FUNDAÇÃO GETULIO VARGAS
ESCOLA DE ADMINISTRAÇÃO DE EMPRESAS DE SÃO PAULO

EDUARDO KIVES OSTRONOFF

GOVERNANÇA DA PRIVACIDADE:
IMPLANTANDO EM UMA EMPRESA

SÃO PAULO - SP

2023

EDUARDO KIVES OSTRONOFF

GOVERNANÇA DA PRIVACIDADE: IMPLANTANDO EM UMA EMPRESA

Dissertação apresentada à Escola de Administração de Empresas de São Paulo, da Fundação Getulio Vargas, como requisito para obtenção do título de Mestre em Administração Empresas.

Linha de Pesquisa: Tecnologia da Informação

Orientador: Prof. Dr. Adrian Kemmer Cernev

SÃO PAULO
2023

Ostronoff, Eduardo Kives.

Governança da privacidade : implantando em uma empresa / Eduardo Kives Ostronoff. - 2023.

66 f.

Orientador: Adrian Kemmer Cernev.

Dissertação (mestrado profissional MPA) – Fundação Getulio Vargas, Escola de Administração de Empresas de São Paulo.

1. Lei Geral de Proteção de Dados Pessoais (LGPD). 2. Tecnologia da informação. 3. Proteção de dados. 4. Direito à privacidade. 5. Pesquisa-ação. I. Cernev, Adrian Kemmer. II. Dissertação (mestrado profissional MPA) – Escola de Administração de Empresas de São Paulo. III. Fundação Getulio Vargas. IV. Título.

CDU 004.056

Ficha Catalográfica elaborada por: Isabele Oliveira dos Santos Garcia CRB SP-010191/O
Biblioteca Karl A. Boedecker da Fundação Getulio Vargas - SP

EDUARDO KIVES OSTRONOFF

GOVERNANÇA DA PRIVACIDADE: IMPLANTANDO EM UMA EMPRESA

Dissertação apresentada à Escola de Administração de Empresas de São Paulo, da Fundação Getulio Vargas, como requisito para obtenção do título de Mestre em Administração Empresas.

Linha de Pesquisa: Tecnologia da Informação

Data de aprovação: 30/05/2023

Banca examinadora:

_____

Prof. Dr. Adrian Kemmer Cernev
FGV-EAESP

_____

Prof. Dr. José Luiz C. Kugler
FGV-EAESP

_____

Prof. Dr. Marcelo Fantinato
EACH-USP

_____

Profa. Dra. Tania Pereira Christopoulos
EACH-USP

Dedico este trabalho à minha esposa Daliane, que muito me incentivou para buscar um mestrado.

RESUMO

A Lei Geral de Proteção de Dados coloca para as empresas a necessidade de implantação da governança da privacidade como um fator mitigador dos riscos de privacidade em sua operação e como um fator atenuante na aplicação de penalidades pela Agência Nacional de Proteção de Dados na aplicação da referida lei. Este trabalho busca entender como se implanta a governança da privacidade numa empresa, identificando metodologias que auxiliem neste processo e avaliando a adequação destas metodologias à Lei Geral de Proteção de Dados.

O trabalho intervém, através da pesquisa-ação, o processo de implantação da governança da privacidade em uma empresa do mercado segurador. Dada a baixa quantidade de referencial teórico ou prático da governança da privacidade, de início são utilizados modelos de governança de dados para implantar a governança da privacidade, com alguma complexidade operacional. No meio do desenvolvimento do projeto o *National Institute of Standards and Technology* lançou o *Privacy Framework*, com uma função dedicada à governança da privacidade (GOVERN-P). Acompanhamos o processo de implantação deste modelo.

A função de GOVERN-P do *Privacy Framework* do *National Institute of Standards and Technology* mostrou-se um modelo factível de utilização para a implantação em uma empresa, trazendo ferramentas para a avaliação e mitigação dos riscos de privacidade e para facilitar a mudança organizacional necessária à implantação da governança da privacidade. Também mostrou-se adequado à definição de governança da privacidade da Lei Geral de Proteção de Dados, desde que complementado por subcomponentes de outras funções do *Privacy Framework* do *National Institute of Standards and Technology*.

Palavras-chaves

Lei Geral de Proteção de Dados; Governança da Privacidade; Pesquisa-ação; Tecnologia da Informação; NIST Privacy Framework

ABSTRACT

The Brazilian Lei Geral de Proteção de Dados (General Data Protection Law) places the need for companies to implement privacy governance as a mitigating factor of privacy risks in their operation and as a mitigating factor in the application of penalties by the Agência Nacional de Proteção de Dados (Brazilian National Data Protection Agency) in the application of said law. This work seeks to understand how privacy governance is implemented in a company, identifying methodologies that help in this process and evaluating the adequacy of these methodologies to the Lei Geral de Proteção de Dados.

The work intervenes, through action-research, in the process of implementing privacy governance in a company in the insurance market. Given the low amount of theoretical or practical references on privacy governance, initially data governance models are used to implement privacy governance, with some operational complexity. Midway through project development, the National Institute of Standards and Technology released the Privacy Framework, with a dedicated privacy governance function (GOVERN-P). We followed the implementation process of this model.

The GOVERN-P function of the National Institute of Standards and Technology's Privacy Framework proved to be a feasible model for use in a company, providing tools for assessing and mitigating privacy risks and facilitating the organizational change necessary for implementation of privacy governance. It also suited the General Data Protection Act's definition of privacy governance, as long it is complemented by subcomponents of other functions of the Privacy Framework of the National Institute of Standards and Technology.

Key words

Lei Geral de Proteção de Dados; Privacy Governance; Action research; Information Technology; NIST Privacy Framework

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE SIGLAS

ANPD - Agência Nacional de Proteção de Dados

CNSP - Conselho Nacional de Seguros Privados

CRM - Gestão do relacionamento com o cliente, do inglês *Customer Relationship Management*

DPO - Encarregado de proteção de dados pessoais, do inglês *Data Protection Officer*

GDPR - *General Data Protection Regulation*

GSS - Grupo Silvio Santos

KYC - *Know Your Customer*, conheça o seu cliente

KYE - *Know Your Employee*, conheça o seu empregado

KYS - *Know Your Supplier*, conheça o seu fornecedor

LGPD - Lei Geral de Proteção de Dados

NIST - *National Institute of Standards and Technology*

NIST CSF - *National Institute of Standards and Technology Cyber Security Framework*

NIST PF - *National Institute of Standards and Technology Privacy Framework*

OCDE - Organização para a Cooperação e Desenvolvimento Econômico

PLDFT - Prevenção à Lavagem de Dinheiro e ao Financiamento ao Terrorismo

POPIA - *Protection of Personal Information Act*

ROPA - *Report of Processing Activities*, relatório de atividades de processamento

SUSEP - Superintendência de Seguros Privados

TI - Tecnologia da Informação

SUMÁRIO

1 Introdução

Em 14 de agosto de 2018 foi sancionada a lei nº13.709/2018, a Lei Geral de Proteção de Dados (LGPD). O Brasil já dispunha de mais de 40 normas tratando da proteção de dados pessoais e privacidade de maneira não integrada e, por vezes, conflitante. Esta consolidação, se por um lado unifica o tratamento de dados pessoais e traz maior segurança legal, por outro impõem uma nova carga às empresas com o aumento de controles e obrigações em relação aos dados pessoais. A implantação da conformidade a essa lei numa empresa que tem o dever legal de processar os dados de seus clientes é um projeto multidisciplinar, envolvendo áreas como Jurídico, Marketing e Tecnologia da Informação, com interesses conflitantes em relação ao tratamento dos dados dos clientes (MONTEIRO, 2018).

Em linha com as orientações da Organização para a Cooperação e Desenvolvimento Econômico (OCDE) para a proteção da privacidade, a LGPD traz as bases legais para o tratamento de dados pessoais por "pessoas naturais e jurídicas e de direito público ou privado" (BRASIL, 2018) e os princípios a serem observados no tratamento. O conceito de tratamento é amplo, abrangendo o ciclo de vida dos dados através da coleta, processamento, armazenamento, análise, modificação, transferência e eliminação, entre outros. Os direitos do titular de dados e as obrigações inerentes ao tratamento de dados em seus diversos aspectos também estão dispostos na LGPD (BRASIL, 2018; OECD, 1980; TEFFÉ; VIOLA, 2020).

Entre as sanções possíveis pelo descumprimento da LGPD estão multas de até 2% do faturamento da firma, limitadas a R$ 50.000.000,00 (cinquenta milhões de reais), sendo que um dos fatores a serem considerados na definição do valor da sanção está a adoção de boas práticas e governança (BRASIL, 2018). Portanto a adoção efetiva de uma governança de privacidade tem a dupla vantagem de, em tese, reduzir a probabilidade de ocorrência de um incidente que leve a uma sanção e reduzir o valor da eventual sanção.

O legislador detalhou os requisitos do programa de governança:

> Art. 50. Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais.

> [...] § 2º Na aplicação dos princípios indicados nos incisos VII e VIII do caput do art. 6º desta Lei, o controlador, observados a estrutura, a escala e o volume de suas operações, bem como a sensibilidade dos dados tratados e a probabilidade e a gravidade dos danos para os titulares dos dados, poderá:
> I – implementar programa de governança em privacidade que, no mínimo:
> a) demonstre o comprometimento do controlador em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais;
> b) seja aplicável a todo o conjunto de dados pessoais que estejam sob seu controle, independentemente do modo como se realizou sua coleta;
> c) seja adaptado à estrutura, à escala e ao volume de suas operações, bem como à sensibilidade dos dados tratados;
> d) estabeleça políticas e salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade;
> e) tenha o objetivo de estabelecer relação de confiança com o titular, por meio de atuação transparente e que assegure mecanismos de participação do titular;
> f) esteja integrado a sua estrutura geral de governança e estabeleça e aplique mecanismos de supervisão internos e externos;
> g) conte com planos de resposta a incidentes e remediação; e
> h) seja atualizado constantemente com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas. (BRASIL, 2018).

Apesar da LGPD definir os componentes da governança da privacidade que espera, estes componentes não são suficientes para se implantar a governança de privacidade. Os oito requisitos do *caput* do artigo 50 e os outros oito itens do inciso I do mesmo artigo podem ser catalogados como princípios ou funcionalidades e resultados esperados (ver Tabela 1 e Tabela 2). Tais componentes não são suficientes para estruturar a governança de privacidade, portanto é necessário agregar um modelo externo para a governança da privacidade.

Tabela 1 – Categorização *caput* Art. 50 LGPD

Aspecto de boas práticas e governança do Art. 50 da LGPD	Categoria
As condições de organização	Resultado
O regime de funcionamento	Resultado
Os procedimentos incluindo reclamações e petições de titulares	Resultado
As normas de segurança	Resultado
Os padrões técnicos	Resultado
As obrigações específicas para os diversos envolvidos no tratamento	Resultado
As ações educativas	Resultado
Os mecanismos internos de supervisão e de mitigação de riscos	Resultado
Outros aspectos relacionados ao tratamento de dados pessoais	-

Fonte: elaboração própria.

Tabela 2 – Categorização inciso I do Art. 50 LGPD

Componentes da governança de privacidade do Art. 50, inciso I da LGPD	Categorias
a) demonstre o comprometimento do controlador em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais;	Princípio
b) seja aplicável a todo o conjunto de dados pessoais que estejam sob seu controle, independentemente do modo como se realizou sua coleta;	Princípio
c) seja adaptado à estrutura, à escala e ao volume de suas operações, bem como à sensibilidade dos dados tratados;	Princípio
d) estabeleça políticas e salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade;	Princípio
e) tenha o objetivo de estabelecer relação de confiança com o titular, por meio de atuação transparente e que assegure mecanismos de participação do titular;	Princípio
f) esteja integrado a sua estrutura geral de governança e estabeleça e aplique mecanismos de supervisão internos e externos;	Requisito
g) conte com planos de resposta a incidentes e remediação;	Requisito
h) seja atualizado constantemente com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas;	Requisito

Fonte: elaboração própria.

A governança da privacidade, proposta na lei, é um conceito novo na academia. O conceito de governança está ligado à divisão de poderes em uma sociedade ou empresa, a governança corporativa trata das estruturas, processos e mecanismos relacionais para o alinhamento dos interesses dos investidores e administradores e redução de externalidades na geração de valor pela empresa (DE HAES; VAN GREMBERGEN, 2005; HUBERTS, 2014; MONKS; MINOW, 2011; SHLEIFER; VISHNY, 1997). Por esta lente, a governança da privacidade seria as estruturas, processos e mecanismos relacionais para alinhar os interesses da empresa (acionistas e administradores) aos das partes que fornecem os dados (clientes, fornecedores e funcionários) para a operação desta, reduzindo as externalidades no tratamento dos dados pessoais.

Dado que a LGPD se aplica a todas as organizações que tratam dados pessoais e que os riscos financeiros e reputacionais advindos das sanções são significativos, a implantação de mecanismos de mitigação dos riscos de problemas no tratamento de dados pessoais é de grande relevância. Por outro lado, o tratamento dos dados pessoais, em suas várias formas, pode ser uma parte relevante dos processos das empresas. A governança da privacidade, ao buscar alinhar os interesses da empresa aos dos titulares de dados e reduzir as externalidades, trabalha para se obter um compromisso entre os riscos do tratamento de dados e as

necessidades das organizações. Desta forma, o estudo da implantação da governança da privacidade pode trazer ganhos para as organizações e para a sociedade.

O estudo da governança da privacidade, e mais especificamente dos processos necessários para a sua implantação efetiva são o foco deste trabalho, buscando responder à questão de **como se implanta a governança da privacidade numa empresa.** Os objetivos da pesquisa são: identificar metodologias para a implantação da governança da privacidade e avaliar a sua adequação à LGPD.

Para tanto, este trabalho acompanhou e interveio no processo de implantação da conformidade à LGPD na Liderança Capitalização S/A (Liderança), empresa do Grupo Silvio Santos (GSS), regulada pela Superintendência de Seguros Privados (SUSEP). A metodologia utilizada foi a pesquisa-ação. A pesquisa se desenvolveu em duas fases, interrompida pela pandemia do COVID-19. Na primeira fase, em dois ciclos de pesquisa-ação, buscou-se estruturar a governança da privacidade previamente à implantação das ações de adequação à LGPD. Na segunda fase, com um ciclo de pesquisa-ação, a implantação da governança da privacidade e da adequação à LGPD se deram em paralelo.

No início dos trabalhos da pesquisa, em 2019, uma consulta na base de dados SCOPUS com os termos TITLE-ABS-KEY (“privacy governance” OR “governance of privacy”) trazia somente 50 documentos. Para comparação, a pesquisa na mesma base e período com os termos TITLE-ABS-KEY (“information technology governance” OR “it governance”) trazia 2.016 documentos. Buscando uma alternativa, pela limitação das visões teóricas de governança da privacidade, usamos a definição de Dennedy, Fox e Finneran (2014), para quem a proteção de dados privados é um componente da governança de dados de informações pessoais. À mesma época, uma consulta na mesma base de dados dos termos TITLE-ABS-KEY (“data governance”) trazia 767 documentos, mostrando que a governança de dados é um campo de estudo com uma ordem de grandeza a mais de estudos. Utilizamos na primeira fase da pesquisa uma abordagem partindo da governança de dados como um componente da governança de tecnologia da informação (TI) para entende-la como uma disciplina separada (KHATRI; BROWN, 2010; WEILL; ROSS, 2004) adotando os modelos os conceituais da governança de dados de Alhassan, Sammon e Daly (2018) e de Abraham, Schneider e Vom Brocke (2019).

