UNIVERSIDADE FEDERAL DE PERNAMBUCO

CENTRO DE ARTES E COMUNICAÇÃO

DEPARTAMENTO DE CIÊNCIA DA INFORMAÇÃO

GESTÃO DA INFORMAÇÃO

MICHELE DA MOTA MENDES

A NOVA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS: principais aplicações da Lei sob a ótica da Ciência da Informação nas Organizações no Brasil

Recife

2020

MICHELE DA MOTA MENDES

A NOVA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS: principais aplicações da Lei sob a ótica da Ciência da Informação nas Organizações no Brasil

Trabalho de Conclusão de Curso apresentado como requisito para aprovação na Disciplina de Trabalho de Conclusão de Curso 2, do Curso de Gestão da Informação, do Departamento de Ciência da Informação, da Universidade Federal de Pernambuco, sob orientação da Profª. Dra. Edilene Maria da Silva.

Recife

2020

Catalogação na fonte
Biblioteca Joaquim Cardozo – Centro de Artes e Comunicação

S538n Mendes, Michele da Mota
A nova Lei Geral de Proteção de Dados Pessoais: principais aplicações da Lei sob a ótica da Ciência da Informação nas Organizações no Brasil / Michele da Mota Mendes. – Recife, 2020.
41f.

Orientadora: Edilene Maria da Silva.
Trabalho de Conclusão de Curso (Graduação) – Universidade Federal de Pernambuco. Centro de Artes e Comunicação. Departamento de Ciência da Informação. Curso de Gestão da Informação, 2020.

Inclui referências.

1. Dados pessoais. 2. Governança de dados. 3. Lei Geral de Proteção de Dados Pessoais. 4. Segurança da informação. I. Silva, Edilene Maria da (Orientadora). II. Título.

020 CDD (22. ed.) UFPE (CAC 2020-200)

MICHELE DA MOTA MENDES

A NOVA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS: principais aplicações da Lei sob a ótica da Ciência da Informação nas Organizações no Brasil

Trabalho de Conclusão de Curso apresentado como requisito para aprovação na Disciplina de Trabalho de Conclusão de Curso 2, do Curso de Gestão da Informação, do Departamento de Ciência da Informação, da Universidade Federal de Pernambuco, sob orientação da Profª. Dra. Edilene Maria da Silva.

Data da Aprovação: 30 / 11 / 2020

BANCA EXAMINADORA

_____

Profª. Dra. Edilene Maria da Silva
Universidade Federal de Pernambuco

_____

Prof. Me. Márcio Henrique Wanderley Ferreira
Universidade Federal de Pernambuco

_____

Profa. Dra. Thaís Helen do Nascimento Santos
Universidade Federal de Pernambuco

_____

Profª. Dra. Adriana Carla Silva de Oliveira
(Dra. em Ciência da Informação)

Agradecimentos

Aos meus pais, por todo suporte que me possibilitou trilhar a vida acadêmica tão distante de casa.

À família Souza, por acreditar em mim, me motivar e apoiar.

Aos meus grandes amigos, e à João Pedro, que esteve ao meu lado nos momentos mais difíceis dessa jornada, me motivando, incentivando, alegrando-se com minhas conquistas e me impulsionando para a conclusão deste trabalho.

À minha orientadora Profª. Dra. Edilene Maria da Silva pelos ensinamentos constantes, pela dedicação, pelo suporte, pela paciência, pelas orientações e por todo o conhecimento e crescimento que me proporcionou.

Aos professores do curso de Gestão da Informação, em especial ao Prof. Me. Márcio Henrique Wanderley Ferreira, pelos ensinamentos e contribuição para a realização desse estudo.

Aos colegas da graduação, pelo convívio e aprendizado.

Aos membros da banca avaliadora, Profª. Dra. Adriana Carla Silva de Oliveira, Profª. Dra. Thaís Helen do Nascimento Santos e Prof. Me. Márcio Henrique Wanderley Ferreira.

A todos que diretamente ou indiretamente contribuíram para a conclusão e sucesso desse trabalho.

Muito obrigada.

Resumo

A nova Era da Informação tem revolucionado a forma como a sociedade lida com os dados e a informação. Nos últimos anos, esses elementos vêm ganhando destaque e sendo reconhecidos como insumos vitais para qualquer organização que deseja atuar ou continuar atuando no mercado dos negócios. Com a vasta quantidade de informação e dados que circulam, atualmente, dentro das organizações e, com a velocidade na qual se propagam, surgiu a premente necessidade de se gerir todo esse recurso informacional e de adotar práticas de governança de dados e de segurança da informação. E, como uma tendência mundial, surgiu também a necessidade de legislação específica de proteção desse recurso, a fim de regular sua utilização e promover o respeito à privacidade e à titularidade dos dados e informação. Este trabalho tem como objetivo observar a relação entre a Segurança da Informação, a governança de dados e a Lei Geral de Proteção de Dados Pessoais (LGPD) e apontar as principais mudanças que deverão ocorrer nas organizações para que elas se adequem à nova lei. O trabalho, de cunho exploratório e qualitativo, utiliza a bibliografia como principal fonte de informação. A coleta de dados foi realizada por meio de pesquisas em livros, artigos científicos, relatórios de palestras e seminários e as legislações relacionadas ao tema. Como resultado, identifica as práticas de governança de dados, quais sejam: identificação, organização, análise de fluxo informacional, revisão de políticas, contratos e termos e modificação de quadro profissional; bem como as práticas de segurança da informação com a observância aos princípios e adoção de medidas técnicas que as organizações devem adotar para garantir a confidencialidade, integridade, disponibilidade e, em alguns casos, a anonimização dos dados e informações. Conclui que o esforço para adequação à LGPD deve ser realizado nas organizações de forma multidisciplinar, compreendendo o trabalho conjunto entre a governança de dados e a segurança da informação.

Palavras-chave: Dados pessoais. Governança de dados. Lei Geral de Proteção de Dados Pessoais. Segurança da informação.

Abstract

The new Information Age has revolutionized the way society handles data and information. In recent years, these elements have gained prominence and are recognized as vital insums for any organization that wants to act or continue to operate in the business market. With the vast amount of information and data that currently circulate within organizations and, with the speed at which it propagates, the urgent need to manage all this information resource and adopt data governance and information security practices has arisen. And, as a global trend, there has also been a need for specific legislation to protect this resource in order to regulate its use and promote respect for privacy and the ownership of data and information. This work aims to observe the relationship between Information Security, data governance and the General Law for the Protection of Personal Data (LGPD) and point out the main changes that should occur in organizations for them to comply with the new law. The exploratory and qualitative work uses bibliography as the main source of information. Data collection was performed through research in books, scientific articles, lecture reports and seminars and legislation related to the subject. As a result, it identifies data governance practices, namely: identification, organization, information flow analysis, policy review, contracts and terms and modification of professional framework; as well as information security practices with compliance with the principles and adoption of technical measures that organizations must take to ensure the confidentiality, integrity, availability and, in some cases, anonymization of data and information. It concludes that the effort to adapt to the LGPD should be carried out in organizations in a multidisciplinary manner, understanding the joint work between data governance and information security.

Keywords: Personal data. Data governance. General Law for the Protection of Personal Data. Information security.

Lista de Abreviações

ABNT	Associação Brasileira de Normas Técnicas
BPM	Business Process Management
CI	Ciência da Informação
GD	Governança de Dados
GDPR	General Data Protection Regulation
GI	Gestão da Informação
GIC	Gestão da Informação e do Conhecimento
GTI	Governança de Tecnologia da Informação
ICT	Informação Científica e Tecnológica
LGPD	Lei Geral de Proteção de Dados Pessoais
MP	Medida Provisória
PL	Projeto de Lei
PR-SP	Partido da República de São Paulo
SERPRO	Serviço Federal de Processamento de Dados
SI	Segurança da Informação
TI	Tecnologia da Informação

SUMÁRIO

1 INTRODUÇÃO

Há mais de 20 anos, o austríaco Peter Drucker, renomado consultor de empresas considerado o pai da Administração, já previa, em seus estudos de mercado, que a atual era da informação em que vivemos, seria responsável por profundas modificações na economia, no mercado, nas estruturas setoriais, nos produtos e serviços e no comportamento do consumidor. Segundo Drucker:

> logicamente, trata-se apenas de previsões. Contudo, elas são feitas segundo a premissa de que a Revolução da Informação evoluirá como as várias revoluções tecnológicas nos últimos 500 anos, como a revolução da imprensa de Gutenberg, em torno de 1455. Sobretudo, a premissa é que a Revolução da Informação será como foi a Revolução Industrial no final do século XVIII e início do século XIX. E é exatamente assim que tem sido a Revolução da Informação nestes seus primeiros 50 anos." (Drucker, 2000, p.1).

Drucker (2000) previu que a revolução da informação teria como força motriz o comércio eletrônico, "o aparecimento explosivo da Internet como um canal importante, talvez principal, de distribuição mundial de produtos e serviços (...)". Entretanto, o que o austríaco não previu foi que tipo de produtos e serviços seriam oferecidos. Para ele, ainda não era possível saber tudo o que poderia ser comprado e vendido pelo comércio eletrônico. Atualmente sabe-se que quase tudo é suscetível de compra e venda, inclusive os próprios dados e informações.

Essa prática de trocar, vender ou comprar informações se tornou habitual entre as empresas que perceberam a importância dos dados e da informação quando o assunto é vantagem competitiva. Segundo Assis (2008, p.19):

> as organizações estão vivendo nos dias de hoje uma época de crescente concorrência global. Para serem bem-sucedidas, elas, necessariamente, devem saber mais sobre o mercado em nível mundial, bem como sobre planos e intenções, tanto dos seus consumidores quanto dos seus concorrentes. A concorrência, hoje, é muito agressiva e complexa. Verbas maiores para pesquisa e desenvolvimento, alianças e parcerias estratégicas com o objetivo de conquistar parcelas de mercado, acirrada competição de preço e qualidade são algumas das características desta nova realidade.

O advento da rede mundial de computadores contribuiu para essa prática e, com a coleta e as demais etapas de tratamento dos dados, é possível traçar perfis dos indivíduos para, por exemplo, servir como parâmetro para tomadas de decisões, como fornecer ou não um determinado serviço, ou ainda, oferecer produtos de forma personalizada.

