UNIVERSIDADE FEDERAL DO PARANÁ

LARISSA LOURENÇO NUNES BENCK

LGPD E SEU DESAFIO PARA AS ORGANIZAÇÕES: UM ESTUDO DEMONSTRATIVO ENTRE AS ESTRUTURAS DE DADOS (*FRAMEWORKS*) DE ADEQUAÇÃO À LEI

CURITIBA

2023

LARISSA LOURENÇO NUNES BENCK

LGPD E SEU DESAFIO PARA AS ORGANIZAÇÕES: UM ESTUDO DEMONSTRATIVO ENTRE AS ESTRUTURAS DE DADOS (*FRAMEWORKS*) DE ADEQUAÇÃO À LEI

Dissertação apresentada como requisito parcial à obtenção do grau de Mestre, no Programa de Pós-Graduação em Gestão da Informação, do Setor de Ciências Sociais Aplicadas, da Universidade Federal do Paraná. Linha de Pesquisa: Informação e Tecnologia.

Orientador: Prof. Dr. José Simão de Paula Pinto.

CURITIBA

2023

DADOS INTERNACIONAIS DE CATALOGAÇÃO NA PUBLICAÇÃO (CIP)
UNIVERSIDADE FEDERAL DO PARANÁ
SISTEMA DE BIBLIOTECAS – BIBLIOTECA DE CIÊNCIAS SOCIAIS APLICADAS

Benck, Larissa Lourenço Nunes
LGPD e seu desafio para as organizações : um estudo demonstrativo entre as estruturas de dados (frameworks) de adequação à lei / Larissa Lourenço Nunes Benck. – Curitiba, 2023.
1 recurso on-line : PDF.

Dissertação (Mestrado) – Universidade Federal do Paraná, Setor de Ciências Sociais Aplicadas, Programa de Pós-Graduação em Gestão da Informação.
Orientador: Prof. Dr. José Simão de Paula Pinto.

1. Gestão da informação. 2. Proteção de dados – Legislação – Brasil. 3. Estruturas de dados (Computação). 4. Segurança da informação. I. Pinto, José Simão de Paula. II. Universidade Federal do Paraná. Programa de Pós-Graduação em Gestão da Informação. III. Título.

Bibliotecária: Maria Lidiane Herculano Graciosa CRB-9/2008

MINISTÉRIO DA EDUCAÇÃO
SETOR DE CIÊNCIAS SOCIAIS E APLICADAS
UNIVERSIDADE FEDERAL DO PARANÁ
PRÓ-REITORIA DE PESQUISA E PÓS-GRADUAÇÃO
PROGRAMA DE PÓS-GRADUAÇÃO GESTÃO DA INFORMAÇÃO - 40001016058P1

TERMO DE APROVAÇÃO

Os membros da Banca Examinadora designada pelo Colegiado do Programa de Pós-Graduação GESTÃO DA INFORMAÇÃO da Universidade Federal do Paraná foram convocados para realizar a arguição da dissertação de Mestrado de **LARISSA LOURENÇO NUNES BENCK** intitulada: **LGPD E SEU DESAFIO PARA AS ORGANIZAÇÕES: UM ESTUDO DEMONSTRATIVO ENTRE AS ESTRUTURAS DE DADOS (FRAMEWORKS) DE ADEQUAÇÃO À LEI**, sob orientação do Prof. Dr. JOSÉ SIMÃO DE PAULA PINTO, que após terem inquirido a aluna e realizada a avaliação do trabalho, são de parecer pela sua APROVAÇÃO no rito de defesa.

A outorga do título de mestra está sujeita à homologação pelo colegiado, ao atendimento de todas as indicações e correções solicitadas pela banca e ao pleno atendimento das demandas regimentais do Programa de Pós-Graduação.

CURITIBA, 03 de Abril de 2023.

JOSÉ SIMÃO DE PAULA PINTO
Presidente da Banca Examinadora

CLEVERTON JULIANO ALVES VICENTINI
Avaliador Externo (INSTITUTO FEDERAL DE EDUC., CIÊNCIA E TECNOLOGIA DO PARANÁ)

MARCOS ANTÔNIO TEDESCHI
Avaliador Interno (UNIVERSIDADE FEDERAL DO PARANÁ)

DEDICO

Aos meus pais Gisela e Jocelito e aos meus avós maternos e paternos.

AGRADECIMENTOS

A Deus pela vida, bênção e proteção.

A Universidade Federal do Paraná e ao curso de Pós-Graduação de Gestão da Informação.

Ao meu orientador, Prof. Dr. José Simão de Paula Pinto, pela orientação, ensinamentos, paciência e dedicação.

Aos meus pais e irmãs e minha família pelo incentivo e paciência.

À Laura, colega de pós-graduação, agradeço pelas conversas, incentivos e compartilhamento de conhecimento.

Aos colegas (Adriana, Bryan, Laura) adquiridos durante a realização do programa, que sempre em momentos de ansiedade e insegurança estavam ali presentes com palavras de fortalecimento e confiança.

A minha noiva, Camila, pelo suporte em todo esse processo, por me ouvir e ser paciente, pela ajuda nas correções e sabedoria com as palavras.

RESUMO

A privacidade dos dados pessoais vem se tornando uma preocupação para os gestores, principalmente seu uso indevido e a exploração não autorizada, como acontece nos casos de vazamentos de dados. Assim, leis e regulamentos estão sendo criados na tentativa de garantir proteção aos direitos do cidadão. A Lei europeia de proteção de dados, GDPR (*General Data Protection Regulation*), encontra-se em vigor e incide multas elevadas na União Europeia e na Inglaterra. Seguindo a tendência mundial, a criação da Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709/2018, baseada na GDPR, entrou em vigor em setembro de 2020 e a autorização da aplicação das multas teve início em agosto de 2021, porém até o momento desta pesquisa, a Autoridade Nacional de Proteção de Dados, não iniciou esse processo. Este estudo tem como proposta descrever as diferenças e similaridades das estruturas de dados de adequação à LGPD encontrados na literatura acadêmica fundamentando-se nos conceitos inerentes à Lei e nos artigos que mais incidiram multas da GDPR, no período de agosto de 2018 e maio de 2022, essas estruturas de dados são um suporte que servem de apoio para entendimento do assunto. Como metodologia, esta pesquisa se caracteriza como bibliográfica e documental, de caráter exploratório e descritivo. Para a elaboração referencial teórico, que inclui a descrição da evolução legislativa, a LGPD e seus conceitos inerentes, foi utilizada a seguinte *string*: LGPD* OR "*General Personal Data Protection Law*" OR "*Law 13.709*", nas bases de dados *Scopus*, *Web of Science* e *Dimensions*. Para buscar as estruturas de dados de adequação à Lei na literatura foi utilizada a seguinte *string*: “LGPD” AND "*Frameworks*". Para determinar os artigos da LGPD que têm mais chances de resultar em multas foram utilizados os dados do sítio eletrônico *Enforcement Tracker*, que mapeia todas as multas de inadequações à GDPR. Em seguida, os artigos da GDPR foram lidos e relacionados aos artigos correspondentes da LGPD. Para demonstrar as diferenças e similaridades das estruturas de dados foi realizada a análise de conteúdo, utilizando como categorias os conceitos inerentes à Lei encontrados no referencial teórico, artigos da LGPD correspondentes aos artigos que mais geraram multas da GDPR e as variáveis: metodologia, validação e aplicação das estruturas de dados, resultando em sete redes. Como resultados, destacam-se os seguintes conceitos inerentes à LGPD: anonimização, termo de consentimento, privacidade, *privacy by design*, segurança da informação e governança e gestão de dados. No total, foram selecionadas quatro estruturas de dados para a descrição. Constatou-se que poderão ter mais incidência de multas os seguintes artigos da LGPD: 6º, 7º, 9º, 15, 16, 17, 18, 19, 20, 21, 22 e 46. As estruturas de dados se diferenciaram principalmente nos seguintes aspectos: conceitos da Lei abordados, os passos iniciais para o processo de adequação, o aprofundamento nos detalhes das atividades para a adequação, e uma estrutura que auxilia realizar o mapeamento dos dados pessoais.

Palavras-chave: LGPD. GDPR. Estrutura de Dados. *Enforcement Tracker*. Adequação.

ABSTRACT

The privacy of personal data has become a concern for managers, especially its misuse and unauthorized exploitation, as is the cases of leaks. Thus, laws and regulations are being created to ensure protection of citizens' rights. The European Data Protection Act, GDPR (General Data Protection Regulation), is already in force and imposes high fines in the European Union and England. Following the global trend, the creation of the General Data Protection Law (GDPL), Law nº 13.709/2018, based on GDPR, came into force in September 2020 and the authorization of fines application began in August 2021, however, until the moment of this research, the National Data Protection Authority has not started this process. This study is proposed to describe the differences and similarities of the GDPL compliance Frameworks found in the academic literature based on the concepts inherent to the Law and the application of GDPR fines, in the period between August 2018 and May 2022, these frameworks are a support that supports the subject. This research is defined as bibliographic and documental, of exploratory and descriptive nature. For the theoretical referential elaboration, which includes the description of the legislative evolution, the GDPL and its inherent concepts, the following string was used: LGPD* OR "General Personal Data Protection Law" OR "Law 13.709", in the Scopus, Web of Science and Dimensions databases. To search for the Frameworks of compliance with Law in the literature the following string was used: "LGPD" AND "Frameworks". To determine the GDPL articles that are most likely to result in fines, data from the Enforcement *T*racker website, which maps all GDPR inadequacy fines, was used by extracting and transforming them. Next, the GDPR articles were read and related to the corresponding GDPL articles. To demonstrate the differences and similarities of the Frameworks, the content analysis was performed using the concepts inherent to the Law found in the theoretical reference, the articles of the GDPL corresponding to the articles that most generated GDPR fines, and variables: methodology, validation and application of frameworks, resulting in seven networks. As a result, the following concepts inherent to the GDPL stand out: anonymization, privacy term, privacy by design, information security and data governance and management. In total, four data structures were selected for the description. It was found that the following LGPD articles may have a higher incidence of fines: 6th, 7th, 9th, 15, 16, 17, 18, 19, 20, 21, 22 and 46. The data structures differ mainly in the following aspects: concepts of the Law, the initial steps for the orientation process, the deepening in the details of the activities for the adequation, and a structure that helps to carry out the mapping of the personal data.

Keywords: GDPL. GDPR. Framework. Enforcement Tracker. Adequacy.

LISTA DE FIGURAS

LISTA DE QUADROS

LISTA DE ABREVIATURAS E SIGLAS

ANPD – Autoridade Nacional de Proteção de Dados

DPO – *Data Protection Officer*

FIP – *Fair Information Practices*

FW – *Framework*

GD – Governança de Dados

GDPR – *General Data Protection Regulation*

IP – *Internet Protocol*

LAI – Lei de Acesso à Informação

LGPD – Lei Geral de Proteção de Dados

MP – Medida Provisória

NIST – *National Institute of Standards and Technology*

OECD - *Organization for Economic Co-operation and Development*

PII – Informação Pessoalmente Identificada

PbD – *Privacy by Design*

PSI – Política de Segurança de Informação

SI – Segurança da Informação

SUMÁRIO

1 INTRODUÇÃO

Com a mudança na dinâmica econômica global, os dados pessoais tomaram posição central na vida em sociedade (DONEDA, 2021) e o avanço da tecnologia e o aumento de casos de incidentes de vazamentos de dados pessoais aumentaram a notoriedade e a importância do tratamento de dados.

A era digital gera desafios cada vez maiores na integridade da privacidade de informações pessoais, por muitos motivos, como: coleta e comercialização de listas de *marketing* com dados (telefone, endereço, e-mail), rastreamento de indivíduos, suas movimentações e observações de padrões de comportamento pessoais em sites (CHIK, 2013). A tecnologia de reconhecimento facial também é um deles, tendo em vista a grande quantidade de dados sensíveis coletados que necessita ser regulamentada para garantir mecanismos de prevenção de abusos por parte de entidades que aplicam esses sistemas (MORAES *et al*., 2021).

Diante desse cenário, Chik (2013) afirma que a informação digital contribui para o ambiente que não respeita a privacidade dos dados pessoais, pois facilita sua coleta e disseminação. Além disso, a falta de conhecimento e o mal uso da ferramenta por parte dos usuários também contribuem para aumentar esse problema, assim como a portabilidade e o crescente uso de nuvens para o armazenamento remoto de dados. Tudo isso ressalta a importância da segurança e do controle pessoal dos dados dos cidadãos.

Sabe-se também que os dados pessoais podem ser considerados informações, dotadas de significado e de valor para as organizações e para as pessoas. A informação é uma base competitiva na atual economia, porém a posse de terceiros pode representar uma ameaça (PIURCOSKI *et al*., 2019).

Assim, torna-se clara a necessidade de uma regulamentação única para o uso dos dados pessoais. Em 2016, foi publicada a Lei de proteção de dados europeia, vigente desde 2018, na Europa e Inglaterra, denominada Regulamento Geral de Proteção de Dados ou *General Data Protection Regulation*, a GDPR.

No Brasil, em 14 de agosto de 2018, foi aprovada a Lei n° 13.709, Lei Geral de Proteção de Dados Pessoais (LGPD), que cria determinações e salvaguardas em relação ao uso de dados pessoais no país. Essa Lei muda o paradigma atual de como as organizações lidam com dados pessoais de seus usuários e impacta diretamente setores públicos e privados, pois regulamenta quais dados podem ser

coletados, como devem ser processados e como devem ser utilizados, assegurando ao cidadão o controle sobre suas informações pessoais.

Lemos e Passos (2020) ressaltam que uma Lei de Proteção de Dados gera implicações econômicas e políticas internas e externas, não apenas empresas precisam se adequar, mas o Poder Público.

Assim, os profissionais e empresas enfrentam o desafio de fazer a transição dos artigos da lei e seus resultados para o dia a dia, bem como implantar um conjunto de processos que se tornarão parte do modelo padrão de processos organizacionais (Grupo Assaf, 2019).

Encontra-se na literatura acadêmica estruturas de dados que auxiliam as organizações a se organizarem, sendo um conjunto de regras ou molduras, com intuito de ampararem as ações a serem tomadas. Este estudo se propõe a demonstrar as diferenças e similaridades das estruturas de dados (*frameworks*), fundamentando-se nos conceitos inerentes à Lei e nos artigos que mais incidiram multas da GDPR, no período de agosto de 2018 e maio de 2022, com intuito de auxiliar futuras pesquisas na área e organizações que necessitem de um norteador para iniciar o processo de adequação.

1.1 PROBLEMA DE PESQUISA

Embasado no que foi apresentado anteriormente, este trabalho buscou responder ao seguinte problema de pesquisa: Quais as diferenças e similaridades das estruturas de dados (*frameworks*) de adequação à LGPD encontrados na literatura acadêmica fundamentando-se nos conceitos inerentes à Lei e nos artigos que mais incidiram multas da GDPR, no período de agosto de 2018 e maio de 2022.

1.2 OBJETIVOS DA PESQUISA

Para responder o problema de pesquisa delinearam-se os seguintes objetivos geral e específico.

1.2.1 Objetivo Geral

O objetivo geral desta pesquisa é demonstrar as diferenças e similaridades das estruturas de dados (*frameworks*) de adequação à LGPD encontrados na literatura acadêmica fundamentando-se nos conceitos inerentes à Lei e nos artigos que mais incidiram multas da GDPR, no período de agosto de 2018 e maio de 2022.

1.2.2 Objetivos específicos

Para atingir o objetivo geral, os seguintes objetivos específicos foram delineados:

a) Descrever uma breve evolução legislativa, a LGPD e seus conceitos inerentes.
b) Buscar quais são as estruturas de dados (*frameworks*) de adequação à Lei na literatura.
c) Investigar quais são os artigos da LGPD que têm mais chances de resultar em multas, baseando-se na GDPR.
d) Compreender as diferenças e similaridades das estruturas de dados (*frameworks*) selecionadas.

1.3 JUSTIFICATIVA

Iramina (2020) comenta que atualmente já são mais de cem países com marcos regulatórios para proteção de dados pessoais em todo o mundo. O site *United Nations Conference on Trade and Development*, confirma que de 194 países 137 já adotaram alguma legislação de proteção de dados (UNCTAD, 2021).

Este estudo é justificado socialmente pela relevância das organizações necessitarem se adequar à LGPD, tendo em vista o desenvolvimento da tecnologia e a intensificação dos fluxos de informação, novas possibilidades de armazenamento, utilização e manipulação de informações pessoais, refletindo em mudanças no conceito de direito à privacidade, de modo que a informação que antes era dispersa, torna-se organizada (FINKELSTEIN, 2020).

As informações pessoais estão cada vez mais expostas e vulneráveis à economia digital, pois vivemos em um mundo cada vez mais conectado, onde podemos otimizar nossas rotinas por meio de aplicativos que controlam nosso dia a

dia, como de gerenciamento financeiro, saúde e relações interpessoais, por exemplo. Diante dessa realidade muitos casos e notícias de vazamento de dados aumentaram. A ISTOEDINHEIRO (2022) divulgou que o Brasil assumiu o 6º lugar no ranking de países com mais vazamentos de dados no mundo, de janeiro a novembro de 2021, foram 24,2 milhões de perfis de brasileiros com informações expostas. Por exemplo: em janeiro de 2021 houve um mega vazamento de dados de CPFs (223 milhões) e no fórum tinha um anúncio com amostra de dados à venda (VENTURA, 2022). Em 21 de janeiro de 2022, o Banco Central comunicou vazamento de dados pessoais vinculado a chaves PIX, 160.147 chaves foram potencialmente expostas com informações como: nome, CPF, número da agência e conta ocorrido em 3 e 5 de dezembro de 2021 (ARAGÃO, 2022). Em 02 de dezembro de 2020, uma reportagem do jornal o Estado de São Paulo revelou que 243 milhões de dados brasileiros cadastrados no Sistema Único de Saúde (SUS) ficaram expostos, como nome completo, CPF, endereço e telefone (CAMBRICOLI, 2020).

Além desses incidentes ocorridos no Brasil, justifica-se o estudo de modo econômico pela preocupação em amenizar a organização da aplicação de multas relacionadas à não adequação à Lei, levando como base as multas que foram aplicadas às instituições europeias desde 2019, os valores já ultrapassaram os 1,6 bilhão de euros (KAMPS, 2022). Isso porque, a Lei de proteção de dados europeia, denominada Regulamento Geral de Proteção de Dados (ou *General Data Protection Regulation,* GDPR), foi publicada em 2016 e entrou em vigor em 2018.

Na Europa, a organização CMS, através do sítio eletrônico *Enforcement Tracker*[1] realiza um relatório anual sobre o processo de multas, além de ter uma ferramenta para rastrear a aplicação de multas da GDPR. No Brasil, a Associação Nacional dos Profissionais de Privacidade de Dados (ANPPD) apresenta uma ferramenta[2] semelhante para rastrear aplicação de multas, que no momento da pesquisa, são decorridas de processos judiciais.

Ao comparar as cinco multas mais caras até o momento aplicadas no Brasil e na Europa (convertendo os valores das multas em reais), pode-se analisar o **Quadro 1** comparativo a seguir.

[1] Link https://www.enforcementtracker.com/ acessado em 16 de mai. de 2022.

[2] Link https://anppd.org/violacoes acessado em 16 de mai. de 2022.

QUADRO 1 – MULTAS DE MAIOR VALOR GDPR X LGPD

GDPR			**LGPD**		
Data	(1€ = R$ 5,19 reais) **	Organização*	Data	Reais	Organização*
16/07/2021	€ 746.000,000 / R$ 3.874.623,29	Amazon Europe Core S.à.r.l	18/03/2021	R$ 2.500.000,00	Mercado de software
02/09/2021	€ 255,000,000 / R$ 1.324.435,58	WhatsApp Ireland Ltd.	12/05/2021	R$ 100.000,00	Metrô
31/12/2021	€ 90,000,000 / R$ 467.447,85	Google LLC	21/05/2021	R$ 11.457,68	Banco
31/12/2021	€ 60,000,000 / R$ 311.631,90	Google Ireland Ltd.	24/03/2021	R$ 10.000,00	Imprensa
31/12/2021	€ 60,000,000 / R$ 311.631,90	Facebook Ireland Ltd.	21/01/2021	R$ 10.000,00	Alimentício

FONTE: A autora baseada em GDPR *Enforcement Tracker* (2022) e anppd (2022).
*O descritivo da organização está de acordo com o que foi divulgado no site. **Os valores foram baseados na cotação da moeda europeia do dia 16 de maio de 2022.

É possível perceber que as multas europeias já aplicadas são mais elevadas que as brasileiras até o momento. No Brasil, esse processo teve início em agosto de 2021, dois anos mais tarde do que na Europa.

A LGPD apresenta como diferencial a sua importância decisória no contexto brasileiro, pois traz como consequência uma modificação nas relações pessoais e organizacionais versus os dados que devem ser protegidos. Assim, as empresas brasileiras precisarão avaliar e ajustar aspectos culturais, políticas de gestão e procedimentos que envolvem a implementação de tecnologias, de modo a garantir a segurança dos usuários e de seus negócios, transformando os dados dos clientes em ativos de confiança e credibilidade.

Além disso, o estudo se justifica academicamente pela novidade e relevância do tema, pois abre um campo novo de estudos para os pesquisadores já que de acordo com uma pesquisa realizada na base de dados de teses e dissertações para o Programa de Pós-graduação de Gestão da Informação (PPGGI) da Universidade Federal do Paraná (UFPR) na linha de pesquisa Informação e Tecnologia, apenas uma dissertação sobre a LGPD foi detectada, permeando espaço para mais estudos e processo de construção da ciência.

A aderência da pesquisa ao Programa de Pós-Graduação em Gestão da Informação (PPGGI) e à linha de pesquisa Informação e Tecnologia deve-se ao caráter interdisciplinar, que engloba três áreas do conhecimento: Gestão da Informação, Tecnologia da Informação e Lei Geral de Proteção de Dados.

No campo da Gestão da Informação, a pesquisa apresenta os conceitos de informação, gestão da informação, ecologia da informação e cultura organizacional, sendo que suas contribuições se referem especialmente à competência informacional, qualidade de dados e ao tratamento ético da informação. Na Tecnologia da Informação, a pesquisa abrange conceitos de anonimização, privacidade, *privacy by design*, segurança da informação e governança e gestão de dados. No campo da LGPD, a pesquisa engloba alguns conceitos da Lei.

Dessa maneira, essas áreas do conhecimento se entrelaçam, não sendo possível separá-las, mas verificar de que maneira se relacionam.

1.4 ESTRUTURA DO TRABALHO

A presente pesquisa é dividida em cinco seções. Nesta primeira seção, apresentou-se introdução e contextualização do tema, justificativa, problema de pesquisa, objetivos do estudo.

A segunda trata do referencial teórico, aborda-se o contexto e evolução legislativa sobre a LGPD e também a descrição da Lei.

Em seguida, discute-se alguns conceitos inerentes que englobam a LGPD encontrados na literatura e o que é uma estrutura conceitual.

A terceira seção detalha os procedimentos metodológicos, desde as escolhas relacionadas as estruturas conceituais selecionadas e que serão estudadas, como ocorrerá a coleta de dados e sua análise.

Já a quarta seção descreve os resultados encontrados, a quinta seção a discussão, a sexta seção as considerações finais e, por fim, as referências utilizadas e o anexo.

2 REFERENCIAL TEÓRICO

Este capítulo apresenta o referencial teórico utilizado na pesquisa nas seguintes seções: contexto e evolução legislativa, Lei Geral de Proteção de Dados. Após isso, apresenta alguns conceitos essenciais que envolvem a LGPD dispostos nos seguintes itens: anonimização, termo de consentimento, privacidade, *privacy by design*, segurança da informação, governança e gestão de dados, informação, gestão da informação e seus delineamentos e estrutura conceitual.

2.1 CONTEXTO E EVOLUÇÃO LEGISLATIVA

Por volta de 1970, com o aumento do comércio europeu e a disseminação da Tecnologia da Informação (TI), houve a necessidade da adoção de mecanismos que permitissem maior gestão das informações pessoais para garantir que os indivíduos pudessem exercer controle de seus dados sem causar impacto no desenvolvimento econômico. Então em 1995, por meio da publicação da Diretiva 95/46/CE do Parlamento Europeu, buscou-se harmonizar as legislações europeias no que tange ao tratamento de dados pessoais e à livre circulação desses dados. Após isso, em 2016, a União Europeia (EU) publicou, o Regulamento Geral de Proteção de Dados (do inglês *General Data Protection Regulation* – GDPR), que buscou unificar e reforçar a proteção de dados para os indivíduos do continente europeu. Com a publicação da GDPR, o tema privacidade ganhou ainda mais relevância no contexto global. Transações comerciais e as próprias pessoas passaram a demandar mais cuidado com os dados pessoais (TCU, 2020).

A GDPR tem como objetivo principal harmonizar as leis de privacidade de dados no bloco europeu, regulando o processamento por indivíduos, empresas ou organizações de dados pessoais relacionados a indivíduos do bloco (IRAMINA, 2020).

No segundo capítulo, o Regulamento Europeu, expõe os princípios que a Lei rege, esses são descritos em artigos, destaca-se o artigo 6º, no qual conceitua as seis bases legais obrigatórias para se usar os dados pessoais. O terceiro capítulo destaca-se por trazer os direitos dos cidadãos, como o direito de: acesso à informação, de retificação, de oposição, de exclusão dos dados, de portabilidade, transparência na coleta, transmissão de dados e a revisão de decisões automatizadas.

Na sua forma de aplicação, a GDPR traz a inclusão do princípio de *accountability* no art. 24, demandando às organizações que: (a) adotem políticas, procedimentos e medidas para implementação das obrigações; e b) sejam capazes de demonstrar tal implementação (IRAMINA, 2020).