Na segunda fase adotamos como base a função de governança do National Institute of Standards and Technology Privacy Framework (NIST PF). Publicado em sua primeira versão em janeiro de 2020, busca trazer para a gestão de privacidade o que o NIST Cyber Security Framework (NIST CSF) trouxe para a segurança cibernética. O NIST CSF se tornou um padrão de fato para os *frameworks* de segurança nos EUA (NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, 2020; “Whitepaper”, 2016).

Na próxima seção deste documento aprofundamos a base teórica utilizada ao longo do projeto, tratando da privacidade e proteção de dados, conceitos gerais de governança corporativa e partindo para as governanças de TI, de dados e da privacidade. Na terceira seção apresentamos as bases metodológicas da pesquisa-ação e da sua aplicação em organizações onde o pesquisador atua profissionalmente. Na quarta seção o desenvolvimento da pesquisa é detalhado, tratando dos três ciclos da intervenção na Liderança. Os resultados são discutidos na quinta seção, confrontando-os com a base teórica. Por fim apresentamos as conclusões.

2 Base teórica

2.1 Privacidade e proteção de dados pessoais

O fundamento da LGPD é a proteção da privacidade, ou seja, a proteção dos dados pessoais. A história da do direito à privacidade é usualmente associada a um artigo de Samuel Warren e Louis Brandeis publicado em 1890 na Harvard Law Review, definindo o direito à privacidade como o "direito de ser deixado a sós". Por outro lado, privacidade é um conceito antigo, aparecendo na Bíblia e em códigos legais da antiguidade (GAJDA, 2007; LEPORE, 2020; LUKÁCS, 2016; WARREN; BRANDEIS, 1890).

Na visão de Westin (1967), privacidade é a autodeterminação de quando, como e quanta informação sobre o indivíduo ou grupo é comunicada a outras partes. A privacidade surge com as origens animais do homem e está presente desde a pré-história. Numa visão de privacidade como uma dinâmica bidirecional entre partes que varia no tempo, para Altman (1975) privacidade é "controle seletivo de acesso ao *self*".

A questão da privacidade pode ser associada ao espaço físico de convivência comunal. A distância entre as propriedades nas colônias da América do Norte permitia um isolamento que não se encontrava em pequenas comunidades rurais ou nas cidades do velho mundo, levando a uma percepção maior da privacidade. Com o avanço da urbanização e da tecnologia, os tabloides de fofocas e a fotografia instantânea, surgiram novas ameaças à privacidade, levando ao argumento de Warren e Brandeis de que as mudanças sociais, políticas e econômicas na sociedade devem se refletir na evolução das leis em resposta a demandas da sociedade (HOLVAST, 2007; LUKÁCS, 2016; SOLOVE, 2006).

Privacidade substantiva é o direito de cada um definir e viver a sua vida com autodeterminação, dividida por Dennedy, Fox e Finneran (2014) em três formas:

a) privacidade decisória é tomar decisões sem escrutínio de terceiros, é a autodeterminação da vida privada;

b) privacidade comportamental é agir conforme a sua vontade sem intromissão ou observação de terceiros; e,

c) privacidade física é ter controle sobre o acesso ao seu próprio corpo.

Estas categorias não são mutuamente exclusivas. Para os autores, a proteção de dados é uma derivação da privacidade substantiva. A privacidade dos dados surge a partir do momento em que um terceiro se envolve com dados que descrevem uma pessoa, passando a ter uma responsabilidade fiduciária quanto ao acesso a estes dados.

Lukács (2016) aponta o surgimento de um novo direito associado à privacidade com a informatização, o direito à proteção de dados. Ao longo do século 20, diversas declarações de direitos já incluíam o direito à privacidade. Um dos primeiros esforços para a padronização internacional da situação legal da privacidade foi a publicação pela Organização para a Cooperação e Desenvolvimento Econômico (OCDE) em 1980 das "*Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data*", que estabelecia diversos dos princípios hoje nas legislações: limitação da coleta, qualidade dos dados, definição da finalidade, limitação de utilização, *back-up* de segurança, abertura, participação do indivíduo e responsabilização (KRAMER; HOAR, 2017; LUKÁCS, 2016; OECD, 1980, 2002).

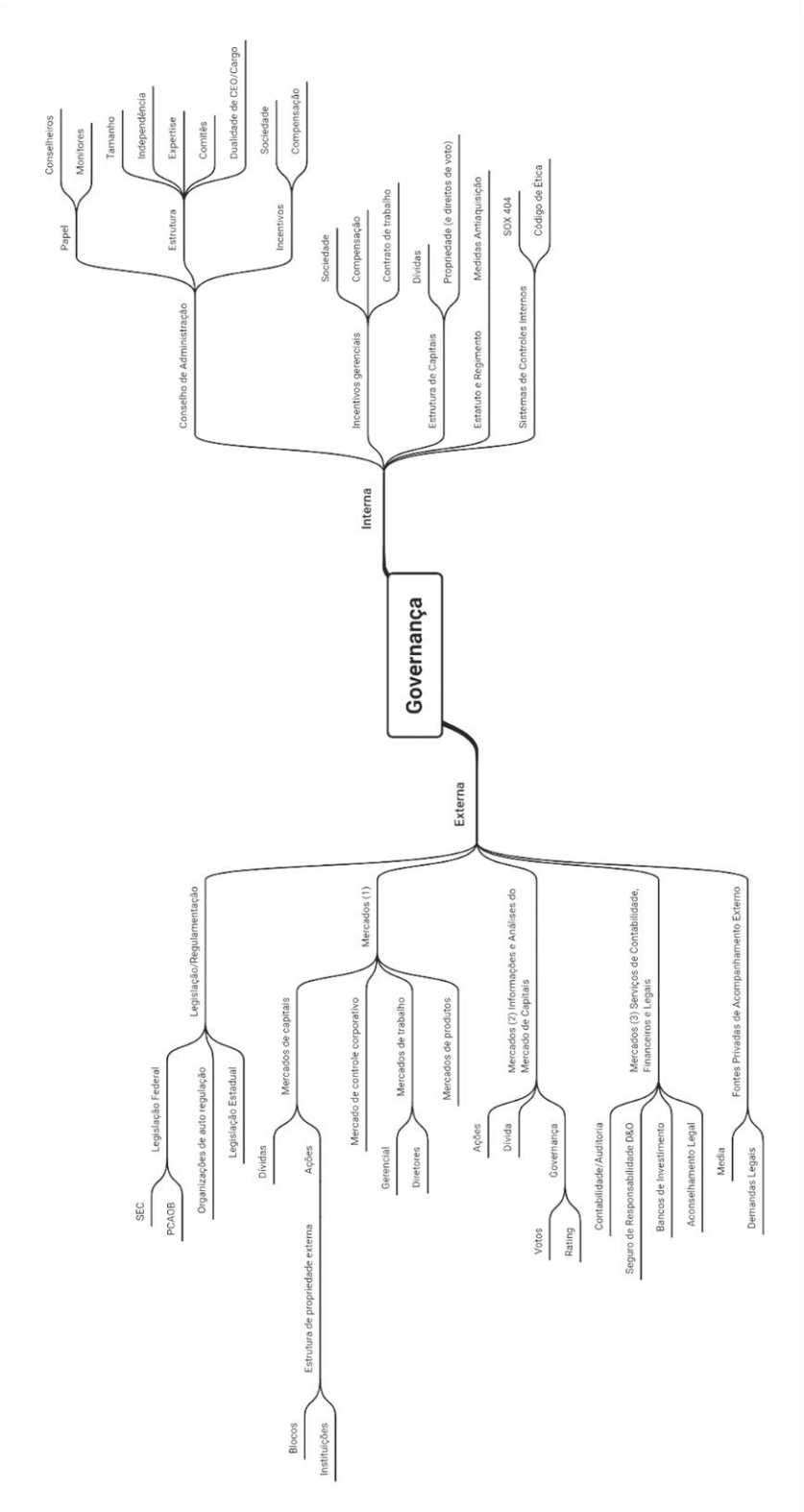
Outro predecessor da LGPD foi o *General Data Protection Regulation* (GDPR) europeu. Aprovado em 2016 e vigorando em 2018, incluía, entre outras determinações, a criação de obstáculos para a transferência internacional de dados pessoais para países sem uma legislação adequada de proteção de dados. A LGPD, sendo uma legislação que protege a privacidade, favorece a troca de dados com empresas sujeitas à GDPR (MONTEIRO, 2018).

2.2 **Governança e Governança Corporativa**

Na definição de Fukuyama (2013), governança é "a capacidade de um governo criar e fazer cumprir regras e entregar serviços", claramente voltada para a questão pública do Estado e governos locais. Numa abordagem mais ampla, Huberts (2014) vê governança relacionada às dinâmicas da divisão de poder e autoridade em governos, na sociedade civil e nas empresas. Trazendo o foco para as empresas, Shleifer e Vishny (1997) veem a governança corporativa lidando com a questão da agência, ou seja, a separação entre administradores e fornecedores de capital. A função da governança corporativa seria garantir que os administradores retornem o capital aos investidores alinhando os objetivos das partes.

Segundo Monks e Minow (2011), governança corporativa é uma maneira de responder a duas questões: como fazer com que os administradores se comprometam com a criação de valor aos acionistas como se comprometeriam caso o dinheiro fosse deles mesmos e como gerar valor nas empresas reduzindo as externalidades na sociedade. O conceito de governança para a OCDE é “estrutura através da qual os objetivos da empresa são definidos e se determina os meios para alcançar esses objetivos e para monitorizar o desempenho” (2016). Isto é feito por meio do sistema de pesos e contrapesos da governança corporativa. Gillan (2006) divide os componentes em Internos e Externos e os apresenta uma visão dos componentes que identifica como chaves na Figura 1. Nem todos estes componentes são tradicionalmente identificados com a governança corporativa, mas são parte do ambiente que afetam a governança corporativa. As conexões entre os elementos de governança, além da hierarquia, não são desenhadas dada a dificuldade em sua representação, mas diversos nós são correlacionados e se influenciam.

Figura 1 – Componentes da governança corporativa



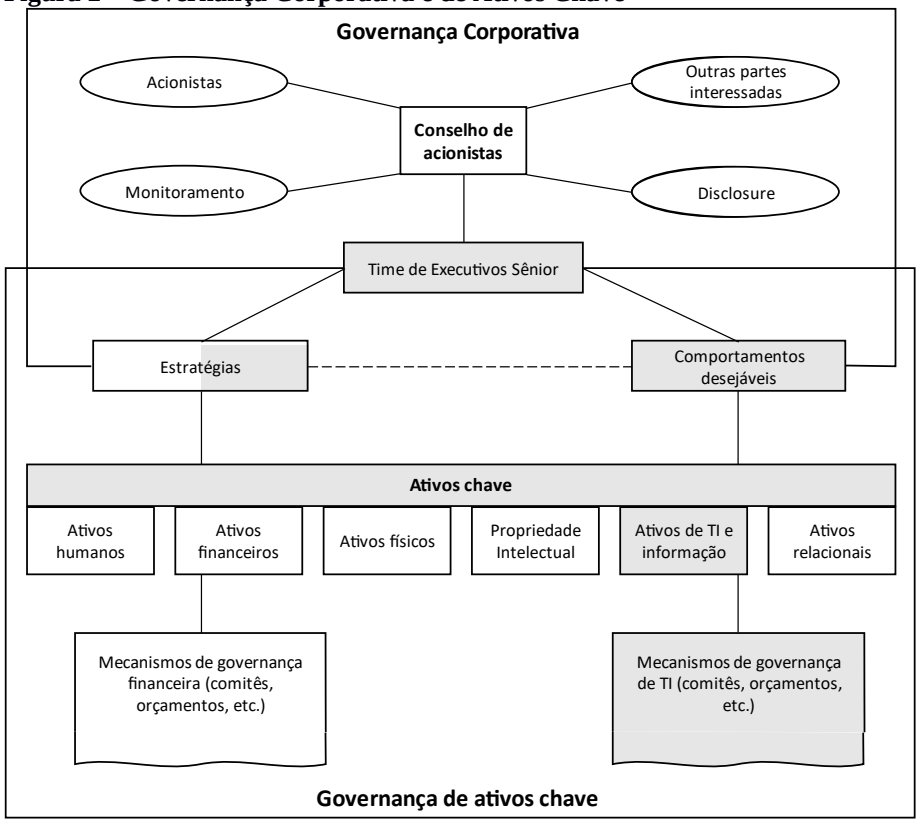
Fonte: adaptado de (GILLAN, 2006).

2.3 **Governança de TI**

Segundo Weill e Ross (2004), governança de TI é a especificação de alçadas de decisão e responsabilidades para encorajar comportamentos desejáveis no uso da TI. O alinhamento estratégico entre o negócio e TI objetiva garantir que os gastos em TI gerem valor para o negócio (DE HAES; VAN GREMBERGEN, 2005).

Weill e Ross (2004) mapeiam o relacionamento da governança de TI com a governança corporativa na Figura 2. O Time Executivo Sênior articula as escolhas estratégicas e os comportamentos desejáveis conforme os direcionamentos do Conselho de Administração. Estas estratégias e, principalmente, os comportamentos desejáveis governam a forma como os Ativos Chave são gerenciados individualmente e em grupo. Os mecanismos de governança dos ativos são listados na parte de baixo da figura.

Figura 2 – Governança Corporativa e de Ativos Chave



Fonte: adaptado de (WEILL; ROSS, 2004).

As principais decisões a serem tomadas pela governança de TI são: princípios de TI, arquitetura de TI, infraestrutura de TI, necessidades de aplicações de negócio e priorização e investimento de TI. Estas questões são interrelacionadas conforme demonstrado na Figura 3.

Os princípios de TI, por traduzir os objetivos corporativos para TI, ficam no topo. Os princípios descem através das decisões da arquitetura para definirem os requisitos de padronização e integração e as decisões de investimento dirigem os recursos financeiros para a tradução dos princípios. O fluxo para as decisões de necessidades de aplicações de negócios podem ser *top-down*, com os princípios, arquitetura e investimentos limitando as aplicações, ou necessidades de negócio podem subir, influenciando a infraestrutura e investimentos.

Figura 3 – Decisões chave de Governança de TI

<table>
<tr><td colspan="3">Decisões de princípios de TI
Definições de alto nível sobre como TI é usada no negócio</td></tr>
<tr><td rowspan="2">Decisões de arquitetura de TI
Organização lógica para dados, aplicações e infraestrutura capturada em um conjunto de políticas, relacionamentos e escolhas técnicas para atingir o alinhamento desejado com o negócio e padronização e integração técnicas</td><td>Decisões de infraestrutura de TI
Serviços compartilhados de TI, coordenados centralizadamente, que provem a fundação para as capacidades de TI da empresa</td><td rowspan="2">Decisões de investimentos e priorização de TI
Decisões sobre quanto e aonde investir em TI, incluindo aprovação de projetos e justificativas técnicas</td></tr>
<tr><td>Necessidades de aplicações de negócio
Especificação das necessidades de negócio para aplicações de TI adquiridas ou desenvolvidas internamente</td></tr>
</table>

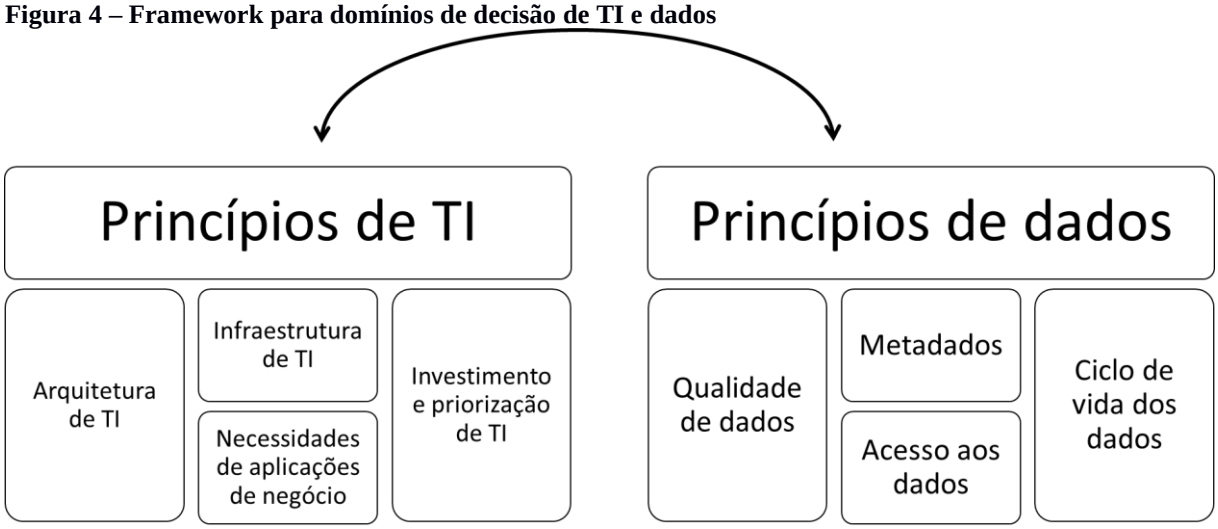
Fonte: adaptado de (WEILL; ROSS, 2004).