Com informações relacionadas à renda, localização, hábitos, profissão e condição física e mental, por exemplo, é possível classificar e agrupar os indivíduos com base nos interesses de mercado da organização. Que empresa não gostaria de ter, em suas bases de dados, informações sobre potenciais clientes para seu ramo de atuação? E, de posse dessas informações, diminuir custos e direcionar precisa e eficazmente suas campanhas de marketing? E ainda, por outro lado, que empresa, possuindo tal base de dados, não gostaria de lucrar com a troca ou venda dessas informações? Transformando, assim, um insumo adquirido de forma gratuita, em um produto final extraordinariamente rentável.

Certamente, todos se lembram da campanha de *Donald Trump* nas eleições presidenciais de 2016 nos Estados Unidos, e das acusações à empresa de consultoria contratada *Cambrigde Analityca* e à rede social *Facebook*. O *Facebook*[1] foi acusado de fornecer, indevidamente, dados de seus usuários à consultoria que, por sua vez, com a utilização desses dados, criou mecanismos para traçar perfis de eleitores e auxiliar na campanha presidencial. A rede social foi acusada ainda de conceder, durante anos, dados de seus usuários às maiores empresas de tecnologia do mundo, como a *Microsoft*, a *Amazon*, a *Netflix* e o *Yahoo*[2]. No Brasil também temos casos semelhantes, como a suposta venda ilegal de dados pessoais dos cidadãos brasileiros pelo Serviço Federal de Processamento de Dados (SERPRO)[3].

Práticas como estas demonstram como a Revolução da Informação trouxe aspectos peculiares para o mercado global. Davenport (1998, p. 11) chegou a afirmar que “de acordo com as autoridades e as equipes de vendas das empresas, estamos em meio a uma nova Era da Informação, que irá revolucionar a maneira como se trabalha, compete e até mesmo como se pensa, no mercado.” Os dados e a informação se tornaram os principais produtos do que hoje se conhece como a indústria da informação.

De acordo com alguns autores como Costa (1995, p. 10):

> as sociedades mais desenvolvidas no mundo hoje são chamadas sociedades da informação, em função de sua atividade econômica

---

[1] MATTHEW ROSENBERG (United States). The New York Times. **How Trump Consultants Exploited the Facebook Data of Millions.** 2018. Disponível em: <https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html?module=inline>. Acesso em: 20 abr. 2019.

[2] GABRIEL J.X. DANCE (United States). The New York Times. **As Facebook Raised a Privacy Wall, It Carved an Opening for Tech Giants**. 2018. Disponível em: <https://www.nytimes.com/2018/12/18/technology/facebook-privacy.html>. Acesso em: 20 abr. 2019.

[3] SERVIÇO FEDERAL DE PROCESSAMENTO DE DADOS (Brasília). Assessoria de Imprensa. **Serpro assegura compromisso com o sigilo de dados dos cidadãos brasileiros: nota à imprensa**. 2018. Disponível em: <http://www.serpro.gov.br/menu/imprensa/notas-a-imprensa-1/nota-oficial-01-06-2018>. Acesso em: 20 abr. 2019.

> ser fortemente baseada na produção do setor informacional, composto do que se convencionou chamar indústrias de informação.

Significa dizer que a informação se revelou imprescindível para a competitividade das empresas. Não apenas as informações utilizadas internamente nas empresas para fins de criação de planos estratégicos, mas também as utilizadas como produto econômico final. Davenport (1998, p. 117) explica que:

> no Ocidente, quem defende a troca de informações costuma restringi-la ao interior das corporações. Entretanto, algumas empresas descobriram que trocar informes com parceiros de negócios, e até mesmo com concorrentes, apresenta nítidas vantagens. Vários pesquisadores têm estudado essa troca dentro de uma atividade específica, chamada *comércio da informação*, e seus resultados sugerem que esse campo pode oferecer benefícios competitivos e econômicos.

Para além do comércio 'informal' da informação, existem ainda os casos de vazamentos acidentais. A falta de diligência na criação e manutenção de bases informacionais, aliada à falta de uma cultura informacional e de legislações e fiscalizações mais rigorosas, possibilita que informações pessoais dos indivíduos sejam expostas, como foi no caso da rede varejista *Netshoes*[4]. No ano de 2018, o Ministério Público do Distrito Federal alertou sobre o que seria um dos maiores incidentes de segurança da informação já registrados no Brasil: o vazamento de uma lista contendo informações de aproximadamente 2 milhões de clientes da empresa. A empresa assumiu o erro e acordou com o Ministério Público formas de minimizar o incidente.

Diante das atuais transformações que a informação vem provocando no mundo, da importância e do valor mercadológico que possui, e das constantes notícias de usos inadequados e de vazamentos de dados pessoais de indivíduos em todo mundo, fez-se necessária a criação de leis que regulamentem o uso dessas informações, com a finalidade de proteger os indivíduos de empresas que não empregam o tratamento adequado ou que visam unicamente a monetização desses dados.

No Brasil, em 14 de agosto de 2018, foi sancionada a Lei Geral de Proteção de Dados Pessoais (LGPD), primeira lei nacional que trata única e especificamente

---

[4] BRASÍLIA. Ministério Público do Distrito Federal e Territórios. Secretaria de Comunicação. **MPDFT recomenda providências à Netshoes após vazamento de quase 2 milhões de dados de clientes**. 2018. Disponível em: <http://www.mpdft.mp.br/portal/index.php/comunicacao-menu/noticias/noticias-2018/9775-mpdft-recomenda-providencias-a-netshoes-apos-vazamento-de-quase-2-milhoes-de-dados-de-clientes>. Acesso em: 20 abr. 2019.

do assunto. O país encontra-se em preocupante atraso no que diz respeito à proteção de dados. Outros países na América Latina, como Argentina[5], Chile[6] e Peru[7], já têm legislação específica há anos.

Na seara jurídica, é garantido aos indivíduos o direito à privacidade, previsto na Constituição Federal, em seu artigo 5º, inciso X, que estabelece que: "são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas [...]" (BRASIL, 1988). Desta forma, Silva (2010, p. 206) entende que inviolável é o "conjunto de informação acerca do indivíduo que ele pode decidir manter sob seu exclusivo controle, ou comunicar, decidindo a quem, quando, onde e em que condições".

Significa dizer que, mesmo antes da publicação de uma lei específica para proteção de dados, o conjunto de informações de um indivíduo, que são seus dados pessoais, tinha como base legal de proteção a Lei Maior, que já previa tal proteção como um direito fundamental.

Além do campo científico do Direito, outra área da Ciência tem se preocupado com a proteção dos dados dos indivíduos: a Ciência da Informação (CI). Na área da Ciência da Informação, a Gestão da Informação (GI), a Governança de Dados (GD) e a Segurança da Informação (SI) têm se preocupado com a informação no sentido de preservar o seu valor, tanto para os indivíduos quanto para as organizações.

Portanto, com base no que foi exposto, este estudo pretende analisar a legislação pátria, no que concerne à Segurança da Informação e Governança de Dados, para tanto, tenta responder a seguinte pergunta de pesquisa: **quais são os aspectos relevantes da segurança da informação e da governança de dados que contribuem na aplicação da LGPD nas organizações no Brasil?**

O trabalho foi construído com base em estudos e análises da lei nacional, bem como em aspectos da segurança da Informação e da governança de dados aplicáveis à lei.

O objetivo geral do trabalho é evidenciar a relação entre a segurança da informação, a governança de dados e a Lei Geral de Proteção de Dados Pessoais,

---

[5] CELE. Centro de Estudios En Libertad de Expresión y Acceso a La Información. **Lei No. 25.326 Dados Pessoais**. 2000. Disponível em: https://observatoriolegislativocele.com/pt/dados-pessoais/. Acesso em: 05 out. 2020.

[6] BCN, Biblioteca del Congreso Nacional de Chile /. **LEY 19628 SOBRE PROTECCION DE LA VIDA PRIVADA**. 1999. Disponível em: https://www.bcn.cl/leychile/navegar?idNorma=141599. Acesso em: 05 dez. 2020.

[7] CELE. Centro de Estudios En Libertad de Expresión y Acceso a La Información. **Perú Ley N°29.733 (Ley de Protección de Datos Personales)**. 2011. Disponível em: https://observatoriolegislativocele.com/ley-29733/. Acesso em: 05 dez. 2020.

apontando os principais aspectos que se aplicam a lei, nas organizações no Brasil. Os objetivos específicos são: verificar os princípios e técnicas da segurança da informação sob a ótica da Ciência da Informação; apontar as principais mudanças que a nova lei estabelece para as práticas da segurança da informação e relacioná-las com as boas práticas de governança de dados nas organizações.

Sendo assim, no primeiro momento, apresenta os conceitos básicos de ciência da Informação, de gestão da Informação, de governança de dados e de segurança da Informação. Discorre brevemente sobre os princípios da segurança da Informação e as principais medidas técnicas da área para a proteção de dados. Em seguida, apresenta breve histórico da lei, com suas origens, trajetórias e conceitos. E, por fim, realiza análise acerca dos principais aspectos que inter-relacionam a segurança da Informação, a governança de dados e a lei brasileira no que se refere à proteção de dados nas organizações no Brasil.

2 CIÊNCIA DA INFORMAÇÃO

A Ciência da Informação nasceu da explosão informacional decorrente do avanço científico e tecnológico alcançado durante a Segunda Guerra Mundial, e da necessidade de se facilitar e agilizar o trabalho de profissionais de diversas áreas do conhecimento. Por volta da década de 1920, esses próprios profissionais:

> Começaram a se dedicar ao trabalho de elaborar índices, resumos, promover canais de disseminação, de forma a facilitar a agilizar o trabalho de seus pares. Depois de algum tempo, eles começaram a designar a si mesmos cientistas da informação (ARAÚJO, 2014, p.7).

Apenas ter o documento não era suficiente para a realização eficiente dos trabalhos desses profissionais. Era necessário que as informações contidas nos documentos fossem analisadas, tratadas e disseminadas entre eles. Vários pesquisadores estudaram esse processo de produção, análise e compartilhamento de informações entre os profissionais, e chegaram à conclusão de que “a Ciência da Informação tinha por objeto o estudo dos fluxos, dos caminhos percorridos pela informação, sua materialização em diferentes produtos e serviços.” (ARAÚJO, 2014).