No capítulo IV, pode-se destacar os art. 37,38 e 39 que trazem a definição do encarregado de dados, intitulado como *Data Protection Officer (DPO)*, ou seja, a pessoa responsável pela proteção de dados da empresa, ou grupo de empresas,

podendo ser um membro da organização ou contratado. E que também será responsável por orientar, aconselhar e informar, a organização aos processos de adequação, de responder os questionamentos e exercícios dos direitos dos titulares de dados, fornecer aconselhamento respeito à avaliação do impacto na proteção de dados, entre outras funções (UE, 2016).

A GDPR prevê a figura das autoridades supervisoras de proteção de dados, ao menos uma para cada Estado Membro da União Europeia, responsáveis por supervisionar, por meio de poderes investigativos e corretivos, a aplicação da Lei de proteção de dados, inclusive para que as autoridades de proteção de dados reguladoras imponham multas de até 20 milhões de euros ou 4% do faturamento do volume de negócios anual total mundial do exercício anterior, consoante o que for mais elevado (IRAMINA, 2020).

Não muito distante, refletindo todo o contexto no Brasil, pode-se iniciar com o direito à inviolabilidade do domicílio e ao sigilo de correspondência que esteve em todos os textos constitucionais e apenas na Constituição de 1988 foi inserido o direito à intimidade e à proteção privada. Na constituição Norte Americana de 1788 não havia menção expressa ao direito de inviolabilidade do domicílio, nem à intimidade. Porém, com a Quarta e Quinta emendas, e ainda, com a Declaração Universal dos Direitos do Homem esse direito passou a ser contemplado (FINKELSTEIN, 2020).

Passando a Leis mais recentes, o Marco Civil da Internet, Lei nº 12.965/14, apresenta vários artigos visando à proteção, à confidencialidade e inviolabilidade da vida privada digital e os fluxos de tráfego da Internet, além de garantir que a guarda e a disponibilização de registros de conexão e de acesso a aplicações a internet resguardem a intimidade, honra e imagem de seus usuários. O artigo 7º assegura os direitos ao usuário de informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que poderão ser utilizados para finalidades que: justifiquem sua coleta, não sejam vedadas pela legislação e estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet.

Além do dispositivo do Marco Civil, o Brasil já vinha caminhando aos poucos no processo de construção de direitos, transparência pública e prevenção da violação de dados, como é o caso da Lei de Acesso à Informação (LAI), Lei n° 12.527/11, marco legal na transparência pública e a prestação de contas por parte

do governo para a sociedade, trazendo empoderamento ao cidadão em busca de seu direito de acesso à informação.

Nesse meio também, evidencia-se a Lei de tipificação criminal de delitos informáticos, Lei n° 12.737/12, com previsão legal e alteração no Código Penal, tipificando os chamados delitos ou crimes informáticos, também conhecida como Lei Carolina Dieckmann, devido a situação enfrentada pela atriz, que teve arquivos copiados de seu computador, como fotos íntimas e conversas e posteriormente divulgadas na internet.

O avanço da tecnologia e o aumento de casos de incidentes de vazamentos de dados pessoais aumentaram a notoriedade e a importância do tratamento de dados.

Segue-se no Brasil então, as discussões e a criação da LGPD (Lei Geral de Proteção de Dados).

2.2 LEI GERAL DE PROTEÇÃO DE DADOS (LGPD)

Seguindo a tendência mundial, a Lei nº 13.709/2018, denominada Lei Geral de Proteção de Dados Pessoais foi publicada no Brasil, foi inspirada no GDPR e dispõe sobre o tratamento de dados pessoais por pessoa natural ou por pessoa jurídica, com o intuito de proteger os direitos de liberdade e privacidade.

A Lei foi promulgada em 14 de agosto de 2018 e, entraria em vigência dezoito meses após a publicação. Porém a Medida Provisória (MP) n°869 de 27 de dezembro de 2018 prorrogou esse prazo por mais seis meses. Entretanto, devido à pandemia da Covid-19, foi publicada nova MP (959/2020) que prorrogaria novamente o prazo citado e que levaria a entrada em vigor da legislação para maio de 2021. No entanto, após discussão no Senado, o prazo de 24 meses foi mantido e a Lei passou a vigorar em setembro de 2020, após sanção presidencial (TCU, 2020).

Outra mudança foi a Lei nº 13.853/2019, de 08 de julho de 2019, que atualizou alguns artigos, sendo a maior alteração a criação da Autoridade Nacional de Proteção de Dados (ANPD). E a promulgação da Lei nº 14.010, de 10 de junho de 2020, que adiou as sanções e multas referentes à aplicação da LGPD para o mês de agosto de 2021.

Para Lemos e Passos (2020), uma Lei de proteção de dados gera implicações econômicas e políticas internas e externas, não apenas as empresas precisam se adequar, mas também o Poder Público.

O objetivo da LGPD é regulamentar o tratamento dos dados pessoais, inclusive em 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, 2021).

A disciplina de proteção de dados apresentada na LGPD é fundamentada na seguinte base (Brasil, 2021):

> I - O respeito à privacidade;
> II - a autodeterminação informativa;
> III - a liberdade de expressão, de informação, de comunicação e de opinião;
> IV - a inviolabilidade da intimidade, da honra e da imagem;
> V - o desenvolvimento econômico e tecnológico e a inovação;
> VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e
> VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

Além disso, a Lei traz princípios que regem o tratamento de dados pessoais, lembrando que ela determina a necessidade de observar a boa-fé. Para Teixeira (2021, p. 80) os princípios são norteadores para a aplicação das regras jurídicas positivadas.

Os princípios se descrevem no **Quadro 2**.

QUADRO 2 – PRINCÍPIOS LGPD

Princípios Norteadores (Art. 6º)	
Finalidade	propósitos legítimos [lícitos, morais], específicos, explícitos e informados ao titular.
Adequação	compatibilidade do tratamento com as finalidades informadas ao titular.
Necessidade	limitação do tratamento dos dados ao mínimo necessário.
Livre Acesso	garantia de acesso e integralidade dos dados.
Qualidade dos Dados	garantia de dados exatos, relevantes e atualizados.
Transparência	garantia de informações claras e facilmente acessíveis.
Segurança	utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais.
Prevenção	adoção de cuidados para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais.
Não Discriminação	impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos.
Responsabilização e prestação de contas	demonstração da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento da legislação.

FONTE: Adaptado de BRASIL (2018).

Cada princípio norteador apresenta uma finalidade de aplicação que as organizações devem atender quando estiverem realizando seus projetos de conformidade à Lei (OLIVEIRA *et al*., 2020). Assim, pode-se entender a relevância e a importância do art. 6° para que as organizações estejam atentas.

Afinal o que é dado pessoal e dado pessoal sensível, segundo a Lei (art.5°, I) dado pessoal é uma informação relacionada a pessoa natural identificada ou identificável (BRASIL, 2018).

Ou seja, algum dado que identifica alguém como por exemplo: nome, CPF, e-mail, endereço, data de nascimento, hábito de consumo, geolocalização, entre outros.

Já o dado sensível, para Lei (art. 5°, II) é:

> "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";

Ao saber da distinção dos dois conceitos, é necessário entender o que é considerado tratamento de dados para a Lei. É toda a operação realizada como: coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação, controle, modificação, comunicação, transferência, difusão ou extração.

E sabe-se que para realizar o tratamento dos dados pessoais é necessário que esteja presente uma das bases legais, só podendo ser realizado nas seguintes hipóteses: I) consentimento do titular; II) cumprimento da obrigação legal ou regulatória; III) pela Administração Pública, à execução de políticas públicas; IV) estudos por órgão de pesquisa; V) execução de contrato ou de procedimentos preliminares; VI) exercício regular de direitos; VII) proteção da vida ou da incolumidade física; VIII) tutela da saúde; IX) interesses legítimos do controlador ou de terceiros; e X) proteção do crédito (BRASIL, 2018).

Esse rol é taxativo, sendo obrigatório às organizações especificarem qual ou quais bases legais serão utilizadas para o tratamento dos dados.

Mas quem são os envolvidos na Lei, em outras palavras, quais são os papéis no processo de tratamento de dados pessoais? Tem-se o titular de dados, o controlador, o operador e o encarregado de dados.

A Lei se preocupa com empoderamento do titular de dados por meio de controle e escolha significativa em relação às suas informações (IRAMINA, 2020). O titular de dados é a pessoa natural a quem se referem os dados pessoais que são objeto de tratamento (BRASIL, 2018). Para Oliveira *et al*. (2020), o titular de dados não é aquele que detém o dado, o titular de dados é aquela pessoa a qual os dados se referem, independente de quem tem a tutela desses dados.

O art. 18º informa esses direitos que são: confirmação da existência de tratamento; acesso aos dados; correção de dados incompletos, inexatos ou desatualizados; anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei; portabilidade; eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16º desta Lei; informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados; informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa; revogação do consentimento (BRASIL, 2018).

O controlador é a “pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais”, já o operador é a “pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador”, ambos são considerados agentes de tratamento, conforme o inciso IX do art. 5º.

O controlador, independentemente de estar em conformidade com as normas sobre a proteção de dados, também deverá se preocupar com todas as pessoas que poderão tratar dados em seu nome. Nesse contexto, destaca-se a importância de contratar pessoas e se preocupar com contratos, adicionando medidas que assegurem que o operador cumpra com as instruções dadas e de acordo com as normas da LGPD (TEIXEIRA, 2021).

O encarregado dos dados é a “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)”, que tem como atribuições: I) aceitar reclamações, prestar esclarecimentos; II) receber comunicações da autoridade nacional e adotar providências; III) orientar os funcionários e os contratados da entidade com relação às práticas em relação à proteção de dados pessoais; e IV) executar demais atribuições determinada pelo controlador. Ou seja, um intermediador entre a organização e a ANPD.

Diante de suas atribuições, percebe-se o importante papel do encarregado nas organizações e, portanto, relevante a escolha desse membro, sendo esse um dos primeiros passos para a adequação à LGPD. Compactuando com isso, o artigo (art.41º, §2º) impõem que as informações de identificação e de contato do encarregado de dados deverão ser divulgadas publicamente, preferencialmente em sítio eletrônico.

Já a Autoridade Nacional de Proteção de Dados (ANPD) é o "órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento da Lei em todo o território nacional que está submetida a regime autárquico especial e vinculada à Presidência da República" (art.55-A). Será formada por um Conselho Diretor constituído por cinco diretores, nomeados pelo Presidente da República, e os membros do conselho terão mandato de quatro anos (IRAMINA, 2020).

Se ocorrer qualquer problema com os dados coletados a empresa detentora, deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares, de acordo com o art. 48º (BRASIL, 2018).

O descumprimento da Lei resultará em penalidades, dependendo do grau da infração, iniciando por uma advertência até a aplicação de multas com valores elevados, que podem chegar a 2% do faturamento total da empresa, grupo ou conglomerado brasileiro no seu último exercício, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração.

2.3 CONCEITOS INERENTES DA LGPD

Neste item, serão demonstrados alguns conceitos importantes intrínsecos à Lei, entre eles estão: anonimização, termo de consentimento, privacidade, *privacy by design*, segurança da informação, governança e gestão de dados, informação, gestão da informação e estrutura/*framework* conceitual.

2.3.1 ANONIMIZAÇÃO

Um dos temas inerentes à Lei é a anonimização de dados, conceituada na LGPD no artigo 5º, inciso III e XI e definida como direito do titular de dados nos artigos 11º, inciso II, alínea c, 16º, inciso II e IV, e 18º, inciso IV.

A anonimização (artigo 5º, IX, da LGPD): É um processo técnico de dissociação entre determinado dado pessoal e o seu respectivo titular. Inúmeros procedimentos específicos podem ser utilizados para implementação, que ocorre quase sempre a partir da eliminação de determinados elementos identificadores que constam em uma base de dados, por meio de supressão do dado, generalização, randomização ou pseudonimização (MARTINS; FALEIROS JÚNIOR, 2019, p. 61).

Para Faleiros Júnior e Martins (2021), o intuito de retirar dos dados pessoais coletados elementos que permitam identificar e expor a pessoa à qual dizem respeito é a força motriz da anonimização que, junto com processos técnicos, prometem viabilizar o uso desses dados sem risco de que se descubra os dados pessoais originais.

O parâmetro utilizado na aferição dos processos de anonimização pode ser chamado de “grau de identificabilidade” e tem como objetivo prevenir a reversão impedindo a recuperação da informação originalmente anonimizada (BIONI, 2021).

Para isso, são utilizados procedimentos de supressão, ocultação ou fragmentação da informação, como exemplificado no **Quadro 3**:

QUADRO 3 – PROCEDIMENTOS ANONIMIZAÇÃO

Procedimentos	
Supressão do CPF	Identificador que diferencia pessoas homônimas, sendo único, quando sua disponibilização, mesmo que parcial, deve ser evitada.
Generalização do Nome Completo	Deveria mostrar apenas o prenome, com objetivo de reduzir que um nome possa ser atribuído especificamente a uma pessoa.
Generalização da Localização Geográfica	Disponibilizar apenas os primeiros dígitos do CEP, a fim de quebrar o vínculo de identificação.
Generalização da Idade	Optar por divulgar a faixa etária como jovens, adultos, idosos.

FONTE: Adaptado de Bioni (2021, p. 62).

Mesmo utilizando esses procedimentos que dificultariam a descoberta do titular de dados, ainda se questiona a confiabilidade dos processos de anonimização. Bioni (2021, p. 63) demonstra que se torna cada vez mais recorrente a publicação de estudos que demonstram que o processo de anonimização é algo falível. Um exemplo desse estudo é o caso de Narayanan e Shmatikov (2010 *apud* Bioni, 2010), que afirmam que qualquer informação que diferencie uma pessoa da

outra pode ser utilizada para a reidentificação de dados anônimos e que existem muitas características humanas que permitem isso, por exemplo: o consumo preferências, transações comerciais, navegação na Web, históricos de pesquisa, entre outros.

Faleiros (2021) confirma o pensamento de Bioni, indicando que é imprescindível ter elementos mínimos de confiabilidade para a anonimização, porque existem meios para a reidentificação do usuário pelo acesso a outros bancos de dados, algo praticamente impossível de ser mensurado do ponto de vista de segurança.

Considerando que na Lei um dado pessoal é uma informação relacionada à pessoa natural identificada ou identificável, pode-se pensar que uma informação, direta ou indiretamente, pode identificar o sujeito, ou seja, para Bioni (2021, p.64) o dado pessoal é um conceito expansionista.

Assim, é possível concluir que a anonimização nem sempre é garantia de proteção dos dados e que a proteção de dados pessoais, como um novo direito da personalidade, dirige-se a todo e qualquer dado em que se denote o prolongamento de um sujeito (FINOCCHIARO *apud* BIONI, 2021).

2.3.1.1 Anonimização e Consentimento do Titular

Modesto (2020) traz em seu artigo a polêmica da monetização dos dados pessoais. Nela, organizações criam artimanhas para coletar dados pessoais dos usuários, sendo alguns exemplos: obrigam os indivíduos a fornecer uma quantidade demasiada e desnecessária de dados; coletam esses dados por meio de *cookies*[3], muitas vezes sem o conhecimento do titular desses dados; solicitam dados pessoais para fornecer serviços “gratuitos”, como é o caso do *Facebook*; coletam e tratam os dados dos clientes, e, a partir dessas informações, personalizam o serviço prestado (marketing), podendo também coletar e tratar os dados de seus clientes e repassá-los a terceiros.

[3] São pequenos arquivos que são gravados em seu computador quando você acessa sites na Internet e que são reenviados a estes mesmos sites quando novamente visitados. São usados para manter informações sobre você, como carrinho de compras, lista de produtos e preferências de navegação. Disponível em: https://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf.

Nesse artigo, Modesto (2020) pretende responder quais são os impactos da LGPD na atividade de monetização de dados pessoais. Segundo a autora, o primeiro ponto a ser observado pelos agentes que monetizam informações pessoais é que a LGPD somente autoriza o tratamento de dados mediante o fornecimento do consentimento pelo titular ou, independentemente deste, no caso de situações específicas expressamente previstas. Portanto, a menos que o tratamento de dados pessoais esteja fundado em outra hipótese legal, o agente monetizador deverá obter o consentimento do titular, o qual deve ser livre, inequívoco e informado. Isso significa que a LGPD não autoriza que o silêncio seja considerado como manifestação da vontade. Além disso, o indivíduo deverá ser informado dos dados que estão sendo coletados, assim como a finalidade para a qual serão utilizados. Por fim, Modesto conclui que a anonimização pode ser uma alternativa viável aos agentes monetizadores, uma vez que a LGPD não incide sobre o tratamento e manipulação de dados anonimizados, afastando-se a exigência do consentimento do titular, como informado no artigo 12º da Lei.

No entanto, nem sempre a anonimização será uma grande vantagem, pois se os dados forem cruzados com outras bases de dados talvez seja possível identificar essas informações, ou seja, ainda existe um dilema entre a adoção do termo de consentimento e a anonimização.

2.3.1.2 Anonimização e Privacidade Diferencial

Após identificar que anonimização nem sempre pode ser confiável, como citado nos itens anteriores, surge o conceito denominado privacidade diferencial.

Chen (2020) define a privacidade diferencial como uma técnica matemática que torna o processo de anonimização rigoroso, medindo a quantidade de privacidade quando uma imprecisão ou ruído é adicionada, ou seja, quanto mais ruído mais difícil se torna a desanonimização. Costa (2020) concorda e ressalta que a privacidade diferencial torna inviável o rastreamento da fonte por meio do cruzamento de informações entre bancos de dados relacionais.

Chen (2020) cita o exemplo do uso da privacidade diferencial, que ocorre no departamento de censo dos Estados Unidos, denominado (*Census Bureau*) onde são coletados os dados de 330 milhões de habitantes em 2020, mantendo suas identidades privadas. Esses dados foram divulgados em tabelas estatísticas

utilizadas pela administração pública e por setores acadêmicos com o objetivo de redigir legislação ou realizar pesquisas acadêmicas. Por Lei, esse departamento deve certificar-se de que nenhum indivíduo pode ser reconhecido. Então, eles injetam imprecisões, ou “ruídos”, nos dados tornando algumas pessoas mais jovens e outras mais velhas, ou rotulando algumas pessoas brancas como negras e vice-versa, mantendo os totais de cada idade ou grupo étnico iguais. Além do censo dos Estados Unidos, esse método também é usado pela *Apple* e *Facebook* para coletar dados agregados sem identificar usuários específicos.

Pode-se concluir que o compartilhamento seguro e responsável de dados pessoais, mesmo que anonimizados, será uma tarefa mais complexa do que um mero consentimento previsto na LGPD. Nesse sentido, Costa (2020) justifica que simplesmente anonimizar dados pessoais na busca por isenção de responsabilidades, porque a Lei assim o permite, não é estar em *compliance*[4], visto que a LGPD deixa em aberto a maneira de se proteger os dados.

2.3.2 TERMO DE CONSENTIMENTO

Uma das hipóteses de tratamento dos dados é o consentimento pelo titular. Proposto na Lei, no art. 5°, inciso XII o consentimento é “manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada” (BRASIL, 2018).

No entanto, apesar do consentimento ser uma afirmação dos direitos dos usuários existe uma assimetria entre o usuário e a organização. No que diz respeito à infraestrutura, conhecimento sobre a ciência dos dados e a interpretação de dados massivos por meio da inteligência artificial, o conhecimento da organização sempre ultrapassará aquilo que pode ser compreendido pelo usuário, caracterizando a assimetria informacional. Assim, no contexto da LGPD, o usuário entrega seus

[4] *compliance* é o ato de estar em conformidade com determinadas as leis, normas e regras. Pode ser tanto em relação às leis federais ou às políticas corporativas. Nas empresas, sua aplicação trata-se basicamente de estar em conformidade com os regulamentos, diretrizes e, claro, leis que regem sua atuação. Disponível em: https://www.totvs.com/blog/negocios/compliance/#:~:text=O%20compliance%20%C3%A9%20o%20ato,leis%20que%20regem%20sua%20atua%C3%A7%C3%A3o.

dados via consentimento, e assim, passa a ser renderizado e analisado pelas empresas (que o monetizam no mercado de previsão de comportamentos), as quais retornam valor ao usuário na forma de melhoria nos serviços prestados (FORNASIER e KNEBEL, 2021).

2.3.3 PRIVACIDADE

O termo privacidade (*privacy*) surgiu na obra de dois juristas, Samuel Warren e Louis Brandeis, no final do século XIX, em um artigo intitulado *The Right to Privacy*, publicado em 1890 (MARRAFON e COUTINHO, 2020).

Esse termo, segundo Stallings (2019, p.2), entrou na enciclopédia de filosofia de *Stanford* com duas características gerais: o direito de ser deixado em paz — ou seja, livre de ser observado ou perturbado — e a capacidade de controlar as informações divulgadas sobre si mesmo. Além disso, ressalta que um relatório do Conselho Nacional de Pesquisa dos EUA afirma que o termo privacidade geralmente se refere a tornar informações ostensivamente privadas sobre um indivíduo indisponível para partes que não deveriam ter essa informação.

O documento X.800 (*Security Architecture for Open Systems Interconnection*) criado em 1991 pela *International Telecommunication Union – Telecomunicattion* (ITU-T), agência da ONU especializada em tecnologias de informação e comunicação, que padroniza e regula ondas de rádio e telecomunicações composta por todos os 193 países membros, define o conceito de privacidade de informação como o direito dos indivíduos de controlar ou influenciar quais informações relacionadas a eles podem ser coletadas e armazenadas e por quem e a quem essas informações podem ser divulgadas. Além disso, uma vez que a privacidade diz respeito ao direito do indivíduo de controlar suas informações, ela não pode ser muito precisa e seu uso deve ser evitado, exceto como uma motivação para exigir segurança da informação.

Para Finkelstein (2020), nesta sociedade da informação, a geração, o armazenamento e a transferência das informações são realizados em tempo real, sendo que as novas tecnologias agregam valor à informação. A informação passou a ser considerada um produto, podendo, inclusive, vir a ser objeto de transações comerciais. Os interesses de privacidade se conectam à coleta, controle, proteção e uso de informações sobre indivíduos.

Assim, o termo privacidade, que é frequentemente usado em linguagem comum, discussões filosóficas, políticas e legais, é um conceito em desordem, ou seja, ninguém consegue articular exatamente seu significado, pois é um conceito muito abrangente, envolvendo liberdade de pensamento, controle sobre o próprio corpo, liberdade na sua própria casa, controle sobre informações pessoais e estar livre de vigilância (SOLOVE, 2008, p.9). Esse conceito ultrapassa o “isolamento do indivíduo”, conhecido como liberdade negativa, e permite o exercício “de exigir conhecimento, controle e disposição de dados relativos à sua individualidade”, ou seja, uma liberdade positiva (Mendes e Fonseca *apud* QUEIROZ, PONCE, 2020, p. 78-79).

Para Stéfano Rodotá (2008 *apud* Finkelstein, 2020), a definição da privacidade como o direito de ser deixado só perdeu o sentido na sociedade da informação. Agora, a privacidade abrange novas dimensões relativas à coleta e ao tratamento de dados pessoais. Então, há uma necessidade de reformulação conceitual que deve ser acompanhada pelas modernas legislações.

Assim, apesar de o conceito de privacidade ser antigo, a LGPD o retoma e o reforça, evidenciando sua importância por meio de multas.

2.3.3.1 Informação Pessoalmente Identificada (PII)

O Instituto Nacional de Padrões e Tecnologia (*National Institute of Standards and Technology*, NIST) criou um guia (SP 800-12) em 2010, para auxiliar as agências federais na proteção da informação pessoalmente identificável (PII). É possível entender que PII é qualquer informação sobre um indivíduo mantida por uma agência, incluindo informações que podem ser utilizadas para distinguir ou rastrear a identidade de um indivíduo, tais como: nome, número de segurança social, data e local de nascimento, nome de solteira da mãe, registos biométricos; e qualquer outra informação que esteja ligada ou ligável a um indivíduo, tal como informação médica, educacional, financeira e de emprego, IP (*internet protocol*), raio-x, imagem biométrica.

O que a NIST designa por PII é o que a LGPD denomina de dados pessoais e dados pessoais sensíveis.

2.3.3.2 Fair Information Practices (FIP)

A OECD - *Organization for Economic Co-operation and Development* é uma organização composta por governos, formuladores de políticas e cidadãos, que trabalham para estabelecer padrões internacionais baseados em evidências para encontrar soluções para uma série de desafios sociais, econômicos e ambientais com intuito de construir boas políticas.

Essa organização criou, em 1980, as Diretrizes de Privacidade (*Privacy Guidelines*), que foram revisadas em 2013 devido a preocupações com as consequências de leis nacionais de proteção de dados inconsistentes e em resposta a novos meios automatizados de processamento de informações.

Essas diretrizes, apresentam o que são as Práticas Justas de Informação (*Fair Information Practices*) sendo estas (OECD):

- Princípio de Limitação da Coleta de dados: deve haver limites na coleta de dados pessoais e devem ser obtidos por meio lícitos e justos, quando necessário com consentimento do usuário.
- Princípio da Qualidade de Dados: os dados pessoais devem ser para determinado fim, exatos, completos e atualizados.
- Princípio da Especificação de Propósito: qual é a finalidade dos dados pessoais coletados, devem ser especificadas no momento de sua coleta e o seu uso somente poderá ocorrer para o propósito sinalizado
- Princípio do Uso Limitado: os dados pessoais não devem ser divulgados, disponibilizados ou usados para outros fins não especificados, exceto: com consentimento e ou autoridade da Lei.
- Princípio de Salvaguardas de Segurança: os dados pessoais devem ser protegidos por medidas de segurança razoáveis contra riscos como perda, acesso não autorizado, destruição, uso, modificação ou divulgação.
- Princípio de Abertura: Deve haver uma política geral de abertura sobre desenvolvimento, prática e políticas com relação a dados pessoais, estas deverão estar disponíveis juntamente com a sua finalidade e uso.
- Princípio de Participação individual: se remete ao direito do cidadão que pode ter direito: a) a confirmação da existência de seus dados. b) comunicar em prazo razoável o cidadão sobre seus dados. c) se os direitos a e b forem

indeferidos podem contestar d) contestar os dados a seu respeito, podendo mandar apagar, retificar, completar e alterar.