2.4 **Governança de Dados**

Governança está relacionada a quais decisões devem ser tomadas por quem para garantir um efetivo gerenciamento, ou seja, inclui não só os temas a serem decididos como também os atores da decisão. Portanto, governança de dados trata das alçadas e decisões que devem ser tomadas para um efetivo gerenciamento dos dados. Esta também pode ser entendida como um framework para o gerenciamento de dados como um ativo estratégico (ABRAHAM; SCHNEIDER; VOM BROCKE, 2019; ALHASSAN; SAMMON; DALY, 2018; FU et al., 2011).

Weill e Ross (2004), ao tratarem dos ativos organizacionais chaves para serem governados, incluem a informação (dados) na mesma categoria que os ativos de TI. Khatri e Brown (2010) separam os ativos de TI, *hardware*, *software* e ativos de comunicação, dos ativos de informação e derivam um modelo dos domínios de decisão para a governança de dados a partir dos domínios definidos por Weill e Ross para a governança de TI (vide Figura 4).

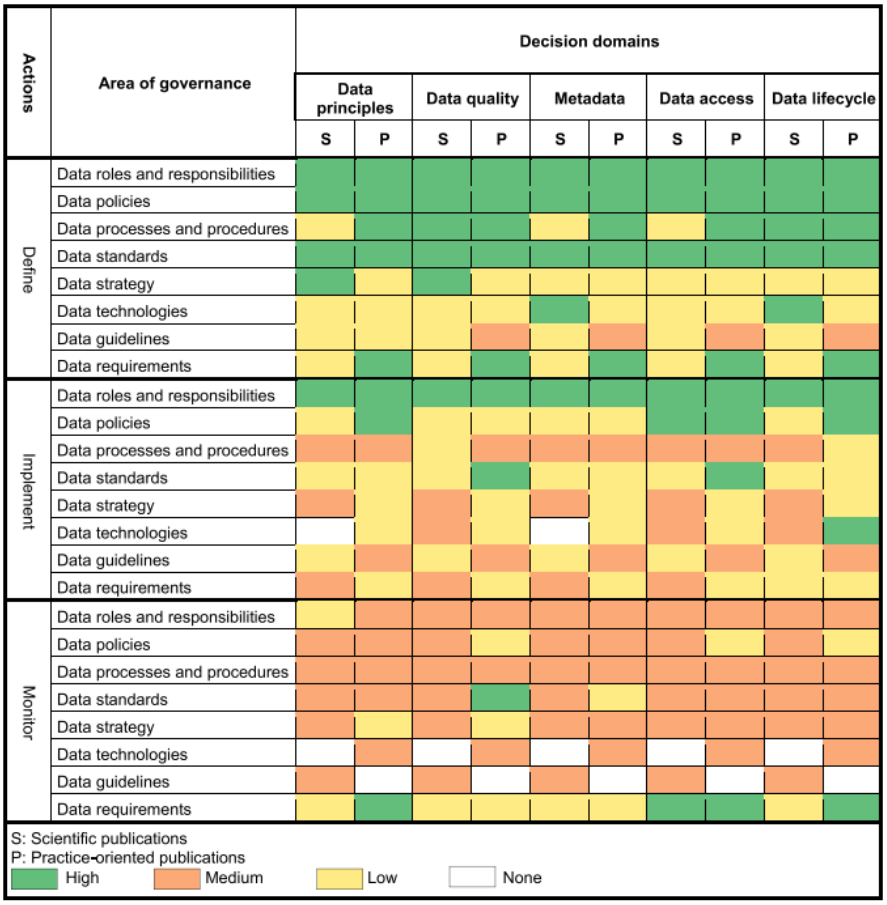
Figura 4 – Framework para domínios de decisão de TI e dados



Fonte: adaptado de (KHATRI; BROWN, 2010).

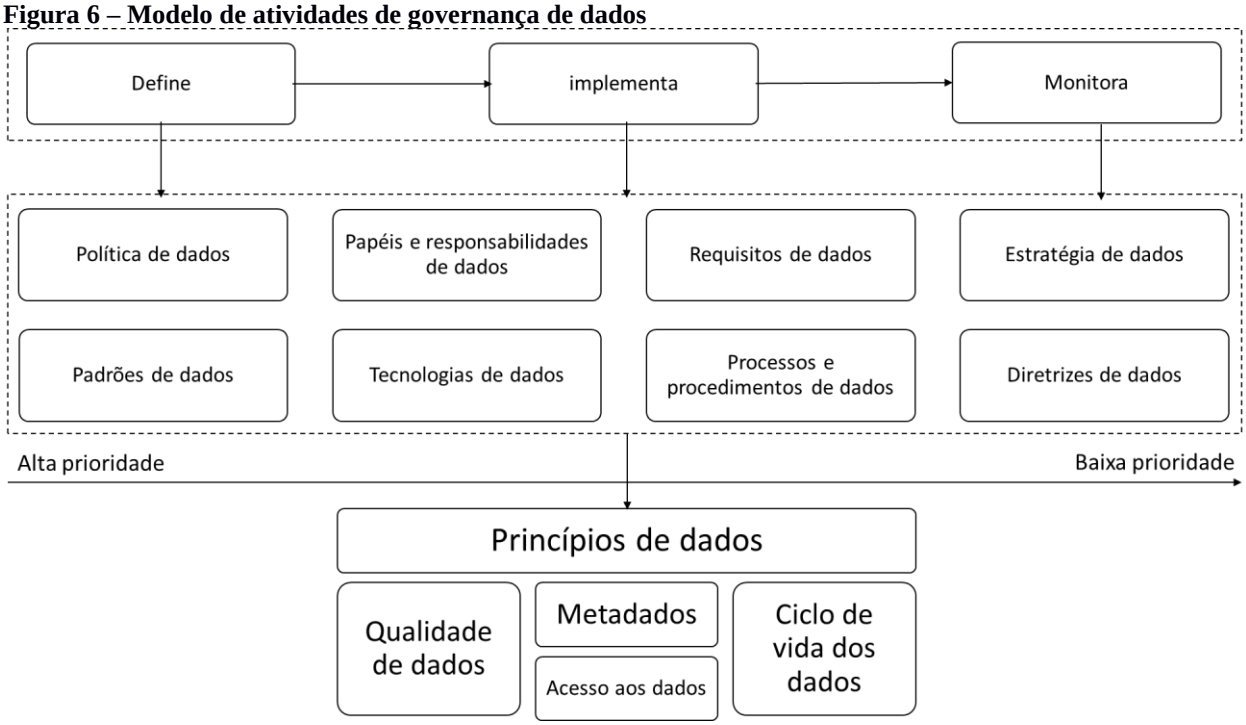
Alhassan, Sammon e Daly (2018) fizeram um trabalho de revisão de literatura que identifica, categoriza e prioriza as atividades de governança de dados em publicações científicas e orientadas à prática alinhadas aos domínios de decisão da governança de dados de Khatri e Brown. Eles chegam a três ações, aplicadas a oito áreas de governança dentro dos cinco domínios de decisão da governança de dados que foram analisadas de acordo com a frequência de citação na literatura científica e prática, demonstrada na Figura 5. Da análise da frequência sai o modelo de implantação da governança de dados (ver Figura 6): inicialmente se definem as oito áreas de governança através dos cinco domínios de decisão, passando então para a implantação e monitoramento das áreas de governança. E as áreas com maior frequência de citação, e consequente maior prioridade, são “política de dados”, “padrões de dados” e “papéis e responsabilidades de dados”.

Figura 5 – Análise do nível de frequência das atividades de governança de dados nas publicações selecionadas



Fonte: adaptado de (ALHASSAN; SAMMON; DALY, 2018)

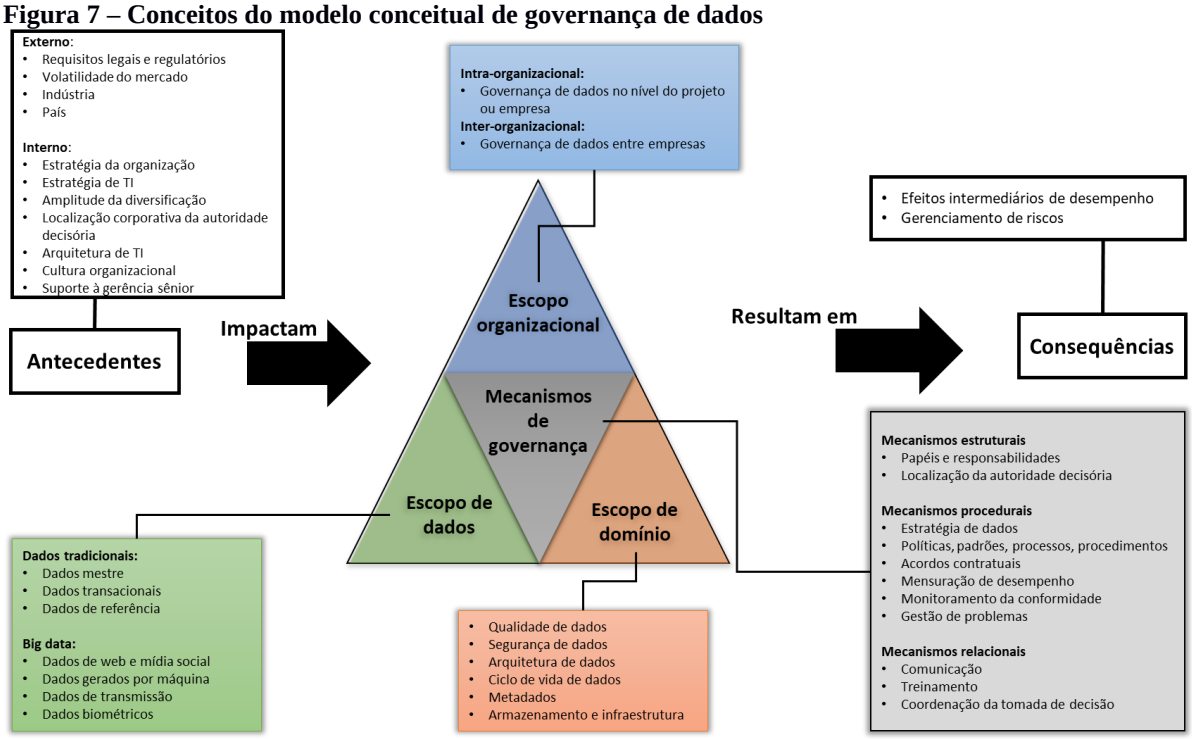
Figura 6 – Modelo de atividades de governança de dados



Fonte: adaptado de (ALHASSAN; SAMMON; DALY, 2018)

Num outro trabalho de revisão da literatura, Abraham, Schneider e Vom Brocke (2019) montam um *framework* conceitual com 6 dimensões (ver Figura 7): os mecanismos *core* de governança, que podem ser estruturais, procedurais ou relacionais; o escopo organizacional, identificando a abrangência organizacional da governança, o escopo de dados e o escopo de domínios; os antecedentes, que englobam as contingências que impactam a governança de dados e as consequências ou os efeitos da governança.

Figura 7 – Conceitos do modelo conceitual de governança de dados



Fonte: adaptado de (ABRAHAM; SCHNEIDER; VOM BROCKE, 2019)

2.5 **Governança da Privacidade**

A governança de privacidade é um campo de estudos relativamente novo. A pesquisa na base de dados SCOPUS com os parâmetros TITLE-ABS-KEY ("privacy governance" OR "governance of privacy") retorna 66 artigos em dezembro de 2022 e o mais antigo destes é de 2000. Os artigos foram categorizados conforme o tema segundo a Tabela 3. As categorias “Computação em nuvem”, “Governança da inteligência artificial”, “Governança da internet das coisas” e “Segurança cibernética” são autoexplicativas. A “Governança da privacidade aplicada à medicina” se refere aos artigos que tratam dos aspectos da governança de privacidade em ambientes médicos ou de pesquisas biológicas, com um nível de exigência mais estrito que o necessário em ambientes corporativos, dado o tratamento massivo de dados pessoais sensíveis. A categoria “Jurídico” se refere aos artigos que tratam do viés jurídico da governança da privacidade, sem abordar as questões sob a lente da administração. Os artigos na categoria “Modelagem da privacidade” tratam de questões teóricas da privacidade. A categoria “Programa de privacidade” abrange os artigos que apresentam questões ligadas à gestão da privacidade. Os artigos de “Tecnologia” tratam de aspectos tecnológicos ligados à

privacidade. A "Visão regulatória" apresenta a visão do regulador da governança da privacidade, incluindo também as questões de transferência internacional de dados. O autor não conseguiu acesso aos sete documentos da categoria "Sem acesso" por falta de convênios da FGV com os editores e falta de informações de contato dos autores. Dentre os artigos da "Governança de privacidade", o único que trata de um modelo de governança da privacidade aplicável a uma empresa que não trate dados sensíveis é o de Swartz, da Veiga e Martins (2019), o outro trata de um modelo de questionário para avaliar a percepção dos funcionários sobre a governança da privacidade (SWARTZ; DA VEIGA; MARTINS, 2021).

Tabela 3 – Categorização dos artigos

Categoria	Artigos
Computação em nuvem	2
Governança de inteligência artificial	1
Governança da privacidade aplicada à medicina	5
Governança de privacidade	2
Governança da internet das coisas	1
Jurídico	2
Modelagem da privacidade	8
Programa de privacidade	7
Segurança cibernética	4
Sem acesso	7
Tecnologia	11
Visão regulatória	16

Fonte: elaboração própria

O modelo conceitual de Swartz, da Veiga e Martins é baseado na comparação de políticas de governança existentes e propõem um modelo conceitual consolidado. O artigo seleciona quatro *frameworks* de governança da privacidade de órgãos reguladores da privacidade com base no atendimento aos princípios de privacidade da OCDE e por mapearem os princípios do *Protection of Personal Information Act* (POPIA), a legislação de proteção de dados sul-africana. Os *frameworks* selecionados são: "*Information and Privacy Commission of New South Wales: Privacy Governance Framework*", "*Common Privacy Framework of the Information Privacy Commissioner of Ontario – CCIM Assessment Projects*", "*Privacy Management Program The Office of the Privacy Commissioner of Canada*", e "*The Office of the Australian Information Commissioner (OAIC) – Privacy Management Framework*" (SWARTZ; DA VEIGA; MARTINS, 2019).