Assim, ao contrário da Biblioteconomia, da Arquivologia e da Museologia, que, segundo Araújo, são ciências voltadas para a custódia, a posse, o manuseio e a preservação de documentos físicos, a CI não estava preocupada com os

documentos e sua custódia, mas sim, com o seu conteúdo, e sua circulação e disseminação, a fim de promover o conhecimento científico e tecnológico.

Desta forma, a Ciência da Informação figura como transmissora do conhecimento, como no conceito dado pelo renomado pesquisador Saracevic, que entende que:

> A Ciência da Informação é um campo dedicado às questões científicas e à prática profissional voltadas para os problemas da efetiva comunicação do conhecimento e de seus registros entre os seres humanos, no contexto social, institucional ou individual do uso e das necessidades de informação. No tratamento destas questões são consideradas de particular interesse as vantagens das modernas tecnologias informacionais. (SARACEVIC, 1996, p. 47).

Buscando sua própria identidade e autonomia, a partir da década de 1960, a CI passou a se consolidar como uma área do conhecimento e, com isso, observou o surgimento de diversas subáreas dentro de seu campo de pesquisa.

A primeira subárea encontrada na Ciência da Informação foi a Informação Científica e Tecnológica (ICT) em que, segundo Araújo (2014, p.11):

> Os estudos iniciais estiveram voltados para a busca de caracterizações universais das diferentes fontes e recursos informacionais presentes na prática científica (tempo de produção de cada um deles, vantagens e desvantagens, completude, custos, etc.).

Posteriormente, outra subárea foi encontrada na CI: a Gestão da Informação e do Conhecimento (GIC). Esta se desenvolveu seguindo a mesma instrumentalidade da primeira, porém, com foco no ambiente organizacional e seus processos. A GIC buscou realizar estudos sobre a gestão de recursos informacionais, analisando as diversas fontes de informação e sua influência nos processos decisórios, e sobre os tipos de conhecimentos que circulam dentro de uma organização, além de estudar a cultura organizacional como mais um elemento que influencia a GIC.

Além dessas subáreas, a CI tem ainda diversas outras que estudam a política e a economia da informação, a representação e recuperação da informação, o comportamento informacional dos usuários e as métricas da informação, a segurança da informação, a governança de dados, entre outras.

A fim de alcançar os objetivos desta pesquisa, faz-se necessário contextualizar o tema com alguns conceitos de gestão da Informação, segurança da Informação e governança de Dados, o que será feito nas seções seguintes.

2.1 Gestão da Informação

A Gestão da Informação nasceu a partir da percepção da importância da informação como recurso dentro das organizações. Inicialmente, a GI se preocupava com o excesso de informações gerado depois da Segunda Guerra Mundial. Naquela época, havia dificuldade no uso das informações, tanto em se encontrar a informação desejada, quanto na circulação adequada dessa informação. Além de dificuldades relacionadas ao tamanho do suporte físico onde todas essas informações eram armazenadas. Segundo Araújo (2014, p.63), “as primeiras reflexões sobre a gestão da informação incidiram, pois, sobre sua natureza física: reduzir o excesso, otimizar a circulação, identificar com precisão as necessárias e descartar as inúteis ou redundantes.”

Com o advento da nova era, a era “pós industrial” (ou “era da informação”), e a utilização dos computadores e da rede mundial de computadores, as preocupações iniciais da gestão da informação deram lugar a outras, já que os computadores e a internet trouxeram mecanismos inovadores e mais eficientes para armazenamento da enorme quantidade de informação.

A descoberta mais importante empreendida foi que, além das informações que existem materialmente, outro tipo de informação é tão ou mais valioso: a informação que está na mente das pessoas, se transformando em conhecimento. Daí surgiu a expressão “gestão da informação e do conhecimento”. “Não bastava gerir os recursos informacionais, era preciso também gerir o conhecimento, criando as condições propícias para transformá-lo em informação.” (ARAÚJO, 2014, p.64).

Na década de 1990, alguns autores como Nonaka e Takeuchi (1997) trouxeram a ideia de que não bastaria gerir o conhecimento nas mentes das pessoas, era necessário gerir também a própria cultura organizacional, criando mecanismos para transformar esses conhecimentos individuais em conhecimento da organização. Segundo os autores, os conhecimentos que cada pessoa dentro de uma organização detem, são construídos coletivamente, influenciando e construindo também a cultura informacional e o conhecimento organizacional. Eles explicam que a criação do conhecimento organizacional é “a capacidade de uma empresa de criar novo conhecimento, difundi-lo na organização como um todo, e incorporá-lo a produtos, serviços e sistemas.” (NONAKA; TAKEUCHI 1997, p.1).

Assim, no contexto atual, a gestão da informação vem atuando nas organizações gerenciando todos os tipos e formatos de informações e, gerenciando também, os contextos nos quais o conhecimento acontece. Intrinsecamente ligada à gestão da informação está à área de governança de dados.

2.2 Governança de Dados

Uma área que vem conquistando cada vez mais notoriedade dentro das empresas por sua extrema importância, é a área de governança de dados. Ela surgiu da necessidade de se ter maior controle sobre os dados e informações, especialmente com o advento dos bancos de dados, nos anos 1970. Entretanto, naquela época, a governança de dados era relacionada à área de tecnologia da informação, e não à área de negócios, pois os dados e informações não eram entendidos como importantes insumos dos negócios. Atualmente, o entendimento é outro. Já se entende que os dados e informações são insumos vitais para qualquer organização, e a governança de dados ganhou e vem ganhando cada vez mais espaço na gestão das organizações.

Segundo Barbieri (2020) “a governança de dados foca em princípios de organização e controle sobre esses insumos essenciais para a produção de informação e conhecimento das empresas”. Pode-se entender a governança de dados como a prática de gerenciar a utilização dos dados em uma organização. Inclui: **a)** a identificação dos dados, ou seja, a organização deve conhecer quais são os dados de terceiros que ela utiliza em suas atividades; **b)** a tipificação desses dados, que podem ser sensíveis ou não; **c)** o acompanhamento do fluxo desses dados, ou seja, por onde eles passam dentro da organização, quais são os departamentos responsáveis pelo tratamento; **d)** a análise das medidas técnicas utilizadas para o tratamento dos dados; e **e)** a revisão e adequação de políticas, contratos e termos.

Nesse sentido, Espíndola (2018, p.280) corrobora com a ideia de que:

> A governança de dados determina políticas, acordos, papéis e responsabilidades com relação aos dados gerados na organização, bem como define quais métodos devem utilizados nas atividades de criação, armazenamento, avaliação, uso e eliminação de dados.

A partir dos conceitos de Barbieri e Espíndola é possível observar que a governança de dados perpassa por diversos setores, não apenas na área de

tecnologia da informação, não apenas na área de gestão, mas em todas as áreas de uma organização.

É possível que ainda existam dúvidas acerca da relação entre governança de tecnologia da informação e governança de dados. Barata (2015, p. 15) distingue claramente os conceitos de ambos. Segundo o autor, “a GTI é responsável pelo gerenciamento do portfólio de serviços, projetos e infraestruturas em TI, enquanto a GD é responsável pelo gerenciamento de dados e a tomada de decisões a partir da análise dos dados”. Certamente são áreas complementares, embora a governança de dados apresente certa transversalidade e maior abrangência, percorrendo todos os setores de uma organização onde existam dados e informações.

Para que se elucide essa distinção entre essas áreas do conhecimento, a próxima seção apresentará os conceitos, princípios e técnicas de segurança da informação.

2.3 Segurança da Informação

A informação é um ativo de vital importância para as organizações. Mesmo quando ela era encontrada apenas em meio físico, mesmo antes da existência dos computadores, da internet e de *softwares* específicos para gerenciamento dessas informações. O que difere a informação de antigamente e a informação de hoje é a forma como ela pode ser encontrada.

Antigamente as informações eram registradas em papel e guardadas em gavetas e cofres, protegidas, de certa forma, de acessos não autorizados. Atualmente, as informações podem ser encontradas, em sua maior parte, em meio digital. Dificilmente, hoje, uma organização aceita o risco de armazenar informações vitais em meios físicos apenas. Isto porque os meios físicos se mostraram insuficientes e menos eficientes e seguros em comparação aos meios digitais. Os modos pelos quais, hoje, as informações são utilizadas e protegidas, estão cada vez mais complexos e sofisticados.

Machado (2014) afirma que:

> Não seria exagerado afirmar que as informações na sociedade dependem cada vez mais dos sistemas de informação e da utilização de computadores pessoais e equipamentos móveis. E, por isso, interpretamos a segurança da informação como como assunto diretamente relacionado com a tecnologia da informação.

Quando se fala em segurança da informação, o primeiro pensamento que surge é que ela está associada aos sistemas computadorizados e às práticas técnicas da computação para proteção dos dados. Contudo, não se trata apenas da implantação de sistemas e métodos de segurança, deve-se levar em consideração também os aspectos orgânicos na prática da segurança da informação. Segundo Fernandes (2010, p.8) “as soluções tecnológicas não solucionarão os problemas de segurança da informação, da mesma forma que o computador não é solução isolada para a melhor organização da informação”.

Marciano (2006, p. 43) reitera que:

> A fim de melhor compreender-se a inserção da segurança da informação sob os diferentes aspectos em que se apresenta, tendo em vista evitar-se o reducionismo tecnológico sob o qual é geralmente apresentada, é fundamental que ela seja vislumbrada à luz de alguns conceitos da disciplina da qual é tributária - a Ciência da Informação.

No âmbito da Ciência da Informação, a segurança da informação é definida de forma mais abrangente. Para Fernandes citado por Cunha e Cavalcanti (2010), “segurança da informação consiste em procedimentos para proteção do acervo informacional de uma organização contra acesso ou uso por pessoas não autorizadas”. Percebe-se que a Ciência da Informação compreende a SI não apenas sob o viés tecnológico, reconhecendo a importância da utilização da tecnologia, mas também sob o viés informacional, reconhecendo a importância do objeto da proteção à informação.

Isso fica bem claro na definição de Fontes (2006, p.15) para quem a “segurança da informação é o conjunto de orientações, normas, procedimentos, políticas e demais ações que tem por objetivo proteger o recurso informação.”

Também a norma projetada para servir de referência nas aplicações de segurança da informação dentro das organizações, a ABNT NBR ISO/IEC 27002/2013, define segurança da informação como “um conjunto adequado de controles, incluindo políticas, processos procedimentos, estrutura organizacional e funções de *software* e *hardware*”. (ABNT, 2017).