- Princípio da Responsabilidade: O responsável pelo tratamento de dados deve ser responsável por cumprir os princípios listados acima.

Aos citar esses princípios já dispostos na documentação de práticas justas de informação, verifica-se uma semelhança com os princípios fundamentais expostos na LGPD, criada anos depois. Por exemplo: o princípio da limitação de coleta de dados identifica-se com o princípio da Lei disposto no art. 6°, II, da necessidade, ou seja, deve haver uma limitação no tratamento ao mínimo necessário. O princípio da qualidade de dados corresponde ao art. 6°, V, da qualidade dos dados, ou seja, a garantia da relevância, clareza, exatidão e atualização dos dados e entre outros. Verifica-se a existência de princípios e orientações na LGPD, que na verdade já existiam, criados por outras organizações e em épocas distintas, mas que não eram necessariamente aplicados.

Ao lidar com a privacidade do PII, surgiram dois novos conceitos: Privacidade por *Design* (PbD) e engenharia de privacidade.

A partir da concepção de um novo sistema de TI, o objetivo do PbD é levar em conta os requisitos de privacidade em todos o processo de desenvolvimento (design, implementação e operação). Já a ISO 29100 (*Information Technology - Security Techniques - Privacy Framework*) vê o PbD como a prática de considerar medidas de proteção à privacidade no momento da concepção do sistema; ou seja, os *designers* devem considerar a conformidade com a privacidade durante a fase de projeto para o processamento de sistemas PII, em vez de abordar a conformidade apenas em uma fase subsequente.

Já a engenharia de privacidade envolve levar em conta a privacidade durante todo o ciclo de vida dos sistemas de TIC (tecnologia da informação e comunicação), de tal forma que a privacidade é e continua sendo parte integrante de sua função. O NISTIR 8062 (Uma Introdução à Engenharia de Privacidade e Gestão de Riscos em Sistemas Federais) define a engenharia de privacidade como uma disciplina especializada de engenharia de sistemas focada em alcançar a liberdade de condições que podem criar problemas para indivíduos com consequências inaceitáveis que surgem do sistema à medida que processa o PII. A engenharia de privacidade se concentra na implementação de técnicas que diminuem os riscos de

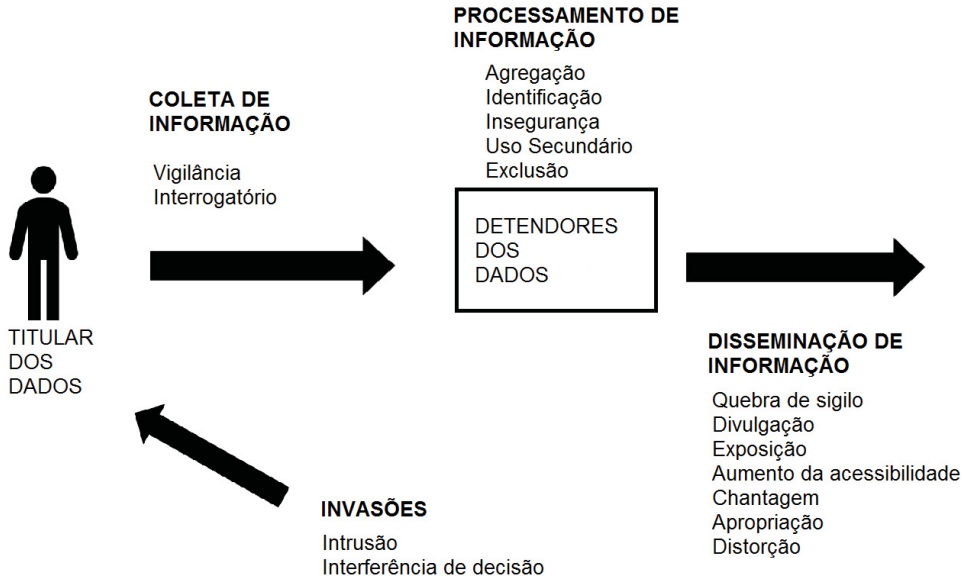
privacidade e permite que as organizações tomem decisões propositais sobre alocação de recursos e implementação eficaz de controles em sistemas de informação. Tais técnicas diminuem os riscos relacionados a danos à privacidade e permitem decisões propositais sobre alocação de recursos e implementação efetiva de controles.

Mas, afinal, quais seriam os riscos e problemas de privacidade?

2.3.3.3 Problemas de Privacidade

Em seu livro, Daniel Solove (SOLOVE, 2008) propôs identificar os problemas da privacidade de uma forma abrangente e concreta, através de uma taxonomia com objetivo de auxiliar a elaboração de leis e políticas com foco nas atividades que criam problemas. A **Figura 1** mostra a taxonomia criada por ele, em que existem 4 grupos nocivos nas atividades:

FIGURA 1 – MODELO DE TAXONOMIA



FONTE: Solove (2008, p.104) traduzido.

1- Coleta de informações (*information collection*): o primeiro grupo de atividades que afeta a privacidade é a coleta de informações;

- vigilância (*surveillance*): é a observação, ouvir, registrar as atividades de um indivíduo;
- interrogatório (*interrogation*): consiste em formas de questionar ou sondar informações.

2- Processamento de informações (*information processing*): é a maneira como as informações são armazenadas, manipuladas e usadas. As entidades, empresas, governo (*data holders*) coletam essas informações e processam, armazenam, combinam, manipulam, usam.

- agregação (*aggregation*): envolve a combinação de vários dados sobre uma pessoa;
- identificação (*identification*): vincula informações a indivíduos;
- insegurança (*insecurity*): envolve descuido na proteção de informações armazenadas de vazamentos e do acesso adequado;
- uso secundário (*secondary use*): é o uso de informações coletadas para um propósito diferente do uso para o qual foi coletado com o consentimento do titular de dados;
- exclusão (*exclusion*): é uma falha em permitir que os dados do titulares sejam conhecidos por outros (data holders) e participem do seu uso e manuseio.

3- Disseminação de informações (*information dissemination*): são atividades que podem ser criadas quando os dados pessoais são transferidos ou divulgados. A natureza da disseminação pode criar muitos problemas diferentes:

- violação da confidencialidade (*breach of confidenciality*): em que se está quebrando uma promessa de manter as informações confidenciais de uma pessoa;
- divulgação (*disclosure*): envolve a revelação de informações verdadeiras sobre uma pessoa, que afeta a maneira como os outros julgam sua reputação;
- exposição (*exposure*): envolve revelar a nudez, luto ou funções corporais de outra pessoa;
- aumento da acessibilidade (*increased accessibility*): amplia a acessibilidade das informações;

- chantagem (*blackmail*): é uma ameaça para divulgar informações pessoais;
- apropriação (*appropriation*): envolve o uso da identidade do sujeito dos dados, atendendo aos objetivos e interesses do outro;
- distorção (*distortion*): consiste em disseminar informações falsas ou enganosas sobre os indivíduos.

4- Invasão: são atividades que interferem na vida privada do indivíduo. Ao contrário dos outros grupos, a invasão nem sempre envolve informações (embora aconteça em muitos casos):

- intrusão (*intrusion*): diz respeito aos atos invasivos que perturbam a tranquilidade ou solidão, por exemplo, a invasão do domicílio.
- interferência de decisão (*decisional interference*): envolve a interferência do governo nas decisões do indivíduo sobre seus assuntos privados.

Por fim, após essa breve conceituação, percebe-se nesse capítulo que a taxonomia de Solove nos faz compreender uma gama de problemas de privacidade, semelhanças, diferenças e relações entre eles. Muitas vezes a tecnologia está envolvida em vários problemas, pois facilita a coleta, processamento, divulgação ainda mais agora com a *Internet of Things* (IoT), que tem como objetivo conectar itens usados no dia a dia, como eletrodomésticos, meios de transporte, tênis, roupas à *internet*, porém ressalta-se que esses problemas não são apenas causados pela TI, mas também por pessoas, empresas e governos.

2.3.4 PRIVACY BY DESIGN

As primeiras ideias sobre privacidade desde o design tiveram origem na década de 1970 e foram incorporadas, nos anos 90, à Diretiva Europeia de Proteção de Dados: a RL 95/46/EC. Em sua origem, o *privacy by design* (PbD) instrui a ideologia de que a privacidade deve tornar-se parte integrante das prioridades organizacionais e tem de ser incorporada em todos os padrões, protocolos e processos que tocam as nossas vidas (CAVOUKIAN, 2010).

Como reafirma Marrafon e Coutinho (2020), o PbD exige que as organizações adotem padrões especiais e medidas técnicas que assegurem que apenas os dados

pessoais necessários sejam processados com um propósito. Eles caracterizam a privacidade como sendo muito mais do que a proteção das informações pessoais contra acessos não autorizados, permitindo também que os titulares mantenham controle individual sobre as informações de identificação pessoal na coleta, análise, armazenamento, uso, manipulação e divulgação.

Na LGPD, o PbD foi proposto no artigo 46°, § 2º da Lei “as medidas de que trata o capítulo deste artigo deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução” (BRASIL, 2018), indicando que os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais. Na GDPR, o PbD foi incluído no artigo 25º tendo um capítulo específico sobre proteção de dados *by design* e *by default*.

O conceito de PbD foi proposto por Ann Cavoukian, professora da Universidade de Ryerson, no Canadá e comissária de Informação e Privacidade de Ontário. Segundo Cavoukian (2010) esse conceito é dividido em 7 pilares:

1) Um projeto proativo, não reativo, não repressivo e sim preventivo: esse pilar se baseia em uma abordagem que antecipa e previne eventos invasivos antes que ocorram, evitando a materialização dos eventos, ou seja, a PbD vem antes do fato e não depois, iniciando com o reconhecimento de forma explícita do valor e do benefício da adoção proativa de práticas de privacidade fortes, impedindo em primeiro lugar a ocorrência de violações internas de dados.

Cavoukian (2010) vai além e insinua que isso implica em três comportamentos:

- Compromisso claro, ao mais alto nível, em estabelecer e aplicar padrões elevados de privacidade, geralmente maior que os da Lei.
- Compromisso de que a privacidade é comprovadamente compartilhada por todas as comunidades e partes interessadas, em uma cultura de melhoria contínua.
- Que existam métodos para reconhecer a falta de privacidade (“antecipar pobres práticas de privacidade”) e corrigir os impactos, muito antes de ocorrerem de forma proativa, sistemática.

2) A privacidade de dados como configuração padrão: esse pilar visa proporcionar o máximo grau de privacidade de forma a assegurar que os dados pessoais são automaticamente protegidos em qualquer sistema informacional, ou seja, mesmo o usuário não fazendo nada sua privacidade continua intacta.

Esse princípio também pode ser denominado *privacy by default* ou privacidade por padrão. Nesse pilar, a autora remete a algumas práticas institucionalizadas nos *FIPS* (estrutura de padrões de segurança) criada pelo *NIST* (Instituto Nacional de Padrões e Tecnologia) que compreendem esse princípio, são eles: especificação da finalidade dos dados recolhidos; limitação do uso dados, recolhendo somente as informações justa, lícita e limitada; minimização dos dados, ou seja, recolher somente as informações estritamente necessárias; utilização, retenção e limitação de divulgação, com as informações pessoais sendo retidas apenas durante o tempo necessário para cumprir os fins declarados e depois destruídas em segurança; e, caso a necessidade ou a utilização de informações pessoais não for clara, deverá haver uma presunção de privacidade e aplicar-se-á o princípio da precaução: as definições por padrão serão as mais protetoras da privacidade. Esses princípios já foram citados no item 2.3.3.2.

3) A privacidade incorporada ao projeto: a privacidade estará embutida na arquitetura e construção do projeto, ou sistemas informacionais. Deve ser incorporada em tecnologias, operações e arquiteturas de informação de uma forma holística, integradora e criativa.

Segundo Cavoukian (2010), pode ser aplicado sempre que possível, realizando avaliação de impacto e riscos, documentando todas as medidas tomadas para mitigá-los.

4) A funcionalidade total (soma positiva, não soma zero): procura acomodar todos os interesses e objetivos de forma a somar, evitando falsas dicotomias como privacidade versus segurança. Ao incorporar a privacidade em uma tecnologia, processo ou sistema, deve ser feito de modo a não prejudicar a plena funcionalidade e otimizar todos os requisitos.

5) Segurança de ponta a ponta e proteção total do ciclo: nesse item, é necessário assegurar a privacidade da informação em todo o ciclo do dado nos sistemas de informações, usando medidas de segurança fortes garantido que no final do processo as informações possam ser destruídas em segurança. Cavoukian (2010) afirma que o princípio da segurança tem uma relevância especial porque, em sua essência, sem uma segurança forte, não pode haver privacidade. Além disso, as organizações devem assumir responsabilidade pela segurança da informação pessoal ao longo de todo o seu ciclo de vida, e as normas de segurança aplicadas

devem assegurar a confidencialidade, integridade e disponibilidade dos dados pessoais.

6) Visibilidade e transparência: baseia-se no fato de que as partes componentes e operações permanecem visíveis e transparentes, tanto para o usuário como para os fornecedores do serviço. Nesse item, deve ser dada uma ênfase especial à: responsabilização (*accountability*), ou seja, a responsabilidade por todas as políticas e procedimentos relacionados à privacidade deve ser documentada e comunicada conforme apropriado e atribuída a uma pessoa específica; ao transferir informações pessoais a terceiros, deve ser assegurada uma proteção equivalente da privacidade por meio de meios contratuais ou outros; transparência das informações sobre as políticas e práticas relacionadas à gestão de informações pessoais devem ser prontamente disponibilizadas aos indivíduos; cumprimento (*compliance*), ou seja, devem ser estabelecidos mecanismos de reclamação e reparação, e as informações devem ser comunicadas aos indivíduos, além de ter medidas para monitorar, avaliar e verificar o cumprimento das políticas e procedimentos de privacidade.

7) Respeito pela privacidade do usuário: deve-se levar em conta a utilização do software pelo usuário, ou seja, sua usabilidade, não deixando de respeitar a privacidade. Além disso, manter a aplicação centrada no usuário, deixando-o desempenhar a gestão dos seus próprios dados. A *FIPs* traz como adequação o uso do consentimento livre e específico do indivíduo para a utilização das informações exceto quando a Lei permite. A necessidade das informações estarem exatas, completas, atualizadas, de terem o direito ao acesso das informações pessoais e serem informados sobre a utilização e divulgação delas e do cumprimento das organizações em estabelecer mecanismos de reclamação, reparação e comunicação ao público.

2.3.5 SEGURANÇA DA INFORMAÇÃO

Um dos temas inerentes à LGPD é a segurança da informação, mencionada no seu artigo 6º, inciso VII e no Capítulo VII (Da Segurança e Boas Práticas) na Seção I (Da Segurança e do Sigilo dos Dados).

Os princípios da segurança da informação são importantes para assegurar a proteção das informações contra acessos não autorizados (confidencialidade), para manter a disponibilidade, integridade e autenticidade.

A segurança da informação já não é somente um problema de organizações de Tecnologia da Informação, mas também de ambientes industriais e de serviços sempre mais interligados, não sendo sistemas corporativos isolados e devendo ser protegidos (MUNCINELLI *et al*., 2020).

De acordo com NBR ISO/IEC 27002:2013 a segurança da informação é alcançada pela implementação de um conjunto adequado de controles, incluindo políticas, processos, procedimentos, estrutura organizacional e funções de software e hardware. Ou seja, uma forma de garantir padrões e procedimentos de TI eficazes é a formulação de políticas associadas à TI.

Nesse ínterim, Souza *et al*. (2020) ressalta que o impacto de vazamento de dados vai além de perdas financeiras, pois a exposição do cidadão pode ser um dano irreversível, e que sem uma política de segurança de informação, os problemas de roubos de dados e invasões de sistemas vitais podem ser ainda piores. Esses autores confirmam que “a formulação de políticas associadas às tecnologias da informação (TI) é umas das melhores maneiras de garantir padrões e procedimentos de TI eficazes, que protegem os recursos de TI organizacionais e controlam o compartilhamento de informações.”

2.3.5.1 Confidencialidade, Integridade, Disponibilidade e Autenticidade

A segurança da informação é baseada nos princípios confidencialidade, integridade e disponibilidade da informação (NBR ISO/IEC 27002, 2013).

Para Fontes (2012), confidencialidade significa que a informação deve ser acessada e utilizada exclusivamente pelos que necessitam dela para a realização de suas atividades profissionais na organização; para tanto, deve existir uma autorização prévia. Barreto (2018) complementa, enfatizando que é a capacidade de um sistema impedir que usuários não autorizados “vejam” determinada informação que foi delegada somente a usuários autorizados a vê-la. Para Piurcosky *et al*. (2019), quando os dados são inseridos no banco de dados da organização, inicia-se o processo de confidencialidade.

O princípio da integridade determina que a informação deve estar correta, ser verdadeira e não estar corrompida. A integridade é um atributo de segurança que garante que a informação seja alterada somente de forma autorizada, sendo mantida, assim, correta e completa (BARRETO, 2018).

Ter uma informação íntegra significa dizer que ela não foi alterada, ou atualizada, ou seja, a informação é a mesma de quando foi disponibilizada pelo proprietário e sem interferência de terceiros, sendo responsabilidade da organização protegê-la contra alterações indevidas (PIURCOSKY *et al*., 2019).

O princípio da disponibilidade indica que a informação deve estar acessível e ser utilizável sob demanda por uma entidade autorizada (ISO/IEC 27001:2006), devendo garantir que as informações estejam aptas a serem usadas a qualquer momento. Se em algum momento ela ficar indisponível poderá comprometer o seu uso.

Por fim, a autenticidade é a garantia de que um indivíduo, processo ou computador é realmente quem ele diz ser (BARRETO, 2018).

A garantia e a manutenção desses princípios constituem um objetivo para atingir a preservação da informação. Uma das formas de garantir esses princípios são as normas e políticas de uma organização, as quais serão abordadas no próximo item.

2.3.5.2 Documentação e Política de Segurança da Informação

A Política de Segurança de Informação (PSI) tem como objetivo suprir uma orientação e coordenar as ações na organização de acordo com requisitos de negócio, leis e regulamentações. Para aplicá-la necessita-se de uma boa gestão e envolvimento da alta administração da organização, de forma que haja conscientização e comunicação da política para todos os usuários em todos os níveis hierárquicos (NBR ISO/IEC 27002, 2013).

A ISO/IEC 27002 (2013) declara que é importante que a PSI contenha: as definições da segurança da informação, objetivos e princípios para orientar as atividades relativas a si, as atribuições de responsabilidades, gerais e específicas para o gerenciamento e processos para o tratamento dos desvios e exceções.

Além dessa política, convém que existam documentos que a apoiem e que tratem de tópicos específicos como: controle de acesso, classificação e tratamento da informação, segurança física do ambiente, backup, transferência da informação, gerenciamento de vulnerabilidades técnicas, proteção e privacidade da informação de identificação pessoal, entre outros. Além disso, que tenham tópicos importantes para os usuários finais, como: quais ativos poderão utilizar, mesa limpa e tela limpa, transferência de informações, dispositivos móveis e trabalho remoto e restrições sobre o uso e instalação de software (NBR ISO/IEC 27002, 2013).

Com toda essa documentação “convém que todos os funcionários da organização, e, onde pertinente, partes externas devem receber treinamento, educação e conscientização apropriados...” (NBR ISO/IEC 27002, 2013, p. 20).

2.3.6 GOVERNANÇA DE DADOS E GESTÃO DE DADOS

Pessoas, equipamentos, imóveis e dados fazem parte do funcionamento de uma organização e são ativos, devendo ser bem geridos e governados de modo a maximizar o seu valor. Assim, tem-se a governança de dados (GD) como a responsável por gerir princípios da organização e controle de dados e informações, que envolve interação com outras funções e estabelece políticas e diretrizes, atribuindo papéis e responsabilidades. Ou seja, é um conjunto de práticas que tem como objetivo organizar o uso e o controle adequado dos dados. Segundo Barbieri (2020), a GD busca organizar os dados visando disponibilidades, integridade, consistência, usabilidade, segurança, controle etc.

A importância de adotar a GD é ter subsídios para obter informações corretas, de fácil acesso e com agilidade para tomadas de decisões, assim como possuir conhecimento completo dos dados do negócio da empresa e difundir esse conhecimento para o restante da empresa. A GD também evita prejuízos decorrentes de baixa qualidade dos dados e reduz custos de operações com dados e torna a empresa apta a seguir regulamentações, como controles internos e/ou leis como a LGPD.

Juntamente à GD, há a Gestão de Dados, que diz respeito ao funcionamento do dia a dia de programas e de organizações no contexto de estratégias, políticas, processos e procedimentos que tenham sido estabelecidos pelo órgão (WORLD BANK, 2013).

Segundo Rêgo (2013, p. 48), a Gestão de Dados é “a disciplina responsável por definir, planejar, implantar e executar estratégias, procedimentos e práticas necessárias para gerenciar de forma efetiva os recursos de dados e informações das organizações, incluindo planos para sua definição, padronização, organização, proteção e utilização”.

Enquanto a Gestão é inerente e integrada aos processos organizacionais, sendo responsável pelo planejamento, organização, direção e controle, enfim, pelo manejo dos recursos e poderes colocados à disposição de órgãos e entidades para a execução de seus objetivos, a governança provê direcionamento, monitora, supervisiona e avalia a atuação da gestão, com vistas ao atendimento das necessidades e expectativas dos cidadãos e demais partes interessadas.

O *Data Management Body of Knowledge* (DAMA DMBOK®) é um exemplo de *framework* de boas práticas, que constitui um conjunto de princípios e orienta as boas práticas de gerenciamento de dados. Esse *framework*, estrutura 11 áreas de conhecimento de gerenciamento de dados (**Figura 2**) e centraliza a disciplina Governança de Dados das atividades de gerenciamento de dados, já que a governança é necessária para a consistência e o equilíbrio entre as funções. As outras áreas de conhecimento (arquitetura de dados, modelagem de dados, etc.) são balanceadas em torno do centro. Todas são partes necessárias da função madura de gerenciamento de dados, mas podem ser implementadas em momentos diferentes, dependendo dos requisitos da organização.

FIGURA 2 - DAMA-DMBOK

FONTE: DAMA-DMBOK2 traduzido (2017).

Em relação à Gestão de Dados, é importante especificar quais tipos de dados estão sendo armazenados, em especial os que se enquadram na classificação de dados sensíveis e explicar como, por quem e para qual finalidade os dados serão utilizados. Nesse sentido, Rached e Farias (2019) afirmam que a gestão de dados na empresa implicará uma grande mudança cultural, pois muitas empresas não têm conhecimento dos dados que possuem, onde e como são armazenados, muito menos têm um controle claro sobre quem tem ou deveria ter acesso a eles.

Outra questão são os dados compartilhados em cadeias de e-mails esquecidos, em que, normalmente, não existe uma política de eliminação desses dados armazenados, mesmo após o cumprimento da finalidade do e-mail ou após o término da relação comercial.

2.3.7 INFORMAÇÃO, GESTÃO DA INFORMAÇÃO E SEUS DELINEAMENTOS

Neste item, serão expostos os conceitos de informação, gestão da informação, ecologia da informação e cultura organizacional.

2.3.7.1 Informação

A informação é insumo tanto para o domínio acadêmico ou empresarial, e essa informação somente é um “novo” conhecimento quando apropriada pelo indivíduo por meio de relações cognitivas, ou seja, só se pode denominar informação se a compreendemos (FADEL *et al*., p.14, 2010). Estes partem do pressuposto de que a busca, o uso e apropriação da informação está relacionada à uma ação.

Os ambientes organizacionais também se apoiam por informação e o processo de aprendizagem organizacional a desenvolve e fortalece. A aprendizagem organizacional se dá quando os colaboradores se envolvem nas transformações do ambiente e as correções se dão por meio de modificações estratégicas e normas. Ou seja, uma organização aprende construindo, testando e reconstruindo sua teoria de ação (CHOO, 2003, p.348).

A aprendizagem organizacional é um processo dual, pois simultaneamente relaciona e isola, associa e dissocia, analisa e sintetiza, proporcionando a ação (FADEL *et al*., p.17, 2010).

Sabe-se que existe grande produção informacional nas organizações e que ela precisa ser estruturada para garantir acesso e uso, ou seja, a informação precisa ser gerenciada para que haja uma construção de conhecimento organizacional. Por isso, a implantação de um modelo de Gestão da Informação (GI) é necessário, determinando procedimentos de coleta, tratamento e uso da informação, de forma a compor o seu ciclo de vida, já que o universo informacional é dinâmico (MOLINA *et al*., p.147, 2010).

2.3.7.2 Gestão da Informação

A origem do termo *information* (*resource*) *management*, ou, gerenciamento de informação, é creditada ao Paperwork Reduction Act de 1980, que demanda a adoção de boas práticas de gestão da informação nas agências federais norte-americanas. Em contrapartida, Black e Brunt sugerem que esse conceito é mais antigo, de 1850, a partir das estruturas administrativas de empresas de negócios, indústrias que aumentavam em grande escala, com sistemas de informações mais complexos (MARCHIORI, 2014). Com o volume de informação, era necessário planejar e sistematizar atividades de gestão da informação, inexistentes na época. Também se comenta que os serviços de inteligência e contraespionagem, surgidos no início do século XX e que precedem a tecnologia dos computadores, são reconhecidos como pioneiros nas atividades de gestão da informação (BLACK; BRUNT, 1999 *apud* Marchiori, 2014).