Swartz, da Veiga e Martins analisam os componentes dos quatro frameworks de governança de privacidade e elencam 13 componentes comuns que podem ser adotados pelas organizações para implementar a sua governança de privacidade. O modelo tem uma abordagem de fluxo de processos, iniciando com o **compromisso organizacional** pela alta direção definindo as estratégias e objetivos de privacidade e criando a estrutura de gestão da privacidade. Com base nestas estratégias são definidos **políticas e procedimentos** que definem os **controles do programa de privacidade** e o **processo de avaliação contínua** da privacidade que retroalimenta o fluxo, como mostra a Figura 8 (SWARTZ; DA VEIGA; MARTINS, 2019).

Figura 8 – Modelo conceitual de governança da privacidade

Fonte: adaptado de (SWARTZ; DA VEIGA; MARTINS, 2019)

Num desenvolvimento relativamente fora da academia, o *National Institute of Standards and Technology* (NIST, instituto governamental americano de desenvolvimento de padrões e normas técnicas) veio desenvolvendo um framework de gestão da privacidade desde 2018, publicando a versão inicial em 2020. O framework de privacidade do NIST (NIST PF, do inglês *NIST Privacy Framework*) segue a estrutura do NIST Cybersecurity Framework, um dos frameworks de segurança cibernética mais adotados nos EUA (“Whitepaper”, 2016), buscando facilitar o uso dos dois modelos em conjunto. O modelo visa facilitar o diálogo entre os níveis da organização (do executivo para o operacional) e da organização com os públicos externos (indivíduos, parceiros de negócio e reguladores). O modelo é composto

pelo *Core*, *Profiles* e *Implementation Tiers*. O *Core* lista cinco funções que agrupam 18 categorias que se dividem em 100 subcategorias de atividades e resultados de proteção da privacidade. As funções, categorias e subcategorias escolhidas para serem priorizadas pela organização para a gestão da privacidade estão nos *Profiles*, que podem representar a situação atual ou desejada da organização. Os *Implementation Tiers* descrevem os níveis de implementação dos controles específicos e traduzem o nível de formalização destes controles, que devem ser alinhados ao *Profile* buscado pela organização. O modelo estimula uma abordagem diferenciada para cada organização, fugindo de uma solução de tamanho único (KOERNER, KATHARINA, 2021; NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, 2020).

Uma das funções do *Core* é a governança (GOVERN-P), composta por 4 categorias e 20 subcategorias (vide Tabela 4 – Função GOVERN-P do NIST PF).

Tabela 4 – Função GOVERN-P do NIST PF

NIST Privacy Framework Core		
Função	Categoria	Subcategoria
GOVERN-P (GV-P): Desenvolver e implementar a estrutura de governança organizacional para habilitar uma comprrensão contínua das prioridades de gerenciamento de riscos da organização que são informadas pelo risco de privacidade	**Governance Policies, Processes, and Procedures (GV.PO-P):** As políticas, processos e procedimentos para gerenciar e monitorar os requisitos regulatórios, legais, de risco, ambientais e operacionais da organização são compreendidos e informam o gerenciamento do risco de privacidade.	**GV.PO-P1:** Valores e políticas de privacidade da organização (por exemplo, condições de processamento de dados como uso de dados ou períodos de retenção, prerrogativas individuais com relação ao processamento de dados) são estabelecidos e comunicados. **GV.PO-P2:** Processos para incutir os valores de privacidade da organização no desenvolvimento e operações de sistemas/produtos/serviços são estabelecidos e implementados. **GV.PO-P3:** Os papéis e responsabilidades no que diz respeito à privacidade são estabelecidas para a força de trabalho. **GV.PO-P4:** Os papéis e responsabilidades de privacidade são coordenadas e alinhadas com as partes interessadas (por exemplo, provedores de serviços, clientes, parceiros). **GV.PO-P5:** Os requisitos legais, regulatórios e contratuais relativos à privacidade são compreendidos e gerenciados.

		GV.PO-P6: Políticas, processos e procedimentos de governança e gerenciamento de riscos abordam riscos de privacidade.
	Risk Management Strategy (GV.RM-P): As prioridades, restrições, tolerâncias a riscos e hipóteses da organização são estabelecidas e usadas para dar suporte às decisões de risco operacional.	**GV.RM-P1:** Os processos de gerenciamento de riscos são estabelecidos, gerenciados e acordados pelas partes interessadas da organização. **GV.RM-P2:** A tolerância ao risco da organização é definida e claramente expressa. **GV.RM-P3:** A determinação da tolerância ao risco da organização é informada por sua(s) função(ões) no ecossistema de processamento de dados.
	Awareness and Training (GV.AT-P): A força de trabalho da organização e terceiros envolvidos no processamento de dados recebem educação de conscientização sobre privacidade e são treinados para desempenhar seus papéis e responsabilidades relacionadas à privacidade de acordo com políticas, processos, procedimentos e acordos relacionados e valores de privacidade da organização.	**GV.AT-P1:** A força de trabalho é informada e treinada sobre seus papéis e responsabilidades. **GV.AT-P2:** Os executivos seniores entendem suas funções e responsabilidades. **GV.AT-P3:** A equipe de privacidade entende seus papéis e responsabilidades. **GV.AT-P4:** Terceiros (por exemplo, provedores de serviços, clientes, parceiros) entendem seus papéis e responsabilidades.
	Monitoring and Review (GV.MT-P): As políticas, processos e procedimentos para revisão contínua da postura de	**GV.MT-P1:** O risco de privacidade é reavaliado de forma contínua assim como fatores-chave, incluindo o ambiente de negócios da organização (por exemplo, introdução de novas tecnologias), governança (por exemplo, obrigações legais, tolerância ao risco), processamento de dados e mudança de sistemas/produtos/serviços .

	privacidade da organização são compreendidos e informam o gerenciamento do risco de privacidade.	**GV.MT-P2**: Valores, políticas e treinamento de privacidade são revisados e quaisquer atualizações são comunicadas. **GV.MT-P3**: Políticas, processos e procedimentos para avaliar a conformidade com requisitos legais e políticas de privacidade estão estabelecidos e em vigor. **GV.MT-P4:** Políticas, processos e procedimentos para comunicar o progresso no gerenciamento de riscos de privacidade estão estabelecidos e em vigor. **GV.MT-P5:** Políticas, processos e procedimentos são estabelecidos e implementados para receber, analisar e responder a ações problemáticas de dados divulgadas à organização de fontes internas e externas (por exemplo, descoberta interna, pesquisadores de privacidade, eventos profissionais). **GV.MT-P6:** Políticas, processos e procedimentos incorporam lições aprendidas com ações problemáticas de dados. **GV.MT-P7:** Políticas, processos e procedimentos para receber, rastrear e responder a reclamações, preocupações e perguntas de indivíduos sobre práticas de privacidade da organização são estabelecidos e implementados.

Fonte: NIST (2020), tradução do autor.

O NIST tem um modelo formal de avaliação de riscos de segurança e privacidade (JOINT TASK FORCE TRANSFORMATION INITIATIVE, 2012) e documentos com controles que podem ser aplicados na mitigação dos riscos encontrados (JOINT TASK FORCE, 2020a, 2020b). Além destes documentos, o NIST fornece um conjunto de planilhas e um catálogo de ações de dados problemáticas para a análise, avaliação e priorização de riscos de privacidade e escolha dos controles e respostas aos riscos ("PrivacyEngCollabSpace/tools/risk-assessment/NIST-Privacy-Risk-Assessment-Methodology-PRAM at master · usnistgov/PrivacyEngCollabSpace", [s.d.]). Além destes recursos, há uma versão reduzida do processo de gestão do risco de privacidade, que inclui a preparação e implantação da gestão da privacidade (LEFKOVITZ; BOECKL, 2021).

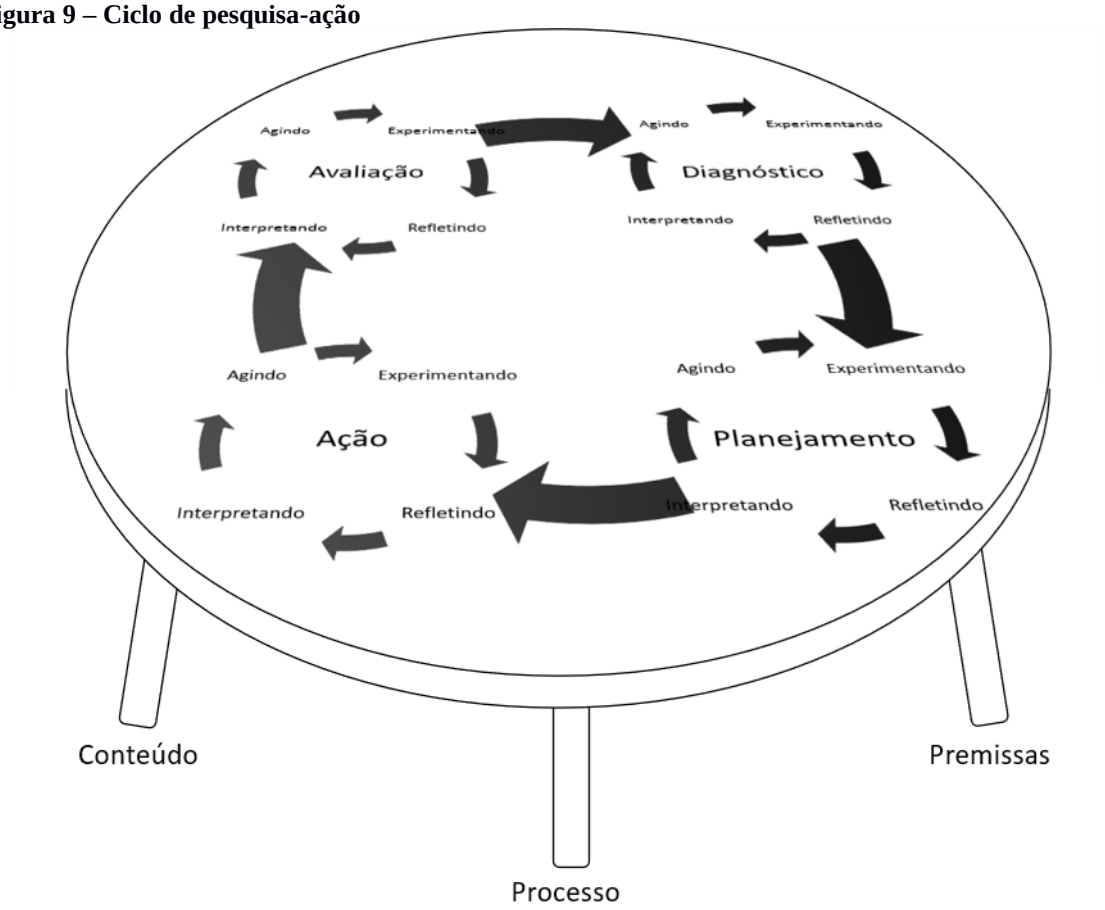
3 Metodologia

Este projeto de pesquisa adotou abordagem qualitativa, usando a pesquisa-ação. Pesquisa-ação é um método de estudo de ciências sociais pós-positivista, adequado para o estudo do contexto humano da tecnologia. Por ser um método intervencionista, quase clínico, é muito adequado para o estudo da mudança organizacional, como é o caso deste projeto (BASKERVILLE; WOOD-HARPER, 1996; COGHLAN; BRANNICK, 2005).

A pesquisa-ação trabalha em ciclos de 4 etapas: diagnóstico, planejamento da ação, tomada da ação e avaliação da ação. Dentro de cada etapa há um ciclo de aprendizado de experiência, reflexão, interpretação e tomada de ação. Em paralelo com o ciclo da pesquisa propriamente dita há um meta ciclo de inquisição refletindo sobre o conteúdo sendo trabalhado, o processo de trabalho e as premissas subjacentes que governam atitudes e comportamentos (vide Figura 9) (COGHLAN; BRANNICK, 2005).

O setor de seguros, onde a capitalização está inserida, é um bom modelo para o estudo da LGPD, pois é um setor regulado e que tem que coletar os dados cadastrais dos clientes para fins de registro e prevenção à lavagem de dinheiro. Isto atende ao princípio da necessidade proposto pela LGPD, mas os demais princípios devem ser endereçados pela conformidade.

Figura 9 – Ciclo de pesquisa-ação



Fonte: adaptado de (COGHLAN; BRANNICK, 2005)

Um ponto relevante da utilização da Liderança para este projeto é o fato de não estar ligada a um conglomerado financeiro. Os bancos, devido à questão do sigilo bancário e outras regras do Banco Central, já têm um ambiente mais maduro em relação a segurança de dados e sua governança. A Liderança, ligada a um grupo de mídia e comercial, está inserida num contexto menos regulado.

A pesquisa-ação é mais adequada ao entendimento de processos humanos complexos, já que estuda uma situação particular e não verdades universais. Ocorre o alinhamento de objetivos entre o pesquisador e o pesquisado, pois a pesquisa deve aportar valor na organização pesquisada. O pesquisador deve impor uma metodologia rigorosa no estudo para garantir a explicitação das lições aprendidas no processo (BASKERVILLE; WOOD-HARPER, 1996).

Quando o pesquisador é um membro completo da organização pesquisada, o processo da pesquisa-ação pode ser caracterizado como oportunista, já que o objeto de pesquisa ocorreria independentemente do seu processo de inquisição. Deve haver uma diferenciação entre o pesquisador e o sistema onde ocorre o projeto de pesquisa-ação. Os projetos podem ser

classificados quanto à intenção de autorreflexão do sistema e do pesquisador. No caso de ambos se engajarem intencionalmente em processos de auto estudo, o trabalho do pesquisador envolve a participação na autorreflexão e aprendizado coletivos e na articulação dos acontecimentos (COGHLAN; BRANNICK, 2005).

Boa parte das limitações da pesquisa-ação são dificuldades gerais da pesquisa social, como a falta de imparcialidade do pesquisador ou a sua falta de rigor. Outra questão é a confusão de pesquisa-ação com consultoria. Ambas têm a mesma origem teórica, mas há diferenciações de método e ênfase que, quando o pesquisador mantém o rigor do método, não ocorrem (BASKERVILLE; WOOD-HARPER, 1996).

O fato de a pesquisa-ação ser limitada pelo contexto faz com que o conhecimento produzido seja mais estreito, já que cada situação é única. Entretanto, as teorias levantadas nas situações estudadas podem ser descartadas ou validadas. Estudos adicionais e triangulações de casos são necessários para a generalização de relações causais sugeridas na pesquisa-ação. Dadas as limitações deste projeto estes estudos não serão viáveis (BASKERVILLE; WOOD-HARPER, 1996).