Sendo assim, proteger os dados e a informação envolve não somente a utilização de soluções tecnológicas, mas também, a observância de princípios, o treinamento de recursos humanos e a implementação de recursos administrativos políticos e estratégicos.

2.3.1 Princípios da Segurança da Informação

A segurança da informação é norteada por princípios e técnicas mundialmente reconhecidas que visam a implementação de um conjunto de boas práticas de segurança da informação nas organizações[8].

Para Machado (2014), “a segurança da informação é uma maneira de proteger os sistemas de informação e a sociedade contra diversos ataques, mantendo documentos e arquivos dentro dos princípios de confidencialidade, integridade e disponibilidade”. Já para Lyra citado por Bastos & Caubit (2015, p.10),

> A segurança de informação é caracterizada pela aplicação adequada de dispositivos de proteção sobre um ativo ou um conjunto de ativos visando preservar o valor que este possui para as organizações. A aplicação destas proteções busca preservar a confidencialidade, a integridade e a disponibilidade, não estando restritos somente a sistemas ou aplicativos, mas também informações armazenadas ou veiculadas em diversos meios além do eletrônico ou em papel.

Com isto, entende-se que segurança da informação não se trata apenas de aplicar técnicas para tratamento dos dados, como também observar princípios que revelam a relevância da informação para as organizações. Os princípios mais importantes que regem a SI são os princípios da confidencialidade, da integridade e da disponibilidade da informação.

2.3.1.1 Confidencialidade

O princípio da confidencialidade se refere à garantia de que apenas pessoas autorizadas deverão ter acesso às informações. Seria a prática de restringir o acesso à determinadas informações, permitindo que apenas um grupo selecionado de usuários estejam autorizados a conhecê-las.

Para a adoção desse princípio, é necessário que haja a junção de medidas técnicas e administrativas, como explica Machado (2014):

> A confidencialidade pode ser fornecida por meio de técnicas de criptografia de dados e da forma como eles são armazenados e transmitidos, assim como por meio de acompanhamento de tráfego de rede, controle de acesso rigoroso, classificação de dados e treinamento de pessoal sobre os procedimentos adequados na utilização de informações na empresa.

---

[8] ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR ISO/IEC 27002:2013: **Tecnologia da informação - Técnicas de segurança - Código de prática para controles da segurança da informação**. 2a. ed. Rio de Janeiro, 2013.

A confidencialidade está relacionada ao grau de sigilo de um dado ou informação. Segundo Lyra e outros (2015, p.38), “toda a informação deverá ter sua classificação conforme o nível de sigilo atribuído a seu conteúdo, cada dado ou a informação deve estar acessível apenas a quem tem declarada autorização para conhecê-la”.

Segundo o seu conteúdo, as informações podem ser classificadas como confidenciais, restritas, internas ou públicas, e o grau de sigilo varia conforme a classificação. (LYRA, 2015).

As informações confidenciais são as que possuem maiores restrições, podendo ser acessadas apenas por usuário autorizados e com necessidade específica de acesso comprovado e aprovado. Já as informações consideradas restritas são aquelas que podem ser utilizadas apenas por determinado setor na organização, tendo em vista a necessidade do acesso para a realização das atividades. (LYRA, 2015).

As informações internas são aquelas de conhecimento de grande parte dos colaboradores e não representam tanta ameaça. Ainda assim, devem ser tratadas com segurança, pois jamais devem extrapolar o ambiente da organização. Já as informações públicas são as que já são de conhecimento geral, e a sua divulgação é permitida e não acarreta em riscos para a organização. (LYRA, 2015).

2.3.1.2 Integridade

O princípio da integridade está relacionado à garantia de que a informação não sofra modificações não autorizadas. Segundo Machado (2014):

> Os mecanismos de hardware, software e comunicação devem trabalhar de maneira conjunta para manter e processar dados corretamente e movimentar dados para os destinos desejados sem qualquer alteração não autorizada ou não esperada.

O principal embasamento deste princípio está na autorização. O autor reitera que uma informação íntegra é diferente de uma informação exata. A informação exata sempre será íntegra, porém, a informação íntegra nem sempre será exata. A integridade está na análise das modificações sofridas pelas informações, se autorizadas ou não. Uma organização pode, deliberadamente, alterar informações, visando protegê-las, por exemplo, sem que se descaracterize sua integridade. É o caso de empresas que já utilizam alguma técnica de anonimização dos dados.

Por exemplo, a organização pode suprimir uma parte dos dados, somente aquela que é capaz de identificar o titular, sem perder a sua integridade, ou seja, a informação continuará correta, embora incompleta. A privacidade do titular será respeitada, visto que ele não será identificado, mas os dados continuarão viáveis e úteis para a organização, permitindo com que ela analise e conheça os padrões do grupo no qual o indivíduo titular faz parte. Todo esse procedimento deve ser realizado com planejamento e somente por pessoas autorizadas.

Uma informação íntegra é aquela que se encontra em seu estado original, ou aquela que sofreu modificações autorizadas. Uma informação que sofre modificações não autorizadas não pode ser considerada íntegra, pois pode derivar de erros ou fraudes.

2.3.1.3 Disponibilidade

O princípio da disponibilidade tem relação com a garantia de que a informação esteja disponível sempre que necessário, ou seja, sempre que os usuários autorizados dela necessitem. Machado (2014) afirma que a disponibilidade "é a capacidade que os sistemas e as redes devem ter para executar e disponibilizar os dados de forma previsível e adequada às necessidades da empresa."

Lyra e outros (2015) compreendem que existem dois aspectos a serem observados para verificar a disponibilidade de uma informação: o tempo e a forma de acesso. O autor entende que, em alguns casos, a informação pode demorar para ser recuperada e disponibilizada para acesso, por isso, existem informações que necessitam de um prazo para disponibilização, prazo este que deve ser previsto pela organização.

2.3.2 Principais medidas técnicas de Segurança da Informação

Além da observância dos princípios, existem diversas medidas técnicas que podem e devem ser utilizadas pelas organizações a fim de garantir a segurança dos dados e informações.

Com o surgimento das leis de proteção de dados, a técnica de anonimização dos dados têm se tornado uma das técnicas mais estudadas na atualidade. Ela consiste em um conjunto de diversas outras técnicas aninhadas, cada qual com

suas especificidades, devendo ser analisadas para que se opte pela que mais se adequa às necessidades da organização.

Desta forma, nas subseções seguintes deste trabalho, serão conceituadas as principais técnicas de anonimização de dados, além de exemplificadas as aplicabilidades de cada uma.

2.3.2.1 Anonimização

Para Machado (2019, p. 12), “a abordagem mais promissora para solucionar o problema da preservação de privacidade consiste em anonimizar os dados antes de sua liberação para uso, visando impedir a exposição de dados sensíveis dos indivíduos”. O termo anonimização vem do adjetivo “anônimo”, referindo-se à possibilidade de um indivíduo não ser identificado em um grupo de indivíduos.

Segundo Pinho (2017, p. 29), a anonimização pode ser entendida como “um processo de eliminação ou modificação da informação pessoal existente numa base de dados, com o objetivo de dificultar ou impedir a identificação unívoca dos indivíduos.” O autor explica ainda que a aplicabilidade das diversas técnicas que compõem a anonimização devem ser analisadas de acordo com cada contexto e objetivos a serem alcançados.

O conceito de anonimização inclui diversas outras técnicas como a pseudonimização, a randomização e a generalização. Importa ressaltar que algumas técnicas não impedem por completo a identificação do indivíduo e outras podem ser irreversíveis. Como enfatiza Machado (2019, p.14):

> Uma vez anonimizado os dados, através de técnicas de generalização, supressão ou perturbação, é possível permitir o compartilhamento de informações com outras entidades, as quais poderão utilizá-las para diversas finalidades, sem que haja violação de privacidade. Todavia, a modificação dos dados originais no processo de anonimização causa perda de utilidade dos mesmos. Portanto, é necessário encontrar um equilíbrio entre a proteção desejada e a utilidade dos dados, a fim de se permitir operações de agregação ou mesmo análise dos dados.

Desta forma, percebe-se que a anonimização é uma saída atual e viável para as organizações que desejam tratar dados sem correr o risco de uma violação à privacidade. Entretanto, é necessário que se analise o contexto de cada organização a fim de optar pela melhor técnica de anonimização que não inviabilize o exercício das atividades empresariais.

2.3.2.1.1 Pseudonimização

É uma técnica que consiste em mascarar ou substituir os dados pessoais por pseudônimos que podem ser letras, palavras ou códigos gerados artificialmente e aleatoriamente. A pseudonimização é reversível, o que significa que é possível voltar a identificar o indivíduo, como esclarece Pinho (2017, p. 32):

> Caso se pretenda re-identificar o indivíduo associado a um conjunto de dados, será necessário consultar previamente uma tabela de mapeamento, armazenada separadamente. Essa tabela terá de estar sujeita a apertadas medidas de segurança, de forma a assegurar que não é acedida nem partilhada com entidades não autorizadas.

Significa dizer que, se a organização tiver interesse em pseudonimizar os dados, ela deverá providenciar documento com informação adicional que deverá ser armazenado separadamente em ambiente seguro e controlado.

Dentre as técnicas de pseudonimização mais conhecidas está a encriptação ou criptografia. Segundo Branco Júnior (2014, p.8), a técnica de encriptação “utiliza esquemas criptográficos normalmente baseados em chave pública ou chave simétrica para substituir dados sensíveis (identificadores, semiidentificadores e atributos sensíveis) por dados encriptados”.

Por meio da encriptação, os dados são codificados, ou seja, recebem um código único, de forma que apenas quem possui a chave que desvenda, ou desencripta esse código pode ter acesso aos dados.

2.3.2.1.2 Randomização

A randomização, ou aleatorização, é uma técnica que consiste na introdução de fatores de incerteza entre os dados a fim de mascará-los e diminuir a possibilidade de se relacionarem a seus titulares. Esses fatores de incerteza podem ser de diversos tipos e são selecionados aleatoriamente.

A técnica já é consolidada e amplamente utilizada em pesquisas científicas na área da saúde, com a finalidade de aumentar a validade de ensaios clínicos que avaliam os efeitos causais das intervenções medicinais. Agora, essa mesma técnica vem ganhando utilização na área da proteção de dados.

Exemplo de técnica de randomização utilizada por empresas como Google[9], a denominada “adição de ruído”, adiciona variações a valores numéricos e datas, possibilitando que o valor verdadeiro seja ocultado (PINHO, 2017).

