TRABALHO DE CONCLUSÃO DO CURSO DE GRADUAÇÃO EM ADMINISTRAÇÃO

Lei Geral de Proteção de Dados:

uma análise das ferramentas de administração moderna na perspectiva da legalização da Lei

Gabriel Oliveira de Miranda / RA: 1710963

Jessica Francine Pereira / RA: 1710958

Luiz Felipe da Silva Pires / RA: 1710947

Graduandos do Curso de Graduação em Administração do Centro Universitário UniDomBosco. E-mail: felipepires20@hotmail.com

Adriana Franzoi Wagner

Professora e orientadora do Projeto Interdisciplinar (TCC)

Coordenadora de cursos da Escola de Gestão (presencial e educação à distância)

CENTRO UNIVERSITÁRIO UNIDOMBOSCO

RESUMO: O presente artigo teve como objetivo estabelecer estratégias na área de administração sobre a análise da implantação, regularização e legalização da Lei Geral de Proteção de Dados (LGPD). Este trabalho baseou-se nos conceitos da administração moderna utilizando métodos, sistemas e processos. Utilizou-se como estratégia de investigação a revisão bibliográfica, com influência principal em sites confiáveis. Constatou-se por meio desta pesquisa que, com as ferramentas de organização, sistemas e métodos podem-se aumentar a Segurança da Informação. A Tecnologia da Informação e Comunicação é o facilitador na comunicação por meio de ferramentas tecnológicas. A Governança, Riscos e Compliance identifica seus atores na tomada de decisão para otimizar sua resiliência organizacional. Os resultados indicam a emergência na disseminação da implantação da LGPD para todas as empresas que possuem ou possuirão tratamento de dados pessoais no Brasil.

Palavras chave: Dados pessoais, Lei, Métodos, Segurança da Informação.

1 INTRODUÇÃO

A Lei Geral de Proteção de Dados (LGPD) foi a maior mudança no formato de tratamento de dados pessoais no Brasil, e ela promete segurança e transparência, tanto para os titulares quanto para os controladores desses dados, as relações de comércio ou jurídicas são realizadas com trocas de informações baseadas em dados, como por exemplo, para garantir um cadastro que forneça um desconto em uma determinada compra ou em uma reserva de um estabelecimento.

A facilidade da internet permite que se possa ter a opção do trabalho home Office, contudo, essa prática pode ser muito vulnerável a ciberataques, levando riscos para a organização e para os colaboradores em terem seus dados ou de terceiros vazados, podendo ser pela falta de treinamento técnico em segurança da informação ou em muitos casos, esses dados gerados na modalidade de trabalho virtual, são armazenadas por tempo indeterminado e sem garantias da segurança da informação.

Com a globalização e os avanços da tecnologia moderna, e com a crescente escala de dados, ou seja, (Big Data) que estão sendo processados e manipulados diariamente, identificou-se a necessidade de ter controle sobre o tratamento de dados. Para isso, a Lei passou a se posicionar contra vazamentos de dados ou uso sem consentimento dos seus titulares para a LGPD pode ser passivo de autuação caso seja identificado o descumprimento da Lei.

Com essa mudança, muitas empresas e gestores precisaram e precisarão buscar informações para a adequação, ou reconhecer que seus métodos, sistemas e processos já existentes possam ser modificados, aperfeiçoados e treinados por toda cadeia de colaboradores, parceiros e fornecedores da organização.

Com o objetivo de trazer relevância para as organizações, esse artigo buscou atender às principais questões que podem ser identificadas para a implantação da LGPD: O que é a Lei Geral de Proteção de Dados? Quais empresas serão impactadas? Quando a Lei entrará em vigor? Quem vai fiscalizar minha empresa? Quais serão as principais áreas afetadas dentro de uma empresa? A quem a Lei não se aplica? Qual será a punição para quem não cumprir com a Lei.

No estudo se iniciou com as definições sistemáticas e metodológicas que, levadas em práticas, definem os elementos em que as organizações precisam identificar e aprimorar, visando a LGPD.

2 FUNDAMENTAÇÃO TEÓRICA

Partindo do princípio em que as organizações são impactadas com mudanças normativas e transformações tecnológicas, surge a necessidade de se conhecer os processos, métodos e desafios da Lei Geral de Proteção de Dados, foi apresentado nesse capítulo a revisão de textos, artigos, livros, periódicos, sites e materiais pertinentes à revisão da literatura.

2.1 ORGANIZAÇÃO, SISTEMAS E MÉTODOS (OSM)

Para Cury (2012, p. 122),

> a Organização, Sistemas e Métodos podem ser definidos como uma das funções da administração responsáveis pela modelagem da empresa, tendo como responsabilidade aplicar melhorias nos setores, acompanhar o processo, contribuir com sugestões, observar e gerar conclusões utilizando de técnicas e material adequado para um bom resultado.

"Sistema: aludem tanto à organização ou à empresa como uma entidade integrada, como também às suas partes relevantes, isto é, às suas (diretorias) aos, seus departamentos e às suas divisões (gerências), ou aos seus processos de trabalho" (CHIAVENATO, 2010, p. 5).

Complementa o autor "Nesse sentido, a palavra organização significa o ato de organizar, estruturar, pôr ordem, consolidar, atribuir autoridade e reponsabilidade, definir quem faz o quê e quais serão as tarefas organizacionais relevantes e essenciais para o negócio" (CHIAVENATO, 2010, p. 5).

"O conceito de método utilizado em administração provém do método científico. Este é um conjunto de regras básicas para desenvolver uma experiência a fim de produzir novo conhecimento, bem como corrigir e integrar conhecimentos já existentes" (CHIAVENATO, 2010, p. 191).

Segundo Chiavenato (2010, p. 8).

> os principais objetivos da OSM são: 1) Organizar e reorganizar a atividade organizacional; 2) Metodizar e racionalizar a atividade organizacional; 3) Melhorar continuamente o trabalho organizacional; 4) Criar condições para utilizar adequadamente e otimizar o uso dos

dados recursos da organização; 5) Promover a integração das atividades que compõem o trabalho organizacional; 6) Aumentar a eficiência e a eficácia organizacional e, consequentemente, aumentar a qualidade e a produtividade do trabalho; 7) Agregar valor ao negócio da empresa e às pessoas nele envolvidas; 8) Identificar os indicadores de desempenho da organização e de suas unidades e alavancar resultados.

2.2 ADMINISTRAÇÃO DE SISTEMAS DE INFORMAÇÃO

"A palavra "sistema" denota um conjunto de elementos interdependentes e interagentes ou um grupo de unidades combinadas que forma um todo organizado. Sistema é um conjunto ou combinações de coisas ou partes formando um todo unitário" (CHIAVENATO, 2014, p. 471). Enquanto para informação, "é essencial compreender a diferença entre dado e informação. O dado pode ser processado pela tecnologia da informação, mas ele se torna informação após adquirir certo significado" (HINTZBERGEN, et al. 2018, p. 56).

"Um sistema de informação pode ser definido tecnicamente como um conjunto de componentes inter-relacionados que coletam (ou recuperam), processam, armazenam, e distribuem informações destinadas a apoiar a tomada de decisões" (LAUDON e LAUDON, 2007, p. 9). "Existem três atividades básicas em um sistema de informação que geram resultados úteis para a empresa: Entrada, processamento e saída" (BELMIRO, 2012, p. 19).

Para Chiavenato essas atividades são denominadas de parâmetro, "parâmetros são constantes arbitrárias que caracterizam, por suas propriedades, o valor e a descrição dimensional de um sistema ou componente do sistema. Os parâmetros dos sistemas são: entrada, saída, processamento, retroação e ambiente" (CHIAVENATO, 2014, p. 473).

"Entrada: captura ou coleta dados brutos de dentro da organização ou de seu ambiente externo. Processamento: converte esses dados brutos em uma forma mais significativa. Saída: transfere as informações processadas aquelas que a utilizarão" (BELMIRO, 2012, p.19). "Retroação: função do sistema que compara a saída com um critério ou padrão previamente estabelecido. [...] Ambiente: meio que envolve externamente o sistema. [...] Para que o sistema seja viável e sobreviva, ele deve adaptar-se ao ambiente por meio de uma constante interação" (CHIAVENATO, 2014, p. 474).

"Os sistemas de informações também precisam de feedback, que nada mais é do que uma resposta que retorna determinadas pessoas e atividades da organização para que possam avaliar e, se necessário, corrigir o estágio de entrada" (BELMIRO, 2012, p. 19).