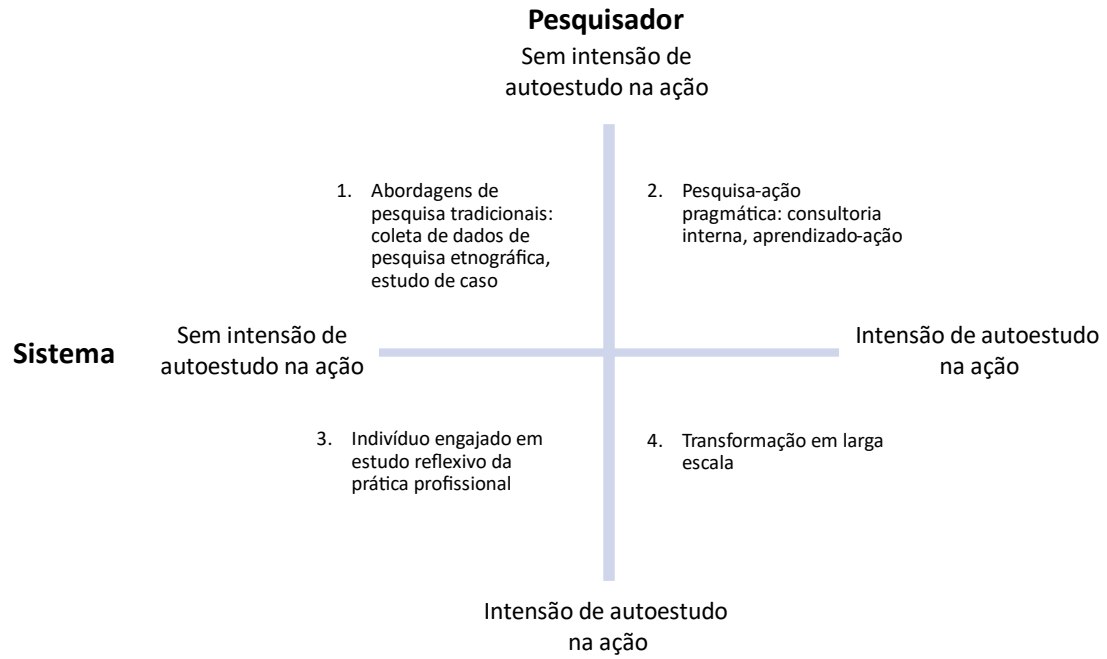
3.1 **Pesquisa-ação em sua própria organização**

Executar um trabalho de pesquisa-ação em uma organização em que o pesquisador é um membro completo (funcionário da empresa ou voluntário da organização não governamental onde ocorre a pesquisa) traz uma série de consequências. Há um maior entendimento por parte do pesquisador de diversas dinâmicas e contextos da organização, mas podem ocorrer dificuldades para o pesquisador ter uma visão objetiva em determinadas situações (ADLER; ADLER, 1987; COGHLAN; BRANNICK, 2005; DE GUERRE, 2002).

Os focos do pesquisador e da organização (sistema) onde ele está desenvolvendo o projeto podem variar quanto a intensão de autoestudo (ver Figura 10). O posicionamento da pesquisa ao longo dos eixos do foco pretendido pelo pesquisador e pelo sistema levam a uma classificação em quatro quadrantes. No Quadrante 1 não existe intensão de autoestudo por parte do pesquisador nem por parte do sistema. Esta é uma situação caracterizada como autoetnografia. O papel do etnógrafo é fazer uma observação discreta, contrastando com o

papel do pesquisador na pesquisa-ação, que é habilitar uma mudança invasiva. Portanto, este quadrante não representa um trabalho de pesquisa-ação (COGHLAN; BRANNICK, 2005).

Figura 10 – Focos do pesquisador e sistema



Fonte: adaptado de (COGHLAN; BRANNICK, 2005)

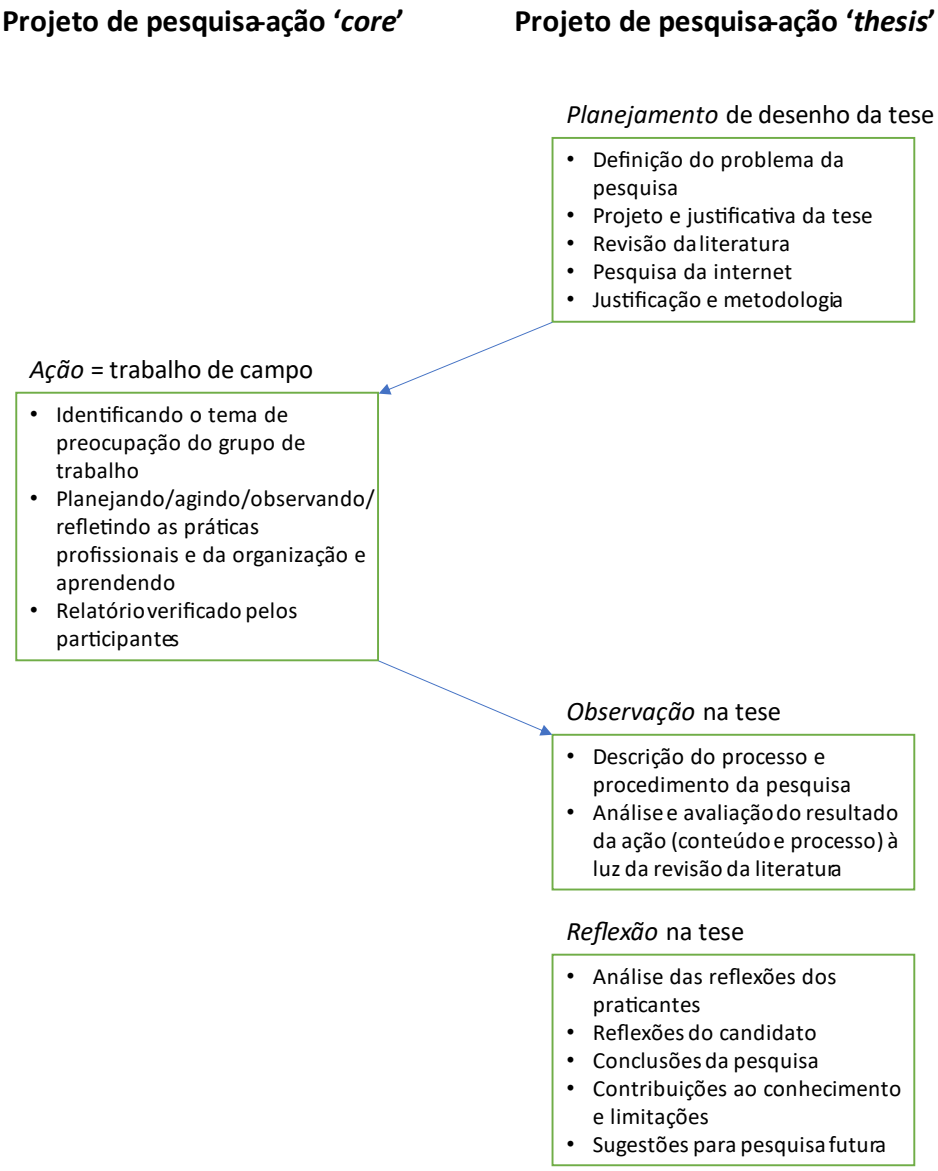
No Quadrante 2 não há intensão de autoestudo por parte do pesquisador e há essa intenção por parte do sistema. Esse tipo de pesquisa-ação pragmática é muito comum em programas de MBA, como é o caso deste trabalho. O projeto já aconteceria independentemente da pesquisa-ação, e foi oportunisticamente adotado pelo pesquisador. Este arranjo pode levar ao aumento da dificuldade na gestão das questões políticas da pesquisa (COGHLAN; BRANNICK, 2005).

O Quadrante 3 representa os projetos onde o pesquisador busca o autoestudo, mas o sistema não. São pesquisas de autorreflexão, buscando melhorar a prática profissional do pesquisador ou questionando os seus pressupostos e formas de ação. As pesquisas deste quadrante podem ser pré-selecionadas ou emergentes (COGHLAN; BRANNICK, 2005).

Os processos em que há a busca pelo autoestudo na ação por parte do pesquisador e do sistema se enquadram no Quadrante 4. Há um compromisso do sistema com a mudança, esses projetos normalmente são grandes processos de mudança organizacional (COGHLAN; BRANNICK, 2005).

Necessitamos distinguir dois projetos na pesquisa-ação executada para o desenvolvimento de uma dissertação. Existe o projeto '*core*', que é a intervenção do pesquisador na organização, que se encaixa como fase de ação de um projeto de pesquisa-ação '*thesis*' (ver Figura 11) que é o desenvolvimento da dissertação (COGHLAN; BRANNICK, 2005; ZUBER-SKERRITT; PERRY, 2002).

Figura 11 – Relacionamento entre projetos 'core' e 'thesis'



Fonte: (ZUBER-SKERRITT; PERRY, 2002)

Gummesson (2000) define o conceito de pré-compreensão, que é 'o conhecimento, percepções, e experiência das pessoas antes delas se envolverem num programa de pesquisa'. O conceito abarca o conhecimento da teoria e os conhecimentos tácito e explícito da organização. Isto pode ser uma vantagem para quem faz pesquisa-ação em sua própria

organização, por já ter o conhecimento da cultura e dos relacionamentos informais da organização, que só se obtém com tempo de experiência. Mas também pode causar dificuldades na hora de ter uma visão distanciada da cultura. É um exercício de equilíbrio para usar as vantagens da pré-compreensão sem se deixar levar pelos vieses e preconceitos (COGHLAN; BRANNICK, 2005; GUMMESSON, 2000).

Fazendo pesquisa-ação como membro completo de uma organização ocorre um acúmulo de papéis, o papel de pesquisador é adicionado ao seu papel original. Esses papéis podem apresentar uma alta integração ou alta segmentação, podendo variar ao longo do projeto. Dependendo das características do papel original do pesquisador na organização a dualidade de papéis pode levar com mais ou menos facilidade a situações de confusão e ambiguidade. Os dilemas que surgem dessa dualidade podem ser o destacamento dos papéis, quando o pesquisador passa a se sentir um estranho em ambos os papéis. Outro dilema é relatar os achados na pesquisa e enfrentar os seus superiores e colegas, ou aliviar o seu relato para manter o seu emprego (ADLER; ADLER, 1987; COGHLAN; BRANNICK, 2005).

O fato de pertencer a organização sendo pesquisada permite o acesso à organização e permite a realização da pesquisa, que Coghlan e Brannick (2005) chamam de acesso primário. Este acesso primário não garante o acesso a outras áreas da organização de interesse da pesquisa, o acesso secundário. Estas outras áreas podem ser áreas funcionais ou níveis hierárquicos e o acesso pode ser restrito por questões de hierarquia, segregação de funções ou questões políticas da organização.

4 Relatório e Análise da Ação

O escopo desta pesquisa-ação foi a implantação da Governança da Privacidade para atendimento da LGPD na Liderança Capitalização. Iniciaremos contextualizando a empresa e as contingências do momento da pesquisa e depois relataremos os ciclos da pesquisa-ação, em seus componentes de diagnóstico, planejamento, ação e avaliação.

A principal fonte de dados para esta pesquisa foram os diários de pesquisa que o pesquisador manteve. Com algumas falhas na disciplina, o pesquisador buscou relatar os acontecimentos relacionados ao processo de implantação da governança da privacidade nestes diários o mais próximo possível do ocorrido. Também foram utilizados documentos gerados por outros membros da equipe e atas de reuniões.

4.1 Contexto e propósito

A Liderança Capitalização é uma empresa do GSS, grupo empresarial familiar diversificado, em processo de transição da gestão para a segunda geração da família. Dentre as empresas do GSS, a Liderança Capitalização é a única que atua num mercado regulado. Fundada em 1945 e adquirida pelo GSS em 1975, desde 1991 a Liderança Capitalização opera praticamente com apenas um produto, a Tele Sena, título de capitalização da modalidade popular (LIDERANÇA CAPITALIZAÇÃO S.A., [s.d.], [s.d.]).

As empresas de capitalização são reguladas pela Superintendência de Seguros Privados (SUSEP) e pelo Conselho Nacional de Seguros Privados (CNSP), no âmbito do mercado segurador. Um dos principais foco destes reguladores é a solvência das empresas, buscada por meio de limites técnicos para a gestão das reservas e acompanhamento mensal de solvência. Além da solvência, a prevenção à lavagem de dinheiro e ao financiamento ao terrorismo (PLDFT) é outro tema importante para os reguladores de seguros. A SUSEP e o CNSP demandam das empresas do mercado uma estrutura de gestão de riscos compatível com seu porte e riscos e mecanismos de PLDFT que exigem a captura e tratamento de dados pessoais de seus clientes, parceiros de negócio e funcionários (CONSELHO NACIONAL DE SEGUROS PRIVADOS, 2021; SUPERINTENDÊNCIA DE SEGUROS PRIVADOS, 2020).

Os mecanismos de PLDFT incluem os processos de “conheça seu cliente” (*KYC* – do inglês *know your customer*), “conheça o seu funcionário” (*KYE* – do inglês *know your employee*) e “conheça o seu fornecedor” (*KYS* – do inglês *know your supplier*) que envolvem o tratamento dos dados pessoais das contrapartes. A determinação da profundidade e extensão destes processos é, em grande parte, responsabilidade da empresa, levando em conta os riscos envolvidos e características da operação e produto envolvidos (SUPERINTENDÊNCIA DE SEGUROS PRIVADOS, 2020).

No início do projeto o pesquisador atuava como Diretor de TI e Controles Internos, sendo responsável perante a SUSEP pelos procedimentos de PLDFT e Controles Internos. Também havia sido encarregado do projeto de adequação da empresa à LGPD pela Vice-Presidência, que incluía a implantação da governança da privacidade.

Prevista inicialmente para entrar em vigor em vigor em fevereiro de 2020, 18 meses após a sua publicação, a LGPD teve seu prazo de vigência alterado pela Lei nº 13.853/19 para 27/08/2020. No bojo das ações legislativas mitigadoras da pandemia do novo coronavírus, o prazo de vigência das sanções administrativas (artigos 52, 53 e 54) passou para 01/08/2021 pela Lei nº 14.010/20 (GUILHEM, 2020; OPICE BLUM, BRUNO E VAINZOF ADVOGADOS ASSOCIADOS, 2020).

4.2 **Ciclos da pesquisa-ação**

O Projeto se desenrolou em duas grandes fases, separadas por um hiato causado pela pandemia do COVID-19. No início ocorreram dois ciclos onde se buscou estruturar a governança da privacidade previamente ao desenvolvimento das ações de adequação à LGPD e gestão da privacidade. Na segunda fase ocorreu um ciclo onde a prioridade foi dada à adequação, com desenvolvimento da governança em paralelo.

4.2.1 Primeiro Ciclo

O primeiro ciclo se iniciou em março de 2019. A Diretoria da Liderança designou uma equipe multidisciplinar, com membros das equipes de TI e Controles Internos para identificar os pontos que em que a LGPD afetava as operações da Liderança Capitalização.

O diagnóstico inicial foi que não havia um processo consciente de gestão da privacidade na Liderança. Medidas de proteção eram tomadas, os dados pessoais de clientes e de funcionários eram tratados de forma minimamente adequada, ainda que sem as devidas formalizações, e havia gestão da segurança da informação, mas sem um processo unificado e documentado.

Partindo da constatação de que para a adequação à LGPD seria necessária a criação de um processo contínuo de gestão e não apenas a execução de um projeto estanque, focou-se de início na construção da governança da privacidade (ABRAHAM; SCHNEIDER; VOM BROCKE, 2019). O entendimento da equipe era que a data da implantação da lei não marcava o fim do projeto, mas o início do processo contínuo de *compliance*. O volume de trabalho estimado e a assimetria entre os volumes, controles e riscos envolvidos nos processos de tratamento dos dados de clientes, funcionários e fornecedores também indicavam a necessidade de uma estrutura de governança para que as priorizações e compromissos antevistos pudessem ser alinhados à governança corporativa.

O planejamento inicial era a criação de uma estrutura de governança da privacidade enquanto se estruturava um plano de gestão dos dados pessoais e se analisavam os *gaps* de TI no tratamento de dados pessoais. O pesquisador forneceria a base teórica para a construção do modelo de governança de privacidade, as equipes de TI e Controles Internos desenvolveriam o plano de gestão de dados pessoais e uma consultoria, contratada para auxiliar na gestão do plano, faria a análise dos *gaps* de segurança de TI.

O pesquisador não conseguiu encontrar um modelo teórico de governança de privacidade aplicável ao contexto da Liderança. Além dos modelos teóricos foram analisadas as políticas de governança da privacidade de algumas organizações. Buscou-se um modelo de governança em um domínio semelhante e por analogia iniciou-se a pesquisa de modelos de governança de dados, assumindo-se como pressuposto que a privacidade, num contexto corporativo, é equivalente à proteção dos dados privados (DENNEDY; FOX; FINNERAN, 2014).