A técnica também é conhecida como “perturbação”, isto porque, os fatores de incerteza adicionados podem fazer com que a informação se torne sem sentido para os usuários. Segundo Brito (2017, p. 107):

> Ao contrário das técnicas de generalização e supressão, que preservam a veracidade dos dados, a perturbação resulta em um conjunto de dados com valores sintéticos. Muitas vezes isso acarreta em informações sem sentido para aqueles que irão utilizá-las.

Essa técnica é reversível e segundo Pinho (2017, p.34) “isoladamente, não reduz a singularidade de cada registo, embora permita minimizar o sucesso de um eventual ataque”.

2.3.2.1.3 Generalização

A generalização consiste na supressão de parte dos dados ou na substituição de alguns dados por outros mais genéricos, reduzindo sua precisão. Essa técnica também é utilizada pelo Google para proteção dos dados pessoais de seus usuários.

A empresa utiliza essa técnica para agrupar indivíduos em uma determinada categoria, sem identificá-los. Por exemplo, indivíduos que possuem o mesmo código postal fazem parte de um mesmo grupo, que pode ser identificado pelo código, porém, não é possível identificar, individualmente, cada usuário pertencente ao grupo.

Essa técnica não possibilita a re-identificação do indivíduo, por isso é bem aceita entre as técnicas de anonimização de dados. Porém, há que se ter cautela na prática dessa técnica, isto porque, no caso de prática imprudente, é possível que se perca a utilidade dos dados, como lembra Brito (2017, p. 104):

> Operações de generalização aplicadas de maneira ingênua sobre atributos semiidentificadores podem não gerar dados úteis para eventuais análises. Por esse motivo, é necessário encontrar uma generalização mínima, isto é, o conjunto mínimo necessário de alterações que devem ser aplicadas a um conjunto de dados, com o objetivo de manter sua utilidade e ao mesmo tempo atender aos requisitos de privacidade estabelecidos.

---

[9] GOOGLE. **Google Privacidade & Termos**: como o google anonimiza os dados. 2020. Disponível em: https://policies.google.com/technologies/anonymization?hl=pt-BR. Acesso em: 20 out. 2020.

Desta forma, deve haver um equilíbrio na generalização dos dados, para que se alcance a proteção desejada sem perder a utilidade e impossibilitar até mesmo a análise dos dados.

2.4 Lei Geral de Proteção de Dados Pessoais

De autoria do deputado Milton Monti, do Partido da República de São Paulo (PR-SP), o Projeto de Lei (PL) nº 4060/12 foi apresentado ao Plenário da Câmara dos Deputados, no ano de 2012, como proposta para criação de uma nova lei baseada em direitos e garantias fundamentais, com a finalidade de proteger os direitos fundamentais de liberdade e privacidade, estabelecendo regras para o tratamento dos dados pessoais dos indivíduos. Após seis anos de espera, finalmente foi sancionada a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/18), no dia 14 de agosto de 2018.

Inicialmente, a lei foi sancionada com a *vacatio legis* de dezoito meses, entrando em vigor em fevereiro de 2020. Entretanto, com a revogação do artigo 65, dada pela lei nº 13.853, de 8 de julho de 2019, foi estabelecido novo prazo para que a LGPD entrasse em vigor, em agosto de 2020. Ocorre que o ano de 2020 vem sendo marcado por incertezas e preocupações, tanto para o governo, quanto para as demais entidades públicas e privadas, em decorrência da atual situação de pandemia que o mundo enfrenta. Uma Medida Provisória (959, de 29 de abril de 2020) foi editada com previsão de vigência para a lei apenas em maio de 2021, mas a MP, aprovada na Câmara e no Senado, teve o dispositivo que altera sua vigência retirado pelo Senado.

Em junho de 2020, em decorrência da pandemia do Coronavírus, foi sancionada a lei 14.010 que trata de diversos assuntos emergenciais, entre eles, a previsão para a vigência das sanções prescritas na LGPD, que ficou mantida para agosto de 2021. Porém a LGPD já está em vigor, desde o dia 18 de setembro de 2020.

A LGPD foi fortemente inspirada no Regulamento Geral sobre a Proteção de Dados (*General Data Protection Regulation*, GDPR) da União Europeia, que entrou em vigor em maio de 2018. E, assim como o GDPR, a LGPD promete quebrar paradigmas no que tange à gestão de dados e informações, alertando para a construção de uma nova cultura de tratamento e proteção de dados no Brasil.

A lei tem como princípios fundamentais o respeito à privacidade, a autodeterminação informativa, a liberdade de informação, a inviolabilidade da intimidade, a defesa do consumidor, o desenvolvimento econômico, tecnológico e a inovação. Além desses, o artigo 6º da norma estabelece ainda 10 princípios específicos que orientam as organizações na aplicabilidade de medidas técnicas e administrativas, são eles: princípio da finalidade, da adequação, da necessidade, do livre acesso, da qualidade dos dados, da transparência, da segurança, da prevenção, da não discriminação, da responsabilização e prestação de contas.

Com base nesses princípios, a norma pretende tutelar os dados pessoais de pessoas naturais, realizando mudanças significativas na forma como, hoje, as organizações lidam com esses dados, e já é possível perceber pequenas alterações nas práticas empresariais no sentido de adequação à nova lei.

O artigo 1º da lei introduz que:

> 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)

A lei define como dado pessoal, qualquer “informação relacionada à pessoa natural identificada ou identificável”. Na prática, pode-se entender como dado pessoal: nomes, apelidos, endereço residencial, endereço eletrônico, números de cartões de identificação, endereços de IP, dados de geolocalização, testemunhos de conexão (*cookies*), dados hospitalares, etc. E define como tratamento:

> Toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração. (BRASIL, 2018)

Significa dizer que qualquer operação de tratamento de dados que identifique, ou possa vir a identificar um indivíduo, realizada por pessoa natural ou empresa, com fins econômicos, está sujeita à aplicação da lei.

Com isto, a lei devolve aos indivíduos a titularidade real dos seus dados, partindo do pressuposto de que os dados pertencem unicamente aos seus titulares, ainda que organizações tenham o consentimento para sua utilização. (MENDES, 2019).

Essa determinação informacional, ou seja, essa titularidade real dos dados e a necessidade de consentimento para utilização por terceiros, já foi estudada por autores como Bioni (2016, p. 02), que explica que:

> Historicamente, a proteção dos dados pessoais tem sido compreendida como o direito do indivíduo autodeterminar as suas informações pessoais – *autodeterminação informacional*. Recorre-se, por isso, à técnica legislativa de erigir o consentimento do titular dos dados pessoais como seu pilar normativo. Por meio do consentimento, o cidadão emitiria autorizações sobre o fluxo de seus dados pessoais, controlando-os.

Administrativamente, políticas internas, políticas de privacidade e termos de uso deverão ser revistos e reestruturados. Deverão ser realizadas análises do ativo informacional e dos processos e procedimentos de tratamento de dados que já ocorrem nas organizações.

Tecnicamente, outras medidas deverão ser adotadas para que as organizações possam se adequar à lei, como a implantação de sistemas de segurança da informação que assegurem aos indivíduos o total controle de seus dados, disponibilizando mecanismos que possibilitem o seu amplo acesso, porém, com as garantias imprescindíveis de segurança. Para tal, devem ser observados os princípios da segurança da informação e devem ser utilizadas as medidas técnicas adequadas a cada contexto.

Organizações que não se adequarem estarão sujeitas às sanções previstas na lei. Embora o valor pecuniário da multa por descumprimento não seja de substancial relevância (até 2% do faturamento do último exercício, e limitada a cinquenta milhões de reais), as organizações podem sofrer outros tipos de penalidades, como a divulgação da infração, o bloqueio e até a eliminação definitiva dos dados, além da suspensão ou proibição parcial ou total das atividades relacionadas ao tratamento dos dados. Para certas organizações de determinados ramos de negócios, as medidas punitivas não pecuniárias podem afetar muito mais o seu funcionamento do que a própria pena de multa.

3 METODOLOGIA

Segundo Santos (2006, p. 25), as pesquisas científicas podem ser caracterizadas “segundo os objetivos, segundo as fontes utilizadas na coleta de dados ou, ainda, segundo os procedimentos de coleta.” Desta forma, segundo os

objetivos, a presente pesquisa pode ser caracterizada como exploratória, visto que intenciona realizar uma primeira aproximação com o tema a fim de se criar maior entendimento sobre a nova lei nacional de proteção de dados pessoais.

Segundo as fontes utilizadas na coleta de dados, a pesquisa utiliza a bibliografia a respeito do assunto como principal fonte de informação, fazendo uso de livros e artigos publicados na área da Ciência da Informação, bem como de conteúdo escrito eletronicamente e relatórios de palestras, cursos e seminários relacionados à lei. Também usa levantamento documental acerca da LGPD e outras legislações pertinentes. E, finalmente, segundo os procedimentos de coleta, a pesquisa pode ser caracterizada como bibliográfica.

O trabalho observa o contexto atual da informação e sua imprescindibilidade para o exercício das atividades das organizações e o relaciona com as mais atuais práticas de segurança da informação e governança de dados indicadas pela nova legislação pátria de proteção de dados.

Para tal, realiza pesquisas acerca do uso contemporâneo da informação e apresenta os conceitos básicos de ciência da informação, gestão da informação, governança de dados e segurança da informação. Analisa as orientações da Lei Geral de Proteção de Dados Pessoais para tratamento dos dados nas organizações e procura relacioná-las aos princípios da Segurança da Informação e às principais medidas técnicas da área para a proteção de dados e informações e às práticas de governança de dados.

A pesquisa adota abordagem qualitativa que visa compreender o fenômeno objeto de estudo com base em suas motivações, propósitos e aplicabilidade e, com isso, desenvolver ideias e incentivar trabalhos posteriores.

Para alcançar os objetivos propostos e responder à pergunta de pesquisa, o presente trabalho, inicialmente, realiza pesquisas, em veículos de comunicação digitais acerca do uso contemporâneo da informação e dos dados na nova era da informação e dos impactos desse uso na vida dos indivíduos. Para realizar tal pesquisa, utiliza as palavras-chave “comércio de dados”, “venda de dados”, “importância dos dados”, “compartilhamento de dados”, “era da informação”, “revolução da informação”, entre outras.