2.2.1 SEGURANÇA DA INFORMAÇÃO

"As organizações estão cada vez mais expostas aos riscos causados pelo vazamento de suas informações. Esse vazamento poderá ser dado através de uma invasão física, lógica ou humana" (FONSECA, 2009, p. 2). "A segurança de informações visa garantir a integridade, confidencialidade, autenticidade e disponibilidade das informações processadas pela instituição" (TRIBUNAL DE CONTAS DA UNIÃO, 2012, p. 9). "A autenticidade é a propriedade da informação que garante que ela é da fonte anunciada e, além disso, não sofreu modificações ao longo de um processo" (SITE INFONOVA, 2018, p. 1). "A preservação da confidencialidade dessas informações é de responsabilidade de todos os colaboradores, que na maioria das vezes não estão preparados para lidar e reconhecer situações de riscos" (FONSECA, 2009, p. 2). "Por meio da autenticação é possível confirmar a identidade da pessoa ou entidade que presta as informações" (TRIBUNAL DE CONTAS DA UNIÃO, 2012, p. 9). "A disponibilidade é a propriedade que garante que a informação sempre esteja disponível para uso legítimo" (SITE INFONOVA, 2018, p. 3). "Uma das principais ameaças que as organizações estão suscetíveis é a de serem atacadas e exploradas pela falta de controles de Segurança da Informação contra a invasão cibernética" (MANOEL, 2014, p. 22).

2.3 TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO

"Informações sigilosas podem ser facilmente acessadas sem uma proteção ideal. [...] Para que essa segurança seja realizada da forma correta é preciso investir em Tecnologia da Informação" (SITE SEGS, 2020, p. 1).

A tecnologia da informação e comunicação "também chamada de (TIC), é a área que utiliza ferramentas tecnológicas com o objetivo de facilitar a comunicação e o alcance de um alvo comum". (SILVA, SILVA e COELHO, 2015, p. 2). "O século

XXI pode, até agora, ser considerado o ápice do vislumbre da passagem".

"de uma sociedade industrial a uma sociedade informacional" (SALDANHA, BRUM e MELLO, 2015, p. 463). "Nesse início de século XXI, o acesso ao conhecimento, por meio do domínio das chamadas tecnologias da informação e comunicação (TICs) caracteriza um importante diferencial competitivo, tanto individual quanto coletivo" (FELICIANO, 2008, p. 14). "As transformações decorrentes da evolução tecnológica vêm definindo mudanças significativas, em todos os segmentos da sociedade" (CASTILHO, 2015, p. 12). "Com o avanço tecnológico, as Tecnologias da Informação (TI) têm se desenvolvido de forma rápida e cada vez mais eficiente. Fazendo com que, o uso da TI se torne cada vez mais popular e indispensável à vida de um indivíduo ou empresa" (SILVA, SILVA e COELHO, 2015, p. 2).

"Ter controle, facilidade de acesso e manter um gerenciamento integrado sobre as informações, [...] se faz necessário em virtude do potencial de produção informacional existente nas comunidades atendidas pelos projetos de inclusão digital" (FELICIANO, 2008, p. 16). "Esta integração favorecida pela internet e os serviços que esta oferece, possibilita, através da queda das barreiras geográficas, o acesso às informações que circulam em todo o planeta, permitindo assim a socialização do conhecimento" (CASTILHO, 2015, p. 12).

"Dessa forma, para que os dados, as informações e o conhecimento não sejam perdidos, a gestão do conhecimento vem contribuir, por meio de processos, para o registro, retenção, produção e gestão local" (FELICIANO, 2008. p. 16). Além disso, "As tecnologias da informação e comunicação podem contribuir com o acesso universal da educação, com a igualdade na educação, a qualidade de ensino e aprendizagem, e o desenvolvimento profissional" (SILVA, SILVA e COELHO, 2015, p. 4).

Segundo apresentado por Feliciano (2008, p. 16),

> do ponto de vista das ações governamentais, a inclusão digital permite a criação de um canal de comunicação mais dinâmico e presente, no qual os cidadãos passam da passividade do recebimento de informações e orientações à condição de fomentadores, produtores críticos e sugestivos. Esse é um diferencial social, e um ativo importante para as organizações, sobretudo do setor público, que podem, com base nas informações e conhecimentos dos usuários, alterar, adaptar e mesmo criar novos produtos e/ou serviços.

2.4 GOVERNANÇA, RISCO E COMPLIANCE (GRC)

"Atualmente, com a transformação da economia, da política e da própria conduta da sociedade, no campo empresarial têm se falado muito a respeito de Governança, Riscos e Compliance, sempre juntos, como se significassem um mesmo conceito" (LEITE, 2018, p. 1). "As primeiras discussões organizadas sobre o tema remontam à década de 1990, tendo como marco inicial a publicação do relatório Cadbury, em 1992, na Inglaterra" (CONFEDERAÇÃO NACIONAL DE EMPRESAS DE SEGUROS GERAIS, 2018, p. 7). "Apresenta-se assim, um cenário que exige maior e melhor resiliência organizacional, além de melhores controles e mecanismos promotores de transparência, previsibilidade e confiabilidade" (BIDNIUK, 2017, p. 1).

Conforme apresentado pela Confederação Nacional de Empresas de Seguros Gerais (CNseg) (2018, p. 7),

> a expressão Governança, Risco e Compliance, mais conhecida pela sigla GRC, passou a ser recentemente utilizada no mundo dos negócios. No entanto, só utilizá-la não basta para compreendê-la, sendo imperativo entender cada um dos seus três componentes a partir da constatação de que cada um deles, isoladamente, já faz parte do vocabulário do mundo corporativo há bem mais tempo.

"A governança corporativa passou a ser tema de grande destaque nas últimas décadas do século XX, e evoluiu advindo do aumento de demandas visando a melhorar as práticas e a transparência por partes das empresas" (LEITE, 2018, p. 1).

Em seu conceito é apresentado pelo Instituto Brasileiro de Governança Corporativa (SITE IBGC) (2015, p. 20),

> governança corporativa é o sistema pelo qual as empresas e demais organizações são dirigidas, monitoradas e incentivadas, envolvendo os relacionamentos entre sócios, conselho de administração, diretoria, órgãos de fiscalização e controle e demais partes interessadas.

"A gestão de riscos é o conjunto de procedimentos por meio dos quais as organizações identificam, analisam, avaliam, tratam e monitoram os riscos que podem afetar negativamente o alcance dos objetivos" (VIEIRA e BARRETO, 2019, p. 12). "Um risco pode ser expresso pela combinação da sua probabilidade de ocorrência e do impacto resultante da ameaça – ou oportunidade quando benéfico" (PEREIRA e BERGAMASCHI, 2018, p. 9).

Segundo o Tribunal de Contas da União (2018, p. 8),

> a gestão de riscos, quando corretamente implementada e aplicada de forma sistemática, estruturada e oportuna, fornece informações que dão suporte às decisões de alocação e uso apropriado dos recursos e contribuem para a otimização do desempenho organizacional.

"Em nosso país, o termo "Compliance" é utilizado para denominar um departamento ou setor de uma empresa, ou ainda para referir-se aos procedimentos ou as práticas relacionadas à área de auditoria interna" (BLOK, 2017, p. 79).

"É um processo contínuo que envolve a identificação das exigências (éticas, administrativas e legais), a análise e mitigação dos riscos de não conformidade e a adoção das medidas preventivas e corretivas necessárias" (VIEIRA e BARRETO, 2019 p. 12).

Para Leite (2018, p. 3),

> o compliance tem atuação transversal, não se confunde com controles internos ou auditoria interna, já que atua de forma detectiva e protetiva na manutenção da cultura e conformidade, e desafia as áreas quanto ao ambiente regulatório externo e interno, verificando se a organização está de acordo com leis, determinações de órgãos fiscalizadores, normas regulamentadoras, melhores práticas e a sua própria política.

"A partir de meados da década de 90, todas as organizações públicas e privadas passaram a adotar o compliance como uma de suas regras mais primárias e fundamentais para a transparência de suas atividades" (BLOK, 2017, p. 17).

2.4 REGULAMENTO GERAL DE PROTEÇÃO DE DADOS (GENERAL DATA PROTECTION REGULATION - GDPR)

Desde maio de 2018 está em vigor a GDPR (General Data Protection Regulation ou Regulamento Geral de Proteção de Dados em português) na União Europeia (EU). "O novo pacote de medidas, tem por objetivo preparar a Europa para a era digital" (COMISSÃO EUROPEIA (a), 2020, p.1), visando "proteger a privacidade dos cidadãos e oferecer maior controle e transparência em relação às informações pessoais que são armazenadas em bancos de dados de empresas" (SANTANDER, 2020, p. 2).

Com o avanço da Inteligência Artificial (IA), sendo "um segmento da computação

que busca simular a capacidade humana de raciocinar, tomar decisões, resolver problemas" (MINISTÉRIO DA INDÚSTRIA, COMÉRCIO E SERVIÇO, 2020, p. 2). O Big Data tornou-se uma ferramenta altamente poderosa "para capturar, administrar e processar, incluindo-se correlacionar com alguma rapidez às informações que estão a nossa volta, provenientes de diferentes fontes" (TAURION, 2013, p. 5). Devido a isso "os dados de clientes são um insumo cada vez mais importante para as organizações" (SITE FIA: FUNDAÇÃO INSTITUTO DE ADMINISTRAÇÃO, 2020, p. 2). Tornando-se uma mercadoria competitiva essencial na economia digital.