Buscando a aceitação e o engajamento das diversas áreas envolvidas no tratamento de dados da empresa, além de facilitar a comunicação e alinhamento, criou-se um comitê de governança expandido, com participação das diversas áreas envolvidas na gestão dos dados (DENNEDY; FOX; FINNERAN, 2014). Além de TI e Controles Internos foram agregadas as

áreas Operacional, Marketing, RH e Jurídico. Para direcionar o plano de gestão de dados pessoais, começaram a discutir uma política de privacidade mais abrangente do que a então em uso nos sites da companhia, abordando os dados pessoais obtidos em outras interações com os clientes, fornecedores e funcionários.

Entre agosto e novembro de 2019 o comitê se reuniu em cinco ocasiões, tentando adaptar a governança de dados dos trabalhos de Khatri e Brown (2010), Alhassam, Sammon e Daly (2018) e Abraham, Schneider e Vom Brocke (2019). Khatri e Brown, baseando-se no modelo de governança de TI de Weill e Ross (2004), trabalham com mais ênfase a localização das alçadas de decisão dentro da estrutura da empresa. Alhassam, Sammon e Daly (2018) trazem uma avaliação da frequência de citação das atividades de governança de dados na literatura que permite deduzir priorização das atividades de governança de dados, facilitando o desenho de um caminho de implantação. O trabalho de Abraham, Schneider e Vom Brocke é efetivamente um modelo conceitual que consolida o conhecimento no tema de governança de dados e permite uma visão integrada de seus componentes.

O comitê decidiu atuar em quatro ações de governança de dados com alta prioridade no modelo de atividades de Alhassam, Sammon e Daly (2018) (vide Figura 6), as definições de papéis e responsabilidades de dados, políticas de dados, padrões de dados e tecnologia de dados.

O comitê atribuiu os papéis conforme a Tabela 5, seguindo o *framework* de Abraham, Schneider e Vom Brocke (2019). As políticas de dados seriam definidas pela equipe de processos da Liderança, e os padrões e tecnologia dos dados seriam responsabilidade da equipe de TI.

Tabela 5 – Papéis e responsabilidades da Governança

Grupo	Papel	Descrição	Responsabilidade	Responsável
Gerencial	**Patrocinador**	Executivo de alto nível	Fornece orientação estratégica, priorização e financiamento	***Diretor de Compliance/TI***
	Conselho de governança	Órgão multifuncional de hierarquia abrangente	Estabelece a direção estratégica do programa de governança	***Comitê LGPD***
	Líder de governança	Administrador do programa de governança	Supervisiona a conformidade com as políticas e coordena as tarefas dos administradores de dados	***Responsável por Compliance***
	Escritório de governança	Equipe administrativa de apoio	Estabelece canais de comunicação, prepara reuniões, cuida de treinamentos e resolve problemas	***Staff de Compliance***
Operacional	***Proprietário***	Executivo responsável pelos ativos de dados de uma unidade de negócio	Comunica requisitos e riscos de dados	***Responsável pelo processo de negócio*** (com foco em elementos específicos do negócio e orientado a regulamentação de dados importantes)
	Administrador	Especialista com conhecimentos sólidos sobre requisitos e dados do negócio. Pode ser da área de negócio, de TI ou ambas.	Traduz requisitos do negócio em especificações técnicas	***Responsável por TI***
	Produtor	Responsável por criação e manutenção dos dados	Cria ou agrega dados e atualiza dados criados por outros	***Key-user do sistema***
	Consumidor	Usuário dos dados	Usa dados, especifica requisitos e relata problemas	***Key-user do sistema***

Fonte: Elaborado pelo Comitê LGPD da Liderança

A avaliação dos *gaps* de segurança de TI em relação à norma ISO/IEC 27.001 foi iniciada. Dados o volume de controles da norma e a sua natureza certificatória, o trabalho de avaliação dos *gaps* e a análise de riscos necessária ao alinhamento com a norma, estes acabaram sendo tratados em um projeto à parte.

A avaliação do pesquisador ao final do ciclo foi que houve um avanço na conscientização da Liderança quanto a governança de privacidade, ainda que indiretamente através da governança de dados. Parte do problema da implantação da governança é que o processo ainda era muito abstrato para grande parte dos participantes do comitê. Estes entendiam as necessidades da governança e gestão da privacidade, mas não enxergavam as ações concretas devido à falta de prática na execução das atividades.

Outra dificuldade identificada no processo de implantação da governança de privacidade era a complexidade da governança de dados e seu distanciamento da realidade dos membros do comitê das áreas de negócio.

4.2.2 Segundo ciclo

O diagnóstico para o segundo ciclo foi que os conceitos estavam muito abstratos para o comitê. Os membros não se sentiam confortáveis tomando as decisões necessárias ao avanço

do projeto. As reuniões ficavam rodando em torno dos mesmos temas e os avanços eram lentos.

Visando concretizar os conceitos para os membros do comitê, decidiu-se avançar no levantamento dos fluxos de dados pessoais de clientes nos processos de duas áreas. A área Operacional era responsável pelos processos de atendimento ao cliente, logística de distribuição dos títulos, logística reversa das fichas de cadastro dos clientes e títulos resgatados e pagamento de prêmios aos clientes contemplados em sorteios. A área de Marketing era responsável pelos processos de interação com clientes em redes sociais e divulgação de ganhadores na TV e em redes sociais. Para estas áreas, os colaboradores desenharam os fluxos de dados e fizeram a identificação da fase do ciclo de vida dos dados e das definições de tratamento do inciso X do Art. 5 da LGPD. Os processos foram mapeados dentro da cadeia de valor da Liderança, identificando as fases em que ocorria o tratamento de dados pessoais de clientes. Os responsáveis pelas atividades foram identificados, assim como as bases legais do tratamento dos dados (BRASIL, 2018; TEFFÉ; VIOLA, 2020).

Após o mapeamento foi criada uma relação de tarefas a serem executadas até agosto de 2020 para a adequação à LGPD do tratamento de dados pessoais de clientes. Algumas das tarefas seriam realizadas pela equipe interna, outras, tais como a redação das políticas, seriam realizadas por uma equipe contratada.

No primeiro trimestre de 2020 começaram os primeiros sinais da pandemia do novo coronavírus e o foco da empresa como um todo migrou para ações de reconfiguração das operações para o novo momento. O trabalho migrou para 100% remoto, os contratos com fornecedores e canais de vendas foram renegociados, o canal digital, até o momento pouco explorado para evitar conflitos com o canal físico, teve um impulso significativo de divulgação. As atividades do plano de adequação à LGPD foram deixadas de lado face as necessidades prementes do novo contexto mundial. O posterior adiamento do prazo de vigência da LGPD reforçou a decisão de interromper o projeto por alguns meses. Desta forma a fase da ação deste ciclo foi interrompida, ficando prejudicada a fase de reflexão.

4.2.3 Terceiro ciclo

Com a redução da gravidade dos impactos da pandemia do novo coronavírus e os ajustes do modelo de negócio estabilizados, o trabalho na adequação à LGPD e a consequente implantação da governança de privacidade foram retomados. Neste momento surgiu a oportunidade de contratar um escritório de advocacia conjuntamente com outras empresas do GSS. Se por um lado este processo viabilizava a contratação de um parceiro mais qualificado com um custo menor, por outro lado o controle do processo saia da alçada da unidade de negócio e passava para a gestão corporativa.

O comitê entendeu que a contratação corporativa era mais eficiente e aderiu ao processo, contratando o escritório para a fase de diagnóstico. Os entregáveis desta fase seriam o inventário de dados pessoais, o Relatório das Atividades de Processamento de Dados Pessoais (ROPA do inglês *Report of Processing Activities*), um Relatório de Diagnóstico com análise dos *gaps* e um Plano de Ação, o Relatório de Análise de Impacto a Proteção de Dados Pessoais e a customização de 10 documentos entre normas e políticas.

O pesquisador participou do comitê de gestão deste projeto, mas não houve oportunidade de contribuir com o aporte de teoria e reflexão, responsabilidades da consultoria. A possibilidade de aplicação da pesquisa-ação aparece após o final do projeto de consultoria. A consultoria entregou um Plano de Ação com uma longa lista de itens a serem ajustados na operação e na governança, variando de pequenas mudanças no comportamento pessoal, como tomar mais cuidado com documentos com informações de clientes sobre a mesa de trabalho, até questões complexas de negócio, como conciliar a obrigatoriedade de uma ficha de cadastro detalhada no título com a minimização do tratamento de dados de clientes.

O diagnóstico para este ciclo foi que com a parada nos trabalhos por conta da pandemia do COVID-19 e a retomada com a consultoria houve uma desmobilização da equipe da Liderança em relação à adequação à LGPD. Os adiamentos da entrada em vigor da lei e as indefinições quanto a estrutura da Agência Nacional de Proteção de Dados (ANPD) colaboraram para o ambiente de despreocupação.

O planejamento para o ciclo era buscar modelos de governança de privacidade mais específicos, saindo da complexidade dos modelos de governança de dados. Dois modelos

foram considerados pelo pesquisador: o modelo conceitual de Swartz, da Veiga e Martins (2019) e o NIST Privacy Framework (NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, 2020).

O modelo de Swartz, da Veiga e Martins (2019) parte da definição pela alta direção dos princípios de governança da privacidade que devem ser seguidos pela companhia. Conforme a Tabela 6, elaborada pelo Comitê com base no modelo de Swartz, da Veiga e Martins, este tem um foco nos mecanismos de governança procedurais e estruturais, tendo apenas a Comunicação e a Conscientização e treinamento de privacidade como mecanismos relacionais.

Tabela 6 – Classificação dos componentes do modelo conceitual de governança da privacidade

Componentes principais	Subcomponentes	Tipo de mecanismo
Compromisso organizacional	Compromisso da liderança	Estrutural
	Encarregado de privacidade	Estrutural
	Escritório de privacidade	Estrutural
	Relatórios	Procedural
Políticas e procedimentos	Políticas e procedimentos	Procedural
Controles do programa de privacidade	Inventário de informações pessoais	Procedural
	Gerenciamento de prestadores de serviço	Procedural
	Gerenciamento de incidentes/tratamento de vazamentos	Procedural
	Comunicação	Relacional
	Conscientização e treinamento de privacidade	Relacional
	Ferramentas de avaliação de risco	Procedural
	Garantias e auditoria do programa	Procedural
Avaliações contínuas	Avaliações e revisões contínuas	Procedural

Fonte: Elaborado pelo Comitê LGPD da Liderança sobre (SWARTZ; DA VEIGA; MARTINS, 2019)

O NIST PF foi baseado na estrutura do NIST Cybersecurity Framework e ambos têm uma estrutura que favorece a sua aplicação gradual e customizada para as contingências de cada organização. O próprio *framework* já prevê a utilização de perfis e níveis de implementação para capturar a situação atual e mapear uma situação futura desejável adequada aos riscos e estrutura da organização (KOERNER, KATHARINA, 2021; NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, 2020).

Uma das funções do *Core* é a governança (GOVERN-P), composta por 4 categorias e 20 subcategorias (vide Tabela 4). As subcategorias têm um foco maior em mecanismos de

governança procedurais, com uma ênfase maior nos mecanismos de governança relacionais do que nos estruturais (vide Tabela 7).

Alguns subcomponentes do modelo de Swartz, da Veiga e Martins (2019) não se enquadram no conceito de governança como "estrutura através da qual os objetivos da empresa são definidos e se determina os meios para alcançar esses objetivos e para monitorizar o desempenho" (OECD, 2016). Num mapeamento entre os subcomponentes do modelo conceitual de Swartz, da Veiga e Martins (2019) e as subcategorias do NIST PF (2020), diversos componentes são mapeados para subcategorias de funções que não de governança (ver Tabela 8). Por esta questão conceitual, pelo modelo do NIST facilitar a customização e o planejamento de estados futuros e pela familiaridade da equipe de TI com o NIST CSF, por sugestão do pesquisador, o comitê optou pelo NIST PF como modelo para a gestão e governança da privacidade.

Tabela 7 – Tipos de mecanismo de governança do NIST PF e seu status de implementação

Subcategoria	Tipo de Mecanismo	Nível de implementação
GV.PO-P1	Procedural	Parcialmente implementado
GV.PO-P2	Procedural	Parcialmente implementado
GV.PO-P3	Estrutural	Largamente implementado
GV.PO-P4	Estrutural	Parcialmente implementado
GV.PO-P5	Procedural	Totalmente implementado
GV.PO-P6	Procedural	Largamente implementado
GV.RM-P1	Estrutural	Largamente implementado
GV.RM-P2	Estrutural	Parcialmente implementado
GV.RM-P3	Relacional	Largamente implementado
GV.AT-P1	Relacional	Largamente implementado
GV.AT-P2	Relacional	Largamente implementado
GV.AT-P3	Relacional	Largamente implementado
GV.AT-P4	Relacional	Parcialmente implementado
GV.MT-P1	Procedural	Largamente implementado
GV.MT-P2	Procedural	Parcialmente implementado
GV.MT-P3	Procedural	Largamente implementado
GV.MT-P4	Procedural	Parcialmente implementado
GV.MT-P5	Procedural	Parcialmente implementado
GV.MT-P6	Procedural	Não implementado
GV.MT-P7	Procedural	Parcialmente implementado

Fonte: avaliação do autor.

O modelo de governança usado pela consultoria era muito focado na figura do encarregado de proteção de dados pessoais (DPO, do inglês *Data Protection Officer*), centralizando nele a

gestão dos dados pessoais, com foco nos mecanismos estruturais e procedurais da governança. Também foi recomendada a criação de um comitê de assessoramento do DPO, agregando conhecimentos complementares para auxiliar nos processos de gestão de dados pessoais. O pesquisador foi nomeado o encarregado de dados da Liderança, com o Comitê de Adequação à LGPD se mantendo como fórum de discussão da proteção de dados pessoais.

Para a adequação dos pontos levantados pela consultoria o DPO montou uma equipe de projeto com membros das áreas de projetos e gestão de riscos. Esta equipe tratou da gestão das melhorias apontadas pela consultoria e no trabalho de conscientização dos colaboradores da Liderança sobre a proteção de dados pessoais. Foram feitas ações de divulgação interna e conscientização da proteção dos dados pessoais de clientes, fornecedores e funcionários, incluindo e-mails de divulgação, palestras sobre a LGPD e sessões trimestrais de perguntas e respostas com o DPO.

Outra ação de conscientização e mobilização dos funcionários foi a criação de um grupo agentes de LGPD nas áreas da companhia. A ideia veio da estrutura de agentes de compliance, cuja função principal é responderem o questionário de autoavaliação de controles internos, mas que serviram de mecanismo de comunicação e conscientização no início da implantação da função de compliance. Os agentes de LGPD tem uma função de ligação com o DPO e de reforço local das questões da gestão da privacidade.