Barbosa (2008) discorre que a origem moderna gestão da informação pode ser encontrada nos trabalhos de Paul Otlet, cujo livro *Traité de documentation*, publicado em 1934, foi um marco fundamental do desenvolvimento da gestão da informação, disciplina que, na época, era conhecida como documentação.

Além dos autores citados, Vanevar Bush e Frederick Hayek destacam-se como precursores da moderna gestão da informação e do conhecimento. Em 1945, ambos publicaram trabalhos importantes. Bush publicou o artigo intitulado *As we may think*, no qual fez relatos sobre uma máquina chamada Memex, na qual

poderiam ser armazenados livros, registros que eram consultados com grande velocidade e flexibilidade. Hakey publicou o artigo intitulado *The use of knowledge in society*, descrevendo o problema do conhecimento que não se encontra de forma integrada, mas apenas em pedaços e incompletos (BARBOSA, 2008).

Portanto, a gestão da informação lida com o universo de documentos, dos mais diversos tipos, os quais são produzidos, armazenados e utilizados em um contexto organizacional (BARBOSA, 2008), ou seja, ela interage com vários processos dentro da organização. Um dos modelos propostos para lidar com a gestão da informação é destacado a seguir.

2.3.7.3 Ecologia da Informação

Um autor contemporâneo sobre a gestão da informação é Thomas Davenport, que traz contribuições expressivas no sentido de divulgar a gestão da informação para o contexto empresarial. No livro intitulado, Ecologia da Informação (DAVENPORT, 1998), o autor apresenta a relação estratégica da política e do comportamento pessoal à informação, visando enxergar o ambiente organizacional em um modelo holístico de pensar, não apenas com a visão de um único profissional.

A ecologia da informação recebe essa denominação por ter características encontradas no estudo da Ecologia, como: a ênfase na observação e descrição de ambientes, na integração entre diversos tipos de informação, na descrição de comportamentos e no reconhecimento de mudanças evolutivas, sendo esses itens atributos-chave para a Ecologia.

A integração dos diversos tipos de informação se dá pela administração da informação computadorizada e não-computadorizada, estruturada e não-estruturada, via texto, áudio e vídeo. Além disso, tem sido impulsionada não apenas pelas novas tecnologias, mas também pela necessidade de melhorar o aproveitamento de formas não-tradicionais de informação. Nesse ínterim, há a possibilidade dessas informações serem sigilosas, pessoais, pessoais sensíveis, evidenciando aqui a importância de se saber que tipo de informação é, para quem, o porquê de seu uso, podendo-se remeter à LGPD.

O atributo ecológico de reconhecimento de mudanças evolutivas se refere assim como esperamos que as ecologias físicas evoluam ao longo do tempo, devemos admitir que as ecologias informacionais mudem constantemente (DAVENPORT e PRUSAK, P.42, 2002), ou seja, o ambiente informacional irá se transformar, precisará se adaptar. Remetendo à LGPD, uma Lei, muda o ambiente em que ela será aplicada. A organização que não previa mudanças agora deverá parar para se adequar e pensar em formas de se adaptar.

A maioria dos gerentes de TI reconhecem que os ambientes informacionais estão sempre mudando e já sabem, a essa altura, que as abordagens tradicionais de modelagem e desenvolvimento de sistemas pode facilmente tornar-se obsoleta antes de ser finalizada (DAVENPORT e PRUSAK, P.44,2002). Nesse item, pode-se correlacionar com o conceito de *Privacy by Design*, muitas vezes mudanças nos sistemas pensando na privacidade deverão ocorrer para atender à Lei.

Com relação ao atributo observação e descrição, Davenport e Prusak, revelam a necessidade de tornarmos mais descritivos ao gerenciamento da informação, ou seja, dando mais ênfase a descrição do que acontece no presente que ao planejamento futuro. Os autores citam, como exemplo nos processos informacionais, elaborando uma compreensão profunda dos processos existentes antes de projetar novos, dando ênfase ao concreto. No tocante a Lei, a existência de mapas de processos informacionais atuais da organização são de extrema valia para auxiliar no processo de mapeamento dos dados pessoais ou inventário de dados.

Por fim, a ênfase no comportamento pessoal e informacional, ou seja, requer a participação dos funcionários, mas além disso é também não apenas oferecer a informação, como também facilitar o seu uso efetivo. Essa preocupação com o que o funcionário faz com a informação e como ele pode manipulá-la podemos também inserir no contexto da LGPD, onde os funcionários deverão receber treinamentos e capacitação sobre à Lei.

Davenport e Prusak desenvolveram com base nos atributos acima um “modelo ecológico” para gerenciamento da informação (BARBOSA, 2008). Sendo que o ambiente informacional, constitui-se pelos seguintes elementos (DAVENPORT e PRUSAK, 2002):

a) estratégia da informação girando em torno da pergunta: “o que queremos fazer com a informação nesta empresa?”

b) política da informação, sendo componente crítico em que envolve o poder proporcionada pela informação e as responsabilidades da direção em seu gerenciamento e uso.
c) a cultura e o comportamento em relação a informação, ou seja, o comportamento sendo positivo ou negativo forma a cultura da empresa, determinando se os envolvidos valorizam a informação, se a compartilham entre outros.
d) a equipe de informação, neste item o autor expõe que as pessoas são os melhores “meios” para identificar, categorizar, filtrar, interpretar e integrar a informação.
e) os processos de administração informacional este componente se refere em como o trabalho é feito, definindo os processos e como todas as atividades desenvolvidas.
f) a arquitetura da informação, nesse modelo a arquitetura se remete a um guia para estruturar a localizar a informação dentro de uma organização.

Observa-se que os dados que estão na organização, podem estar em qualquer componente do ambiente informacional transpassando esse ambiente, muitas vezes sem regra ou equilíbrio.

2.3.7.4 Cultura Organizacional

Garcia e Fadel (p. 214, 2010) comentam que a comunicação e os processos decisórios nas organizações são estabelecidos segundo os pressupostos culturais. Ou seja, a cultura de uma organização é entendida como um conjunto de pressupostos e valores compartilhado por um determinado grupo, consequentemente exercendo impacto sobre a GI e Gestão do Conhecimento (GC).

No dia a dia, no contato com os membros da organização, vai se estabelecendo “normas” de conduta e comportamento, estes compartilhados com outros membros até que sejam transformados em bases para a forma de pensar e agir do grupo.

A cultura informacional é aquela que se reconhece o valor e a utilidade da informação com objetivo de alcançar o sucesso operacional e estratégico, onde a informação estabelece a base de tomada de decisões organizacionais (CURRY e MOORE, p. 94, 2003).

Para uma mudança de cultura, relacionada as novas práticas que a LGPD exige, dependerá do quanto as ações dos líderes terão sucesso, assim como menciona Garcia e Fadel (p.213, 2010) o grau de adaptação e modificação depende do líder, proporcionando a equipe coesa no sentido de aprovação das novas práticas, até que essas sejam incorporadas definitivamente e transformadas em elemento integrante da nova cultura organizacional modificada.

2.4 ESTRUTURA CONCEITUAL (FRAMEWORK CONCEITUAL)

De acordo com dicionário Michaelis (2021), “estrutura é uma parte de algo que determina...e lhe dá sustentação; segundo o dicionário de Cambridge, "*Framework* é uma estrutura que serve de suporte para se construir algo”. Já conceito é uma “representação mental das características gerais de um objeto, a compreensão que se tem de uma palavra” (MICHAELIS, 2021). Sendo assim, uma estrutura conceitual é um suporte que serve de apoio e representa características de um objeto.

Segundo Jabareen (2009), estruturas conceituais são produtos de processos qualitativos de teorização que fornecem a compreensão abrangente de um fenômeno e para explorar o processo de criação de estruturas conceituais, primeiro define-se os conceitos e depois a estrutura conceitual.

O papel dos *frameworks* é facilitar o entendimento e a comunicação entre os participantes de uma situação que possam ter diferentes perspectivas, assim como suportar o processo de tomada de decisão e de resolução de problemas, fornecendo as categorias e representações normalmente em uma linguagem de símbolos (ODEH e KAMM, 2003).

Uma estrutura conceitual é muito benéfica para desenvolver questões de investigação e visualizar melhor um problema. Geralmente, é construído de forma interativa. De acordo com Miles e Huberman (1994) *apud* Latham (2016), "Uma estrutura conceitual explica, quer graficamente, quer de forma narrativa, as principais coisas a estudar os fatores chave, as construções ou variáveis e as presumíveis relações entre elas".

Para Shehabuddeen; Probert; Phaal (2000), os *frameworks* são aplicados para comunicar ideias e descobertas a uma comunidade ampliada e para que seja possível produzir comparações entre situações e abordagens diversas. Ademais,

possibilitam definir o domínio ou limites de uma situação, descrever o contexto ou arguir a validade de uma descoberta.

As vantagens de uma estrutura conceitual são: flexibilidade, capacidade de modificação e compreensão. Essas estruturas podem ser desenvolvidas e construídas através de um processo de análise qualitativa, fornecendo um entendimento do objeto a ser estudado.

Nesta pesquisa, serão estudadas as estruturas conceituais que foram criadas por outros pesquisadores com o intuito de auxiliar as organizações a entrarem em conformidade com a LGPD.

3 PROCEDIMENTOS METODOLÓGICOS

Nesta seção de encaminhamentos metodológicos explicita-se a especificação do problema e das perguntas de pesquisa, a matriz de amarração, o desenho da pesquisa, a caracterização da pesquisa, a coleta de dados, assim como uma análise parcial dos dados. Então, aborda-se a validade dos dados da pesquisa.

3.1 ESPECIFICAÇÃO DO PROBLEMA E DAS PERGUNTAS DE PESQUISA

A partir do exposto nas seções anteriores do trabalho, define-se como problema de pesquisa dessa dissertação: **Quais as diferenças e similaridades das estruturas de dados (*frameworks*) de adequação à LGPD encontrados na literatura acadêmica fundamentando-se nos conceitos inerentes à Lei e nos artigos que mais incidiram multas da GDPR, no período de agosto de 2018 e maio de 2022?**

Portanto, os objetivos que acompanham esse problema de pesquisa são:

a) Descrever uma breve evolução legislativa, a LGPD e seus conceitos inerentes.

b) Buscar quais são as estruturas de dados (*frameworks*) existentes na literatura.

c) Investigar os artigos da LGPD que têm mais chances de resultar em multas, baseando-se na GDPR.

d) Compreender as diferenças e similaridades entre as estruturas de dados (*frameworks*).

3.2 MATRIZ DE AMARRAÇÃO

A matriz de amarração está demonstrada no **Quadro 4** a seguir.

QUADRO 4 – Matriz

Pergunta Problema: Quais as diferenças e similaridades das estruturas de dados (*frameworks*) de adequação à LGPD encontrados na literatura acadêmica fundamentando-se nos conceitos inerentes à Lei e na aplicação de multas da GDPR, no período de agosto de 2018 e maio de 2022?
Objetivo Geral: Demonstrar as diferenças e similaridades das estruturas de dados (*frameworks*) de adequação à LGPD disponíveis na literatura entre agosto de 2018 e maio de 2022.

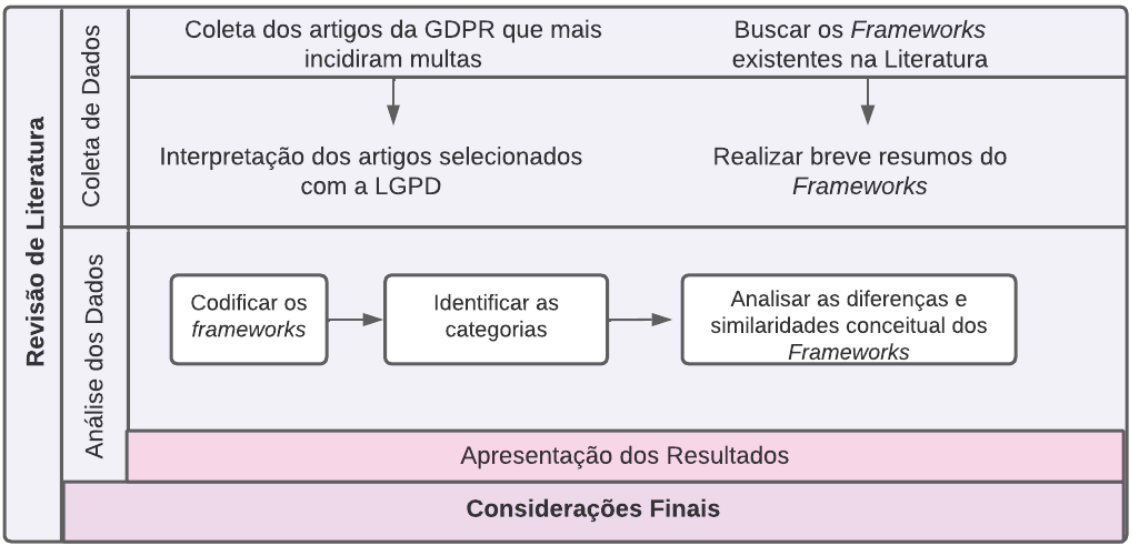
Objetivos Específicos	Referencial Teórico Relacionado
1. Descrever uma breve evolução legislativa, a LGPD e seus conceitos inerentes.	A Lei foi criada com o objetivo de regulamentar o tratamento dos dados pessoais, inclusive em meios digitais [...] com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural (BRASIL, 2021). Além disso, os conceitos inerentes a Lei como anonimização, segurança, privacidade, governança de dados auxiliarão no entendimento da aplicação à Lei.
2. Buscar quais são as estruturas de dados (*frameworks*) de adequação à Lei na literatura.	De acordo com Cambridge Dicionário "*Framework* é uma estrutura que serve de suporte para se construir algo. O papel dos *Frameworks* em facilitar o entendimento e comunicação entre participantes de uma situação que possam ter diferentes perspectivas. Suportam o processo de tomada de decisão e de resolução de problemas, fornecendo as categorias e representações normalmente em uma linguagem de símbolos (ODEH e KAMM, 2003).
3. Investigar os artigos da LGPD que têm mais chances em resultar em multas.	Será usada a metodologia apresentada neste capítulo nas seções 3.5.1 e 3.5.2.
4. Compreender as diferenças e similaridades das estruturas de dados (*frameworks*).	Será usada a metodologia relatada neste capítulo.

Fonte: A autora (2022).

3.3 DESENHO DA PESQUISA

Apresenta-se o desenho da pesquisa na **Figura 3**.

FIGURA 3 – DESENHO DE PESQUISA



Fonte: A autora (2022).

3.4 CARACTERIZAÇÃO DA PESQUISA

No seu propósito, esta pesquisa se caracteriza como descritiva em relação às análises das estruturas de dados (*frameworks*), ou seja, na descrição das características de um fenômeno e estabelecendo a relação entre variáveis (GIL, p.42, 2002).

Quanto à natureza dos dados, a pesquisa se caracteriza como qualitativa, na qual utilizou-se da técnica de análise de conteúdo (BARDIN, 2021; SILVA e LEÃO, 2018).

Quanto ao delineamento ou forma, a pesquisa se encaixa como uma pesquisa bibliográfica, na qual baseia-se em um material já elaborado, constituído principalmente de livros e artigos científicos (GIL, p.44, 2002). Também se caracteriza como documental, pois analisou os dados coletados no sítio eletrônico do *Enforcement Tracker.*

3.5 COLETA DE DADOS

Nesta seção, são apresentadas as técnicas de coleta de dados empregadas na pesquisa, divididas por objetivo específico.

3.5.1 Pesquisa bibliográfica, pesquisa documental

Como citado anteriormente, será realizada uma pesquisa bibliográfica, cuja principal objetivo reside no fato de permitir ao pesquisador a cobertura de uma variedade de fenômenos mais ampla do que poderia pesquisar diretamente (GIL, p.45, 2002).

E uma pesquisa documental, que se utiliza de materiais que não recebem um tratamento analítico sendo fontes mais diversificadas e dispersas (GIL, p.46, 2002) ao coletar dados do sítio eletrônico *Enforcement Tracker*.

A pesquisa documental fornece informações já sintetizadas, reduzindo custos e tempo. Os documentos ainda podem ser acessados quando for conveniente ao pesquisador (CRESWELL, 2010). Para Yin (2006) o método “coletar” refere-se à acumulação de objetos (documentos, artefatos) e que podem ser úteis pelos detalhes que contêm.

Para atender o primeiro objetivo específico, ou seja, descrever uma breve evolução legislativa, LGPD e seus conceitos inerentes, foi empregada a técnica de pesquisa bibliográfica. Para isso, aplicaram-se as estratégias de busca com os descritores do assunto nas bases de dados da *Scopus*, *Web of Science* e *Dimensions* no dia 23 de março de 2022, sendo esses descritores: LGPD* OR "*General Personal Data Protection Law*" OR "*Law 13.709*".

Para a busca na base de dados *Scopus*, os termos pesquisados na opção “tópicos”, que abrange resumo, título e palavra-chave, resultou inicialmente em 63 publicações. Em seguida, foi aplicado o filtro de artigos de acesso aberto (*all open access*), chegando ao número de 15 publicações. Não foi necessário acrescentar a delimitação de tempo por conta da redução de números publicações encontradas.

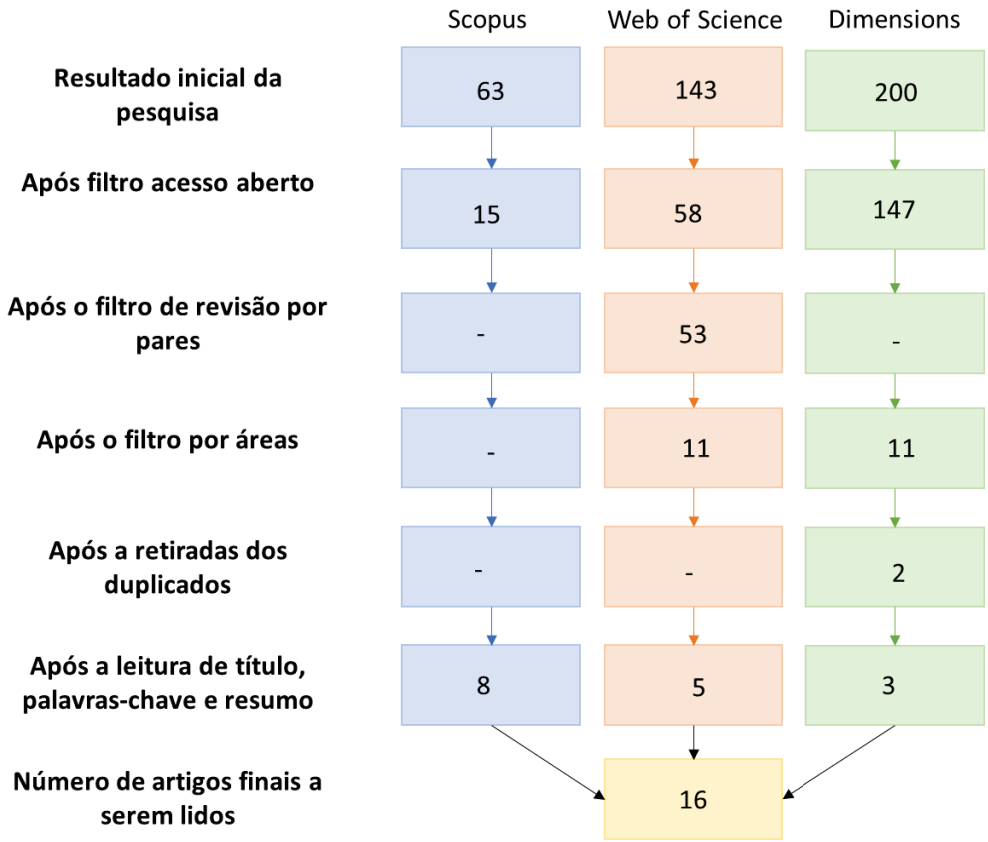
Para a segunda base de dados, *Web of Science*, os mesmos termos foram aplicados na categoria referente ao resumo, título e palavras-chave, resultando em 143 publicações. Então, foram aplicados os seguintes filtros: artigos de acesso aberto (*all open access*), resultando em 58 publicações e, em seguida, o filtro de revisão por pares, resultando em 53 artigos. Notou-se que retornaram artigos de áreas distintas da pesquisa, “confundindo o termo LGPD com algumas outras siglas”, então, foi aplicado o filtro de categorias por área de estudo: *Law, Computer Science Interdisplinary Applications, Multidiplinary Sciences, Business, Computer Science Information Systems*, resultando em 11 artigos.

Por conta de o número total de artigos ser reduzido, realizou-se também a busca na base *Dimensions*, sendo aplicados os mesmos termos na opção “todos os campos”, totalizando 200 artigos. Em seguida, aplicou-se o filtro de acesso aberto, obtendo-se um total de 147 artigos. Depois, aplicou-se o filtro de categorias de área de pesquisa: *Law and Legal Studies, Law, Information and Computing Sciences, Technology, Information Systems, Data Format, Business and Management, Distributed Computing, Other Information and Computing Sciences e Communications Technology*, resultando em 19 publicações.

De um total de 45 artigos, que tiveram seus títulos, palavras-chave e resumos lidos, selecionou-se 8 artigos da *Scopus*, 5 da *Web of Science* e 3 da *Dimensions*.

A **Figura 4** mostra as etapas da busca para o primeiro objetivo:

FIGURA 4 – RESUMO DA BUSCA



FONTE: A autora (2022).

Além desses artigos selecionados, também foram usados os seguintes livros para compor o primeiro objetivo específico, expostos no **Quadro 5**.

QUADRO 5 – LIVROS

Autores	Livros
Bruno R. Bioni	Proteção de Dados Pessoais – A função e os limites do consentimento
Daniel J. Solove	*Understanding Privacy*
Tarcisio Teixeira	A LGPD e o *e-commerce*
William Stallings	*Information Privacy Engineering and Privacy by Design*
Chun Wei Choo	A organização do conhecimento: como as organizações usam a informação para criar significado, construir conhecimento e tomar decisões.

FONTE: A autora (2022).

Para atender o segundo objetivo, ou seja, buscar quais são as estruturas/ *frameworks* de adequação à Lei na literatura, foi empregada a técnica de pesquisa bibliográfica. Para isso, aplicaram-se as estratégias de busca com os descritores do assunto nas bases de dados da *Scopus*, *Web of Science* e *Dimensions e Google* Acadêmico, no dia 22 de maio de 2022, com os seguintes descritores: “LGPD” AND "*Frameworks*".

Para a busca nas bases de dados *Scopus* e *Web of Science* os termos pesquisados na área que abrange resumo, título e palavra-chave, resultaram em 2 publicações em cada base, as quais foram descartadas por não terem relação com o assunto. Na *Dimensions*, os mesmos termos foram aplicados na categoria “todos os campos”, retornando 29 artigos que não tinham relação com o assunto e que também foram descartados.

Assim, justificou-se a procura no *Google* Acadêmico com os mesmos termos citados, que resultou em 5 documentos: 3 dissertações, 1 monografia e 1 artigo. Nesse momento, encontrou-se as propostas de *frameworks* de adequação à LGPD e limitou-se a leitura aos trabalhos de dissertações e o artigo, justificando-se pela quantidade de conteúdo nesses documentos.

Para responder ao terceiro objetivo, ou seja, buscar quais são os artigos da LGPD que tem mais chances de resultar em multas, aderiu-se a técnica da pesquisa documental com a seguinte estratégia: leitura da terceira edição do relatório do ano de 2022, disponível no sítio eletrônico *Enforcement Tracker*, que é uma ferramenta que registra e contabiliza as penalidades aplicadas com base na GDPR, em

decorrência de descumprimentos aos termos da Lei, organizada pela empresa CMS *Law, Tax, Future*. Essa organização é composta por mais de 70 escritórios em mais de 40 países e mais de 5000 advogados, cujo relatório é lançado anualmente com informações de acompanhamento da aplicação da Lei, como: estatísticas, casos de maiores multas aplicadas e as causas que mais incidiram na aplicação da multa. Além disso, utilizou-se outro recurso nessa mesma ferramenta, um buscador de todas as multas aplicadas na União Europeia e na Inglaterra. Exemplo desse buscador está representado na **Figura 5**.

FIGURA 5 – BUSCADOR ENFORCEMENT TRACKER

GDPR Enforcement Tracker

tracked by CMS law·tax·future

The CMS.Law GDPR Enforcement Tracker is an overview of fines and penalties which data protection authorities within the EU have imposed under the EU General Data Protection Regulation (GDPR, DSGVO). Our aim is to keep this list as up-to-date as possible. Since not all fines are made public, this list can of course never be complete, which is why we appreciate any indication of further GDPR fines and penalties. *Please note that we do not list any fines imposed under national / non-European laws, under non-data protection laws (e.g. competition laws / electronic communication laws) and under "old" pre-GDPR-laws.*

New features: "ETid" and "Direct URL"!
We have assigned a unique and permanent ID to each fine in our database, which makes it possible to precisely address fines, e.g. in publications. Once an "ETid" has been assigned to a fine, it remains the same, even if the fine is overturned or amended by courts at a later date, or if we add fines that were issued chronologically before. The "Direct URL" (click "+" or on a specific ETid to view details of a fine) can be used to share fines online, e.g. on Twitter or other media.

Show 10 entries — Search:

ETid	Country	Date of Decision	Fine [€]	Controller/Processor	Quoted Art.	Type	Source
ETid-1316	ITALY	2021-09-29	11,000	Territorial Administration of the Government of Genoa	Art. 5 (1) a), c) GDPR, Art. 6 (1) c), e) Art. 6 (2) GDPR, Art. 6 (3) b) GDPR GDPR, Art. 2-ter (1), (3) Codice della privacy	Insufficient legal basis for data processing	link
ETid-1315	SPAIN	2022-07-26	800	EFS MANTENIMIENTO Y SERVICIOS TÉCNICOS, S.L.	Art. 5 (1) f) GDPR	Non-compliance with general data processing principles	link
ETid-1314	SPAIN	2022-07-26	2,500	Homeowners Association	Art. 5 (1) f) GDPR	Non-compliance with general data processing principles	link

FONTE: *Enforcement Tracker* (2022).