A criação do "regulamento é uma medida essencial para reforçar os direitos fundamentais dos cidadãos na era digital" (COMISSÃO EUROPEIA (a), 2020, p. 1). "O RGPD protege os dados pessoais independentemente da tecnologia utilizada para o tratamento desses dados – é neutra em termos tecnológicos e aplica-se tanto ao tratamento automatizado como ao tratamento manual" (COMISSÃO EUROPEIA, 2020, p. 1).

De acordo com a lei, é obrigatório que as empresas garantam os seguintes direitos para os consumidores: "o direito de ser informado; o direito de acesso; o direito de retificação; o direito de apagar; o direito de restringir o processamento; o direito à portabilidade de dados; o direito de objetar; direitos relacionados à tomada de decisão e criação de perfil automatizado" (SITE INVESTORINTEL, 2018, p. 3).

2.6 MARCO CIVIL DA INTERNET (MCI)

Em 25 de Março de 2014 foi sancionado o Marco Civil da Internet (MCI), oficialmente chamado de Lei nº 12.965/2014. "A Lei surge para regularizar atos que ocorrem na Internet, estabelecendo direitos e deveres a serem seguidos no âmbito virtual, tanto para quem utiliza o serviço, quanto para quem distribui informação" (PRATA, 2017, p. 8). Levantando pontos como a "neutralidade da rede, a responsabilidade civil de provedores e usuários sobre o conteúdo postado e as medidas para preservar e regulamentar direitos fundamentais do internauta, como a liberdade de expressão e a privacidade" (MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA, 2020, p. 1).

"A internet hoje é vista como instrumento essencial de disseminação de informação na sociedade e de interação social [...] é ferramenta essencial de trabalho e estudo de adultos, jovens e crianças e deve ser utilizada com consciência" (FREITAS, 2017,

p. 2). Neste ponto o "MCI preserva a Internet como ela deve ser: uma rede aberta e descentralizada, na qual os internautas são o próprio motor de colaboração e inovação" (SITE INTERVOZES, 2020, p. 1).

"O desenvolvimento tecnológico, a informatização, a difusão do acesso à internet e a popularização dos meios de comunicação em massa facilitaram consideravelmente a violação do direito à privacidade" (FREITAS, 2017, p. 2). "A privacidade do usuário era constantemente ferida antes do Marco Civil da Internet, sendo assim importante saber a proteção agora concedida e suas repercussões" (PRATA, 2017, p. 72).∴

2.7 LEI GERAL DE PROTEÇÃO DE DADOS (LGPD)

"O objetivo da Lei Geral de Proteção de Dados (LGPD), é a criação de regras para o tratamento de dados pessoais e para isso criou termos, direitos, obrigações, multas e até uma agência reguladora, a Autoridade Nacional de Proteção de Dados (ANPD), descrita no artigo 55 dessa nova lei" (GUILHERME, 2019). Podemos dizer sobre as funções da ANPD que "Ela é o grau máximo, hierarquicamente, na esfera administrativa da Lei Geral de Proteção de Dados. Este fator não elimina o poder de fiscalização de outros órgãos, apenas define a limitação de suas competências" (VARELLA, 2019, p. 23). "Art. 55-A. Fica criada, sem aumento de despesa, a ANPD, órgão da administração pública federal, integrante da Presidência da República" (BRASIL, 2018, p. 19).

Para o Senado (2019, p. 2),

> o novo órgão terá a seguinte estrutura organizacional: Conselho Diretor (órgão máximo de direção), Conselho Nacional de Proteção de Dados Pessoais e da Privacidade, Corregedoria, Ouvidoria, órgão de assessoramento jurídico próprio e unidades administrativas necessárias à aplicação da lei. A ANPD será formada por diretores que serão nomeados para mandatos fixos.

"Terá também um importante papel de orientadora e de apoiadora dos órgãos de governo e empresas em relação às situações em que elas podem ou não tratar dados pessoais do cidadão" (SITE SERPRO, 2019, p. 1). "A proposta da ANDP é orientar, orientar e orientar, preventivamente. Após isso, fiscalizar, advertir e, somente após tudo isso, penalizar, se a LGPD continuar sendo descumprida" (SITE SERPRO, 2019, p. 1).

"A Lei Geral de Proteção de Dados pessoais foi sancionada por Michel Temer em 2018 e entrará em vigor em agosto de 2020" (SITE HIGH SECURITY CENTER, 2019, p. 2). "A LGPD estabelece regras sobre coleta, armazenamento, tratamento e compartilhamento de dados pessoais, impondo mais proteção e penalidades para o não cumprimento" (SITE MEUSUCESSO, 2019, p. 2). "Caso os responsáveis pela administração dos dados não se adequem às novas regras podem ser multados em até 2% do faturamento, com o limite de R$ 50 milhões. A partir desta lei, o Brasil iguala-se a mais de 100 países que com norma sobre o assunto" (SITE EPOCANEGOCIOS, 2019, p. 3). Na GDPR "O Google, por exemplo, foi multado em € 50 milhões por não fornecer informações suficientes aos usuários sobre a política de consentimento da empresa" (DUARTE, 2020, p. 1).

Para o site Serpro (2020, p. 2),

> para entender a importância do assunto, é necessário saber que a nova lei quer criar um cenário de segurança jurídica, com a padronização de normas e práticas, [...] define que há alguns desses dados sujeitos a cuidados ainda mais específicos, como os sensíveis e os sobre crianças e adolescentes, e que dados tratados tanto nos meios físicos como nos digitais estão sujeitos à regulação.

"Além disso, a lei é essencial para a harmonização de normas sobre proteção de dados já vigentes no Brasil (como por exemplo o Código de Defesa do Consumidor, a Lei de Acesso à Informação, a Lei do Cadastro Positivo e a Resolução BACEN 4.658/2018" (SITE DANIEL, 2019, p. 2).

Para o site LGPDBrasil (2020, p. 5),

> as áreas que sofrerão mais com os impactos da LGPD, sem dúvidas, são aquelas que tratam do maior volume de dados pessoais, tais como, por exemplo: (I) Recursos Humanos e Departamento De Pessoal pelos dados dos empregados e colaboradores; (II) Atendimento ao Consumidor e pós-venda; (III) Marketing pelo tratamento de dados para campanhas e envio de propaganda por redes sociais, e-mail marketing etc.; (IV) Vendas, se direta ao consumidor por tratar os dados pessoais para concretização da venda; e (VI) Pesquisa e Desenvolvimento. No entanto, é necessário destacar que toda a empresa deve se adequar à LGPD, pois a empresa está integralmente vinculada às regras para todos os seus setores.

"Toda coleta e processamento de dados deverá se atentar à base jurídica imposta pela Lei Geral de Proteção de Dados, onde estão previstas hipóteses que poderiam tornar ilegais o tratamento de dados pessoais pelas organizações" (VARELLA, 2019, p. 8).

"Art. 5° Inciso V - titular: pessoa natural a quem se referem os dados pessoais que são

objetos de tratamento" (BRASIL, 2018, p. 2). "As informações sobre o tratamento de dados pessoais devem ser claras, objetivas, facilmente compreensíveis e acessíveis ao titular durante todo o período em que o tratamento ocorre" (CAVALCANTE, 2019, p. 2).

Segundo o site Fenalawdigital (2018, p. 7),

> quando o tratamento tiver origem no consentimento do titular ou em contrato, o titular poderá solicitar cópia eletrônica integral dos seus dados pessoais, observado os segredos comercial e industrial, em formato que permita a sua utilização subsequente, inclusive em outras operações de tratamento.

"Art. 5° Inciso VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem às decisões referentes ao tratamento de dados pessoais" (BRASIL, 2018, p. 3).

De acordo com Vidor (2019, p. 2),

> desse modo, independente de ser uma pessoa, ou uma empresa, de ser um ente privado ou público, todo aquele que tratar com dados pessoais, no escopo da LGPD, terá de designar uma pessoa dentro da corporação que responderá pelas decisões que forem tomadas em relação ao tratamento de dados de pessoas naturais.

"Art. 5° Inciso VII - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador" (BRASIL, 2018, p. 3). "O operador responde solidariamente pelos danos causados quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador" (GARCIA, 2019, p. 2).

Para Lima (2020, p. 2),

> a distribuição da responsabilidade civil entre controlador e operador de dados pessoais no caso de incidente de privacidade com lesão ao titular, se dá de acordo com o estágio da operação em que residiu a falha, sendo que poderá haver solidariedade entre eles em determinadas hipóteses.

"Art. 5° Inciso 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)" (BRASIL, 2018, p. 3). "Sendo este profissional responsável por representar a empresa/controlador diante da ANPD [...] e deve estar ciente dos processos de gestão de crises da Empresa, que fazem parte de suas atribuições" (MAGALHAES, 2019, p. 1).

"Os controladores, responsáveis pelo tratamento, devem indicar um encarregado pelo tratamento de dados pessoais divulgando publicamente, de forma clara e objetiva, de preferência no site do próprio controlador, a identidade e as informações de contato do encarregado" (SITE DANIEL, 2019, p.12). "Nas relações de trabalho e emprego, como o empregador é detentor de informações pessoais de seus empregados, ele deve observar a LGPD, sob pena de responsabilização civil" (SITE LGPDBRASIL, 2020, p. 14).