Posteriormente, analisa, por meio da leitura de artigos científicos pesquisados em plataformas como SciElo, o papel da ciência da informação, da segurança da informação e da governança de dados na garantia do tratamento adequado da

informação e dos dados. Para realizar a análise utiliza as seguintes palavras-chave na plataforma de busca: “governança de dados e proteção de dados”, “segurança da informação e LGPD”, “LGPD nas empresas”, entre outras.

E, por fim, com uma análise da lei, verifica alguns principais artigos que se aplicam à segurança da informação e à governança de dados, evidenciando a relação entre essas áreas e a lei, e apontando as principais mudanças que deverão ocorrer nas organizações, com adoção de novas práticas e medidas técnicas e administrativas para adequação à lei.

4 ANÁLISE E DISCUSSÃO DOS RESULTADOS

4.1 Principais implicações da LGPD no âmbito da Segurança da Informação nas Organizações

Sendo a informação e os dados os ativos dessa nova era, é necessário que sejam adotadas boas práticas de governança de dados e medidas técnicas de segurança a fim de garantir a observância dos princípios e regras para gestão dos dados, minimizando os riscos de incidentes informacionais.

Desta forma, é possível correlacionar a segurança da informação, a governança de dados e a LGPD indicando as principais mudanças que a lei estabelece e quais podem ser os primeiros passos das organizações rumo a adequação no tratamento dos dados e informações.

Para tal, as subseções seguintes são destinadas a detalhar as quatro práticas essenciais de governança de dados que as organizações deverão realizar e relacioná-las com a segurança da informação e com a LGPD.

4.1.1 Identificação e tipificação dos dados

A primeira medida que uma organização pode adotar para começar a se adequar à LGPD é identificar e tipificar os dados de terceiros utilizados na realização de suas atividades. Ela pode fazer isso analisando seu banco de dados, com o auxílio de ferramentas de análises de dados que podem variar desde o conhecido *Excel* até linguagens de programação como R e *Python*.

Com a leitura do artigo 5º, incisos I, II, III e IV da lei, as organizações podem, facilmente, retirar conceitos relativos aos dados pessoais, dados pessoais sensíveis, dados anonimizados, banco de dados, entre outros. Segundo a norma:

> Para fins desta Lei, considera-se: I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável; 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; 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; e IV - banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico. (BRASIL, 2018)

Desta forma, sob a perspectiva da governança de dados, a lei auxilia as organizações tentando minimizar possíveis dúvidas ou divergências com relação a tais conceitos. É interessante que as organizações realizem um inventário de todos os dados e informações que dispõem.

Ao passo que as organizações devem identificar os dados que utilizam, em alguns casos, pode existir a necessidade e a obrigatoriedade de se realizar a prática contrária, ou seja, anonimizar esses dados. A anonimização dos dados possibilita que um dado, que originariamente identifica um indivíduo, seja tratado por meio de técnicas que o descaracterizam, removendo ou modificando informações, e fazendo com que deixem de identificar o indivíduo.

Desta forma, no que tange à segurança da informação, além da observância dos princípios, existem ainda algumas medidas técnicas de anonimização que podem e devem ser utilizadas pelas organizações, de acordo com a cada necessidade e contexto.

4.1.2 Acompanhamento do ciclo de vida dos dados

Acompanhar o ciclo de vida dos dados em uma empresa não é tarefa simples. Isto porque os dados possuem fases e utilidades diferentes e, por isso, percorrem diversos e inúmeros setores dentro de uma organização. Existem os dados estratégicos, utilizados, geralmente, com embasamento na análise de outros dados, com a finalidade de auxiliar nas tomadas de decisões; os dados operacionais, que são produzidos naturalmente dentro das organizações pelos próprios colaboradores

a partir das atividades que realizam; os dados pessoais de colaboradores, que ficam armazenados em setor específico da organização; e existem os dados dos clientes, que são coletados e armazenados por diversas finalidades, que incluem a realização do atendimento ao consumidor e a análise de estudos comportamentais.

O ciclo de vida dos dados corresponde às fases de coleta, retenção, tratamento, distribuição e eliminação dos dados (ENAP, 2019). Conhecer as fases do ciclo de vida é essencial para o mapeamento do ciclo informacional na organização, ou seja, para compreender cada caminho percorrido por ele. Para Aganette (2018, p.6):

> O fluxo informacional ocorre dentro de um ambiente organizacional, no qual transitam dados e informações para gerar conhecimento, e auxiliar seus indivíduos a realizarem suas atividades e tarefas e efetuarem suas ações, dentre elas a tomada de decisão.

Administrativamente, identificar, tipificar e acompanhar o ciclo de vida de cada um desses dados é essencial para as organizações, pois desta forma é possível adotar medidas técnicas de segurança desses dados. Existem diversas ferramentas de gestão de processos capazes de auxiliar no mapeamento de fluxos informacionais, como o *Business Process Management* (BPM), por exemplo. Conhecendo e mapeando o caminho percorrido pelos dados e pela informação dentro da organização é possível saber por quais setores passam e quais colaboradores têm acesso a eles, e porquê e para quê. Desta forma, é possível limitar o acesso a alguns tipos de dados e informações apenas a colaboradores habilitados.

Na área da Segurança da Informação, o princípio da confidencialidade indica que apenas pessoas autorizadas tenham acesso a determinados dados, e a LGPD, simetricamente, em seu artigo 5º, incisos VI e VII traz as figuras do controlador como “pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;” e do operador como “pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador” (BRASIL, 2018).

Assim, fica evidente a necessidade de se limitar o acesso aos dados e informações de forma a protegê-los de incidentes informacionais.

4.1.3 Análise de medidas técnicas e administrativas

Diversas medidas técnicas podem e devem ser adotadas para que as organizações realizem suas atividades em conformidade com a LGPD. Com a verificação das etapas anteriores, ou seja, com o conhecimento da natureza dos dados utilizados na organização e o seu mapeamento, é possível efetivar uma gestão desses dados, que inclui gerir o consentimento e os requerimentos dos titulares, os marcos de início e término do tratamento dos dados, as finalidades dos dados para a organização, e elaborar formas de acesso aos titulares.

A gestão dessas informações é previsto pela LGPD em seu artigo 7º, inciso I que esclarece que “o tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: I - mediante o fornecimento de consentimento pelo titular” (BRASIL, 2018). E ainda, em seu artigo 9º, incisos I a VI:

> O titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca de, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso: I - finalidade específica do tratamento; II - forma e duração do tratamento, observados os segredos comercial e industrial; III - identificação do controlador; IV - informações de contato do controlador; V - informações acerca do uso compartilhado de dados pelo controlador e a finalidade; VI - responsabilidades dos agentes que realizarão o tratamento. (BRASIL, 2018)

Possivelmente, as maiores dificuldades das organizações seja garantir o acesso facilitado aos titulares dos dados e a total transparência acerca da utilização de seus dados. Essas dificuldades serão minimizadas quando as organizações passarem a incorporar, previamente, metodologias de proteção de dados e proteção à privacidade dos indivíduos titulares.

Dentre essas metodologias está o *privacy by design,* que é um conjunto de princípios que orientam as organizações na adoção de mecanismos de proteção à privacidade desde a concepção dos projetos, pensando no titular e oferecendo a ele possibilidades de total controle sobre seus dados. O termo surgiu na década de 1990, como uma ideia proposta pela Dra. Ann Cavoukian, do Instituto de Privacidade e Big Data da Universidade de Ryerson, em Ontário, no Canadá. O estudo traz sete princípios que devem ser seguidos pelas organizações em todas as etapas, principalmente na etapa de planejamento, visto que o conceito de “privacidade em primeiro lugar” deve ser seguido desde a concepção dos projetos. (CAVOUKIAN, 2001).

A própria LGPD traz a previsão da aplicação do *privacy by design*, em seu artigo 46, § 2º quando trata das medidas de segurança, técnicas e administrativas que devem ser adotadas pelos agentes de tratamento de dados: “as medidas de que trata o caput deste artigo deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução”. (BRASIL, 2018).

No que se refere à Segurança da Informação, o princípio da disponibilidade também orienta que as informações estejam sempre disponíveis a quem dela necessite. Além disso, a norma específica estabelece que “a responsabilidade pelo manuseio da informação de identificação pessoal e a garantia da conscientização sobre os princípios da privacidade, sejam tratadas de acordo com as regulamentações e legislações pertinentes”. (ABNT, 2013).

Para ratificar a relação entre a segurança da informação e a governança de dados, a LGPD estabelece, no Capítulo VII diversas práticas em segurança e governança. O artigo 46 elucida que:

> Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito. (BRASIL, 2018)

Percebe-se que a lei menciona não apenas medidas técnicas de segurança como também medidas administrativas, como explica melhor o artigo 50:

> Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais.” (BRASIL, 2018)

A adoção de medidas técnicas e administrativas está intimamente relacionada à revisão e adequação de políticas internas, contratos, e termos de uso e de privacidade, próximo ponto de análise que as organizações devem realizar.

4.1.4 Revisão e adequação de políticas internas, contratos e termos

Outra medida imprescindível para que as organizações se adaptem à lei é a revisão de todos os contratos, termos de uso e de privacidade e políticas internas

até então adotados. Isto porque a lei estabelece princípios próprios a serem seguidos e proíbe diversas práticas comuns, como uso de dados sem o consentimento do titular, uso de cláusulas obscuras nos contratos e termos de uso e de privacidade e o compartilhamento de dados entre organizações parceiras, entre outras.

O consentimento é uma das bases legais para a realização do tratamento dos dados pessoais e a lei descreve meticulosamente como deve ocorrer o processo. A priori, define, no artigo 5º, inciso XII, o consentimento como: “manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada.” (BRASIL, 2018).

Segundo a norma, o titular dos dados deve fornecer o consentimento, por escrito ou por outro meio, de forma que não reste qualquer dúvida em relação à manifestação de sua vontade. O consentimento deve constar em cláusulas de destaque, a fim de proporcionar maior visibilidade e clareza ao documento.

Relacionada ao consentimento está a obrigatoriedade de definição da finalidade para a qual os dados serão utilizados. As organizações deverão prever todas as possíveis finalidades de uso desses dados, já que as autorizações genéricas estão proibidas pela lei. “Às empresas cabe à disponibilização do máximo de informações possíveis sobre quais dados serão utilizados, além de como, por quanto tempo, por quem e porque eles serão utilizados.” (MENDES, 2019). Uma vez determinada a finalidade e adquirido o consentimento específico do titular, toda e qualquer mudança posterior implicará em novo consentimento.