A intenção de usar esse buscador foi a possibilidade de pesquisar pelas causas das multas, obtendo como resultado as multas aplicadas por país, as datas das decisões e quais os artigos da GDPR incidiram em cada causa. Então, no dia 09 de junho de 2022 foram realizadas as buscas e para cada causa foram extraídas as informações e colocadas em uma planilha do Excel.

3.5.2 Identificação dos artigos da GDPR

Essa seção tem a função de explicar como foi realizada a identificação dos artigos da GDPR.

Inicialmente, no item 3.5.1 foi explicitada onde ocorreram as buscas, quando e que tipo de pesquisa foi realizada.

Após a leitura do relatório *Enforcement Tracker* foi possível identificar quais são as causas mais desrespeitadas pelas organizações na União Europeia e na Inglaterra, exibidas no **Quadro 6**.

QUADRO 6 – CAUSAS DE MULTAS DO GDPR (TRADUZIDA)

Ranking	Types	Tipos
1º	*insufficient legal basis*	base legal insuficiente
2º	*non-compliance*	não conformidade
3º	*insufficient technical and organisational measures to ensure information security*	medidas técnicas e organizacionais insuficientes para garantir a segurança da informação
4º	*insufficient fulfielment of data subjects right*	cumprimento insuficiente do direito dos titulares dos dados
5º	*insufficient fulfiment of information obligations*	cumprimento insuficiente das obrigações de informação
6º	*insufficient cooperation with supervisory authority*	cooperação insuficiente com a autoridade supervisora
7º	*insufficient fulfielment of data breach notification obligations*	cumprimento insuficiente das obrigações de notificação de violação de dados
8º	*insufficient involvement of data protection officer*	envolvimento insuficiente do responsável pela proteção de dados
9º	*insufficient data processing agreement*	contrato de processamento de dados insuficiente

FONTE: *Enforcement Tracker* (2022).

Com a identificação das causas, foi possível então utilizar-se da ferramenta de busca das multas, digitando no campo *type* e filtrando todas as multas. Ao filtrar era obtido como resultado: o identificador (id), o país, a data da decisão, o valor da multa, a empresa e os artigos da Lei da GDPR.

Por exemplo para o tipo (*insufficient legal basis)* os resultados encontrados eram: **Figura 6** (planilha com algumas linhas de exemplo):

FIGURA 6 – PLANILHA DADOS ENCONTRADOS

pais	data da de	valor	empresa	quoted art.	tipo
AUSTRIA	02/08/2021	2,000,000	Unser Ö-Bonus Club GmbH	Art. 6 GDPR, Art. 7 GDPR, Art. 12 GPDR	Insufficient legal basis for data processing
AUSTRIA	01/07/2019	11	Private person (soccer coach)	Art. 6 GDPR	Insufficient legal basis for data processing
AUSTRIA	20/12/2018	2,2	Private person	Art. 5 (1) a) GDPR, Art. 5 (1) c) GDPR, Art. 6 (1) GDPR, Art. 13 GDPR	Insufficient legal basis for data processing
AUSTRIA	10/07/1905	1,8	Kebab restaurant	Art. 5 GDPR, Art. 13 GDPR, Art. 14 GDPR	Insufficient legal basis for data processing

FONTE: A autora (2022).

É possível visualizar na coluna (*quoted. art.*) que cada linha possui mais de um artigo, mas como a intenção do trabalho era coletar o número de artigos que apareciam por causa, foi necessário quebrar as linhas da coluna, para conseguir contar quantas vezes apareciam, por exemplo o art. 5º. Realizou-se o trabalho de quebra através da cópia da coluna no software *notepad*++ e substituindo a vírgula por uma quebra de linha, resultando por exemplo na seguinte **Figura 7**:

FIGURA 7 – EXEMPLO QUEBRA DOS ARTIGOS

Artigos
Art. 5 (1)
Art. 5 (1) (2)
Art. 5 (1) (2)
Art. 5 (1) (2)
Art. 5 (1) a)
Art. 5 (1) a)
Art. 5 (1) a)
Art. 5 (1) a)
Art. 5 (1) a) - d) GDPR

FONTE: A autora (2022).

Com isso, foi possível criar uma tabela juntando os tipos e os artigos, ela foi importada no *software Power Bi* e iniciou-se o processo de criação de relatórios e tabelas para visualização do resultado. A partir dos dados, obteve-se a matriz na **Figura 8**:

FIGURA 8 – MATRIZ DAS CAUSAS POR ARTIGOS

Causas	% de Artigos por Causa	Total de Artigos Repetidos
⊞ Contrato de processamento de dados insuficiente	0,41%	10
⊞ Envolvimento insuficiente do responsável pela proteção de dados	0,81%	20
⊞ Cumprimento insuficiente das obrigações de notificação de violação de dados	1,54%	38
⊞ Cooperação insuficiente com a autoridade supervisora	2,64%	65
⊞ Cumprimento insuficiente das obrigações de informação	6,41%	158
⊞ Cumprimento insuficiente do direito dos titulares dos dados	10,84%	267
⊞ Medidas técnicas e organizacionais insuficientes para garantir a segurança da informação	18,23%	449
⊞ Não Conformidade	23,39%	576
⊞ Insuficiente Base Legal	35,73%	880
Total	100,00%	2463

FONTE: A autora (2022).

Na **Figura 8** é possível observar na coluna que indica o número total de artigos repetidos uma variação muito grande de valores, com alguns muito baixos (10, 20, 38) e outros mais altos, acima de 200. Com isso, optou-se por realizar um corte para selecionar os itens que somassem pelo menos 10% de artigos por causa, ou seja, aqueles que mais se repetiram, resultando nos quatro últimos itens da tabela, destacado em vermelho. Após essa seleção, passou-se a analisar individualmente os artigos que incidiram nessas causas, representada nas **Figuras 9, 10, 11 e 12**. As figuras mostram o artigo na primeira coluna, a porcentagem de repetição e a contagem do número de repetições do artigo.

FIGURA 9 – DETALHAMENTO DA CAUSA DE NÃO CONFORMIDADE

Causa	% de Art. por Causa	Rep. do Nº do Artigo
Não Conformidade	**100,00%**	**576**
5	44,27%	255
13	10,42%	60
6	9,03%	52
32	5,21%	30
9	3,65%	21
35	3,13%	18
12	2,95%	17
25	2,95%	17
14	2,43%	14
30	1,56%	9
17	1,39%	8
21	1,39%	8
24	1,39%	8
15	1,22%	7
37	1,22%	7
7	1,04%	6
28	1,04%	6
33	1,04%	6
16	0,69%	4
22	0,69%	4
34	0,69%	4
18	0,35%	2
19	0,35%	2
20	0,35%	2
27	0,35%	2
44	0,35%	2
58	0,35%	2
23	0,17%	1
46	0,17%	1
48	0,17%	1
Total	**100,00%**	**576**

FONTE: A autora (2022).

FIGURA 10 – DETALHAMENTO DA CAUSA BASE LEGAL INSUFICIENTE

Causa	% de Art. por Causa	Rep. do Nº do Artigo
Insuficiente Base Legal	**100,00%**	**880**
6	43,52%	383
5	28,18%	248
13	4,89%	43
9	4,77%	42
12	3,52%	31
21	2,27%	20
7	2,16%	19
14	1,70%	15
17	1,59%	14
25	1,14%	10
28	0,91%	8
15	0,80%	7
24	0,80%	7
32	0,80%	7
35	0,68%	6
31	0,45%	4
10	0,34%	3
30	0,34%	3
29	0,23%	2
36	0,23%	2
37	0,23%	2
8	0,11%	1
33	0,11%	1
58	0,11%	1
130	0,11%	1
Total	**100,00%**	**880**

FONTE: A autora (2022).

FIGURA 11 – DETALHAMENTO DA CAUSA CUMPRIMENTO INSUFICIENTE DOS DIREITOS DOS TITULARES DE DADOS

Causa	% de Art. por Causa	Rep. do Nº do Artigo
Cumprimento insuficiente do direito dos titulares dos dados	**100,00%**	**267**
15	23,22%	62
12	16,85%	45
17	11,24%	30
21	10,11%	27
5	8,24%	22
13	5,99%	16
6	4,49%	12
14	4,12%	11
25	3,00%	8
48	2,62%	7
28	1,87%	5
18	1,50%	4
23	1,12%	3
24	1,12%	3
31	1,12%	3
32	0,75%	2
44	0,75%	2
16	0,37%	1
30	0,37%	1
34	0,37%	1
58	0,37%	1
166	0,37%	1
Total	**100,00%**	**267**

FONTE: A autora (2022).

FIGURA 12 – DETALHAMENTO DA CAUSA MEDIDAS TÉCNICAS E ORG. INSUFICIENTES A SEGURANÇA DA INFORMAÇÃO

Causa	% de Art. por Causa	Rep. do Nº do Artigo
Medidas técnicas e organizacionais insuficientes para garantir a segurança da informação	**100,00%**	**449**
32	52,34%	235
5	22,72%	102
33	4,01%	18
25	3,79%	17
28	2,90%	13
6	2,67%	12
24	2,45%	11
9	1,56%	7
34	1,56%	7
13	1,11%	5
29	1,11%	5
35	0,89%	4
3	0,45%	2
14	0,45%	2
17	0,45%	2
37	0,45%	2
11	0,22%	1
15	0,22%	1
26	0,22%	1
36	0,22%	1
58	0,22%	1
Total	**100,00%**	**449**

FONTE: A autora (2022).

Analisando os dados das tabelas e com o intuito de selecionar apenas os artigos que mais se destacaram por causa (destacados em vermelho), optou-se por manter o critério de corte de 10% para todas as causas apresentadas nas figuras de 9 a 12. Por exemplo, nas **Figuras 10** e **12** é possível verificar que os dois primeiros artigos de ambas apresentam as maiores porcentagens e os terceiros artigos correspondem a menos de 5% das causas de multas. Já nas **Figuras 9** e **11**, mais artigos com porcentagens menores se destacaram. Assim, o critério de corte de 10% para todas as causas visou balancear os artigos que mais incidiram em multa em cada causa.

Com isso, a pesquisa resultou nos seguintes artigos que serão interpretados e correspondidos à LGPD: base insuficiente legal: artigos 6º e 5º. Não conformidade: artigos 5º e 13. Medida técnicas e organizacionais insuficientes para garantir a segurança da informação: artigos 32 e 5º e cumprimento insuficiente do direito dos titulares dos dados: artigos 15, 12, 17 e 21.

3.5.3 Validade da análise das estruturas de dados (*frameworks*)

A validade da descrição dos *frameworks* pode ser comprovada a partir da triangulação das evidências de múltiplas fontes. Essa prática é extremamente importante para todas as formas de pesquisa empírica, não apenas de pesquisa qualitativa (YIN, 2016).

A ideia de triangulação vem da navegação, em que a intersecção de três pontos de referência determina se os dados de uma ou mais fontes convergem ou levam ao mesmo resultado. Ao demonstrar uma convergência, mais fortes serão as evidências, em que a triangulação ideal não é apenas a confirmação das três fontes, mas também o uso de três tipos diferentes de fontes (YIN, p.86 - 145, 2016).

Neste estudo, a validade é comprovada com a triangulação das seguintes fontes: os conceitos inerentes à Lei encontrados no referencial teórico (bases de dados), os artigos da LGPD correspondentes aos artigos que mais geraram multas da GDPR (*Enforcement Tracker*) e a categorização de variáveis utilizadas na construção dos *frameworks*, como metodologia, validação dos *frameworks* e se foi aplicado na prática (análise da autora).

3.5.4 Análise de Conteúdo das estruturas de dados (*frameworks*)

O processo de análise de conteúdo foi baseado em Bardin (2021) e em Silva e Leão (2018), apresentando três passos para execução: pré-análise, exploração do material e tratamento dos resultados obtidos/interpretação.

Durante a pré-análise, foram escolhidos os documentos (corpus), que estão no **Quadro 7**. Na realização dessa análise foram selecionados somente os capítulos referentes à metodologia da construção do *framework* e o seu descritivo.

QUADRO 7 – DOCUMENTOS ENCONTRADOS

Identificador	Tipo	Autor	Ano	Local
1	Dissertação	Michelle Jociane Ali Zini	2020	Porto Alegre
2	Dissertação	Rogério Hérminio da Silva	2021	Araranguá
3	Dissertação	Artur Potiguara Carvalho	2021	Brasília

4	Artigo	Larama Ferreira, Marcelo T. Okano, Henry de Castro Lobo dos Santos	2021	Bauru

FONTE: A autora (2022).

Após isso, foram adicionados na ferramenta *Atlas.TI* [5] os arquivos das dissertações em formato *pdf*, numerados em ordem e realizada uma leitura flutuante.

O próximo passo da pré-análise foi a referenciação de índices e a elaboração de indicadores. Propôs-se, então, os seguintes índices no primeiro momento:

QUADRO 8 – ÍNDICES CRIADOS NA PRÉ-ANÁLISE

ME	Metodologia de criação do FW.
VAL	Validação do FW.
APL	Aplicação na Prática do FW proposto.
FW	Frameworks

FONTE: A autora (2023).

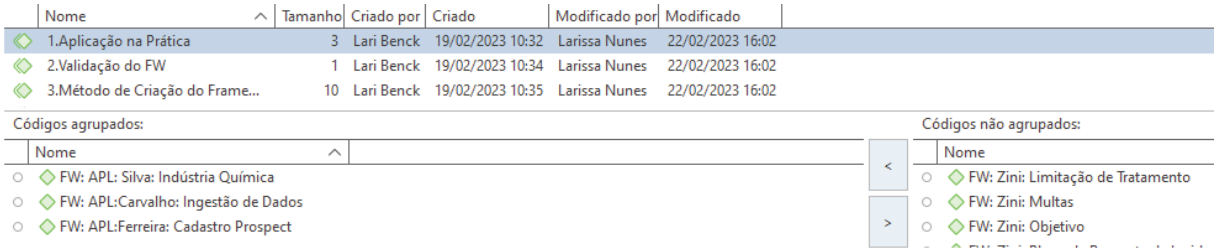
Após isso, deu-se sequência a exploração do material em que são realizadas as codificações e categorizações. Esse processo é importante, pois permite identificar aspectos que parecem importantes na pré-análise, mas que nem sempre serão utilizados na categorização (SILVA e LEÃO, 2018).

Após a referenciação, todos os códigos foram organizados em grupos denominados família, configurando-se como pré-categorias de análise. Esse processo é realizado no *layout* demonstrado na **Figura 13**.

No total, foram criados 135 códigos, divididos entre os 4 índices apresentados no quadro 9.

[5] ATLAS.ti é um software de análise de dados qualitativos assistido por computador que facilita a análise de dados qualitativos para pesquisa qualitativa, pesquisa quantitativa e pesquisa de métodos mistos. Disponível em: https://atlasti.com/pt.

FIGURA 13 – ORGANIZAÇÃO DOS CÓDIGOS EM FAMÍLIAS



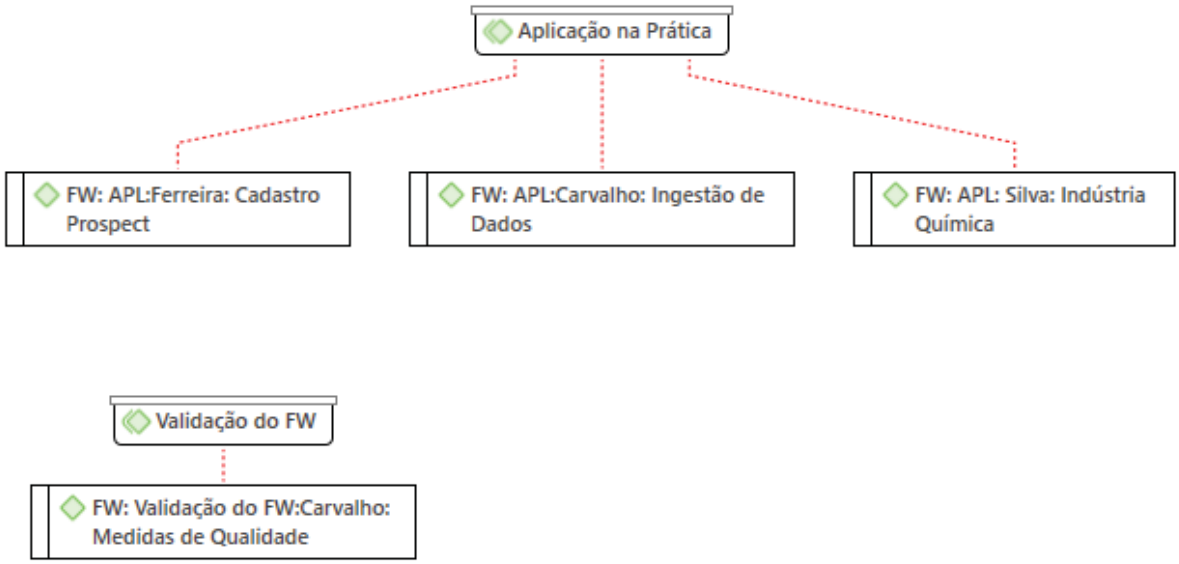
FONTE: A autora (2023).

Na **Figura 13** foram adicionados três códigos (APL: Silva: Industria Química, APL: Carvalho: Ingestão de Dados, APL: Ferreira: Cadastro Prospect) na família Aplicação na Prática. No lado esquerdo superior estão as famílias criadas a partir das codificações dos textos. No lado inferior aparecem os códigos que foram adicionados nessa família.

Ao organizar todos os códigos em famílias, iniciou-se a análise desses para selecionar quais índices seriam utilizados ou reformulados para dar prosseguimento à construção das categorias propriamente ditas (Silva e Leão, 2018). Para isso utilizou-se da funcionalidade chamada *network* (rede) onde organiza-se os códigos e famílias numa rede semântica semelhante a um mapa mental. Essa organização depende da leitura do analista e seu referencial teórico (Silva e Leão, 2018).

A **Figura 14** representa uma parte da rede, onde são exibidas as pré-categorias: aplicação na prática, validação do FW e método de criação do *framework*. Para a primeira categoria foram associados três índices encontrados nas dissertações, indicando que Ferreira, aplicou seu FW em um cadastro *prospect*, Carvalho aplicou utilizando uma ingestão de dados e Silva em uma Indústria Química. Na segunda categoria, observa-se um único índice em que Carvalho realizou a validação do seu FW.

FIGURA 14 – REDE DOS ÍNDICES E PRÉ-CATEGORIAS

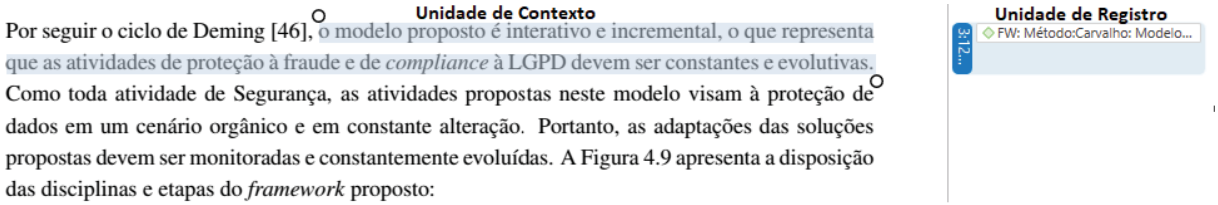


Fonte: A autora (2023).

A partir dessas redes e outras realizadas foi possível observar quais índices eram relevantes e quais não. Então, percebeu-se que o índice proposto inicialmente (FW) estava muito abrangente, ou seja, todos os códigos encontrados nas dissertações estavam sendo direcionados para ele. Assim, optou-se por dividir esse índice em outros quatro, que revalidam a revisão de literatura dessa pesquisa, sendo estes: governança de dados, LGPD (direitos dos titulares, art. 6º e art. 7º), privacidade (anonimização, pbd) e segurança da informação.

Nesse mesmo processo criou-se as unidades de registro a partir de temas e/ou palavras relevantes levantadas a partir dos índices. Para Bardin (2021), para que uma unidade de registro faça sentido é preciso explicitar o contexto em que ela está. A seleção de um trecho imediatamente anterior e/ou posterior é chamada de unidade de contexto. No *Atlas.ti*, o procedimento é semelhante aos códigos, tendo como nomenclatura o termo *quotation* (citação). Na **Figura 15** apresentou-se um exemplo de como foram realizados no texto os códigos e as citações que os representam.

FIGURA 15 - UNIDADE DE REGISTRO E CONTEXTO



Fonte: A autora (2023).

Por fim, a última etapa da exploração do material é a categorização, em que se verificou novamente as redes e suas associações e sucessivas organizações de códigos, família e citações para surgir as categorias. As categorias que surgiram e se tornaram finais são demonstradas na seção de Resultados.

4 RESULTADOS

Nesta seção de resultados, apresenta-se a descrição dos *frameworks*, suas redes e a interpretação dos artigos da GDPR correspondentes à LGPD.

4.1.1 Frameworks

No *framework* 1 (Zini), observou-se que a autora utilizou como metodologia a perspectiva de John R. Latham (2014), que divide a estrutura do projeto em dois grupos, o Grupo T composto por problema, objetivo, questões de pesquisa e estrutura conceitual e o Grupo U composto por revisão bibliográfica, coleta de dados, análise de dados e conclusões.

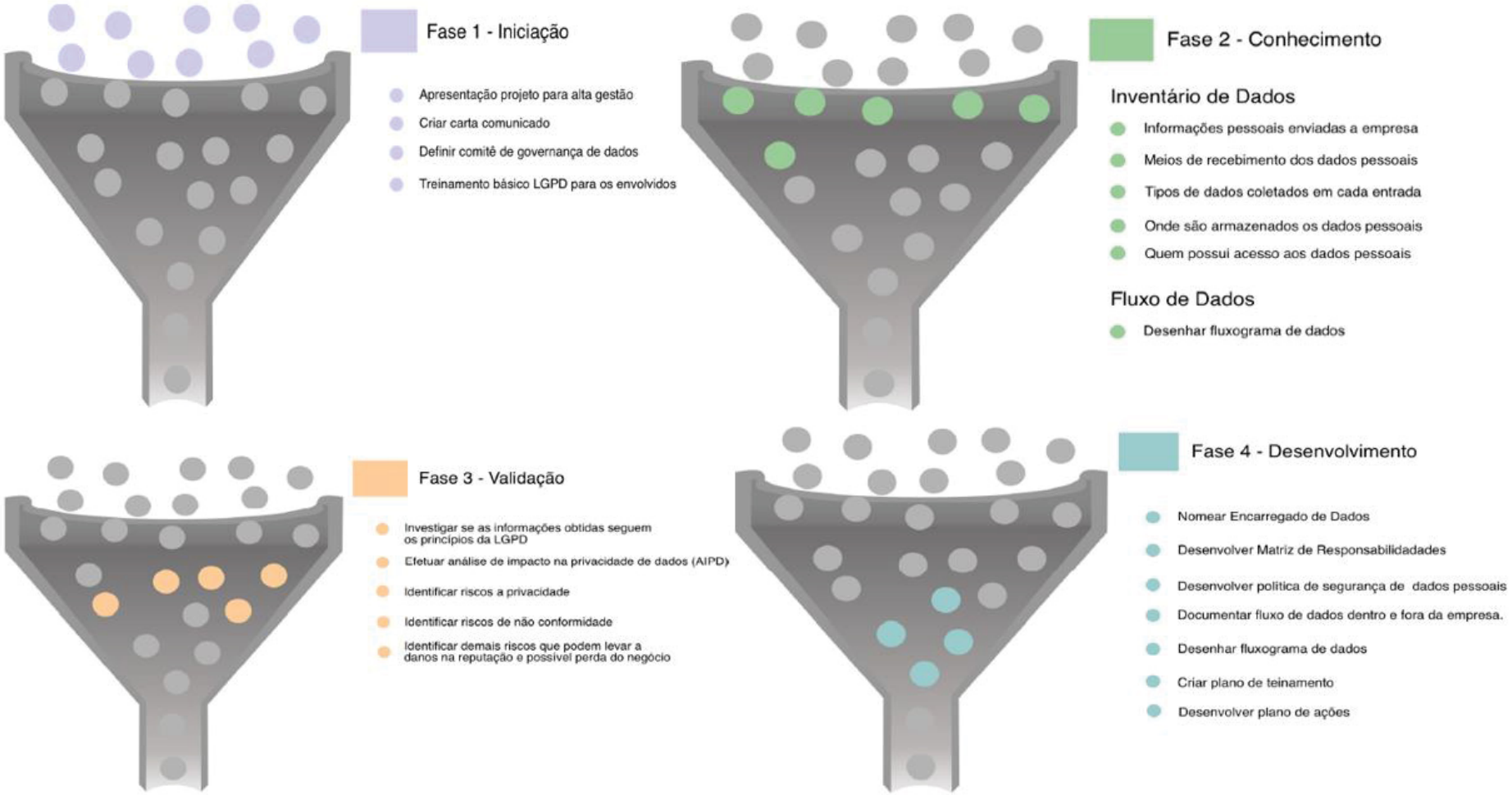
A primeira parte do *framework* foi dedicada para os passos de tratamento dos dados pessoais, da necessidade de identificar o tipo de tratamento (acesso, armazenamento, arquivamento, avaliação entre outras) e que o tratamento deve ter um fim, um propósito específico e ser claro, como também observar as hipóteses legais. A segunda parte está relacionada aos riscos envolvidos de quando a organização não estiver adequada, podendo acarretar sanções como advertência, multas simples e publicização da infração. A terceira parte do *framework* se refere à mitigação dos riscos, ou seja, à segurança da informação, **Figura 16**.