O objetivo é "assegurar o direito à privacidade e à proteção de dados pessoais dos usuários, por meio de práticas transparentes e seguras, garantindo direitos fundamentais" (SITE LGPDBRASIL, 2020, p. 1). "Afinal, os dados são seus, logo os direitos têm que ser em prol de você" (SITE SERPRO E LGPDBRASIL (a), 2020, p. 1).

De acordo a lei existem 04 tipos de dados para o controlador e operador saberem lidar: dados pessoais, dados sensíveis, dados públicos e anonimizados.

"Art. 5° Inciso I dado pessoal: informação relacionada à pessoa natural identificada ou identificável" (BRASIL, 2018, p. 3). "Informação que permite identificar, direta ou indiretamente, um indivíduo que esteja vivo, então ela é considerada um dado pessoal: nome, RG, CPF, gênero, data e local de nascimento, telefone, endereço residencial" (SITE SERPRO E LGPDBRASIL (b), 2020, p. 1).

'Art. 5° Inciso 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" (BRASIL, 2018, p. 3).

Dados sensíveis: "são os que revelam origem racial ou étnica, convicções religiosas ou filosóficas, opiniões políticas, filiação sindical, questões genéticas, biométricas e sobre a saúde ou a vida sexual de uma pessoa" (SITE SERPRO E LGPDBRASIL (c), 2020, p. 1). Dentro dos dados sensíveis abre a questão de crianças e adolescentes, a Lei comenta "é imprescindível obter o consentimento inequívoco de um dos pais ou responsáveis e se ater a pedir apenas o conteúdo estritamente necessário para a atividade econômica ou governamental em questão, e não repassar nada a terceiros" (SITE SERPRO E LGPDBRASIL (c), 2020, p. 1).

Dados públicos: "deve ser tratada considerando a finalidade, a boa-fé e o interesse público que justificaram a sua disponibilização. A LGPD define, por exemplo, que uma organização pode, sem precisar pedir novo consentimento, tratar dados tornados anterior e manifestamente públicos pelo titular" (SITE SERPRO E LGPDBRASIL (d), 2020, p. 1).

"Art. 5° Inciso 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" (BRASIL, 2018, p. 3).

Dados anonimizados: "é aquele que, originariamente, era relativo a uma pessoa, mas que passou por etapas que garantiram a desvinculação dele a essa pessoa. Se um dado for anonimizado, então a LGPD não se aplicará a ele" (SITE SERPRO E LGPDBRASIL (d), 2020, p. 1).

A LGPD "Faz referência a atividades às quais a Lei não se aplica devido à natureza de sua finalidade, como jornalísticas e artísticas, acadêmicas, de segurança pública, de defesa nacional, de segurança do Estado, investigação e repressão de infrações penais" (VARELLA, 2019, p. 10).

"Pesquisa realizada pela plataforma Capterra revela que somente 40% dos pequenos e médios empresários estão totalmente preparados para a entrada em vigor da lei que regulará o uso de dados pessoais no Brasil" (SITE E-COMMERCE BRASIL, 2020, p. 1). Completa, "a pesquisa ouviu 224 CEOs e profissionais com cargos diretivos de companhias de todo o país entre os dias 5 e 6 de fevereiro" (SITE E-COMMERCE BRASIL, 2020, p. 1). "A complexidade da nova norma é apontada como o grande desafio tanto para as empresas que já finalizaram o processo de conformidade (82%) como para aquelas que estão no meio do processo (59%)" (SITE JORNALCONTÁBIL, 2020, p. 1). "As empresas com data centers mais antigos não desejam reconstruí-los, [...] Tecnologia 2019 do Gartner mostram que a porcentagem do orçamento de TI direcionado aos Data Centers diminuiu nos últimos anos e, agora, representa apenas 17% do total" (SITE TIINSIDE, 2020, p. 1). "A preocupação com a proteção de dados além do salvamento em nuvem já pode ser notada nos negócios" (GASPARIN, 2020, p. 2). "Talvez pareça trabalhoso [..] Além de ficar melhor para a área de auditoria, que agora depois do lançamento da Lei Geral de Proteção de Dados está inclusive bem mais pressionada, o controle e visibilidade é financeiramente muito interessante" (NUNES, 2020, p. 4).

Para Bento (2020, p. 3),

> o uso de softwares não obsoletos, reconhecidamente seguros e com suporte do fabricante é uma boa prática. O mesmo se dá com o mapeamento dos dados pessoais na empresa, a criação de processos, políticas e procedimentos, o aculturamento de pessoal sobre o assunto, entre outras ações, visando aumentar a maturidade no assunto.

"Fazer esse controle de forma segura é um processo complexo, que envolvem reconfigurações de CRMs, auditorias de segurança e implantação de sistemas que permitam ao consumidor acessar e, se for o caso, baixar ou excluir suas informações

pessoais" (MEIRELES, 2020, p. 3). "Diante da preocupação imposta pela LGPD, é necessário lembrarmos que o usuário está no centro de tudo. A Lei veio apenas para ratificar esta constatação" (DYLEWSKI, 2020, p. 4).

3 METODOLOGIA

Este artigo de pesquisa qualitativa, visou mensurar os processos e métodos que necessitarão para a implementação nas organizações quanto a Lei Geral de Proteção de Dados. A análise qualitativa foi desenvolvida e utilizada por meio de referências publicadas nos últimos 13 anos, dispostas em repositórios bibliográficos, sites governamentais, livros, textos e sites com base na Lei Geral de Proteção de Dados.

"Em primeiro lugar a pesquisa qualitativa não apresenta preocupação com um grande número de dados, pois não há preocupação em demonstrar resultados para a população. Assim, entendemos que a pesquisa qualitativa tem como principal objetivo interpretar o fenômeno em observação" (NEVES, 2015, p. 19).

Interpretou-se por essa pesquisa o fator de emergência e ineditismo do tema, as quais as organizações apresentam pouco ou nenhum conhecimento do método e/ou sistema de implantação ou adequação interna e externa que a Lei Geral de Proteção de Dados apresenta em sua base. O fator cultural das organizações e investimentos financeiros em tecnologias demonstraram barreiras na adequação da Lei.

4 ANÁLISES E DISCUSSÕES

Com o avanço da tecnologia mundial, e o aumento no processamento de dados (Big Data), surgiu a necessidade de Leis para o seu controle. No Brasil foi sancionado a Lei Geral de Proteção de Dados (LGPD), prevista para entrar em vigor em agosto de 2020 e, com isso, empresas de todos os setores, passaram e passarão a se organizar para a coleta de dados pessoais dos seus consumidores para atender a LGPD, assim, questionou-se: O que é a Lei Geral de Proteção de Dados.

Entendeu-se pela pesquisa que a LGPD é a norma geral de tratamento de dados pessoais nacional, ao qual demonstrou se ter direitos, obrigações e multas. Para a Lei ser cumprida com suas regras, precisaram-se observar boas práticas organizacionais

para estar em conformidade com a Lei. Para entender esse processo precisou fazer a seguinte pergunta, para quais empresas essa Lei se aplica? Observou que o cenário seria para toda e qualquer pessoa natural ou jurídica, de direito público ou privado, que realize o tratamento de dados pessoais.

A LGPD brasileira e a GDPR europeia são Leis com o objetivo muito semelhantes, porém a GDPR foi o primeiro marco mundial sobre a transparência na utilização de dados. O texto da lei europeia é considerado a principal Lei sobre a segurança de dados do mundo e motivou outras legislações incluindo a LGPD que foi criada com base no regulamento europeu.

Iniciando-se uma breve comparação entre as Leis, o primeiro ponto que chama bastante a atenção é que a Lei GDPR foi um aperfeiçoamento para os tempos atuais, acompanhando a era tecnológica, da Lei Diretiva Europeia de 1995 (Diretiva 95/46/CE), portanto existe a mais de 25 anos uma preocupação com o tema e, com isso, os países da União Europeia (UE) possuem uma cultura sólida e avançada para a proteção de dados. Enquanto no Brasil, a primeira lei que aparece citando sobre proteção de dados foi apenas em 2014 com a Lei do Marco Civil da Internet. Contendo algumas referências sobre a privacidade e a segurança de dados, porém de uma forma mais genérica e não muito clara.

Embora a as Leis tenham muitos pontos similares, existem algumas diferenças nítidas comparadas a legislação, por exemplo, ambas possuem definições próximas sobre dados sensíveis, porém a Lei GDPR define também de forma específica termos dentro da definição como “dados biométricos”, “dados de saúde” e “dados genéticos”. Já a Lei brasileira fica com uma definição mais rasa dando espaço para diferentes interpretações.

O tratamento de dados realizados pelo controlador e operador, na lei europeia prevê que precisa ser feito por meio de contrato ou formalidades jurídicas. Na lei brasileira diz que o operador deverá realizar o tratamento de dados de acordo com as instruções do controlado, não estabelecendo um vínculo formal entre ambas as partes.