Os titulares têm o direito de revogar sua autorização a qualquer tempo, bem como ainda pedir o acesso, a correção, a complementação e até mesmo a eliminação de seus dados das bases de dados das organizações. “O intuito da lei é proteger o cidadão do uso abusivo e indiscriminado de seus dados. Já que as organizações só poderão solicitar os dados que realmente forem necessários aos fins determinados, o cidadão poderá a qualquer momento, por exemplo, questionar a exigência significativa de determinados dados.” (MENDES, 2019).

No que se refere à eliminação dos dados, a lei a define como: “exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado.” (BRASIL, 2018). Tal prática remete a um direito longínquo mas que, atualmente, vem sendo discutido em todo mundo devido à facilidade com a qual as organizações coletam e utilizam os dados

pessoais dos indivíduos. O remoto direito de ser esquecido, mencionado no famoso artigo jurídico "*The Right to Privacy*", de Samuel Warren e Louis Brandeis, emergiu no ano de 2014 com uma nova concepção: o direito de ter dados pessoais retirados de mecanismos de buscas. A decisão foi da Corte Europeia de Justiça, que condenou a empresa norte americana Google a eliminar dados de seus usuários.

Acerca dos princípios, no artigo 6º, a lei descreve 10 deles que devem ser seguidos pelas organizações:

> As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades; II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento; III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados; IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais; V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento; VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial; VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão; VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais; IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos; X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas. (BRASIL, 2018).

Significa dizer que as organizações deverão reestruturar suas políticas internas, criando novas regras e procedimentos para o tratamento dos dados. Deverão rever também os contratos firmados entre os *stakeholders*, visto que a lei estabelece que todos os envolvidos tenham ciência de suas obrigações e adotem medidas para adequação, já que em caso de incidentes, todos serão responsabilizados.

Sobre isso, o artigo 11, § 4º da lei estabelece que "é vedada a comunicação ou o uso compartilhado entre controladores de dados pessoais [...]". (BRASIL, 2018).

E o artigo 42, § 1º, inciso II prevê que “os controladores que estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados respondem solidariamente”. (BRASIL, 2018).

As organizações devem, ainda, promover ações educativas destinadas a todos os seus colaboradores, com a finalidade de fomentar o conhecimento sobre as novas políticas adotadas e talvez, sobre uma nova cultura organizacional orientada a dados. Todos devem estar cientes da necessidade de mudança e da importância da segurança no tratamento dos dados e informação.

A norma que rege a segurança da informação também prevê essa prática quando orienta que “convém que estas políticas sejam comunicadas aos funcionários e partes externas relevantes de forma que sejam entendidas, acessíveis e relevantes aos usuários pertinentes [...]”. (ABNT, 2013)

Sob o aspecto da SI, a norma referência na área estabelece que as organizações identifiquem três principais requisitos para a segurança da informação: avaliar os riscos analisando os objetivos e as estratégias globais do negócio; considerar legislações vigentes e o ambiente sociocultural; e analisar os princípios próprios da organização no que tange ao manuseio, processamento, armazenamento e comunicação da informação. (ABNT, 2013).

Além das orientações para revisão e reestruturação de políticas internas, termos de uso e de privacidade e contratos firmados, a Lei Geral de Proteção de Dados Pessoais traz consigo uma inovação: a indicação de profissionais específicos para o tratamento dos dados nas organizações. Os agentes de tratamento de dados pessoais, denominados pela lei como operador e controlador, que são os profissionais responsáveis, respectivamente, por realizar o tratamento dos dados, e por tomar as decisões referentes ao tratamento. Além do operador e do controlador, a lei ainda traz a figura do encarregado, que é o profissional responsável por servir como um canal de comunicação, uma ponte entre a organização, o titular dos dados e a agência fiscalizadora.

Sobre esse aspecto, a Segurança da Informação prevê que as organizações, em suas políticas de segurança da informação, declarem, entre outras, “atribuição de responsabilidades, gerais e específicas, para o gerenciamento da segurança da informação para os papéis definidos” e que “as pessoas indicadas sejam competentes e capazes de cumprir com as responsabilidades pela segurança da

informação e a elas seja dada a oportunidade de manter-se atualizada com os desenvolvimentos". (ABNT, 2013).

Significa dizer que as organizações deverão também preparar seus quadros para a capacitação ou contratação de uma nova categoria de profissionais habilitados e capacitados para realizar legalmente o tratamento dos dados. No âmbito da gestão da informação, os profissionais gestores de informação têm habilidades multidisciplinares e são habilitados a exercer a tarefa de *Data Protection Officer* (DPO) mencionado no GDPR. Essa categoria de profissionais é capacitada para lidar com os dados em todo seu ciclo de vida e para implementar os projetos de adequação das organizações à LGPD.

5 CONSIDERAÇÕES FINAIS

Há tempos a informação é reconhecida como importante ativo pela Ciência da Informação e por outras áreas do conhecimento, mas a internet e as demais inovações tecnológicas promoveu uma nova era que o mundo reconheceu a relevância deste recurso e, em especial, no contexto organizacional.

Estamos vivendo a era da informação. Os dados e a informação ganharam papel de destaque como principais insumos desta nova era. Foram reconhecidas as diversas utilidades para as organizações, como servir de embasamento para tomada de decisões estratégicas, aumento da produtividade e da competitividade, redução de custos, embasamento para campanhas de publicidade e marketing, prospecção de negócios e investimentos, construções de alianças e parcerias, entre outras.

Com o reconhecimento dessa importância veio também a percepção da necessidade de proteção desse insumo vital para as organizações. Atualmente, as empresas detém imenso volume de dados e informações, isso é imprescindível para um bom funcionamento dos negócios, por isso a extrema necessidade de conhecê-los e protegê-los.

Importa ressaltar que os dados e informações não podem ser vistos unicamente sob um ponto de vista, o das organizações. Existe uma grande parte de dados que circulam em uma organização que não são de sua titularidade, são dados pessoais que pertencem a cada um de nós, cidadãos, indivíduos, consumidores de produtos e serviços oferecidos pelas organizações.

Desta forma, além da cautela no tratamento de dados sob uma perspectiva estratégica para as organizações, há que se ter prudência também sob o prisma da proteção à privacidade e respeito à titularidade real desses dados e informações.

Com o surgimento da Lei Geral de Proteção de Dados Pessoais, práticas que antes eram consideradas, de certa forma opcionais, embora essenciais, como solicitar o consentimento do titular e utilizar métodos de anonimização de dados a fim de respeitar sua privacidade, passaram a ser práticas obrigatórias para o funcionamento de toda e qualquer empresa que atue em território nacional.

Isto porque a lei visa não apenas regular e fiscalizar o uso de dados e informações pessoais dos indivíduos, protegendo-os de incidentes informacionais e do uso incauto, abusivo e indiscriminado. Ela visa, principalmente, uma verdadeira mudança cultural no que diz respeito ao tratamento de dados pessoais no Brasil. Essa mudança cultural é benéfica para todos. Ela traz vantagens tanto para as organizações, visto que regula e fiscaliza sem inviabilizar a análise dos dados, quanto para os indivíduos, devido ao alto nível de proteção que estabelece.

A lei auxilia as organizações ao trazer diversos conceitos importantes como os conceitos de dados pessoais, tratamento de dados, dados anonimizados, consentimento, agentes de tratamento de dados, entre outros, a fim de se evitar possíveis equívocos.

A LGPD estabelece uma série de exigências relacionadas às boas práticas de governança de dados e segurança da informação, as quais as organizações devem cumprir, como conhecer o seu ativo informacional, adotar medidas técnicas de proteção desse ativo, revisar políticas, contratos e termos e adequar seu quadro profissional para as atividades de novos colaboradores com conhecimentos, habilidades e responsabilidades específicas.

Ao passo que as organizações conhecem seu ativo informacional, podem ou devem utilizar técnicas que os descaracterizem, como uma ou mais técnicas de anonimização de dados. Independentemente de utilizar medidas técnicas de anonimização, toda organização deve seguir os princípios de confidencialidade, integridade e disponibilidade dos dados e informações.

Retomando a pergunta desta pesquisa, identificou-se os principais aspectos da área de governança de dados que se relacionam com a LGPD, no sentido de apontar as melhores práticas para identificação e tipificação dos dados, acompanhamento de fluxo informacional, análise de medidas técnicas, e criação,

revisão e adequação de políticas internas, contratos e termos de uso e de privacidade.

O trabalho apresentou ainda, os principais aspectos da área de segurança da informação que se relacionam com a LGPD, apontando os princípios universais e as medidas técnicas de proteção à informação, como a anonimização, por exemplo, que devem ser analisados e aplicados conforme os contextos nos quais as organizações se encontram.

A própria legislação criou um vínculo entre a segurança da informação e a governança de dados, e ambas as áreas têm se preocupado em realizar análises do conjunto informacional e buscar o equilíbrio entre a proteção e a utilidade desse elemento para as organizações.

O objetivo geral deste trabalho foi alcançado plenamente, visto que conseguiu-se identificar os principais aspectos que inter-relacionam a segurança da informação, a governança de dados e a LGPD, como explicitados no capítulo de análise.

Certamente este trabalho não esgota o assunto, de forma que outras pesquisas podem e devem ser realizadas a fim de compreender melhor as profundas mudanças que a LGPD promove tanto nas organizações como na vida de cada indivíduo.

REFERÊNCIAS

AGANETTE, Elisângela Cristina. BPM Acadêmico: Mapeamento de Processos e de Fluxos Informacionais na ECI/UFMG. **Pesquisa Brasileira em Ciência da Informação e Biblioteconomia**. João Pessoa, v. 13, n. 1, p. 44-65, 2018.

ARAÚJO, Carlos Alberto Ávila. O que é Ciência da Informação? **Revista Informação & Informação**. V. 19. N. 1. P. 01-30. Londrina: Jan./Abr. 2014.

ARAÚJO, Carlos Alberto Ávila. Fundamentos da Ciência da Informação: correntes teóricas e o conceito de informação. **Perspectivas em Gestão & Conhecimento**. V. 4. N. 1. P. 57-79. João Pessoa: Jan/Jun. 2014.