FIGURA 16 – *FRAMEWORK* CRIADO POR ZINI

FONTE: Zini (2021).

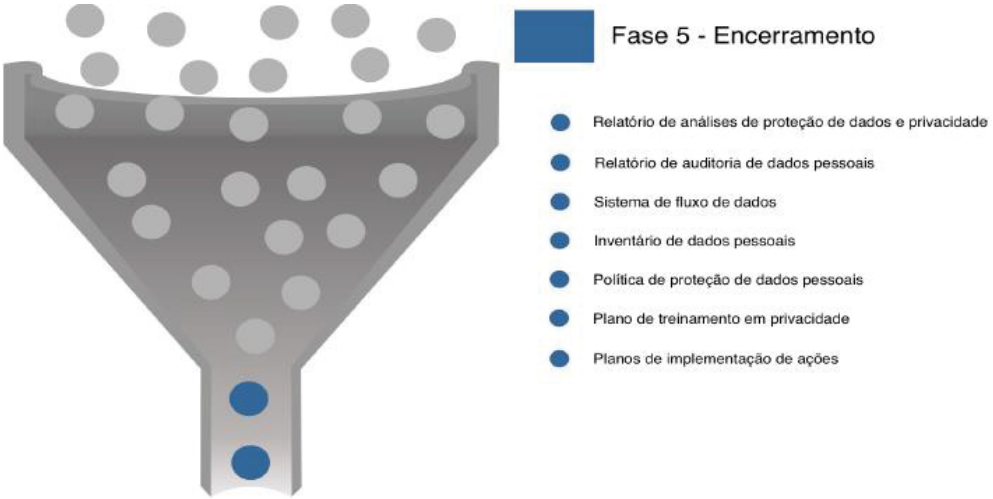
O *framework* 2 (Silva) foi criado com o fim de identificar o nível de conformidade das empresas brasileiras no setor químico e aplicado em uma indústria química. Primeiramente, o autor desenvolveu um questionário para saber o nível de conformidade das empresas e esse questionário teve validação externa. Após isso, ele construiu o modelo baseado na revisão de literatura e no questionário. Este *framework* contém 5 fases: iniciação, conhecimento, validação, desenvolvimento e encerramento; cada fase possui itens a serem desenvolvidos pela organização. As **Figuras 17**, **18** o demonstram:

FIGURA 17 – *FRAMEWORK* SILVA FASE 1,2,3 e 4



FONTE: Silva (2020).

FIGURA 18 – *FRAMEWORK* SILVA FASE 5



FONTE: Silva (2020).

No *framework* 3 (Carvalho), também foi realizada uma revisão de literatura para identificar os principais modelos relacionados à segurança, privacidade e governança, identificando atividades que são distribuídas nessas disciplinas. Após isso, o autor realizou três questionários que foram enviados a profissionais de TI com experiência em dados buscando a validação de quais atividades identificadas pelo autor na revisão de literatura teria mais eficácia. Em seguida, o autor desenvolve seu *framework* e realiza um método de validação. A concepção geral do modelo é baseada em três pilares: segurança, privacidade e governança de dados. E se desenvolve no ciclo PDCA, apresentada na **Figura 19**.

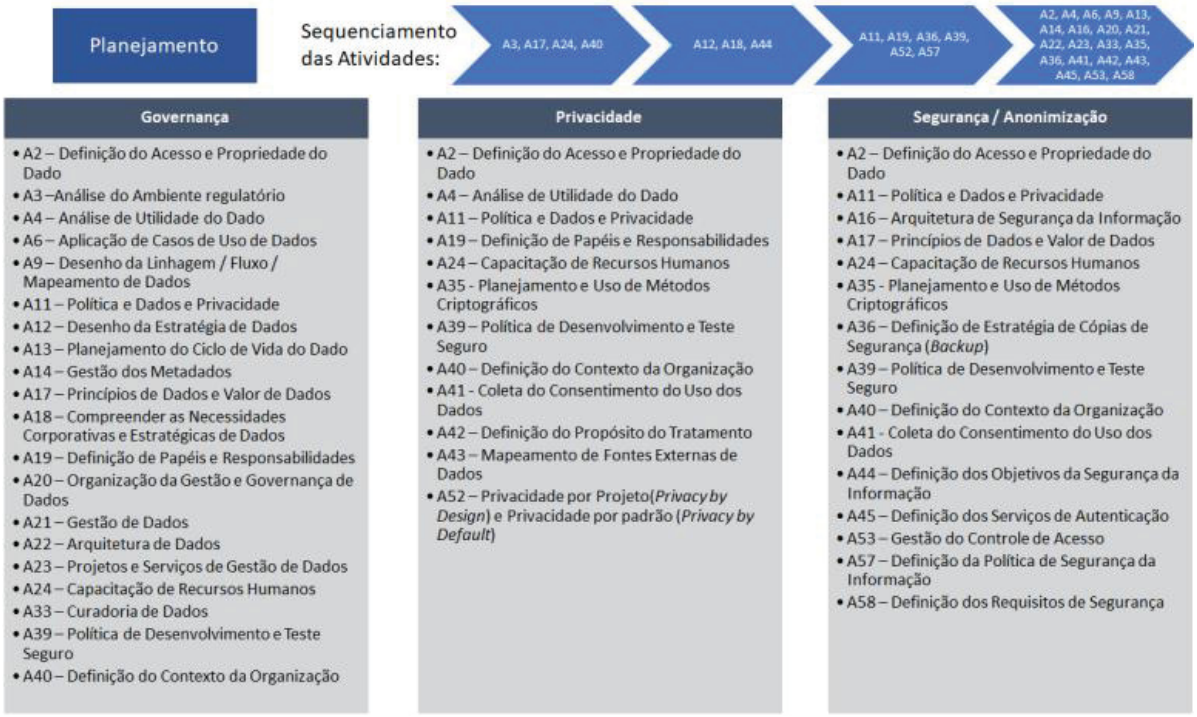
FIGURA 19 – *FRAMEWORK* CARVALHO CONCEPÇÃO GERAL

FONTE: Carvalho (2021).

Em cada pilar (segurança, privacidade e governança), o autor propõe as atividades a serem realizadas. E cada estrutura possui uma sequência de atividades que deve ser seguida em uma ordem estipulada, por exemplo: a atividade A12 depende das saídas da atividade A3, exemplo na **Figura 20**.

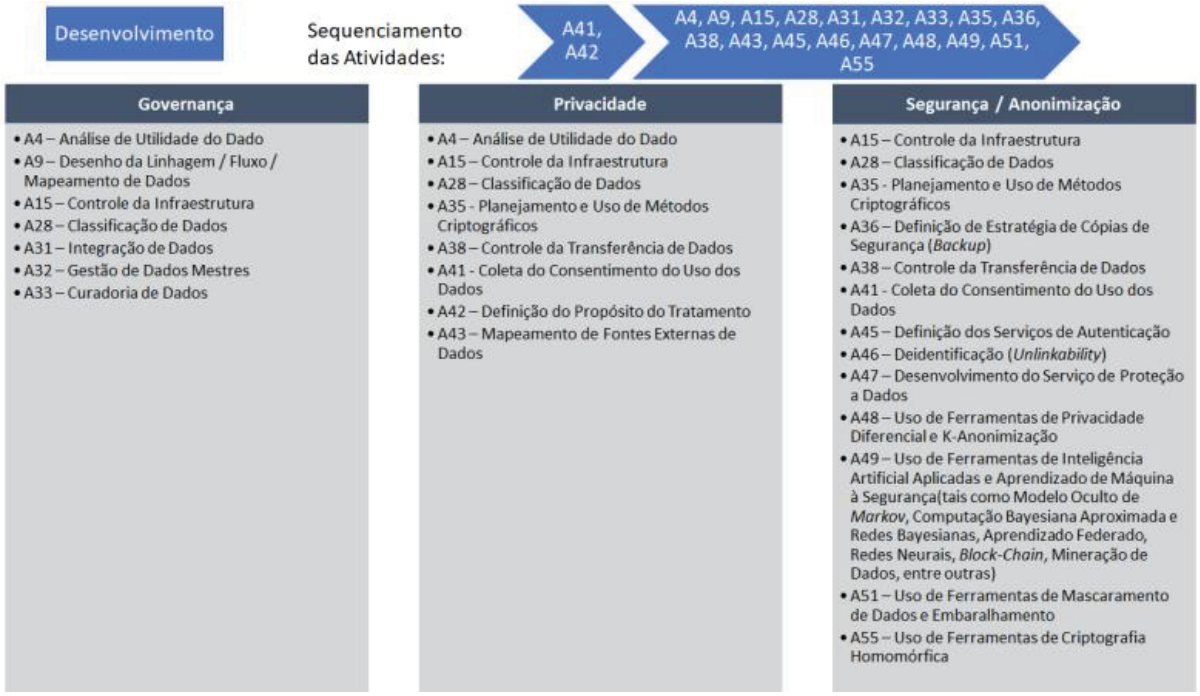
Em seguida, as **Figuras 20**, **21**, **22** e **23** mostram as atividades em cada ciclo e em cada eixo: segurança, privacidade e governança.

FIGURA 20 – *FRAMEWORK* CARVALHO PLANEJAMENTO



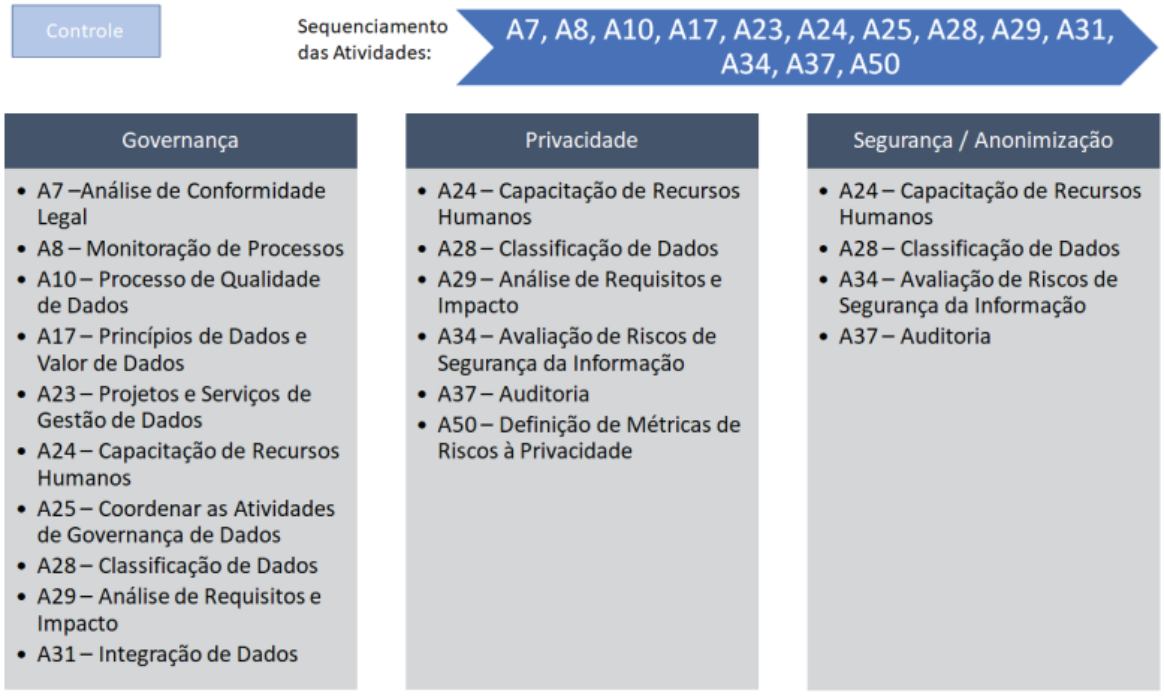
FONTE: Carvalho (2021).

FIGURA 21 – *FRAMEWORK* CARVALHO DESENVOLVIMENTO



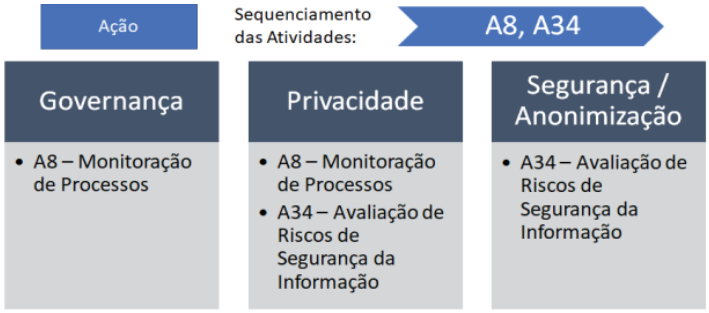
FONTE: Carvalho (2021).

FIGURA 22 – *FRAMEWORK* CARVALHO CONTROLE



FONTE: Carvalho (2021).

FIGURA 23 – *FRAMEWORK* CARVALHO AÇÃO



FONTE: Carvalho (2021).

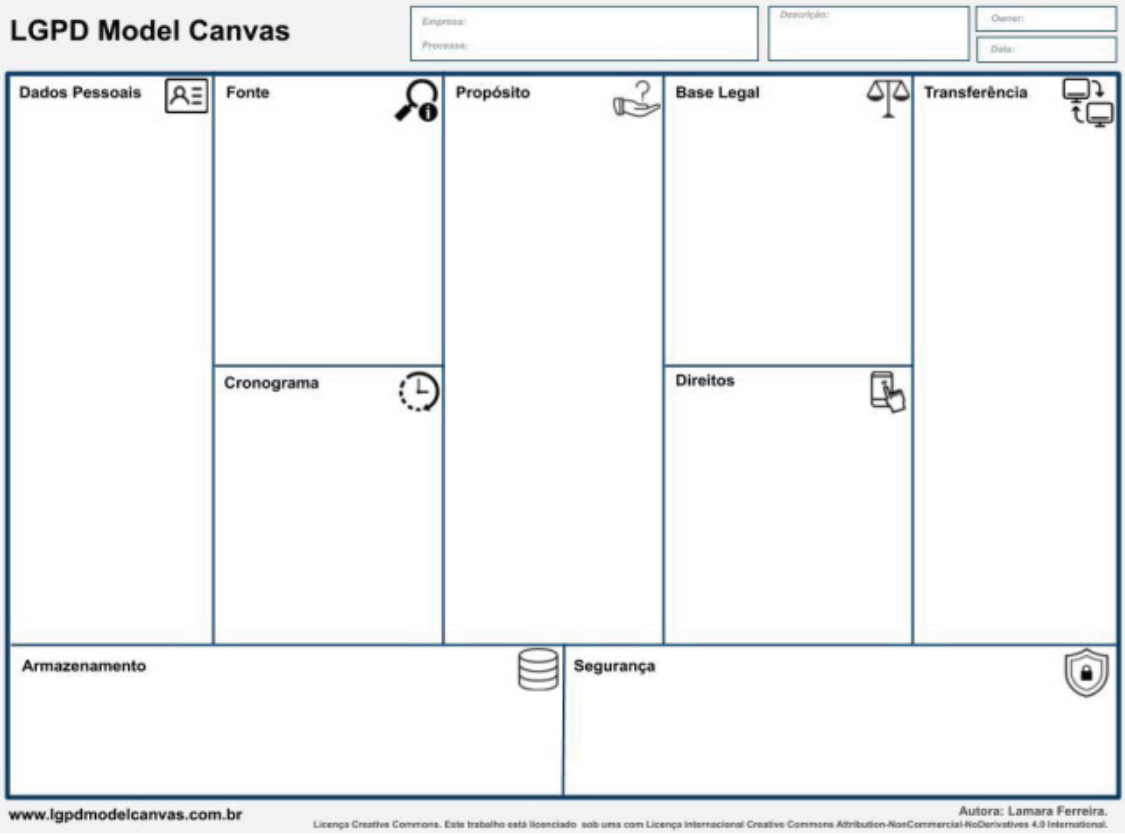
Carvalho (2021, p.89) comenta que as atividades de Governança de Dados ocorrem nos períodos iniciais do projeto, no planejamento e projeto. As atividades de privacidade tendem a se concentrar no período de desenvolvimento e testes. E as atividades de segurança da informação fazem parte da operação/manutenção dos dados, porém isso não é uma regra, a relação temporal somente diz a concentração das atividades.

Por último, o *framework* 4 (Ferreira), foi baseado no modelo de negócio, *business model canvas* (bmc), que é um modelo visual para simplificar organizações complexas. A autora iniciou o trabalho realizando uma revisão de literatura e, depois, ao concluir a construção do modelo, aplicou em um processo de cadastro de *prospect* de uma organização.

O modelo sugere que a privacidade seja considerada em todo o processo de aplicação que é realizado em dois momentos, o AS IS, realizando como se fosse “uma foto do momento atual da organização”, onde todos os processos existentes em que existam dados pessoais serão levantados. Ferreira (2018) comenta que o modelo pode ser aplicado e incorporado na rotina da empresa, assim como ocorre com métodos ágeis. E o segundo momento é chamado, TO BE, onde a organização realizará o levantamento futuro dos processos, através de *brainstorming* para concepção da cultura de privacidade.

É importante informar que o *framework* nesse caso, é uma ferramenta de mapeamento de informações dos processos que tratam de dados pessoais e levantamentos de vulnerabilidades. A **Figura 24** apresenta o modelo proposto e o preenchimento segue a ordem da direita para a esquerda e de cima para baixo, iniciando em “Dados Pessoais” e finalizando em “Segurança”.

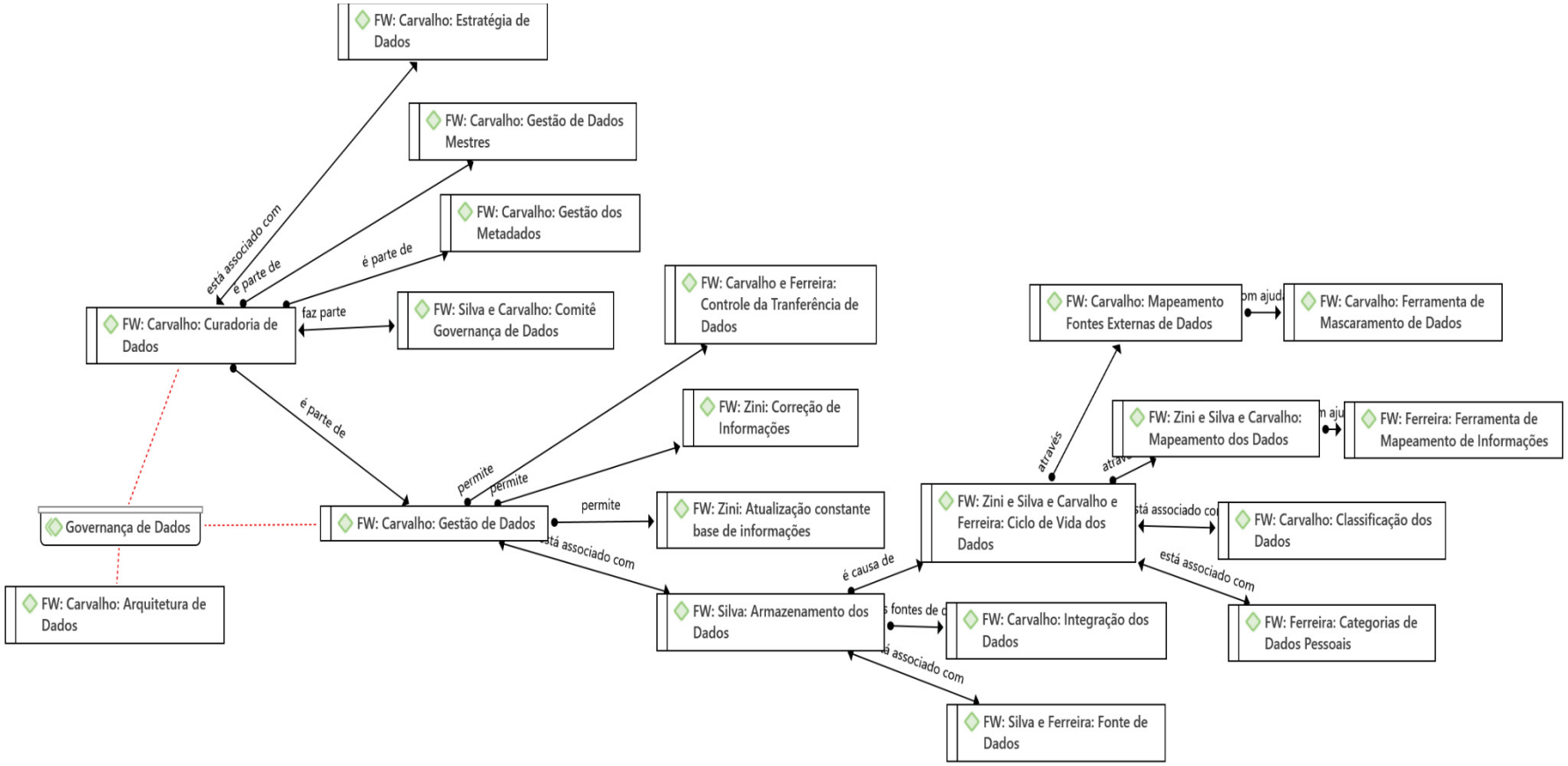
FIGURA 24 – *FRAMEWORK* FERREIRA LGPD MODEL CANVAS



FONTE: Ferreira (2018).

Para apresentar as diferenças e semelhanças dos FW analisados, optou-se por apresentá-las por meio das redes da análise de conteúdo. Cada uma apresenta uma categoria e seus detalhamentos indicando nome do autor/ o tema tratado, ao total foram produzidas 7 redes apresentadas a seguir.

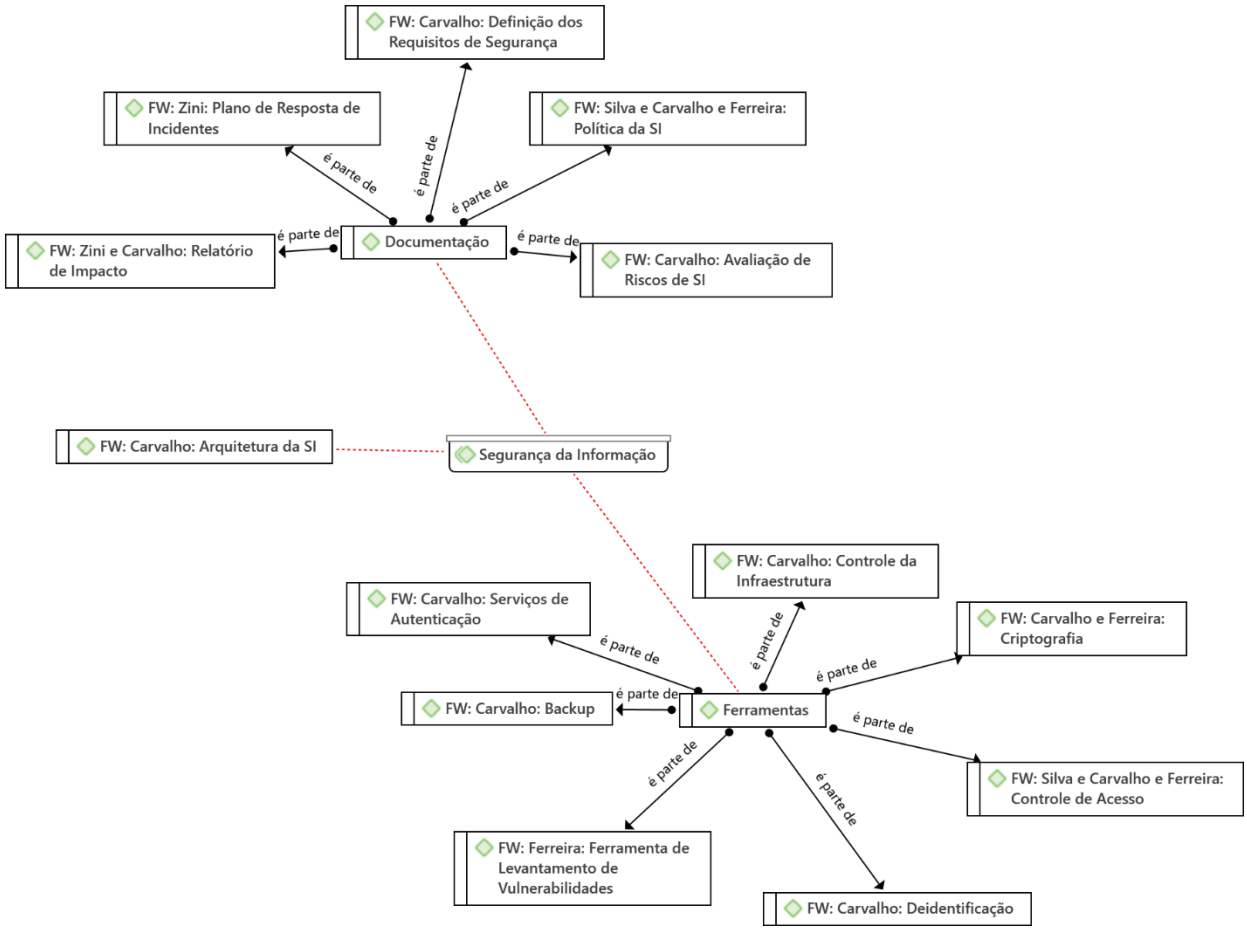
FIGURA 25 – REDE DE GOVERNANÇA DE DADOS



Fonte: A autora (2023).

Na rede sobre a Governança de Dados (**Figura 25**), é possível perceber que Carvalho se aprofundou mais no tema, apresentando diferentes aspectos sobre o assunto, como: arquitetura de dados, gestão de metadados, gestão de dados mestres, curadoria de dados, entre outros. É possível notar que são elementos da estrutura do *Dama DMBOK,* comentado no capítulo de governança de dados. Os outros autores também citam a importância de algumas ações como mapeamento de dados, obter ciclo de vida dos dados, atualização das bases de informações, entre outros.