Diante da pesquisa do trabalho e do relatório da Capterra, observou-se que apenas 40% das empresas demostraram estar de acordo com as exigências e adequações da legalização da Lei, as empresas analisadas mostraram complexidade e desafio no processo, demostrando uma ineficiência e urgência nos parâmetros organizacionais das empresas, para isso buscou-se disseminar as políticas e procedimentos dessa Lei, bem como poderiam ser estruturadas as organizações, com as ferramentas da OSM, por exemplo, sendo: organização, sistemas e métodos.

OSM é uma ferramenta da administração utilizada em grandes organizações para

buscar novos objetivos e, citada, por muitos autores por sua eficiência, ela se torna um recurso de otimização fundamental para as organizações. Mesmo sendo utilizada pelas grandes corporações, empresas de porte pequeno também podem adotar sua metodologia.

Observou-se que a maioria das organizações visualizam barreiras quando existem mudanças nos processos dentro da sua cadeia produtiva, nesse sentido, compreendeu-se que os objetivos da ferramenta OSM, apresentam maneiras para facilitar a implementação de novos procedimentos, rotinas e métodos, visando o desenvolvimento da organização em busca do mesmo objetivo estabelecido, definindo – principalmente, as responsabilidades da realização do trabalho interno e, mais especificamente, nessa nova demandam, com a chegada dessa Lei.

Avançando com a LGPD, compreendeu-se que "Sistemas" é a empresa com todos os setores integrados a qual necessita de mudanças nos processos da gestão de dados, por meio de "Métodos" propriamente dito, tornando as atividades mais eficazes otimizando os recursos, que de forma estruturada e organizada atingirá o objetivo pré-estabelecido de maneira coordenada.

A coleta de dados pode e poderá ser realizada de muitas maneiras, segundo o relatório do Capterra 64% das empresas pesquisadas utilizam redes sociais para realizar suas atividades e 48% utilizam meios ao qual o próprio cliente realiza o preenchimento dos seus dados em formulários e cadastros on-line ou ainda empresas que utilizam esse fornecimento do cadastro de dados pessoalmente, como feiras e eventos.

Diferenciar dados pessoais inseridos em um banco de dados público na internet é importante, pois nem todos os dados são considerados dados pessoais, diante da diversidade da coleta de dados pessoais, garantir a conformidade da Lei é um trabalho de adaptação necessário.

Mas quais dados e sobre o que se referem? O primeiro tipo de dado é o pessoal, que diz respeito a uma pessoa viva, identificada ou identificável. Podendo ser também um conjunto de informações que podem levar a identificação da pessoa específica, como nome ou apelido, endereço, e-mail, ou até mesmo dados detidos por um hospital ou médico, que permitem identificar a pessoa.

Ainda permanece uma lacuna com relação a proteção dos dados do usuário falecido, pois a LGPD não traz em seu texto artigos que versem sobre tal proteção. Alguns provedores já se depararam com essa situação e cada um deles além de oferecem opções aos usuários, possuem suas próprias políticas, o Facebook, por exemplo, tem a ferramenta de "transformação em memorial" onde pode-se definir o que fará da sua conta após o falecimento. Com a falta de legislação específica, pode

ser usado o artigo 12 do Código Civil Brasileiro, que dispõe sobre os direitos da personalidade, onde a família poderá proteger o direito do ente querido. Ainda é um tema controverso, pois não está relacionada apenas a proteção da personalidade "de cujus", ou seja, (lugar do nome do falecido), mas também de uma herança digital e, neste caso, os herdeiros poderiam ter acesso aos seus dados, porém, tais dados podem incluir conversas com outros usuários e sua respectiva privacidade. Portanto, se deparando com esse impasse, a decisão jurisprudencial irá depender do caso concreto, pois como mencionado, os direitos relacionados aos dados do usuário falecido se encontram em conflito e ao mesmo tempo interligados, os quais ainda não são regulamentados por meio de lei em território brasileiro.

Admitiu-se sobre dados sensíveis, que requerem uma atenção maior pelas organizações devido aos riscos que o tratamento indiscriminado pode ocorrer e, esses dados, dizem respeito à origem racial ou étnica, convicções religiosas/filosóficas, opiniões políticas, dados genéticos, dados biométricos, dados relacionados com a saúde e dados relativos à vida sexual ou orientação sexual do indivíduo.

Classificou-se os dados pessoais de crianças e adolescentes, que citado na lei, refere-se a criança com idade até 12 anos incompletos e adolescentes com idade entre 12 e 18 anos de idade. As empresas que solicitarem os dados precisarão pensar em maneiras simples, claras e acessíveis, e com uso de recursos audiovisuais, quando adequado, para que as crianças e adolescentes desenvolvam conhecimento das práticas de tratamento dos dados, para que entendam e possam fazer suas próprias escolhas.

Identificaram-se também os dados anonimizados, que são aqueles dados que pertenciam a uma determinada pessoa, mas que passou por processos e acabou deixando de ter vínculo a essa pessoa, entendendo-se que é impossível identificar a pessoa de origem, estes dados não estão sujeitos a aplicação da LGPD.

Contudo, os artigos da Lei utilizaram de forma genérica a definição de tratamento de dados e assim observou-se a necessidade de conhecer, identificar e analisar cada um deles, isso pode identificar que a empresa esteja cumprindo com uma ou mais definições perante a Lei. Diante disso, cada uma das definições impostas pela Lei deve ser verificada individualmente, para ser analisadas e corrigidas caso tenham os possíveis descumprimentos da LGPD, pois em regra geral, as definições da Lei se estabelecem em: coleta; produção; recepção; classificação; utilização; acesso; reprodução; transmissão; distribuição; processamento; arquivamento; armazenamento; eliminação; avaliação; modificação; comunicação; transferência; difusão ou extração. Na prática, se a empresa tiver acesso de alguma forma a dados pessoais, esta se enquadra na Lei de tratamento de dados.

Entendeu-se a necessidade das organizações com maiores armazenagens de dados,

que estas precisam e precisarão mais do que novas regras e, sim, de capacitações para que seus colaboradores não as viole, terão de ampliar a segurança na tratativa dos dados, terão de designar funcionários para novas funções e acompanhar de forma coordenada, todo esse novo processo/nova mudança. Ela terá de informar basicamente três papeis que serão fundamentais, que são: 1) o "Controlador" que pode ser a própria empresa, ou uma pessoa física que irá definir quais são os objetivos da coleta dos dados, e terá que repensar quais dados são realmente necessários para sua atividade; 2) o "Operador" que será uma ou mais pessoas físicas que tratam e processam os dados pessoais, sob ordens do controlador; e 3) o "Encarregado" ou "DPO" (Data Protection Officer), podendo ser uma empresa terceirizada ou uma pessoa física indicada pelo controlador, porque os dois estarão em constante comunicação, o encarregado precisará garantir que a empresa está fazendo um tratamento de dados em conformidade com a Lei e, também assim, será a interface da organização, com as partes interessadas e a Autoridade Nacional de Proteção de Dados (ANPD) que é o órgão que fiscalizará as empresas segundo as normas da LGPD, podendo responder civil e criminalmente caso ocorra algum vazamento de dados, aqueles que podem trazer sérios problemas ao titular, como dados de etnia ou posição religiosa.

Caso a empresa não esteja em conformidade com a Lei, a ANPD irá surgir como fiscalizadora, penalizadora e orientadora, mas sendo o objetivo principal não de multas e, sim, de educação. Essa autoridade receberá denúncias e buscará verificar a conformidade e adequação pertinente. As organizações que possuem dúvidas das tratativas deverão buscar a ANPD para estarem de acordo com a Lei.

Torna-se indispensável que o profissional "Operador" seja altamente capacitado, sendo que esse ator tem poder de tratamento de dados, o mesmo deve coletar informações perante ordem do "Controlador", contudo o operador é o profissional que tem e terá acesso aos dados e o poder de tratamento do mesmo, dessa forma, terá de criar uma Política de Proteção de Dados. Esse parâmetro seria de ordem interna e seu objetivo é definir o relacionamento entre o Controlador e o Operador, definindo diretrizes sobre coleta e tipos de tratamento de dados.

A Segurança da Informação tem-se tornado um assunto muito recorrente em setores empresariais, analisou-se a preocupação em manter seguro os dados pessoais de seus clientes ou até mesmo seus segredos industriais, que tem feito com que essas empresas pensem em contratações de gerentes de cibersegurança e analistas de infraestrutura de TI, investimento de tempo e dinheiro para manter seus hardwares e softwares verdadeiras "fortalezas" contra crimes cibernéticos, pois as organizações estão suscetíveis aos ataques em rede. Em decorrência desse crime, muitos dados podem ser vazados, sendo assim, com a legalização da LGPD em agosto de 2020,

esse risco pode ser prejudicial à saúde financeira, e com a falta de garantia em que a empresa repassa aos seus clientes, sobre a segurança de seus dados, pode perder credibilidade no mercado.