ASSIS, Wilson Martins de. **Gestão da informação nas organizações:** como analisar e transformar em conhecimento informações captadas no ambiente de negócios. Belo Horizonte: Autêntica, 2008. 182 p.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR ISO/IEC 27002:2013: **Tecnologia da informação - Técnicas de segurança - Código de prática para controles da segurança da informação**. 2a. ed. Rio de Janeiro, 2013.

BARATA, André Montoia. **Governança de dados em organizações brasileiras**: uma avaliação comparativa entre os benefícios previstos na literatura e os obtidos pelas organizações. 2015. Dissertação (Mestrado em Sistemas de Informação) - Escola de Artes, Ciências e Humanidades, University of São Paulo, São Paulo, 2015. doi:10.11606/D.100.2015.tde-28072015-215618. Acesso em: 27 out. 2020.

BARBIERI, Carlos.**Governança de Dados:** Práticas, Conceitos e Novos Caminhos. Rio de Janeiro: Alta Books, 2020.

BCN, Biblioteca del Congreso Nacional de Chile /. **LEY 19628 SOBRE PROTECCION DE LA VIDA PRIVADA**. 1999. Disponível em: https://www.bcn.cl/leychile/navegar?idNorma=141599. Acesso em: 05 dez. 2020.

BIONI, Bruno Ricardo. **Autodeterminação informacional: Paradigmas inconclusos entre a tutela dos direitos da personalidade, a regulação dos bancos de dados eletrônicos e a arquitetura da internet**. 2016. Disponível em: <https://www.researchgate.net/publication/328266211_Autodeterminacao_informacional_paradigmas_inconclusos_entre_a_tutela_dos_direitos_da_personalidade_a_regulacao_dos_bancos_de_dados_eletronicos_e_a_arquitetura_da_internet>. Acesso em: 25 jun. 2019.

BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil**: promulgada em 5 de outubro de 1988. Vademecum Compacto. 30ª Ed. São Paulo: Saraiva, 2020.

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). Brasília, BSB, 14 ago. 2018.

BRASÍLIA. Ministério Público do Distrito Federal e Territórios. Secretaria de Comunicação. **MPDFT recomenda providências à Netshoes após vazamento de quase 2 milhões de dados de clientes**. 2018. Disponível em: <http://www.mpdft.mp.br/portal/index.php/comunicacao-menu/noticias/noticias-2018/9775-mpdft-recomenda-providencias-a-netshoes-apos-vazamento-de-quase-2-milhoes-de-dados-de-clientes>. Acesso em: 20 abr. 2019.

BRITO, Felipe T.. **Preservação de Privacidade de Dados: Fundamentos, Técnicas e Aplicações**. Jornadas de Atualização em Informática, 2017. 40 p. Disponível em: https://www.researchgate.net/profile/Felipe_Brito8/publication/318726149_Preservacao_de_Privacidade_de_Dados_Fundamentos_Tecnicas_e_Aplicacoes/links/597a3540a6fdcc61bb05b98a/Preservacao-de-Privacidade-de-Dados-Fundamentos-Tecnicas-e-Aplicacoes.pdf. Acesso em: 20 out. 2020.

CAVOUKIAN, Ann. **Privacy by Design: the 7 foundational principles**. Ipc.On.Ca, Ontario: 2011.

CELE. Centro de Estudios En Libertad de Expresión y Acceso a La Información. **Perú Ley N°29.733 (Ley de Protección de Datos Personales)**. 2011. Disponível em: https://observatoriolegislativocele.com/ley-29733/. Acesso em: 05 dez. 2020.

CELE. Centro de Estudios En Libertad de Expresión y Acceso a La Información**. Lei No. 25.326 Dados Pessoais**. 2000. Disponível em: https://observatoriolegislativocele.com/pt/dados-pessoais/. Acesso em: 05 out. 2020.

COSTA, Sely Maria de Souza. Impactos sociais das tecnologias de informação. **Revista de Biblioteconomia de Brasília**, Brasília, v. 19, n. 1, p. 3-22, jan./jun. 1995. Disponível em: <http://www.brapci.ufpr.br/documento.php?dd0=0000002457&dd1=d216e>. Acesso em: 20 de abr de 2019.

DAVENPORT, Thomas H; PRUSAK, Laurence. **Ecologia da informação: por que só a tecnologia não basta para o sucesso na era da informação.** Tradução Bernadette Siqueira Abrão. São Paulo : Futura, 1998.

DRUCKER, Peter. Além da Revolução da Informação. **Hsm Management**, [s.i], v. 4, n. 18, p.1-6, jan. 2000.

ENAP. Fundação Escola Nacional de Administração Pública. **Proteção de Dados Pessoais no Serviço Público:** O Ciclo de Vida dos Dados Pessoai**s**. Brasília: 2019.

ESPÍNDOLA, Priscilla Lüdtke. Governança de dados aplicada à ciência da informação: análise de um sistema de dados científicos para a área da saúde. **RDBCI: Revista Digital de Biblioteconomia e Ciência da Informaçã**o, Campinas, SP, v. 16, n. 3, p. 274-298, 2018. DOI: 10.20396/rdbci.v16i3.8651080. Disponível em: https://periodicos.sbu.unicamp.br/ojs/index.php/rdbci/article/view/8651080. Acesso em: 27 out. 2020.

EUROPEAN UNION. **Regulation nº 2016/679, de 2018**. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).General Data Protection Regulation: The GDPR: new opportunities, new obligations. European Union. Disponível em: <https://ec.europa.eu/commission/sites/beta-political/files/data-protection-factsheet-sme-obligations_en.pdf>. Acesso em: 20 abr. 2019.

FERNANDES, Jorge Henrique Cabral. Segurança da informação: nova disciplina na ciência da informação? XI ENCONTRO NACIONAL DE PESQUISA EM CIÊNCIA DA INFORMAÇÃO INOVAÇÃO E INCLUSÃO SOCIAL: QUESTÕES CONTEMPORÂNEAS DA INFORMAÇÃO. p .1-24. Rio de Janeiro: out. 2010. Disponível em: http://200.20.0.78/repositorios/handle/123456789/992. Acesso em: 18 mar. 2020.

FONTES, Eduardo. **Segurança da Informação: o usuário faz a diferença**. São Paulo: Saraiva, 2006.

GABRIEL, J.X. Dance (United States). The New York Times. **As Facebook Raised a Privacy Wall, It Carved an Opening for Tech Giants**. 2018. Disponível em: <https://www.nytimes.com/2018/12/18/technology/facebook-privacy.html>. Acesso em: 20 abr. 2019.

GOOGLE. **Google Privacidade & Termos**: como o google anonimiza os dados. 2020. Disponível em: https://policies.google.com/technologies/anonymization?hl=pt-BR. Acesso em: 20 out. 2020.

LYRA, Maurício Rocha *et al* (org.). **Governança da Segurança da Informação**: classificação dos ativos da informação. Brasília: 2015. 173 p.

MACHADO, Javam C.. Técnicas de Privacidade de Dados de Localização. 34TH BRAZILIAN SYMPOSIUM ON DATABASES: TÓPICOS EM GERENCIAMENTO DE DADOS E INFORMAÇÕES, Fortaleza, v. 1, n. 1, p. 3-123, out. 2019.

MACHADO, Felipe Nery Rodrigues. **Segurança da informação:** princípios e controle de ameaças. 1ªed. São Paulo: Érica, 2014.

MARCIANO, João Luiz Pereira. **Segurança da Informação**: uma abordagem social. 2006. 212 f. Tese (Doutorado) - Departamento de Ciência da Informação, Universidade de Brasília, Brasília, 2006. Disponível em: https://repositorio.unb.br/handle/10482/1943. Acesso em: 20 out. 2020.

MATTHEW, Rosenberg (United States). The New York Times. **How Trump Consultants Exploited the Facebook Data of Millions.** 2018. Disponível em: <https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html?module=inline>. Acesso em: 20 abr. 2019.

MENDES, Michele da M. A nova lei brasileira de proteção de dados pessoais: principais implicações da Lei sob a ótica das organizações no Brasil. In: IX ENCONTRO DE ESTUDOS SOBRE CIÊNCIA, TECNOLOGIA E GESTÃO DA INFORMAÇÃO. Recife: 2019. p. 1 - 16.

NONAKA, Ikujiru; TAKEUCHI, Hirotaka. **Criação de conhecimento na empresa**: **como as empresa japonesas geram a dinâmica da inovação**. 23. ed. Rio de Janeiro: Elsevier, 1997.

PINHO, Frederico António Sá Oliveira. **Anonimização de bases de dados empresariais de acordo com a nova Regulamentação Europeia de Proteção de Dados**. 2017. 94 f. Tese (Mestrado) - Curso de Ciência de Computadores, Departamento de Ciência de Computadores, Universidade do Porto, Porto, 2017. Disponível em: https://repositorio-aberto.up.pt/bitstream/10216/105479/2/201202. Acesso em: 20 out. 2020.

QUEIROZ, Daniela Gralha de Caneda. **Ciência da Informação: história, conceitos e características**. Em Questão. V. 21. N. 3. P. 25-42. Porto Alegre: ago/dez. 2015.

SALIBA, José Carlos Maia. **O direito de ser esquecido.** 2014. Disponível em: <https://jus.com.br/artigos/31705/o-direito-de-ser-esquecido>. Acesso em: 25 jun. 2019.

SANTOS, Antonio Raimundo dos. **Metodologia Científica**: **a construção do conhecimento.** 6. ed. Dp&a. Rio de Janeiro: 2006.

SARACEVIC, Tefko. Ciência da Informação: origem, evolução e relações. **Perspectivas em Ciência da Informação**. Belo Horizonte. v. 1, n. 1, p. 41-62, jan./jun. 1996. Semestral. Disponível em: <http://portaldeperiodicos.eci.ufmg.br/index.php/pci/article/view/235/22>. Acesso em: 26/abril/2020.

SERVIÇO FEDERAL DE PROCESSAMENTO DE DADOS (Brasília). Assessoria de Imprensa. **Serpro assegura compromisso com o sigilo de dados dos cidadãos brasileiros: nota à imprensa**. 2018. Disponível em: <http://www.serpro.gov.br/menu/imprensa/notas-a-imprensa-1/nota-oficial-01-06-2018>. Acesso em: 20 abr. 2019.

SILVA, José Afonso da. **Curso de Direito Constitucional Positivo**. 33ª Ed. revista e atualizada. São Paulo: Malheiros, 2010. P. 175.