FIGURA 26 – REDE DE SEGURANÇA DA INFORMAÇÃO

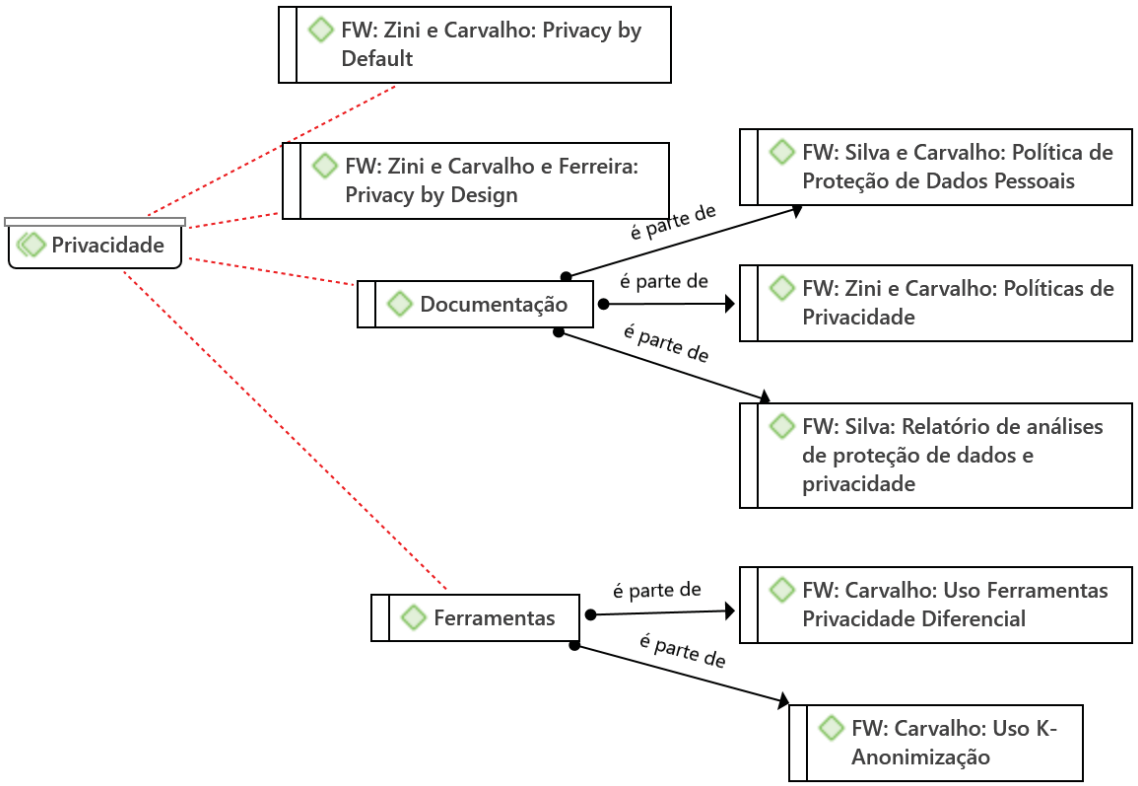


Fonte: A autora (2023).

Na rede a respeito de SI (**Figura 26**), todos os autores abordam este tema como relevante. No entanto, o *framework* de Carvalho é mais detalhista, mencionando, por exemplo, a necessidade da arquitetura da SI, a definição dos requisitos de segurança da informação, o backup, o controle da infraestrutura, os

serviços de autenticação, entre outros. Também são mencionadas as políticas de SI, sem as quais, o risco de vazamento vão além da perda financeira, incluindo também a exposição do cidadão (Souza *et al*., 2020).

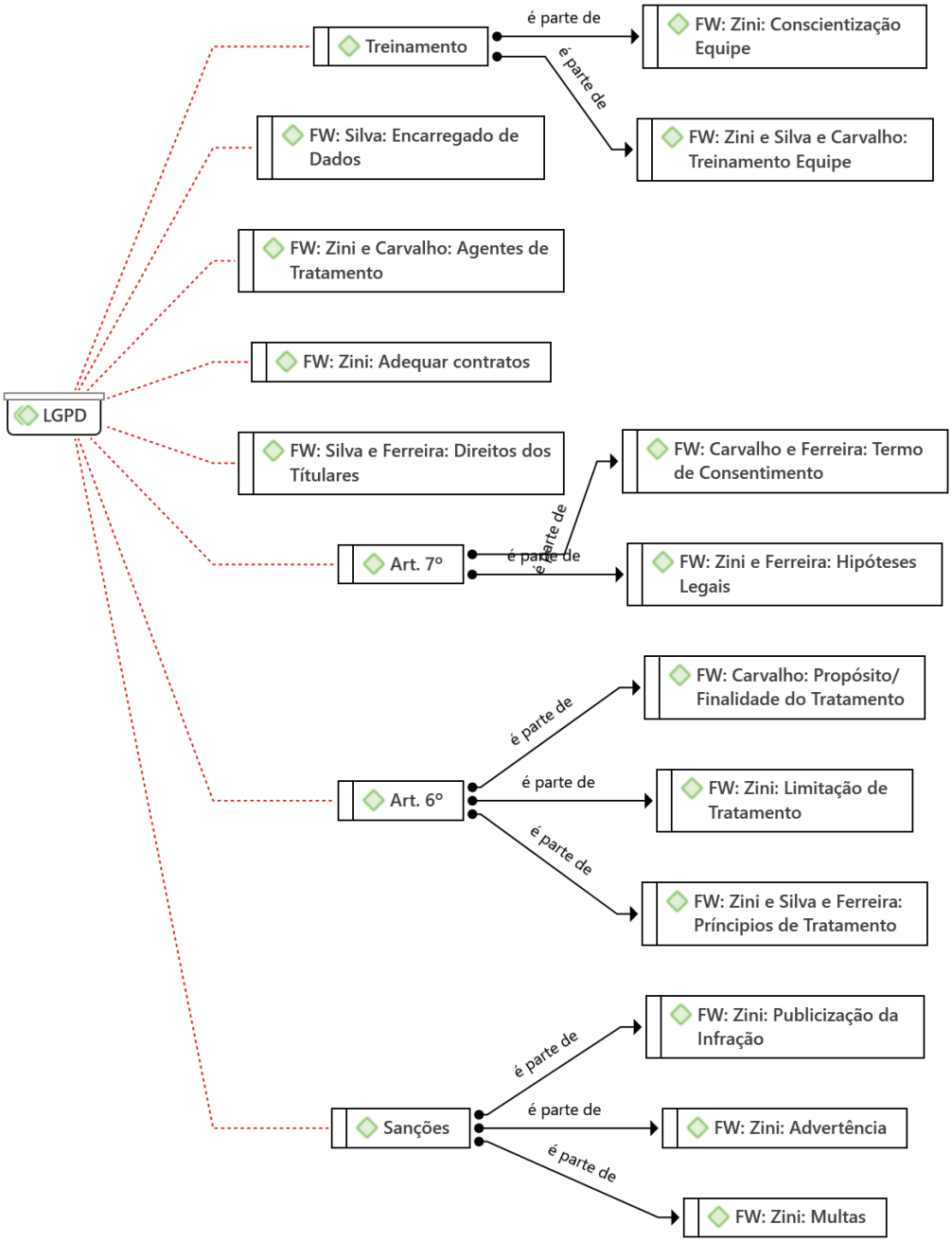
FIGURA 27 – REDE DE PRIVACIDADE



Fonte: A autora (2023).

Em relação à rede de Privacidade (**Figura 27**), nota-se a importância dos conceitos de PbD e *Privacy by Default* mencionados por Zini, Carvalho e Ferreira e das criações de políticas de proteção de dados pessoais e políticas de privacidade. Esses itens vão de encontro ao que destaca Marrafon e Coutinho (2020), que o PbD exige que as organizações adotem padrões especiais e medidas técnicas que assegurem que apenas os dados pessoais necessários sejam processados com um propósito. O *framework* de Carvalho também menciona o uso de ferramentas de privacidade diferencial e uso da k-anonimização.

FIGURA 28 – REDE DA LGPD

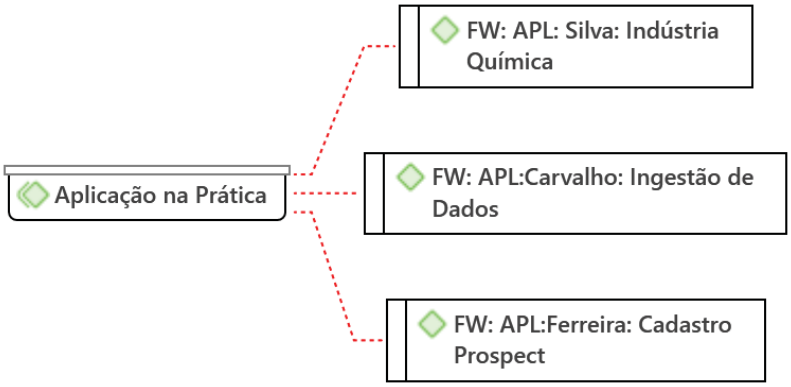


Fonte: A autora (2023).

Acerca da rede LGPD (**Figura 28**), destacam-se os itens relativos ao quadro de correspondência a GDPR, ou seja, as menções relacionadas aos princípios da Lei, as hipóteses legais de tratamento e aos direitos dos usuários. O item relativo à segurança foi colocado na rede específica sobre SI, já citado. Neste tema destaca-se o framework de Zini. Este apresenta mais itens, referenciando inclusive o art. 6º

sobre os princípios de tratamento e suas limitações, o art. 7º sobre as hipóteses legais de tratamento, assim como sanções da Lei. Tanto o framework de Silva, quanto o de Ferreira lembram da necessidade de pensar nos direitos dos titulares de forma abrangente.

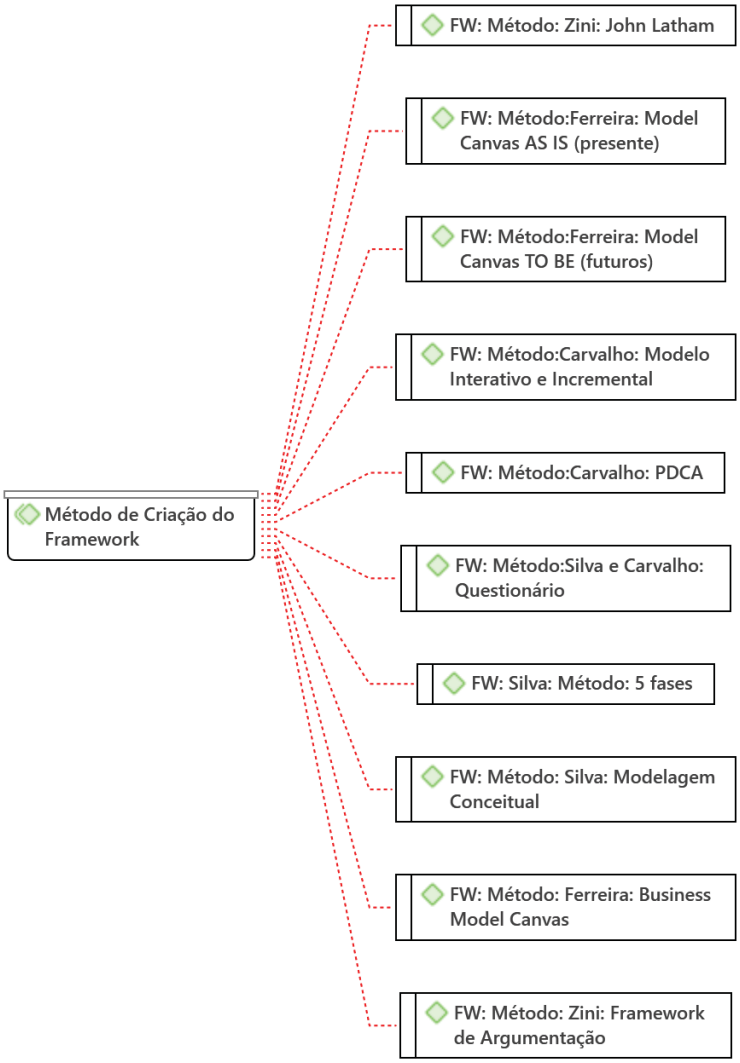
FIGURA 29 – REDE DE APLICAÇÃO NA PRÁTICA



Fonte: A autora (2023).

Na rede referente à aplicação na prática (**Figura 29**), Zini não comenta se realizou algum teste, porém os outros autores, de alguma forma, realizaram a aplicação: Silva em uma indústria química, Carvalho por meio de uma injeção de dados e Ferreira em um cadastro de *prospect*.

FIGURA 30 – REDE DE MÉTODO



Fonte: A autora (2023).

Na rede sobre o método de criação (**Figura 30**), todos os autores usaram um método para basear a criação do seu *framework*. Zini usou do método de John Latham, Silva se baseou em um questionário e fez um modelo dividido em 5 fases, Carvalho também utilizou questionários e baseou-se no ciclo PDCA e Ferreira apoiou-se no modelo *Business Model Canvas*, para criar o seu próprio modelo.

FIGURA 31 – REDE DE VALIDAÇÃO

Fonte: A autora (2023).

Por fim, na rede de validação do *framework* (**Figura 31**), apenas Carvalho validou seu *framework*, usando testes de medidas de qualidade. Os outros autores não deixaram de maneira clara se foi realizada algum tipo de validação.

4.1.2 Interpretação e correspondência entre LGPD e GDPR

Esse item tem a função de explicar como foi realizada a interpretação dos artigos descobertos na seção 3.5.2 e a correspondência com a LGPD.

Esse procedimento foi realizado através de leitura dos artigos da Lei Europeia e da Lei Brasileira, e identificando os pontos de semelhança e correspondência, resultando no **Quadro 9**. Alguns itens foram possíveis deslumbrar a correspondência ou semelhança direta, entretanto outros foi possível apenas identificar os conceitos que englobam o artigo.

QUADRO 9 – CORRELAÇÃO DA GDPR À LGPD

GDPR	**LGPD**
Art. 5 *Principles relating to processing of personal data*	Art. 6º. VER ANEXO 1.
Art. 6 *Lawfulness of processing*	Art. 7º. VER ANEXO 1.
Rights of the data subject Art. 12 *Transparent information, communication and modalities for the exercise of the rights of the data subject* Art. 13 *Information to be provided where personal data are collected from the data subject* Art. 15 *Right of access by the data subject* Art. 17 *Right to erasure ('right to be forgotten')* Art. 21 *Right to Object*	Direitos do Titulares de Dados Art. 9º. Art. 15 Art. 16 Art. 17 Art. 18. IV, VI; § 2º Art. 19 Art. 20 Art. 21 Art. 22 VER ANEXO 1.
Art. 32 Security of processing	Art. 46. VER ANEXO 1.

Fonte: A autora (2022).

Após isso, o quadro de correlação passou pela validação do Cezar Fonseca, que é servidor do Instituto Federal do Paraná (IFPR), com experiência em direito e

ouvidoria e atualmente atua na função de Encarregado de Dados Pessoais do IFPR, ele concorda com a correlações do quadro, no entanto, sugeriu a adição do art. 15º no item sobre os direitos dos titulares de dados, que faz referência ao término de tratamento dos dados pessoais, sendo assim esse artigo foi adicionado posteriormente ao quadro.

5 DISCUSSÃO

Neste estudo, o embasamento das análises se deu por meio da triangulação de três fontes: os conceitos inerentes à Lei, os artigos da LGPD correspondentes aos artigos que mais geraram multas da GDPR e a categorização de variáveis utilizadas na construção dos *frameworks* (metodologia, validação do FW e aplicação na prática). Todos eles foram analisados e estão expostos nas redes, a maioria como categorias na análise de conteúdo (governança de dados, segurança da informação, privacidade, LGPD, metodologia, aplicação e validação na prática) e o restante está inserido dentro dessas categorias (PbD, termo de consentimento e anonimização). Os artigos que mais se destacaram na comparação com a GDPR estão inseridos dentro da categoria LGPD, os art. 6º, art. 7º e os direitos dos titulares, que abrangem vários artigos. O art. 46, que se refere à segurança da informação, por ser um conceito inerente à Lei e um artigo de destaque em comparação com a GDPR, foi alocado em uma categoria própria.

Após a descrição das redes, como mencionado na seção de Resultados, evidenciou-se alguns pontos importantes que diferenciam os *frameworks* analisados. Por exemplo, o *framework* de Carvalho é o mais robusto de todos e embasa toda sua estrutura em governança de dados, SI e privacidade, detalhando várias atividades que devem ser realizadas. Diante desse detalhamento, presume-se que dependendo do porte da organização, o cumprimento de tudo o que é proposto por ele, pode ser um ponto de dificuldade.

No *framework* de Zini, percebe-se uma identificação com a letra da Lei, pois ele traz, de maneira resumida, os seus principais pontos, sem especificar os passos de como fazer a adequação.

O *framework* de Silva se mostra didático, ao ponto de especificar as fases para implementação e por onde começar até alcançar a fase de desenvolvimento. Para empresas menores e que estão iniciando o processo de adequação, talvez seja de grande valia utilizar-se dele.

O *framework* de Ferreira está voltado para o mapeamento dos dados da organização, sendo assim, pode ser usado em conjunto com os outros *frameworks*. O ponto interessante é que, por meio desse modelo, é possível pensar na coleta dos dados pessoais de maneira articulada com a Lei.

Em resumo, todos os *frameworks* têm pontos positivos e podem ser usados pelas organizações, inclusive em conjunto. Em primeiro, viria o *framework* de Zini, para entender os principais aspectos da Lei e sua importância. Em segundo, o *framework* de Silva, pois apresenta os passos iniciais do que se realizar, podendo auxiliar no início do processo de adequação. Com a maturidade da organização, poder-se-ia inserir outros elementos que são propostos no *framework* de Carvalho, que é mais detalhista e requer inclusive uma equipe mais experiente. Nesse processo, o *framework* de Ferreira pode ser usado desde o início para o mapeamento ou inventário dos dados pessoais.

6 CONSIDERAÇÕES FINAIS

Este estudo pautou-se em uma revisão bibliográfica e documental, descrevendo o contexto e informações a respeito da LGPD, a partir dos quais reuniu os principais conceitos inerentes à Lei, tais como: anonimização, termo de consentimento, privacidade, PBD, SI, governança e gestão de dados.

Em seguida, foram encontrados na literatura quatro estruturas de dados (*frameworks*) de adequação à Lei nos seguintes documentos, três dissertações (Zini, Silva e Carvalho) e um artigo (Ferreira).

Com a investigação dos artigos da LGPD que mais têm chances de resultar em multas, baseando-se na GDPR, foi possível concluir que é importante ter uma atenção especial aos seguintes artigos:

- Art. 6º, que se refere aos princípios de tratamento dos dados pessoais.

- Art. 7º, que menciona as bases legais/hipóteses de tratamento dos dados pessoais.
- Art. 9º,15, 16, 17,18 (IV, VI; § 2º),19, 20 e 21, os quais se referem aos direitos dos titulares.
- Art. 46, que se refere às medidas de segurança, técnica e administrativas.

A partir da análise de conteúdo dos *frameworks* propostos por Zini, Silva, Carvalho e Ferreira foram elaboradas sete redes: rede de governança de dados, rede de SI, rede de privacidade, rede da LGPD, rede de aplicação na prática, rede de método de criação e a rede de validação. Nas quatro primeiras redes, todos os autores mencionaram aspectos importantes relacionados a essas categorias, com suas particularidades. Em relação à aplicação na prática, Zini não comenta se realizou algum teste, porém os outros autores, de alguma forma, realizaram a aplicação: Silva em uma indústria química, Carvalho por meio de uma injeção de dados e Ferreira em um cadastro de *prospect*. Com relação à metodologia, Zini usou do método de John Latham, Silva se baseou em um questionário e fez um modelo dividido em 5 fases, Carvalho também utilizou questionários e baseou-se no ciclo PDCA e Ferreira apoiou-se no modelo *Business Model Canvas*, para criar o seu próprio modelo. Por fim, na rede de validação, apenas Carvalho validou seu *framework*, usando testes de medidas de qualidade. Os outros autores não deixaram de maneira clara se foi realizada algum tipo de validação.

Seguindo a interpretação das redes, concluiu-se que os quatro *frameworks*, de forma geral, têm os seguintes pontos em destaque:

- Zini apresenta os principais aspectos da Lei e sua importância.
- Silva apresenta os passos iniciais do que se realizar, podendo auxiliar no início de um processo de adequação.
- Carvalho apresenta um *framework* mais detalhado, a partir do qual organizações maiores e mais maduras poderiam se beneficiar.
- Ferreira apresenta o *framework* que poderia ser usado para o mapeamento ou inventário dos dados pessoais.

Os vazamentos de dados apresentados na mídia de maneira expressiva, assim como a vigência da LGPD trazem à tona a preocupação para a adequação

das empresas à Lei. Há também uma cobrança mundial por conta da aplicação de multas das legislações em outros países. Porém, até o momento, a Autoridade Nacional de Proteção de Dados (ANPD), responsável pela aplicação das multas no Brasil, ainda não está cumprindo essa função. Provavelmente, quando essas penalidades começarem a acontecer, os temas tratados nessa dissertação ficarão ainda mais em evidência ressaltando a importância desse estudo e de estruturas de dados para a adequação das organizações à Lei.

6.1 LIMITAÇÕES

As limitações deste estudo estão relacionadas às dificuldades de interpretar as informações, muitas vezes abstratas, nos *frameworks*, pois sempre haverá a possibilidade de diferentes interpretações sobre determinado tema, e do porquê os autores escolheram tratá-lo de forma mais direta ou mais detalhada, assim como a escolha dos termos utilizados por cada um.

Também houve uma limitação com relação ao quadro que compara os artigos da GDPR com a LGPD, pois caso a ANPD já estivesse aplicando multas, o quadro poderia ser validado utilizando uma base de dados reais.

6.2 PESQUISAS FUTURAS

Vislumbra-se como pesquisa futura, depois de a ANPD já ter iniciado a aplicação das multas e gerado dados suficientes, validar o quadro comparativo das multas, confirmando ou não se os artigos que foram encontrados em correspondência a GDPR se atestam.

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICA. **NBR ISO/IEC 27002:2013: Tecnologia da Informação-Técnicas de Segurança – Código de Prática para controles de segurança da informação**. Rio de Janeiro. 2013.

ALHAZMI, H.; IMRAN, A; ALSHEIKH, M. A. Digital Divide and Social Dilemma of Privacy Preservation. **CoRR Computing Research Repository**. *[S. l.]*, 2021. Disponível em: http://arxiv.org/abs/2110.02669. Acesso em: 22 mar. 2022.

ARAGÃO, Alexandre. 5 grandes vazamentos de dados no Brasil — e suas consequências. **JOTA**, São Paulo, 28 de jan. de 2022. Disponível em: https://www.jota.info/tributos-e-empresas/mercado/vazamentos-de-dados-no-brasil-28012022. Acesso em 28 jun. 2022.

BARBOSA, R.R. Gestão da Informação e do Conhecimento: Origens, Polêmicas e Perspectivas. Informação & Informação. *[S.l]*, v.13, n. esp., p1-25, 2008. Disponível em: https://brapci.inf.br/index.php/res/v/33432. Acesso em: 13 jul. 2022.

BARRETO, J. dos S.; ZANIN, A.; MORAIS, I. S. D.; VETTORAZZO, A. de S. **Fundamentos de segurança da informação**. Grupo A, 2018. 9788595025875. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788595025875/. Acesso em: 05 mai. 2022.

BRASIL. Lei nº 12.527 de 18 de novembro de 2011. Lei de Acesso à Informação. **Diário Oficial da União**. Brasília: DF, 18 de novembro de 2011. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 15 jul. 2022.

BRASIL. Lei nº 12.737 de 30 de novembro de 2012. Tipificação criminal de delitos informáticos. **Diário Oficial da União**. Brasília: DF, 30 de novembro de 2012. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 15 jul. 2022.

BRASIL. Lei nº 12.965 de 23 de abril de 2014. Marco Civil da Internet. **Diário Oficial da União**. Brasília: DF, 24 de abril de 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 16 jul. 2022.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais. **Diário Oficial da União**, Brasília: DF, 14 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm. Acesso em: 22 mar. 2022.

BIONI, B. R. **Proteção de Dados Pessoais - A Função e os Limites do Consentimento**. Grupo GEN, 2021. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788530994105/. Acesso em: 10 mar. 2022.

CARVALHO, A. P. **Proposta de um Framework de Compliance à Lei Geral de Proteção de Dados Pessoais (LGPD): Um estudo de caso para prevenção a fraude no contexto de Big Data**. 200p. Dissertação (Mestrado em Profissional em Engenharia Elétrica) – Universidade de Brasília, Brasília, 2021. Disponível em: https://repositorio.unb.br/handle/10482/42510. Acesso em 20 ago. 2022.

CASTELANNI, L. *et al*. Portal das Violações – LGPD. **ANPPD**. Disponível em: https://anppd.org/violacoes. Acesso em: 12 abr. 2022.

CAMBRIDGE DICTIONARY. Framework. 2020. Disponível em: https://dictionary.cambridge.org/pt/dicionario/ingles/framework. Acesso em: 28 ago. 2022.

CAMBRICOLI, Fabiana. Nova falha do Ministério da Saúde expõe dados pessoais de mais de 200 milhões de brasileiros. **O Estado de S. Paulo**, São Paulo, 02 de dez. de 2020. Disponível em: https://saude.estadao.com.br/noticias/geral,nova-falha-do-ministerio-da-saude-expoe-dados-pessoais-de-mais-de-200-milhoes,70003536340. Acesso em: 28 jun. 2022.

CARTILHA Marco Civil. Disponível em: https://criminal.mppr.mp.br/arquivos/File/Cartilha_Marco_Civil_da_Internet.pdf Acesso em: 22 mar. 2022.