Tabela 8 – Mapeamento modelo conceitual de Swartz et al. x NIST PF

Componentes principais	Subcomponentes	Funções, Categorias ou subcategorias do NIST PF
Compromisso organizacional	Compromisso da liderança	**GV.PO-P1**: Valores e políticas de privacidade organizacional (ex: condições sobre o processamento de dados como o uso dos dados ou períodos de retenção, prerrogativas dos indivíduos em relação ao processamento de dados) são estabelecidos e comunicados.
	Encarregado de privacidade	**GV.PO-P3**: Funções e responsabilidades para a força de trabalho são estabelecidas no que diz respeito à privacidade.
	Escritório de privacidade	**GV.PO-P3**: Funções e responsabilidades para a força de trabalho são estabelecidas no que diz respeito à privacidade.
	Relatórios	**GV.PO-P4**: As funções e responsabilidades de privacidade são coordenadas e alinhadas com partes interessadas de terceiros (ex: provedores de serviços, clientes, parceiros).
Políticas e procedimentos	Políticas e procedimentos	**Políticas, processos e procedimentos de governança (GV. PO-P)**: As políticas, processos e procedimentos para gerenciar e monitorar os requisitos regulatórios, legais, de risco, ambientais e operacionais da organização são compreendidos servem para informar a administração sobre o gerenciamento do risco de privacidade.
		Políticas, processos e procedimentos de processamento de dados (CT.PO-P): Políticas, processos e procedimentos são mantidos e usados para gerenciar o processamento de dados (ex: finalidade, escopo, funções e responsabilidades dentro do ecossistema de processamento de dados e compromisso de gerenciamento) condizentes com a estratégia de risco da organização para proteger a privacidade dos indivíduos.
		Políticas, processos e procedimentos de comunicação (CM.PO-P): Políticas, processos e procedimentos são mantidos e usados para aumentar a transparência das práticas de processamento de dados da organização (ex: finalidade, escopo, funções e responsabilidades no ecossistema de processamento de dados, compromisso de gestão) e riscos de privacidade associados. CM.PO-P1: Políticas, processos e procedimentos de transparência para comunicação de propósitos, práticas e riscos de privacidade associados estão estabelecidos e em vigor.
		Políticas, processos e procedimentos de proteção de dados (PR.PO-P): Políticas de segurança e privacidade (ex: finalidade, escopo, funções e responsabilidades no ecossistema de processamento de dados, e compromisso de gestão), processos e procedimentos são mantidos e usados para gerenciar a proteção de dados.
Controles do programa de privacidade	Inventário de informações pessoais	**Inventário e mapeamento (ID.IM-P)**: O processamento de dados por sistemas, produtos ou serviços é compreendido e mantém os administradores informados sobre o risco de privacidade.
	Gerenciamento de prestadores de serviço	**GV.AT-P4**: Terceiros (ex: prestadores de serviços, clientes, parceiros) entendem suas funções e responsabilidades.
	Gerenciamento de incidentes/tratamento de vazamentos	**PR.PO-P7**: Planos de resposta (Resposta a Incidentes e Continuidade de Negócios) e planos de recuperação (Recuperação de Incidentes e Recuperação de Desastres) são estabelecidos, vigentes e gerenciados.
	Comunicação	**COMUNICAR-P (CM-P)**: Desenvolver e implementar atividades apropriadas para permitir que organizações e indivíduos tenham um entendimento confiável e se envolvam em um diálogo sobre como os dados são processados e sobre os riscos de privacidade associados.
	Conscientização e treinamento de privacidade	**Conscientização e treinamento (GV. ATP)**: A força de trabalho da organização, juntamente com terceiros envolvidos no processamento de dados são instruídos e conscientizados sobre privacidade, sendo treinados para desempenhar suas funções e responsabilidades relacionadas à privacidade de acordo com as políticas, processos, procedimentos, acordos e valores de privacidade organizacional.
		Conscientização sobre processamento de dados (CM.AW-P): Indivíduos e organizações têm conhecimento confiável sobre práticas de processamento de dados e riscos de privacidade associados, e mecanismos eficazes são usados e mantidos para aumentar a previsibilidade consistente com a estratégia de risco da organização para proteger a privacidade dos indivíduos.
	Ferramentas de avaliação de risco	**Avaliação de risco (ID.RA-P)**: A organização entende os riscos de privacidade para os indivíduos e como eles podem impactar futuramente as operações organizacionais, incluindo a missão, funções, outras prioridades de gerenciamento de risco (ex: compliance, financeiro), reputação, força de trabalho e cultura.
	Garantias e auditoria do programa	Sem correpondência
Avaliação contínua	Avaliação e revisão contínuas	**Monitoramento e revisão (GV. MT-P)**: As normas, processos e procedimentos para revisão contínua da postura de privacidade da organização são compreendidos e mantêm a administração informada sobre o risco de privacidade.

Fonte: avaliação do autor.

O Comitê de Governança da Privacidade fez uma avaliação dos níveis de implementação das subcategorias da função GOVERN-P do *Core* do NIST PF num *Profile* da situação atual. Um *Profile* com a situação desejada para dois anos foi desenhado pelo comitê e levado à aprovação da Diretoria.

Buscando avaliar a efetividade da governança da privacidade implantada em relação ao disposto na LGPD foi feito um cruzamento do modelo com as demandas da legislação. O modelo de governança da privacidade apresentado na LGPD busca alinhar as decisões de gestão da privacidade aos interesses dos titulares dos dados. Entretanto, a forma como a governança é apresentada na LGPD, junto com as boas práticas, obscurece esse objetivo, já que as boas práticas não se aplicam só ao domínio da governança. Os aspectos das boas práticas e governança listados no caput do Art. 50 da LGPD em sua maioria se enquadram nas subcategorias da função GOVERN-P do NIST PF (ver Tabela 9). As normas de segurança e os padrões técnicos podem ser mapeados para subcategorias da função PROTECT-P, e o último aspecto é aberto demais para se mapear.

Tabela 9 – Aspectos do Art. 50 da LGPD X NIST PF

Componentes do boas práticas e governança	Subcomponentes do NIST PF
As condições de organização	GV.PO-P2, GV.PO-P3, GV.PO-P4, GV.PO-P6
O regime de funcionamento	GV.RM-P1
Os procedimentos incluindo reclamações e petições de titulares	GV.MT-P7
As normas de segurança	PR.PO-P1, PR.PO-P2, PR.PO-P3, PR.PO-P4, PR.PO-P5, PR.PO-P6, PR.PO-P7, PR.PO-P8, PR.PO-P9, PR.PO-P10
Os padrões técnicos	PR.PT-P1, PR.PT-P2, PR.PT-P3, PR.PT-P4
As obrigações específicas para os diversos envolvidos no tratamento	GV.PO-P3, GV-PO-P4
As ações educativas	GV-AT-P1
Os mecanismos internos de supervisão e de mitigação de riscos	GV-RM-P1, GV-RM-P2, GV-RM-P3
Outros aspectos relacionados ao tratamento de dados pessoais	-

Fonte: avaliação do autor.

Nem todos os componentes do programa de governança listados nos itens do inciso I do parágrafo 2º do Art. 50 da LGPD mapeiam para subcomponentes da função GOVERN-P do NIST PF (ver Tabela 10). Os itens ‘b’ e ‘c’, que tratam do escopo de dados pessoais abrangidos pela governança e da proporcionalidade da governança aos riscos e volumes envolvidos respectivamente, são mais bem mapeados para os *Implementation Tiers* definidos no *Profile* que a organização identifica.

Tabela 10 – Requisitos do Art. 50 da LGPD x NIST PF

Componentes da governança de privacidade do Art. 50, inciso I da LGPD	Subcomponentes do NIST PF
a) demonstre o comprometimento do controlador em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais;	GV.PO-P1, GV.PO-P2
b) seja aplicável a todo o conjunto de dados pessoais que estejam sob seu controle, independentemente do modo como se realizou sua coleta;	Definido no Profile
c) seja adaptado à estrutura, à escala e ao volume de suas operações, bem como à sensibilidade dos dados tratados;	Definido no Profile
d) estabeleça políticas e salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade;	GV.PO-P6, GV.RM-P1, GV.RM-P2, GV.RM-P3
e) tenha o objetivo de estabelecer relação de confiança com o titular, por meio de atuação transparente e que assegure mecanismos de participação do titular;	GV.MT-P7, CT.PO-P3, CM.PO-P1, CM.PO-P2, CM.AW-P1, CM.AW-P2
f) esteja integrado a sua estrutura geral de governança e estabeleça e aplique mecanismos de supervisão internos e externos;	GV.PO-P6, GV.MT-P3
g) conte com planos de resposta a incidentes e remediação;	PR.PO-P7, PR.PO-P8
h) seja atualizado constantemente com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas;	GV.MT-P1, GV.MT-P2, GV.MT-P6

Fonte: avaliação do autor.

A adequação a uma norma como a LGPD é um processo e não um projeto, no sentido que sempre surgem novos processos ou tecnologias que devem ter sua aderência analisada e ajustada. Para fins deste trabalho arbitramos dezembro de 2022 como o encerramento do 3º ciclo de pesquisa-ação, alinhando com o prazo de conclusão das matérias do pesquisador.

A avaliação do pesquisador ao final do ciclo é que uma estrutura básica de governança da privacidade foi implantada na Liderança. Ainda existem muitos pontos de melhoria para atingir o *Profile* definido como desejável, mas os instrumentos para este trabalho já estão implantados.

O desenvolvimento do projeto enfrentou alguns obstáculos, alguns contingenciais e outros ligados às questões mais gerais de governança. As principais questões contingenciais foram a interrupção causada pela pandemia do COVID-19 e mudanças na estratégia da Liderança que levaram a mudanças na equipe e processos da Liderança.

Os obstáculos gerais mais relevantes para esta dissertação foram os causados pela utilização inicial de frameworks que não facilitavam o mapeamento das situações atual e futura desejada, da falta de um modelo com priorização ou ordenação de implantação dos

componentes da governança, a falta de clareza em alguns modelos do que é a governança e o que é a gestão da privacidade e a novidade da governança da privacidade e do NIST PF. Estes pontos serão retomados no capítulo 5.

4.3 **Próximos passos**

Adotamos uma data de fim do projeto para esta pesquisa, mas o processo de implantação da governança e da gestão da privacidade entra num ciclo de melhoria contínua que deve prosseguir indefinidamente. Há um ciclo de revisão e melhoria dos controles da governança e gestão de privacidades embutidos no NIST PF e a própria evolução da companhia, com novos produtos, processos e sistemas, que levam a novas necessidades na gestão e governança da privacidade.

A transformação digital da Liderança, que já tem o canal digital como o segundo maior canal de vendas, traz novas necessidades na gestão da privacidade na medida que novas ferramentas e parceiros se integram no ecossistema. A ampliação do *Customer Relationship Management* (CRM) e da análise dos dados também exigem novas ferramentas e controles na questão da privacidade e devem impactar o processo de governança.

A mudança na estratégia da Liderança, que passou a buscar novos canais de vendas e produtos, também traz novas questões para a gestão da privacidade. Mudanças em processos e a ampliação do quadro de funcionários trazem a necessidade de revisões em controles e novos treinamentos e reforço no processo de conscientização. A mudança deve se acelerar com novos modelos de negócio em discussão que envolveriam a prestação de serviços e o consequente tratamento de dados como operador.

A adoção do NIST PF na Liderança foi limitada, apenas na função GOVERN-P. Um próximo passo natural é a implantação de todo o NIST PF. Com as mudanças nos processos descritos será necessária brevemente uma revisão maior dos controles da gestão da privacidade.

5 Discussão

Aqui apresentamos os temas que apareceram no desenvolvimento do trabalho e merecem uma discussão relacionando a teoria e os resultados práticos. Falaremos sobre o conceito de governança e algumas interpretações conflitantes. Abordamos a seguir a questão da ordem de implantação da governança e seu impacto no projeto. A novidade do NIST PF, é tratada a seguir, e por final discutimos a adequação da pesquisa-ação neste projeto.

5.1 Clareza no conceito de governança

O conceito de governança na literatura está associado às alçadas decisórias e responsabilidades. Na governança corporativa o modelo busca o alinhamento das decisões de gestão aos interesses dos financiadores e evitar as externalidades na criação de valor aos acionistas. Na teoria da governança corporativa os objetivos são muito claros, assim como a separação entre ações e mecanismos de governança e de gestão. Entretanto, conforme vamos avançando para dentro das empresas a divisão entre governança e gestão tende a ser menos clara nos modelos (MONKS; MINOW, 2011; SHLEIFER; VISHNY, 1997; WEILL; ROSS, 2004).

Um caso encontrado é o modelo de governança da privacidade de Swartz, da Veiga e Martins (2019) que tem como um dos componentes ‘Controles do programa de privacidade’, com diversos subcomponentes de gestão e não de governança (veja Tabela 8). O modelo de Swartz, da Veiga e Martins é um modelo conceitual baseado em quatro políticas de governança de privacidade e o componente em questão tem os subcomponentes originados em todas as quatro.

Outro ponto é a especialização excessiva da governança de domínios cada vez mais estreitos. A Figura 2 mostra a visão de Weill e Ross (2004) da governança corporativa em relação à governança de TI e a governança financeira. Os ativos a serem governados são claramente distintos e as sobreposições facilmente resolvidas (por exemplo, os investimentos de TI tem uma alçada de aprovação técnica na governança de TI e uma outra alçada financeira na governança financeira). Quando incluímos novos níveis de governança na figura as sobreposições se tornam mais complicadas de separar: um projeto da gestão de privacidade

pode ter impactos na governança de dados, na governança de TI, na governança financeira e na corporativa e um eventual conflito escala para ser resolvido na governança corporativa.

Ainda que todos os níveis de governança estejam alinhados à governança corporativa, a diferença entre os objetivos de cada estrutura de governança pode levar a conflitos. Uma necessidade da gestão de privacidade pode implicar em mudanças na TI que impactam os projetos e levam a um desvio dos orçamentos. A forma tradicional de se tratar as exceções em governança é escalando as alçadas de aprovação, e estes casos eventualmente chegam a alçadas superiores da governança corporativa. A utilização de diversas hierarquias distintas de governança é a forma mais eficiente? Uma questão para pesquisas posteriores é se a utilização de outros modelos de estruturas organizacionais otimiza a coordenação entre as diversas estruturas de governança.

5.2 **Ordem de implantação de gestão e governança**

Um ponto que se ressalta no processo de implantação da governança de privacidade na Liderança é a necessidade de se implantar a gestão e a governança da privacidade em paralelo. Ao se implementar a gestão da privacidade sem uma estrutura de governança da privacidade corre-se o risco de se perder o alinhamento com a governança corporativa. A estrutura de gestão do projeto de implantação da gestão da privacidade tem interesses diferentes dos da governança da privacidade (concluir o projeto no prazo, dentro do orçamento e atingindo o escopo definido *versus* gerenciar os riscos de privacidade dentro das prioridades da organização) e eventualmente conflitantes (NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, 2020; SAMSET; VOLDEN, 2016).

Por outro lado, a implantação da governança da privacidade sem um processo de gestão da privacidade abaixo também não funcionou, as questões da governança ficam abstratas. Efetivamente não há nada a ser governando.

No processo de implantação abordado neste trabalho o conflito de interesse entre o projeto e a governança foram em parte mitigados pelo comitê expandido de gestão da governança da privacidade. Ainda que não houvesse vários níveis na estrutura de governança, o comitê tinha a responsabilidade perante a Diretoria pela governança da privacidade. A estrutura de decisão do projeto não passava pelo comitê.

O modelo do NIST PF, ao permitir uma avaliação da situação atual em termos de gestão e governança da privacidade e o planejamento de uma situação desejada, facilita a implantação simultânea da governança e gestão da privacidade. O processo de identificação da situação atual e mapeamento da situação pretendida nos Profiles permite a criação de um roteiro das categorias a serem trabalhadas. A criação de uma visão de futuro é um componente significativo de diversas teorias de mudança organizacional, ainda que não seja uma condição suficiente para uma mudança efetiva (AL-HADDAD; KOTNOUR, 2015; GILL, 2003; NILSEN, 2020).

No NIST PF, quais componentes devem ser priorizados, e o nível de maturidade que tal implementação busca ou deve alcançar são definidos nos *Profiles*, mas a ordem de implementação das Funções e componentes não está definida. Dada a novidade do NIST PF ainda não existem *Profiles* de referência divulgados como existem para a NIST CSF. Mesmo os perfis de referência do NIST CSF não trazem uma ordem de implantação, apenas os níveis de completude que se adequa a um nível de risco de uma determinada indústria ou ameaça (“Cyber Risk Institute – Don’t risk risk.”, [s.d.]; “Examples of Framework Profiles”, 2021).