Ao discutir a classificação de quais áreas principais podem ou poderá (ão) ser afetadas dentro de uma organização, entendeu-se que depende ou dependerá muito do porte da empresa, do volume de processamento de dados pessoais e do investimento em Segurança da Informação ao qual a empresa deseja disponibilizar para seus clientes. Dentro das organizações existem possíveis áreas ao qual a Lei pode ter impactos, esses impactos são áreas de: (I) Recursos Humanos e Departamento De Pessoal; (II) Atendimento ao Consumidor e pós-venda; (III) Marketing; (IV) Setor de Vendas. A Lei não informa qual área deve ser estabelecida como setor que cuidará da LGPD dentro da empresa. Neste estudo, sugeriu-se que seja criado um setor dentro do organograma (linha de staff/apoio, por exemplo) que atenda as orientações da Lei, ou que o setor existente com o maior volume de tratamento e banco de dados pessoais da empresa seja o responsável por atender as exigências da LGPD, sendo que independentemente aonde esteja alocado e com quem os dados pessoais encontra-se sob controle, os mesmos deverão estar seguros.

Observaram-se melhorias na gestão da Segurança da Informação, quando empresas empregaram automação por meio da Tecnologia da Informação e Comunicação (TIC). Com o avanço da internet, a tecnologia por meio da TIC é utilizada por recursos tecnológicos integrados entre si, sendo por meio de funções de hardware e software. Pelo meio físico, as TICs oferecem maior segurança pela evolução de meios de transmissão dos dados podendo ser por fios, cabos ou conexão sem fio (WI-FI). Dessa maneira, com maior controle e confiabilidade na entrega dos pacotes de dados, evitando perdas e vazamentos dos dados. A segurança por meio de software viabiliza a segurança em entregas de dados criptografados utilizando o acesso da internet ou com e-mail enviado com dados importantes.

Desta forma, admitiu-se que um dos processos é reformular suas estratégias de negócio para obter a coleta de dados dos seus clientes e assim construir sua política de proteção e segurança dos dados, de forma clara, explícita e em uma linguagem acessível para garantir o entendimento e a confiança do seu cliente, com formulários e pontos de contato (SAC, site, e-mail) para que os clientes possam acessar, afim de esclarecer possíveis dúvidas. O consentimento é uma das formas para a coleta de dados pessoais e, sendo assim, órgãos reguladores podem solicitar que a empresa colete dados pessoais e compartilhe com o governo ou até mesmo para outras empresas privadas, sendo importante entender a Lei, para utilizá-la corretamente.

Verificou-se que organizações que trabalham com business to business (b2b) venda

entre empresas, ou business to consumer (b2c) venda para o consumidor, é indicado um parceiro jurídico, que irá dar apoio em relação a lei e a na parte de adequação de novos contratos, termos e permissões, que é dada com associados e partes internas interessadas. As empresas ainda precisarão revisar seus contratos com colaboradores, os quais possuem dados pessoais que também necessitarão aderir à nova lei.

Organizações que trabalham com a venda de dados de pessoas físicas, poderão continuar com seu negócio, a Lei torna a atividade mais difícil, mas compreendeu-se que quando houver o consentimento do cliente, alertá-lo que além da coleta, a empresa poderá possivelmente vendê-lo (seus dados) e, assim, se estiver em conformidade não se violará a lei. E, caso a empresa queira adquirir dados, é importante buscar e conhecer as políticas de proteção e tratativas de dados, para prevenção de ser penalizado juntamente com a empresa que está vendendo, em um inesperado caso de vazamento de dados.

Acreditou-se que o esperado das organizações brasileiras que trabalham com dados pessoais, é procurar se adequar e se organizar à Lei, mesmo antes de estar em vigor, notificando seus clientes da coleta, tratamento e armazenamento dos seus dados pessoais, assim tornando mais fácil, prático e prevenindo-se no futuro. A Lei informa o patamar mínimo de como deve ser seguido, mas as empresas podem e poderão buscar se aperfeiçoar.

Criou-se junto com a Lei um nicho de empresas de consultorias que podem ajudar organizações a se alinharem de forma organizada em seus métodos e processos, não apenas segundo à Lei LGPD, mas preparadas para a diversidade do mercado, fortalecendo por exemplo o Compliance da organização.

Detectou-se que sem investimentos tecnológicos e de capacitação de equipes na segurança de dados pessoais, a organização pode ou poderá causar perdas financeiras e da imagem da empresa no futuro. Facebook e Uber são exemplos de organizações que vazaram dados de 50 milhões de pessoas e tiveram multas altíssimas.

A recomendação é investir em segurança de informação para se tornar cada vez mais resiliente a violações e não se arriscar em eventuais penalidades. Empresas que possuem maior segurança em seu banco de dados poderão utilizar isto para promover o seu negócio, por meio da propaganda e publicidade, competindo no mercado e atraindo mais clientes.

A cultura com o passar do tempo mudará. Os titulares dos dados passam a entender um fato simples: de que o dado pessoal é dela, e não a percepção de que os dados são das empresas, que criam inovações, métodos de utilização desses dados para gerarem informações - a LGPD explicita que a empresa apenas cria estratégias de

como utilizar os dados em seu benefício, mas o proprietário dos dados pessoais é propriamente a pessoa física.

Vale lembrar que assim como a Lei, as penalizações que estavam previstas para entrar em vigor no mês de agosto de 2020 foram adiadas pelo Senado, devido as recomendações de isolamento social para o combate ao novo coronavírus. A nova data para a Lei entrar em vigor será em 1° de janeiro de 2021, possibilitando o andamento de processos judiciais, ações judiciais e demais recursos jurídicos. E as sanções passam a valer em agosto de 2021, possibilitando maior tempo para as empresas se adequarem.

5 CONCLUSÕES

Esse estudo qualitativo teve seu início entorno de pesquisas no âmbito da disseminação de informações do regulamento em que demonstrou impactos às organizações, as quais não estivessem na conformidade, ao tema da Lei Geral de Proteção de Dados (LGPD). Com isso, a necessidade de informação referente ao tema levou esse trabalho a procurar responder as suas normas e seus processos, utilizando-se de citações de autores notáveis na área da administração e sites confiáveis sobre o tema.

Interpretou-se, com o objetivo de transcrever de maneira clara ou de fácil compreensão as normas e exigências impostas pela LGPD, de forma que o estudo se apresentou como mapa norteador para empresas e gestores estarem em conformidade perante a LGPD, organizando suas gestões para o atendimento/cumprimento desta. Assim, o estudo atendeu seu objetivo geral, ou seja, sobre a pesquisa do tema e seus desdobramentos/aplicações/condutas.

O estudo identificou o significado e os objetivos da Lei Geral de Proteção de Dados, diante disso ficou descrito suas regras, normas e exigências, a Lei não deixa evidente como as empresas devem realizar seus processos internos, ela demostra apenas como as empresas devem estar preparadas para o tratamento, armazenamento e utilização de dados pessoais, além de apresentar a agência reguladora a Autoridade Nacional de Proteção de Dados (ANPD) ao qual será a responsável pela fiscalização das empresas, o órgão máximo referente a proteção de dados no Brasil, bem como de prestação de atendimento.

O estudo apresentou as empresas que podem ser impactadas com a LGPD e quais áreas das empresas podem ser afetadas diretamente com a mudança de processos

e métodos para a adequação da Lei. O estudo identificou as áreas e empresas que não estão suscetíveis perante a Lei pela natureza de sua finalidade como: trabalho jornalístico; artístico; acadêmicos; segurança pública, defesa nacional; segurança do Estado; investigação e repressão de infrações penais.

Identificou-se que o fator de risco em vazamentos de dados ocorre em punições perante LGPD, ao qual pode ser relevante para a saúde financeira da empresa, assim o estudo apresentou as possíveis multas e punições que a Lei pode aplicar na empresa que não estiver em conformidade.

Entendeu-se que para as realizações de implantação das normas da Lei nas empresas, passem e passarão, por dificuldades, principalmente quando não encontram a infraestrutura tecnológica e cultural inserida no ambiente. Assim, buscou-se apresentar ferramentas organizacionais e sistemas de controle dos dados, que atenda as conformidades da LGPD.

O estudo da "Organização, Sistemas e Métodos" apresentou conceitos e objetivos para a empresa identificar e otimizar seus processos. A combinação de elementos da "Administração de Sistemas de Informação" parametrizou o sistema definindo seus processos. A "Segurança da Informação" demostrou a importância na empresa garantir sua integridade contra vazamentos de dados. A "Tecnologia da Informação e Comunicação" demonstrou ser necessário o conhecimento e gerenciamento das tecnologias e informações dentro da instituição. A "Governança, Riscos e Compliance" demostrou a cadeia de relacionamentos da empresa envolvidos com a tomada de decisão e análises de riscos. Assim, o trabalho por meio das ferramentas administrativas modernas confirmou e respondeu de forma satisfatória as dificuldades e dúvidas referente a implantação da LGPD.