CAVOUKIAN, A. (2009). **Privacy by Design**. Disponível em: https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf Acesso em: 22 mar. 2022.

CAVOUKIAN, A. Privacy by Design. **Identity in the Information Society**, *[S. l.]*, v. 3, n. 2, p. 1–12, 2010. Acesso em: data.

CHEN, A. (2020). **Differential privacy**. Disponível em: https://www.technologyreview.com/10-breakthrough-technologies/2020/#differential-privacy. Acesso em: 14 jun. 2022.

CHIK, W. B. The Singapore personal data protection act and an assessment of future trends in data privacy reform. **Computer Law and Security Review**, *[S. l.]*, v. 29, n. 5, p. 554–575, 2013. DOI: 10.1016/j.clsr.2013.07.010. Disponível em: https://ink.library.smu.edu.sg/sol_research/1252/. Acesso em: 14 jun. 2022.

CMS law-tax-future. **GDPR Enforcement Tracker**. Disponível em: https://www.enforcementtracker.com/. Acesso em: 18 jul. 2022.

CONCEITO. *In*: MICHAELIS Dicionário Brasileiro da Língua Portuguesa. Disponível em: https://michaelis.uol.com.br/busca?r=0&f=0&t=0&palavra=conceito. Acesso em 29 dez 2022

COSTA, A. A. C.; FILÓ, M. C. S. O conceito de privacidade diferencial em relação à reidentificação de dados pessoais. **Pragmatizes**, *[S. l.]*, p. 214–231, 2020. Disponível em: https://periodicos.uff.br/pragmatizes/article/download/41180/24694/146235. Acesso

em: 15 jun. 2022.

CHOO, C. W. A organização do conhecimento: como as organizações usam a informação para criar significado, construir conhecimento e tomar decisões. Tradução Eliana Rocha. São Paulo: Editora Senac, 2003.

CRESWELL, J. W. **Projeto de pesquisa: métodos qualitativo, quantitativo e misto**. 3a ed. Porto Alegre: Artmed, 2010.

CURRY, A.; MOORE, C. Assessing information culture: an exploratory model. International Journal of Information Management, Guildford, v. 23, n. 2, p. 91-110, apr. 2003.

DAMA-DMBOK: Data Management Body of Knowledge. 2. ed. New Jersey: Technics Publications, 2017.

DAVENPORT, T. H. Ecologia da informação: por que só a tecnologia não basta para o sucesso na era da informação / Thomas H. Davenport, Laurence Prusak; tradução Bernadette Siqueira Abrão. São Paulo: Futura, 1998.

DAVENPORT, T. H.; PRUSAK, L. Codificação e Coordenação do Conhecimento. In: _____. Conhecimento empresarial: como as organizações gerenciam o seu capital intelectual. Rio de Janeiro: Elsevier, 2003. Cap. 4, p. 42-44.

ESTRUTURA. *In*: MICHAELIS Dicionário Brasileiro da Língua Portuguesa. Disponível em: https://michaelis.uol.com.br/busca?r=0&f=0&t=0&palavra=estrutura. Acesso em 29 dez 2022.

FADEL, B. *et al*. Gestão, Mediação e Uso da Informação. In: VALENTIM, M. L. P. Gestão, Mediação e Uso da Informação. São Paulo: Editora UNESP, 2010. p.14-16.

FALEIROS JÚNIOR, J. L. de M; MARTINS, G. M. Proteção De Dados e Anonimização: Perspectivas à Luz da Lei Nº 13.709/2018. **Rei - Revista Estudos Institucionais**, *[S. l.]*, v. 7, n. 1, p. 376–397, 2021. DOI: 10.21783/rei.v7i1.476. Disponível em: https://www.estudosinstitucionais.com/REI/article/view/476. Acesso em: 17 jun. 2022.

FEDERAL TRADE COMMISSION (FTC). Privacy Online: A Report to Congress. 1998. Disponível em: https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-report-congress/priv-23a.pdf .Acesso em: 28 jun. 2022.

FERREIRA, L. *et al*. Uso do Modelo LGPD Model Canvas para Mapeamento do Processo de Cadastro à Luz da Conformidade com a LGPD. In: SIMPÓSIO DE ENGENHARIA DE PRODUÇÃO, 2021, Bauru. **Artigo...** Bauru: Simpep, 2021, p. 1-14. Disponível em: https://www.simpep.feb.unesp.br/anais_simpep.php?e=16. Acesso em 15 ago. 2022.

FINKELSTEIN, M.E.; FINKELSTEIN, C. Privacidade e Lei Geral de Proteção de

Dados Pessoais. **Revista de Direito Brasileira**. *[S.l]*, v.23, n.9, p-284-301, 2009. Disponível em: 10.26668/indexlawjournals/2358-1352/2019.v23i9.5343. Acesso em: 10 fev. 2022.

FONTES, E. L. G. **Segurança da informação - 1ª edição**. Editora Saraiva, 2012. 9788502122185. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788502122185/. Acesso em: 05 mai. 2022.

FORNASIER, M. de O.; KNEBEL, N. M. P. O titular de dados como sujeito de direito no capitalismo de vigilância e mercantilização dos dados na Lei Geral de Proteção de Dados. **Revista Direito e Práxis**, *[S. l.]*, v. 12, n. 2, p. 1002–1033, 2021. DOI: 10.1590/2179-8966/2020/46944. Disponível em: https://www.scielo.br/j/rdp/a/hTqmGJVy7FP5PWq4Z7RsbCG/. Acesso em: 18 jun. 2022.

FRAMEWORK. *In*: CAMBRIDGE DICTIONARY. Disponível em: https://dictionary.cambridge.org/dictionary/english-portuguese/framework. Acesso em 29 dez 2022.

GARCIA, R.; FADEL, B. Cultura Organizacional e as Interferências nos Fluxos Informacionais (IFI). In: VALENTIM, M. L. P. Gestão, Mediação e Uso da Informação. São Paulo: Editora UNESP, 2010. p.14-16, p. 213-214.

GIL, A. C. **Como Elaborar Projetos de Pesquisa**. 4. ed. São Paulo: Editora Atlas S.A, 2002.

GRUPO ASSAF. 2019. O Framework de Implantação.12 de dez. 2019. Disponível em: https://www.grupoassaf.com/post/framework_lgpd. Acesso em: 11 dez. 2022.

INTERNATIONAL TELECOMMUNICATION UNION. Data Communication Networks: Open Systems Interconnection (OSI); Security, Structure and Applications. **X.800**. Geneva, 1991. Disponível em: https://www.itu.int/rec/T-REC-X.800-199103-I/en. Acesso em: 30 jun. 2022.

ISTOEDINHEIRO. Segurança de dados: Brasil é o 6º país com mais vazamentos, diz pesquisa. 17 de mar. de 2022. Disponível em: https://www.istoedinheiro.com.br/seguranca-de-dados-brasil-e-o-6o-pais-com-mais-vazamentos-diz-pesquisa/. Acesso em 28 jun. 2022.

IRAMINA, A. GDPR v. GDPL: Strategic adoption of the responsiveness approach in the elaboration of Brazil's general data protection law and the EU general data protection regulation. **Revista de Direito, Estado e Telecomunicacoes**, *[S. l.]*, v. 12, n. 2, p. 91–117, 2020. DOI: 10.26512/lstr.v12i2.34692. Disponível em: https://periodicos.unb.br/index.php/RDET/article/view/34692. Acesso em: 17 jun. 2022.

JABAREEN, Y. Building a Conceptual Framework: Philosophy, Definitions, and Procedure. In: **International Journal of Qualitative Methods**, v. 8, p. 49-62. 2009. Disponível em: https://doi.org/10.1177/160940690900800406. Acesso em 06 dez.

2022.

KAMPS, Michael. *et al*. **GDPR Enforcement Tracker Report**. CMS lax.tax.future. 2022. 17p. Disponível em: https://cms.law/en/media/international/files/publications/publications/gdpr-enforcement-tracker-report-may-2022?v=1. Acesso em: 21 mai. 2022.

KOCH, R. What is the LGPD? Brazil's version of the GDPR. Disponível em: https://bit.ly/2RptBUD. Acesso em: 30/11/2019.

LATHAM, J. R. The Research Canvas: A Framework for Designing & Aligning The DNA of Your Research Study. **Organization Design Studio Ltd**. Colorado, USA. 2016. Disponível em: https://www.drjohnlatham.com/wp-content/uploads/2018/06/Research_Canvas_20.pdf. Acesso em 06 dez. 2022.

LEMOS, A. N. L. E.; PASSOS, E. A adequação das bibliotecas à Lei Geral -de Proteção de Dados. **Cadernos de Informação Jurídica**. [S.l], v. 7, n. 1, p.85 - 103, 2020. Disponível em: https://www.cajur.com.br/index.php/cajur/article/view/265. Acesso em: 10 fev. 2022.

MAGHER, M. What Is the Meaning of Conceptual Framework in Research?. **Classroom**. Disponível em: https://classroom.synonym.com/meaning-conceptual-framework-research-6664512.html. Acesso em 06 dez. 2022.

MARCHIORI, P. Z. Gestão da Informação: Fundamentos, Componentes e Desafios Contemporâneos. In: SOUTO, L. F. Gestão da Informação e do Conhecimento Práticas e Reflexões. Rio de Janeiro: Editora Interciência, 2014. P. 27 – 30.

MARRAFON, M. A,; COUTINHO, L. L. C. L.. Princípio da Privacidade por Design: Fundamentos e Efetividade Regulatória na Garantia do Direito à Proteção de Dados. **Revista Eletrônica Direito e Política**, *[S. l.]*, v. 15, n. 3, p. 955–984, 2020. DOI: 10.14210/rdp.v15n3.p955-984. Disponível em: https://app.dimensions.ai/details/publication/pub.1133701529. Acesso em:18 jun. 2022.

MODESTO, J. A. Breves Considerações Acerca Da Monetização De Dados Pessoais na Economia Informacional à Luz Da Lei Geral De Proteção De Dados Pessoais. **Revista de Direito, Governança e Novas Tecnologias**, *[S. l.]*, v. 6, n. 1, p. 37, 2020. DOI: 10.26668/indexlawjournals/2526-0049/2020.v6i1.6558. Disponível em:https://www.indexlaw.org/index.php/revistadgnt/article/view/6558. Acesso em: 13 jun. 2022.

MOLINA, L. G. Tecnologias de Informação e Comunicação para Gestão da Informação e do Conhecimento: Proposta de um Estrutura Tecnológica Aplicada aos Portais Corporativos. In: VALENTIM, M. L. P. Gestão, Mediação e Uso da Informação. São Paulo: Editora UNESP, 2010. p.14-16.

MORAES, T. G.; ALMEIDA, E. C.; PEREIRA, J. R. L. de. Smile, you are being identified! Risks and measures for the use of facial recognition in (semi-)public

spaces. **AI and Ethics**, *[S. l.]*, v. 1, n. 2, p. 159–172, 2021. DOI: 10.1007/s43681-020-00014-3. Disponível em: https://doi.org/10.1007/s43681-020-00014-3. Acesso em: 14 jun. 2022.

MUNCINELLI, G. *et al*. Components of the preliminary conceptual model for process capability in LGPD (Brazilian data protection regulation). **Advances in Transdisciplinary Engineering**, *[S. l.]*, v. 12, p. 635–644, 2020. DOI: 10.3233/ATDE200125. Disponível em: https://doi.org/10.3233/ATDE200125. Acesso em: 25 jun 2022.

NACIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). Guide to Protection the Confidentiality of Personally Identifiable Information (PII). **SP 800-122**. Gaithersburg, 2010. Disponível em: https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=904990. Acesso em: 30 jun.2022.

NACIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). An Introdution to Privacy Engineering and Risk Management in Federal Systems. **NISTIR 8062**. Gaithersburg, 2007. Disponível em: https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8062.pdf. Acesso em: 30 jun.2022.

ODEH, M.; KAMM, R. Bridging the gap between business models and systems models. **Information and Software Technology**, v. 45, n. 15, p. 1053-1060, 2003.

OLIVEIRA, A. C. S. de., et.al. Empoderamento digital, proteção de dados e LGPD, **Pesquisa Brasileira em Ciência da Informação e Biblioteconomia.** Disponível em: https://periodicos.ufpb.br/ojs/index.php/pbcib/article/view/54698/31476. Acesso em: 13 jan. 2022.

ORGANISATION FOR ECONOMINC CO-OPERATION AND DEVELOPMENT (OECD). OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. 2013. Disponível em: https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm#part2. Acesso em: 29 jun. 2022.

PIURCOSKY, F. P. *et al*. A lei geral de proteção de dados pessoais em empresas brasileiras: uma análise de múltiplos casos. **Suma de Negocios**, *[S. l.]*, v. 10, n. 23, p. 89–99, 2019. DOI: 10.14349/sumneg/2019.v10.n23.a2. Disponível em: https://doi.org/10.14349/sumneg/2019.v10.n23.a2. Acesso em: 15 jun. 2022.

RACHED, G. FARIAS, E H. de**.** Privacy in Brazil Analysis on the newlaw on data protection. **IADIS International Conference WWW/Internet 2019**, *[S.l]*, p.177-180. 2019. DOI: 10.33965/icwi2019_201913c025. Disponível em: http://www.iadisportal.org/digital-library/privacy-in-brazil-analysis-on-the-new-law-on-data-protection. Acesso em: 16 jun. 2022.

RÊGO, Bergson Lopes. **Gestão e Governança de Dados**: Promovendo dados como ativo de valor nas empresas. Rio de Janeiro: Brasport, 2013.

SHEHABUDDEEN, N.; PROBERT, D.; PHAAL, R.; PLATTS, K. **Representing and**

approaching complex management issues - role and definition. 20 f. Trabalho Acadêmico (Gestão de Tecnologia) – Instituto de Produção, Departamento de Engenharia, Universidade de Cambridge, Cambridge, 1999. Disponível em: https://www.repository.cam.ac.uk/bitstream/handle/1810/288360/00_03_shehabuddeen_platts.pdf?sequence=1&isAllowed=y. Acesso em: 06 dez. 2022.

SILVA JUNIOR, L. A.; LEÃO, M. B. C.. O software Atlas.ti como recurso para a análise de conteúdo: analisando a robótica no Ensino de Ciências em teses brasileiras. **Ciência & Educação (Bauru)**, v. 24, n. Ciênc. educ. (Bauru), 2018 24(3), jul. 2018.

SILVA, R. H da. **Framework para Identificar o Nível de Conformidade das Empresas Brasileiras do Setor Químico no Processo de Adequação à Lei Geral de Proteção de Dados Pessoais**. 94p. Dissertação (Mestrado em Tecnologias da Informação e Comunicação. Universidade Federal de Santa Catarina, Florianopólis, 2021.

STALLINGS, W. **Information Privacy Engineering and Privacy by Design**. USA: Addison-Wesley,2020.

SWAEN, B.; GEORGE, T. What Is a Conceptual Framework: / Tips & Examples. **Scribbr**. Disponível em: https://www.scribbr.com/methodology/conceptual-framework/. Acesso em 06 dez. 2022.

SOUZA, J. S. de. *et al*. The Brazilian Law on Personal Data Protection. **International Journal of Network Security & Its Applications**, *[S. l.]*, v. 12, n. 6, p. 15–25, 2020. DOI: 10.5121/ijnsa.2020.12602.Disponível em: https://doi.org/10.5121/ijnsa.2020.12602. Acesso em: 15 jun. 2022.

SOLOVE, D. J. **Understanding Privacy**. London: Harvard University Press,2008.

SCHAAR, P. Privacy by design. **Identity in the Information Society**, v. 3, n. 2, p. 267-274, 2010.DOI: 10.1007/s12394-010-0055-x. Disponível em: https://doi.org/10.1007/s12394-010-0055-x. Acesso em: 10 fev. 2022.

TEIXEIRA, T.**A LGPD e o e-commerce**. Editora Saraiva, 2021. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786555598155/. Acesso em: 13 jan. 2022.

TRIBUNAL DE CONTAS DA UNIÃO (TCU). Sefti Secretaria de Fiscalização de Tecnologia da Informação. **Relatório de Auditoria**.2020. Disponível em: https://portal.tcu.gov.br/data/files/B4/21/FE/38/5F9618102DFE0FF7F18818A8/038.172-2019-4-AN%20-%20auditoria_Lei%20Geral%20de%20Protecao%20de%20Dados.pdf. Acesso em: 29 jun. 2022.

UE (2016). Regulamento Geral de Proteção de Dados (GDPR): **Regulamento**. Disponível em: https://gdprinfo.eu/. Acesso em: 30 jun. 2022.

UNCTAD. Data Protection and Privacy Legislation Worldwide. **UNCTAD.** Disponível em: https://unctad.org/page/data-protection-and-privacy-legislation-worldwide. Acesso em: 15 jun. 2022.

VENTURA, F. Mega vazamento de CPFs tinha algo que "não é normal": ser organizado demais. **TECNOBLOG**, 31 de jan. de 2022. Disponível em: https://tecnoblog.net/noticias/2022/01/31/megavazamento-de-cpfs-tinha-algo-que-nao-e-normal-ser-organizado-demais/. Acesso em: 28 jun. 2022.

YIN, R. K. Pesquisa qualitativa do início ao fim;tradução: Daniel Bueno, revisão técnica: Dirceu da Silva. – Porto Alegre : **Penso**, 2016. e-PUB.

ZINI, M. J. A. **Proteção de Dados Pessoais no Mundo Empresarial no Cenário da LGPD no Brasil: uma proposta de Framework**. 2020. 122f. Dissertação (Mestrado Profissional em Direito das Empresas e dos Negócios) – Universidade do Vale do Rio dos Sinos, Porto Alegre, 2020. Disponível em: http://www.repositorio.jesuita.org.br/handle/UNISINOS/9810. Acesso em: 20 ago. 2022.

ANEXO 1 – ARTIGOS LGPD

Art. 6º 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.

Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:

I - mediante o fornecimento de consentimento pelo titular;

II - para o cumprimento de obrigação legal ou regulatória pelo controlador;

III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;

IV - para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;

V - quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;

VI - para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ;

VII - para a proteção da vida ou da incolumidade física do titular ou de terceiro;

VIII - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; (Redação dada pela Lei nº 13.853, de 2019) Vigência

IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou

X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

§ 1º (Revogado). (Redação dada pela Lei nº 13.853, de 2019)

§ 2º (Revogado). (Redação dada pela Lei nº 13.853, de 2019) Vigência

§ 3º O tratamento de dados pessoais cujo acesso é público deve considerar a finalidade, a boa-fé e o interesse público que justificaram sua disponibilização.

§ 4º É dispensada a exigência do consentimento previsto no caput deste artigo para os dados tornados manifestamente públicos pelo titular, resguardados os direitos do titular e os princípios previstos nesta Lei.

§ 5º O controlador que obteve o consentimento referido no inciso I do caput deste artigo que necessitar comunicar ou compartilhar dados pessoais com outros controladores deverá obter consentimento específico do titular para esse fim, ressalvadas as hipóteses de dispensa do consentimento previstas nesta Lei.

§ 6º A eventual dispensa da exigência do consentimento não desobriga os agentes de tratamento das demais obrigações previstas nesta Lei, especialmente da observância dos princípios gerais e da garantia dos direitos do titular.

§ 7º O tratamento posterior dos dados pessoais a que se referem os §§ 3º e 4º deste artigo poderá ser realizado para novas finalidades, desde que observados os propósitos legítimos e específicos para o novo tratamento e a preservação dos direitos do titular, assim como os fundamentos e os princípios previstos nesta Lei. (Incluído pela Lei nº 13.853, de 2019) Vigência

Art. 9º 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; e

VII - direitos do titular, com menção explícita aos direitos contidos no art. 18 desta Lei.

§ 1º Na hipótese em que o consentimento é requerido, esse será considerado nulo caso as informações fornecidas ao titular tenham conteúdo enganoso ou abusivo ou não tenham sido apresentadas previamente com transparência, de forma clara e inequívoca.

§ 2º Na hipótese em que o consentimento é requerido, se houver mudanças da finalidade para o tratamento de dados pessoais não compatíveis com o consentimento original, o controlador deverá informar previamente o titular sobre as mudanças de finalidade, podendo o titular revogar o consentimento, caso discorde das alterações.

§ 3º Quando o tratamento de dados pessoais for condição para o fornecimento de produto ou de serviço ou para o exercício de direito, o titular será informado com destaque sobre esse fato e sobre os meios pelos quais poderá exercer os direitos do titular elencados no art. 18 desta Lei.

Seção IV
Do Término do Tratamento de Dados

Art. 15. O término do tratamento de dados pessoais ocorrerá nas seguintes hipóteses:

I - verificação de que a finalidade foi alcançada ou de que os dados deixaram de ser necessários ou pertinentes ao alcance da finalidade específica almejada;

II - fim do período de tratamento;

III - comunicação do titular, inclusive no exercício de seu direito de revogação do consentimento conforme disposto no § 5º do art. 8º desta Lei, resguardado o interesse público; ou

IV - determinação da autoridade nacional, quando houver violação ao disposto nesta Lei.

Art. 16. Os dados pessoais serão eliminados após o término de seu tratamento, no âmbito e nos limites técnicos das atividades, autorizada a conservação para as seguintes finalidades:

I - cumprimento de obrigação legal ou regulatória pelo controlador;

II - estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;

III - transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos nesta Lei; ou

IV - uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados.

CAPÍTULO III
DOS DIREITOS DO TITULAR

Art. 17. Toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade, nos termos desta Lei.

Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição:

I - confirmação da existência de tratamento;

II - acesso aos dados;

III - correção de dados incompletos, inexatos ou desatualizados;

IV - anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei;

V - portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial; (Redação dada pela Lei nº 13.853, de 2019) Vigência

VI - eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei;

VII - informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;

VIII - informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;

IX - revogação do consentimento, nos termos do § 5º do art. 8º desta Lei.

§ 1º O titular dos dados pessoais tem o direito de peticionar em relação aos seus dados contra o controlador perante a autoridade nacional.

§ 2º O titular pode opor-se a tratamento realizado com fundamento em uma das hipóteses de dispensa de consentimento, em caso de descumprimento ao disposto nesta Lei.

§ 3º Os direitos previstos neste artigo serão exercidos mediante requerimento expresso do titular ou de representante legalmente constituído, a agente de tratamento.

§ 4º Em caso de impossibilidade de adoção imediata da providência de que trata o § 3º deste artigo, o controlador enviará ao titular resposta em que poderá:

I - comunicar que não é agente de tratamento dos dados e indicar, sempre que possível, o agente; ou

II - indicar as razões de fato ou de direito que impedem a adoção imediata da providência.

§ 5º O requerimento referido no § 3º deste artigo será atendido sem custos para o titular, nos prazos e nos termos previstos em regulamento.

§ 6º O responsável deverá informar, de maneira imediata, aos agentes de tratamento com os quais tenha realizado uso compartilhado de dados a correção, a eliminação, a anonimização ou o bloqueio dos dados, para que repitam idêntico procedimento, exceto nos casos em que esta comunicação seja comprovadamente impossível ou implique esforço desproporcional. (Redação dada pela Lei nº 13.853, de 2019) Vigência

§ 7º A portabilidade dos dados pessoais a que se refere o inciso V do caput deste artigo não inclui dados que já tenham sido anonimizados pelo controlador.

§ 8º O direito a que se refere o § 1º deste artigo também poderá ser exercido perante os organismos de defesa do consumidor.

Art. 19. A confirmação de existência ou o acesso a dados pessoais serão providenciados, mediante requisição do titular:

I - em formato simplificado, imediatamente; ou

II - por meio de declaração clara e completa, que indique a origem dos dados, a inexistência de registro, os critérios utilizados e a finalidade do tratamento, observados os segredos comercial e industrial, fornecida no prazo de até 15 (quinze) dias, contado da data do requerimento do titular.

§ 1º Os dados pessoais serão armazenados em formato que favoreça o exercício do direito de acesso.

§ 2º As informações e os dados poderão ser fornecidos, a critério do titular:

I - por meio eletrônico, seguro e idôneo para esse fim; ou

II - sob forma impressa.

§ 3º Quando o tratamento tiver origem no consentimento do titular ou em contrato, o titular poderá solicitar cópia eletrônica integral de seus dados pessoais, observados os segredos comercial e industrial, nos termos de regulamentação da autoridade nacional, em formato que permita a sua utilização subsequente, inclusive em outras operações de tratamento.

§ 4º A autoridade nacional poderá dispor de forma diferenciada acerca dos prazos previstos nos incisos I e II do caput deste artigo para os setores específicos.

Art. 20. O titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade. (Redação dada pela Lei nº 13.853, de 2019) Vigência

§ 1º O controlador deverá fornecer, sempre que solicitadas, informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, observados os segredos comercial e industrial.

§ 2º Em caso de não oferecimento de informações de que trata o § 1º deste artigo baseado na observância de segredo comercial e industrial, a autoridade nacional poderá realizar auditoria para verificação de aspectos discriminatórios em tratamento automatizado de dados pessoais.

§ 3º (VETADO). (Incluído pela Lei nº 13.853, de 2019) Vigência

Art. 21. Os dados pessoais referentes ao exercício regular de direitos pelo titular não podem ser utilizados em seu prejuízo.

Art. 22. A defesa dos interesses e dos direitos dos titulares de dados poderá ser exercida em juízo, individual ou coletivamente, na forma do disposto na legislação pertinente, acerca dos instrumentos de tutela individual e coletiva.

Art. 46. 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.

§ 1º A autoridade nacional poderá dispor sobre padrões técnicos mínimos para tornar aplicável o disposto no caput deste artigo, considerados a natureza das informações tratadas, as características específicas do tratamento e o estado atual da tecnologia, especialmente no caso de dados pessoais sensíveis, assim como os princípios previstos no caput do art. 6º desta Lei.

§ 2º 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.