim, a proposta deste artigo foi alcançada por ter apresentado uma visão macro do impacto e das necessidades de adaptação das instituições no Brasil com a Lei Geral de Proteção de Dados, conotando atitudes e atribuído obrigações para o tratamento das informações.

REFERÊNCIAS

de Dados Pessoais, Lei de Proteção. "DESAFIOS TECNOLÓGICOS NO PROCESSO DE RECEPÇÃO NORMATIVA: adequação e conformidade na perspectiva da." *ANAIS WIDaT 2018* 58.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e

altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Disponível em: <http://

www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>.

Sociedade Brasileira de Informática em Saúde, 1986. Disponível em: < http://sbis.org.br/>.

Santa Anna, Jorge. "Aspectos epistemológicos da ciência da informação e o comportamento informacional: diálogos com Borko, Le Coadic e Saracevic." *RDBCI: Revista Digital de Biblioteconomia e Ciência da Informação* 16.2 (2018): 344-364.

Capurro, Rafael, and Birger Hjorland. "O conceito de informação." *Perspectivas em ciência da informação* 12 (2007): 148-207.

Matheus, Renato Fabiano. "Rafael Capurro e a filosofia da informação: abordagens, conceitos e metodologias de pesquisa para a Ciência da Informação." *Perspectivas em Ciência da Informação* 10.2 (2005).