A metodologia utilizada para o estudo foi realizada pela pesquisa de artigos científicos e sites confiáveis, utilizando autores reconhecidos em suas áreas de pesquisas, contudo constataram-se limitações na pesquisa quando utilizado o tema em questão "Lei Geral de Proteção de Dados" - essa limitação foi concedida pela escassez de material de artigo científico, limitando-se a esse estudo o aprofundamento em materiais disponibilizados em revistas e sites de conteúdos jornalísticos, tecnológicos e empresariais.

Assim, constatou-se na visão de futuros administradores (que seremos em breve), para o efeito da Lei Geral de Proteção de Dados que toda e qualquer empresa que se enquadre nos parâmetros de tratamentos, processamentos e armazenamentos devem estar em conformidades com as normas e exigências impostas pela Lei. Buscar agilidade e eficiência nesse processo possibilita garantir uma imagem de segurança para seus clientes e competitividade para seus concorrentes. Deverão

buscar desenvolver uma cultura transparente e oferecer um serviço sigiloso.

Como indicação, afirmamos que futuras pesquisas podem ser oriundas desta, que apresentou um norte e orientações às organizações em respeito do que trata a Lei nº 13.709/2018.

REFERÊNCIAS

BELMIRO, João N. Sistema de informação. São Paulo: Pearson, 2012. Biblioteca digital Parson.

BENTO, Thiago. Como o fim do Windows 7 se relaciona com a LGPD. 2020. Disponível em: <https://www.cisoadvisor.com.br/como-o-fim-do-windows-7-se-relaciona-com-a-lgpd/>. Acesso em: 15 jun. 2020.

BIDNIUK, Vladimir B. Governança, gestão de riscos e compliance são fatores primordiais para o sucesso das empresas. 2017. Disponível em: <https://administra

dores.com.br/noticias/governanca-gestao-de-riscos-e-compliance-sao-fatores-primordiais-para-o-sucesso-das-empresas>. Acesso em: 8 abr. 2020.

BLOK, Marcella. Compliance e governança corporativa. Rio de Janeiro: Freitas, 2017. Biblioteca digital Pearson.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: 15 mar. 2020.

CASTILHO, Luciane B. O uso da tecnologia da informação e comunicação (TIC) no processo de ensino e aprendizagem em cursos superiores. 2015. Disponível em: <https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=3&cad=rja&uact=8&ved=2ahUKEwiPjay77JzoAhXMILkGHWSlAUoQFjACegQIBRAB&url=http%3A%2F%2Fwww.fumec.

CAVALCANTE, Daniel. Lei Geral de Proteção de Dados (LGPD) sob a perspectiva do ensino superior privado. 2019. Disponível em:<https://www.migalhas.com.br/depeso/307496/lei-geral-de-protecao-de-dados-lgpd-sob-a-perspectivado-ensino-superior-privado>. Acesso em: 15 mar. 2020.

CHIAVENATO, Idalberto. Iniciação a sistemas, organizações e métodos - SO&M. Barueri: Manole. 2010. Biblioteca digital Pearson.

_____. Introdução à teoria da administração. 9 ed. Barueri: Manole, 2014. Biblioteca digital Pearson.

CONFEDERAÇÃO NACIONAL DE EMPRESAS DE SEGUROS GERAIS. Governança, risco e compliance no setor de seguros. 2018. Disponível em:<http://cnseg.org.br/data/files/54/C1/72/EF/4EC4B61069CEB5A63A8AA8A8/CNseg_OSgovernancarisco_140918_er-WEB.pdf>. Acesso em: 8 abr. 2020.

COMISSÃO EUROPEIA. Proteção de dados na UE. 2018. Disponível em: <https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_pt>. Acesso em: 01 mar. 2020.

_____. O que são dados pessoais? 2018. Disponível em: <https://ec.europa.eu/info/law-topic/data-protection/data-protection-eu_pt>. Acesso em: 01 mar. 2020.

CURY, Antonio. Organização e métodos: uma visão holística. São Paulo: Atlas, 2012. Biblioteca digital Pearson.

DUARTE, Tomás. Impactos da Lei Geral de Proteção de Dados. 2020. Disponível em: <https://www.otempo.com.br/opiniao/artigos/experiencia-do-cliente-1.2310588>. Acesso em: 8 abr. 2020.

DYLEWSKI, André. Privacidade de dados: 3 cuidados para campanhas conscientes e efetivas de mídia programática. 2020. Disponível em: <https://www.segs.com.br/info-ti/222444-privacidade-de-dados-3-cuidados-para-cam panhas-conscientese-efetivas-de-midia-programatica>. Acesso em: 8 abr. 2020.

FELICIANO, Antonio M. Contribuições da gestão do conhecimento para ações empreendedoras de inclusão digital. 2008. Disponível em: <https://repositorio.ufsc.

br/xmlui/handle/123456789/91972>. Acesso em: 8 abr. 2020.

FONSECA. Paula F. Gestão de segurança da informação: o fator humano. 2009. Disponível em: <https://www.ppgia.pucpr.br/~jamhour/RSS/TCCRSS08A/Paula%20Fernanda%20Fonseca%20-%20Artigo.pdf>. Acesso em: 8 abr. 2020.

FREITAS. Ryan A. Marco civil da internet e responsabilidade dos provedores de

serviços. 2017. Disponível em: <https://aplicacao.mpmg.mp.br/xmlui/bitstream/handle/123456789/1332/Marco%20civil.pdf?sequence=1>. Acesso em: 1 mar. 2020.

GARCIA, Talita Orsini de Castro. LGPD: controlador e operador devem estar em sintonia para mitigar riscos. 2019. Disponível em:<https://computerworld.com.br/2019/06/06/lgpd-controlador-e-operador-devem-estar-em-sintonia-para-mitigar-riscos/>. Acesso em: 15 mar. 2020.

GASPARIN, Mirian. LGPD Motiva Investimento Em Segurança Cibernética. 2020. Disponível em: <https://miriangasparin.com.br/2020/03/lgpd-motiva-investimento-em-seguranca-cibernetica/>. Acesso em: 15 jun. 2020.

GUILHERME. Luís F. L. F. Um breve entendimento sobre a LGPD – Lei Geral de Proteção de Dados. 2019. Disponível em: <https://administradores.com.br/artigos/lgpd-lei-geral-de-protecao-de-dados-breve-entendimento>. Acesso em: 8 abr. 2020.

HINTZBERGEN, Jule, et al. Fundamentos de segurança da informação. São Paulo: Brasport, 2018. Biblioteca digital Pearson.

LAUDON, Kenneth C., LAUDON, Jane P. Sistema de informação gerenciais. São Paulo: Pearson, 2007. Biblioteca digital Pearson.

LEITE, Carolina S. P. Governança, riscos e compliance: a importância da diferenciação de conceitos. 2018. Disponível em: <https://www.marcosmartins.adv.br/pt/governanca-riscos-e-compliance-a-importancia-da-diferenciacao-de-conceitos/> Acesso em: 8 abr. 2020.

LIMA, Mariana. Titular, Operador e Controlador – o que isso quer dizer?. 2020. Di

sponível em: <https://triplait.com/titular-operador-e-controlador/>. Acesso em: 15 jun. 2020.

MAGALHAES, Alessandro LGPD: Quem é o encarregado ou DPO? Qual o seu papel?. 2019. Disponível em: <https://alessandromagalhaes.com/2019/10/31/lgpd-dpo-encarregado/>. Acesso em: 15 mar. 2020.

MANOEL, Paulo S. Governança de segurança da informação: como criar oportunid

ades para seu negócio. Rio de Janeiro: Brasport, 2014. Biblioteca digital Pearso.

MEIRELES, Leandro. Pequenas e médias empresas brasileiras não estão preparadas para a LGPD. 2020. Disponível em: <https://www.consumidormoderno.com.br/2020/03/23/empresas-brasileiras-nao-estao-preparadas-lgpd/>. Acesso em: 8 abr. 2020.

MINISTÉRIO DA INDUSTRIA, COMÉRCIO E SERVIÇO. Agenda brasileira para a Indústria 4.0: O Brasil preparado para os desafios do futuro. Disponível em: <http://www.industria40.gov.br/>. Acesso em: 07 mar. 2020.

MINISTÉRIO DA JUSTIÇA E SEGURANÇA PUBLICA. Marco Civil da Internet. Disponível em: <https://www.justica.gov.br/seus-direitos/elaboracao-legislativa/participacao-social/marco-civil>. Acesso em: 07 mar. 2020.

NEVES, Miranilde O. A importância da investigação qualitativa no processo de formação continuada de professores: subsídios ao exercício da docência. 2015. Disponível em: <https://www.google.com.br/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=2ahUKEwiu1MHBr6noAhUPIbkGHUkqB88QFjABegQICxAD&url=http3A%2F%2Frevistas.ufpi.br%2Findex.

NUNES, Igor. Desafios dos CIOs em 2020 será manter a segurança e governança dos ambientes multinuvem. 2020. Disponível em: <https://cio.com.br/desafios-dos-cios-em-2020-sera-manter-a-seguranca-e-governanca-dos-ambientes-multinuvem/>. Acesso em: 8 abr. 2020.

PEREIRA, Helena A. S.; BERGAMASCHI, Alessandro B. Manual de gestão de riscos do INPI. 2018. Disponível em: <https://www.bibliotecadeseguranca.com.br/wp-content/uploads/2020/01/manual-de-gestao-de-riscos-do-inpi.pdf>. Acesso em: 8 abr. 2020.

PRATA. Amanda P. O Marco Civil da Internet: Proteção à privacidade e intimidade dos usuários. 2017. Disponível em: <https://repositorio.ufu.br/handle/123456789/20238>. Acesso em: 01 mar. 2020.

SALDANHA, Jânia M. L. BRUM, Márcio M., MELLO, R. C. As novas tecnologias da informação e comunicação entre a promessa de liberdade e o risco de controle total: estudo da jurisprudência do sistema interamericano de direitos humanos. 2016. Disponível em: <https://www.sciencedirect.com/science/article/pii/ S1870465417300144>. Acesso em: 8 abr. 2020.

SANTANDER. GDPR: o que você precisa saber sobre proteção de dados na Europa. 2019. Disponível em: <https://santandernegocioseempresas.com.br/app/empreendedorismo/gdpr-lei-de-protecao-de-dados-na-europa>. Acesso em: 01 mar. 2020.

SENADO. Lei que cria autoridade nacional de proteção de dados é sancionada com vetos. 2019. Disponível em: <https://www12.senado.leg.br/noticias/materias/201

9/07/09/lei-que-cria-autoridade-nacional-de-protecao-de-dados-e-sancionada-com-vetos>. Acesso em: 15 mar. 2020.

SILVA, Karol, SILVA, Taís C., COELHO, Marcos A. P. O uso da tecnologia da informação e comunicação na educação básica. 2015. Disponível em: <http://www.periodicos.letras.ufmg.br/index.php/anais_linguagem_tecnologia/article/view/10553>. Acesso em: 8 abr. 2020.

SITE DANIEL. Conhecendo a lei geral de proteção de dados do Brasil. 2019. Disponível em: <https://www.daniel-ip.com/pt/artigos/mp-869-2018-o-que-muda-na-lei-geral-de-protecao-de-dados-lgpd/>. Acesso em: 8 abr. 2020.

SITE E-COMMERCE BRASIL. Um quarto das PMEs brasileiras ainda desconhec

e a LGPD, revela pesquisa. Disponível em: <https://www.ecommercebrasil.com.br/noticias/pmes-brasileiras-ainda-desconhece-lgpd/>. Acesso em: 8 abr. 2020.

SITE EPOCA NEGOCIOS. 84% das empresas brasileiras não estão preparadas p

ara a LGPD. Disponível em: <https://epocanegocios.globo.com/Tecnologia/noticia/2019/11/84-das-empresas-brasileiras-nao-estao-preparadas-para-lgpd.html>. Acesso em: 8 de abr. 2020.

SITE FENALAWDIGITAL. Finalmente a Lei Geral de Proteção de Dados (LGPD) – resumo dos pontos relevantes. 2018. Disponível em:<https://digital.fenalaw.com.br/legisla-o/finalmente-lei-geral-de-prote-o-de-dados-lgpd-resumo-dos-pontos-relevantes>. Acesso em: 15 mar. 2020.

SITE FIA: Fundação instituto de administração: GDPR: tudo que você precisa saber sobre a Lei. 2019. Disponível em: <https://fia.com.br/blog/gdpr/>. Acesso em: 01 mar. 2020.

SITE HIGH SECURITY CENTER: LGPD: Lei Geral de Proteção de Dados do Brasil. 2019. Disponível em: <https://www.hscbrasil.com.br/lgpd/>. Acesso em: 15 jun. 2020.

SITE IBGC. O que é governança corporativa. Disponível em: <https://www.ibgc.org.br/conhecimento/governanca-corporativa>. Acesso em: 14 abr. 2020.

SITE INFONOVA. Segurança da informação: O que faz? Para que serve?. 2018. Disponível em: <https://www.infonova.com.br/artigo/seguranca-da-informacao-o-que-faz-para-que-serve/>. Acesso em: 8 abr. 2020.

SITE INTERVOZES. Em defesa do Marco Civil. 2012. Disponível em: <https://intervozes.org.br/em-defesa-do-marco-civil/>. Acesso em: 01 mar. 2020.

SITE INVESTORINTEL. GDPR - Big Data e o direito de ser esquecido. 2018. Disponível em: <https://investorintel.com/market-analysis/market-analysis-intel/gdpr-big-data-right-forgotten/?print=print>. Acesso em: 01 mar. 2020.

SITE JORNAL CONTÁBIL. Um quarto das PMEs nacionais ainda desconhece a LGPD. 2020. Disponível em: <https://www.jornalcontabil.com.br/um-quarto-das-pmes-nacionais-ainda-desconhece-a-lgpd/>. Acesso em: 8 abr. 2020.

SITE LGPDBRASIL. LGPD: 8 dúvidas sobre a nova lei. 2020. Disponível em: <https://www.lgpdbrasil.com.br/lgpd-8-duvidas-sobre-a-nova-lei-2/>. Acesso em: 8 abr. 2020.

_____. O que muda com a nova Lei de Dados Pessoais. 2020. Disponível em: <http

s://www.lgpdbrasil.com.br/o-que-muda-com-a-lei/>. Acesso em: 8 abr. 2020.

SITE MEU SUCESSO. Oque é LGPD?. 2019. Disponível em: <https://meusucesso.com/artigos/direito/o-que-e-lgpd-1890/>. Acesso em: 07 abr. 2020.

SITE SEGS. Proteção de dados na internet. 2020. Disponível em: <https://www.segs.com.br/info-ti/222232-protecao-de-dados-na-internet>. Acesso em: 8 abr. 2020.

SITE SERPRO E LGPD. Quais são os seus direitos?. Disponível em: <https://www.serpro.gov.br/lgpd/cidadao/quais-sao-os-seus-direitos-lgpd>. Acesso em: 15 mar. 2020.

_____. Dados pessoais. Disponível em: <https://www.serpro.gov.br/lgpd/menu/protecao-de-dados/dados-pessoais-lgpd>. Acesso em: 15 mar. 2020.

_____. Dados públicos. Disponível em: <https://www.serpro.gov.br/lgpd/menu/protecao-de-dados/dados-publicos-lgpd>. Acesso em: 15 mar. 2020.

_____. Dados anonimizados. Disponível em: <https://www.serpro.gov.br/lgpd/menu/protecao-de-dados/dados-anonimizados-lgpd>. Acesso em: 15 mar. 2020.

_____. O que muda com a LGPD. Disponível em: <https://www.serpro.gov.br/lgpd/menu/a-lgpd/o-que-muda-com-a-lgpd>. Acesso em: 8 abr. 2020.

_____. Quem vai regular a LGPD?. Disponível em: <https://www.serpro.gov.br/lgpd/governo/quem-vai-regular-e-fiscalizar-lgpd>. Acesso em: 15 mar. 2020.

SITE TIINSIDE. Para o Gartner, data center está com os dias contados. 2020. Disp

onível em: <https://tiinside.com.br/13/03/2020/para-o-gartner-data-center-esta-com-os-dias-contados/>. Acesso em: 8 abr. 2020.

TAURION, Cezar. Big Data. Rio de Janeiro: Brasport, 2013. Biblioteca digital Pearson.

TRIBUNAL DE CONTAS DA UNIAO. 10 passos para a boa gestão de riscos. 2018. Disponível em: <https://www.google.com.br/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwj_-ubgYTqAhUgH7kGHUQeCL8QFjAAegQIBRAB&url=https%3A%2F%2Fportal.tcu.gov.br%2Flumis%2Fportal%2Ffile%2FfileDownload.jsp%3FfileId%3D8A81881E64480910016466A1858A41B6&usg=AOvVaw1COXc5OUmApXoS8Xp-NyqE>. Acesso em: 8 abr. 2020.

_____. Boas práticas em segurança da informação. 2012. Disponível em: <http://www4.planalto.gov.br/cgd/assuntos/publicacoes/2511466.pdf>. Acesso em: 8 abr. 2020.

VARELLA, Luisa. Tudo sobre a Lei Geral de Proteção de Dados (LGPD). 2019. Disponível em: <https://www.compugraf.com.br/tudo-sobre-a-lei-geral-de-protecao-de-dados-lgpd/#atores_papeis_agentes_da_lgpd>. Acesso em: 8 abr. 2020.

VIDOR, Daniel Martins. LGPD: conheça o papel do controlador e operador de dados. 2019. Disponível em:<https://www.plugar.com.br/lgpd-conheca-o-papel-do-controlador-e-operador-de-dados/>. Acesso em: 15 mar. 2020.

VIEIRA, James B.; BARRETO, Rodrigo T. S.. Governança, gestão de riscos e integridade. 2019. Disponível em: <https://repositorio.enap.gov.br/bitstream/1/4281/1/5_Livro_Governan%C3%A7a%20Gest%C3%A3o%20de%20Riscos%20e%20Integridade.pdf>. Acesso em: 8 abr. 2020.