A ordem de implementação dos componentes do NIST PF, ou de outro framework em geral, não é um assunto efetivamente abordado na literatura acadêmica. Não foram encontradas referências nas bases consultadas. A ordem ótima com certeza depende das contingências. A maturidade da organização quanto ao escopo do framework, a capacitação e tamanho da equipe e o orçamento disponíveis para a implantação, as expectativas de prazo e os *quick-wins* possíveis, entre outros, impactam na ordem ótima de implantação. Entretanto, essa é apenas uma questão contingencial ou existe alguma característica estrutural que determine a ordem? Esse é um tema que pode ser tratado em estudos futuros.

5.3 **Novidade do NIST PF**

O NIST PF foi lançado em janeiro de 2020 e ainda é um tema praticamente inexplorado no meio acadêmico. A pesquisa na base de dados SCOPUS com os parâmetros TITLE-ABS-KEY (“NIST Privacy Framework”) traz apenas 2 trabalhos, um deles baseado nas versões de trabalho (*draft*) da norma. Entretanto, mesmo a NIST CSF de 2014 ainda é relativamente pouco estudada, a pesquisa na base de dados SCOPUS com os parâmetros TITLE-ABS-KEY (NIST AND cybersecurity AND framework) traz 160 documentos. Pesquisando no Google

Scholar o termo “NIST Privacy Framework” trazia 245 documentos até 2022, enquanto na mesma ferramenta a busca “NIST Cybersecurity Framework” trazia 3.200 documentos até 2022.

Com o avanço das legislações de privacidade no mundo e em diversos estados Americanos a importância de um *framework* para gestão da privacidade cresce. O atual estágio de implantações do NIST PF já permite trabalhos como este e o de Carter (2021), de estudo de casos isolados. Com o aumento das instalações devem ocorrer estudos comparativos.

O trabalho de Carter (2021) e o artigo derivado dele (CARTER; KROLL; BRET MICHAEL, 2021) tratam de um caso com necessidades de privacidade mais estritas do que o caso da Liderança. Carter trata da implantação de um sistema de rastreamento da SARS-COV-19 no ambiente da marinha americana, ou seja, dados sensíveis pela saúde e pela segurança física dos militares. A extrema sensibilidade da privacidade do sistema aparentemente levou a que Carter identificasse problemas no NIST PF que não identificamos neste projeto.

A falta de implantações de referência e de estudos de caso de implantações do NIST PF dificultam atualmente as implantações. O trabalho poderia ser facilitado por *Profiles* de referência, como os do NIST CSF, ou problemas recorrentes poderiam ser identificados previamente com os estudos de caso.

5.4 **O método de pesquisa-ação**

O método adotado no projeto foi a pesquisa-ação. A característica fortemente prática do campo da Tecnologia da Informação favorece a abordagem metodológica da pesquisa-ação, e a pesquisa-ação é adequada aos processos de desenvolvimento organizacional por seu processo consultivo de diagnóstico, planejamento, ação e reflexão (BANVILLE; LANDRY, 1989; BASKERVILLE; WOOD-HARPER, 1996; VAN EYNDE; BLEDSOE, 1990). Ainda que o projeto apenas tangencie a Tecnologia da Informação em seu aspecto mais tradicional de hardware e software, do ponto de vista da governança de TI de Weill e Ross (2004) os ativos de informação (dados) estão no escopo de TI e a governança da privacidade trata da proteção dos dados pessoais de clientes, fornecedores e funcionários.

O pesquisador atuou como líder no projeto ‘*core*’ e, obviamente, no projeto ‘*thesis*’, e as medidas de sucesso eram diferentes em cada um. No projeto ‘*core*’ a medida do sucesso era a implantação da governança de privacidade nos prazos e custos acordados. No projeto ‘*thesis*’ a medida é a qualidade do conhecimento produzido nesta dissertação (COGHLAN; BRANNICK, 2005; ZUBER-SKERRITT; PERRY, 2002).

Na classificação de Coghlan e Brannick (2005), este projeto se enquadra no Quadrante 2, havia intenção de auto estudo em ação por parte do sistema, mas não por parte do pesquisador. A partir de um estudo de três casos, Bartunek et al. (2019) generalizam oito pontos comuns em projetos de pesquisa-ação conduzidos por gerentes das organizações pesquisadas:

> “1. A atribuição do trabalho que leva ao projeto de pesquisa-ação provavelmente vem do superior do gerente e faz parte da descrição do seu cargo.
> 2. Os demais participantes na intervenção provavelmente são subordinados que precisam aderir ao projeto de mudança.
> 3. A intervenção provavelmente objetiva aumento da produtividade.
> 4. Gerentes podem achar útil constituir uma equipe de consultoria para ajudar na intervenção.
> 5. A coleta de dados pode ocorrer por uma variedade de meios formais e informais.
> 6. As sessões de feedback podem ser integradas ao dia a dia do trabalho ou serem conduzidas separadamente.
> 7. O gerente provavelmente tem interesse pessoal no resultado da intervenção.
> 8. Os gerentes estavam todos recebendo treinamento em pesquisa-ação durante a realização de suas intervenções.” (BARTUNEK et al., 2019)

Com pequenas exceções estes pontos são verdadeiros para o projeto em questão. O projeto efetivamente foi uma designação do superior do pesquisador, como no item 1, e passou a fazer parte da descrição do cargo, ainda que apenas a partir do momento em que o pesquisador foi nomeado encarregado de dados para a Liderança. O item 2 também é parcialmente correto, no início do projeto os participantes eram subordinados, porém no avanço do projeto integrantes de outras áreas foram agregados. Equipes de consultoria participaram do projeto, como sugere o item 4. Os itens 5 e 6 são amplos o suficiente para ser verdade em quase todos os projetos. O item 7 é praticamente uma consequência do item 1.

Apenas os itens 3 e 8 não ocorreram neste projeto. A governança da privacidade não está associada a ganhos de produtividade, nem houve treinamentos para os demais gerentes do projeto.

Corroborando Zuber-Skerritt e Perry (2002), este pesquisador identificou claramente os dois projetos concorrentes. Houve um processo de planejamento da pesquisa no projeto '*thesis*', a execução da pesquisa no projeto '*core*', e um processo de reflexão e entendimento na redação deste documento. A observação do projeto '*core*' pelo projeto '*thesis*' trouxe uma perspectiva que permitiu *insights* que não ocorreram no calor da execução. Mesmo questões que estavam presentes desde o início do trabalho de campo (por exemplo, por que as metodologias de adequação à LGPD divulgadas em artigos comerciais não falam da governança da privacidade?), adquirem uma maior profundidade durante a escrita da dissertação.

6 Conclusão

Este trabalho, ao adotar a pesquisa-ação, buscou produzir conhecimento para demonstrar a capacitação do autor para o mestrado profissional e trazer um resultado concreto para a empresa onde foi realizado. A escolha da intervenção no processo de implantação da governança da privacidade aplicando a pesquisa-ação gerou uma oportunidade de entregar um resultado concreto para a Liderança e se desdobrou neste trabalho.

O trabalho visava estudar como se implanta a governança de privacidade numa empresa, através da identificação de metodologias para a implantação da governança da privacidade e avaliação de sua adequação à LGPD. A relevância da governança da privacidade se dá pela LGPD, que determina que a adoção de uma política de governança é um dos critérios de definição a serem considerados na definição das sanções sofridas pela empresa nos casos de violação. Como a governança da privacidade trabalha para mitigar os riscos de privacidade da empresa, a sua adoção traz o duplo benefício de reduzir a probabilidade de sanções e reduzir o seu impacto.

O método adotado foi a pesquisa-ação. A pesquisa se desenvolveu em três ciclos, que ocorreram ao longo do processo de implantação da governança da privacidade e da conformidade à LGPD. O pesquisador foi o responsável pelo projeto.

Os dois primeiros ciclos buscaram a implantação da governança da privacidade antecipadamente à implantação da gestão da privacidade, buscando com isso resolver o conflito de interesses entre o projeto de implantação, com foco nos objetivos, prazo e custos do projeto, e a conformidade com a LGPD, com foco na gestão dos riscos. Por falta de um modelo de governança de privacidade adequado na literatura, nestes ciclos do projeto usou-se a governança de dados como modelo. Esta escolha deriva de, num contexto empresarial, a privacidade se equivaler à proteção dos dados pessoais e a proteção dos dados pessoais ser um caso específico da segurança dos dados da governança de dados (DENNEDY; FOX; FINNERAN, 2014).

O uso de modelos da governança de dados como base para a implantação da governança de privacidade mostrou-se problemático. A proteção de dados pessoais pode ser um caso específico da proteção de dados da governança de dados, mas se olharmos o modelo

conceitual da governança de dados (vide Figura 7), veremos que a governança de dados envolve domínios além dos necessários para a governança da privacidade: arquitetura de dados, metadados e armazenamento e infraestrutura. Estes domínios adicionais adicionaram complexidade ao processo de implantação, complicando o entendimento dos participantes não técnicos e tornando o processo lento (ABRAHAM; SCHNEIDER; VOM BROCKE, 2019; DENNEDY; FOX; FINNERAN, 2014).

Após uma interrupção causada pela pandemia do COVID-19, no terceiro ciclo o comitê mudou a estratégia e passou a buscar a implantação da governança da privacidade em paralelo a implantação da conformidade com a LGPD. Neste ciclo o pesquisador encontrou dois modelos de governança da privacidade com potencial de aplicação no caso, o modelo conceitual de Swartz, da Veiga e Martins (2019) e a função GOVERN-P do NIST PF (2020). O modelo do NIST PF mostrou-se mais adequado pelos seguintes fatores:

a) o conceito de governança do NIST PF está alinhado ao modelo de governança da OECD (“estrutura através da qual os objetivos da empresa são definidos e se determina os meios para alcançar esses objetivos e para monitorizar o desempenho”);

b) o modelo permite a avaliação da situação atual da governança e o desenho de situações futuras, facilitando o processo de melhoria contínua; e,

c) o NIST PF tem estrutura semelhante ao NIST CSF, amplamente difundido e usado.

Com isto, foi implantado um perfil inicial da função GOVERN-P do NIST PF como governança de privacidade na Liderança Capitalização e já se desenhou um caminho de evolução para um nível de implementação mais maduro. Do ponto de vista prático, essa característica do NIST PF de estimular a identificação do *Profile* atual e de se desenhar um *Profile* futuro desejável auxiliou no processo de mudança organizacional.

A implantação do modelo do NIST PF de governança da privacidade na Liderança foi facilitada por já haver uma estrutura de governança para a privacidade antes da adoção do modelo. Já havia o comitê de governança e um DPO definido para avaliarem os riscos de privacidade para a organização e identificarem o *Profile* atual do NIST PF. Com a avaliação

dos riscos de privacidade e o *Profile* atual foi possível desenhar um profile desejável, definir um prazo para a sua implantação e aprovar o plano junto à Diretoria.

A questão da pesquisa, **de como se implanta a governança da privacidade numa empresa**, pode ser considerada respondida pelo pequeno guia doa parágrafos anteriores. Enquanto os modelos de governança de dados, pelo menos neste caso, não se mostraram como metodologias adequadas à implantação da governança da privacidade, a função GOVERN-P do NIST PF atendeu às necessidades da Liderança Capitalização. A Tabela 9 e a Tabela 10 mostram a adequação à LGPD da função GOVERN-P do NIST PF, complementada com alguns subcomponentes de outras funções.

A contribuição à prática deste trabalho é a indicação de um modelo viável de governança da privacidade. A governança da privacidade é uma necessidade de todas as empresas com volume ou complexidade de tratamento de dados pessoais e a ANPD deve começar a fiscalizar e autuar as empresas mais fortemente. Uma ação que mitigue os riscos de problemas de privacidade e reduza as consequências em caso de autuação é muito bem-vinda.

A pesquisa-ação mostrou-se adequada a este projeto de cunho mais exploratório, pois as atividades de reflexão nos ciclos ajudavam a corrigir os impasses eventualmente identificados no caminho. Uma limitação de todos os projetos de pesquisa-ação é o foco em uma situação específica e não objetivar a criação de conhecimento universal (COGHLAN; BRANNICK, 2005). Entretanto, podemos extrapolar o conhecimento obtido para outras situações. Os problemas enfrentados na adaptação da governança de dados para a governança de privacidade têm grande probabilidade de serem encontrados em processos semelhantes em empresas não técnicas de médio porte. A facilidade de absorção do NIST PF deve ser encontrada nas empresas que já utilizam o NIST CSF, e, mesmo para as que não utilizam o NIST CSF, o processo de levantamento do *Profile* atual e o desenho de um *Profile* futuro desejado deve facilitar o processo de implantação do NIST PF.

Outra situação que pode se aplicar a outras empresas e processos de implantação de governança é a separação das estruturas de governança das estruturas de gestão do projeto de implantação. No caso coberto por este trabalho havia uma preocupação nos primeiros ciclos em implantar a governança antes da implantação da adequação à LGPD, antevendo compromissos ou decisões complexas a serem tomadas em relação ao tratamento de dados

pessoais. No terceiro ciclo percebemos que o comitê de governança já era suficiente para tratar as questões de privacidade surgidas durante o projeto e como o comitê não fazia parte da estrutura de decisão do projeto não havia conflito de interesses.

Uma limitação deste projeto é que relata o processo de implantação inicial da função GOVERN-P do NIST PF em apenas uma empresa, de um setor relativamente pouco expressivo (todo o setor de seguros representava em 2021 apenas 3,5% do PIB, capitalização apenas 0,28% (SUPERINTENDÊNCIA DE SEGUROS PRIVADOS, 2022)). Pesquisas futuras podem acompanhar o processo de evolução da governança de privacidade aplicando a função GOVERN-P do NIST PF ao longo do tempo, ou em várias empresas. Também podem estudar a implantação do NIST PF como um todo, ao longo do tempo e em várias empresas. Estudos comparativos podem ser feitos entre os diversos modelos de governança da privacidade implementados nas empresas.

Dois temas encontrados no processo não puderam ser aprofundados e mereceriam a atenção de pesquisas futuras. A questão da ordem de implantação dos fatores dos modelos de governança não foi encontrada explicitamente na literatura. O modelo conceitual da governança de dados de Alhassan, Sammon e Daly (2018) aborda a priorização das atividades da governança de dados, mas não aborda explicitamente a ordem ótima de implantação. O outro tema para estudos futuros é a otimização da coordenação entre as diversas governanças nas empresas. Enquanto alguns casos são largamente estudados, como o alinhamento da governança de TI com a governança corporativa, a questão da coordenação e alinhamento entre as diversas governanças merece a atenção da academia.

REFERÊNCIAS

ABRAHAM, R.; SCHNEIDER, J.; VOM BROCKE, J. Data governance: A conceptual framework, structured review, and research agenda. **International Journal of Information Management**, v. 49, p. 424–438, 1 dez. 2019.

ADLER, P. A.; ADLER, P. **Membership Roles in Field Research**. [s.l.] SAGE, 1987.

AL-HADDAD, S.; KOTNOUR, T. Integrating the organizational change literature: a model for successful change. **Journal of Organizational Change Management**, v. 28, n. 2, p. 234–262, 13 abr. 2015.

ALHASSAN, I.; SAMMON, D.; DALY, M. Data governance activities: a comparison between scientific and practice-oriented literature. **Journal of Enterprise Information Management**, v. 31, n. 2, p. 300–316, 5 mar. 2018.

ALTMAN, I. **The environment and social behavior : privacy, personal space, territory, crowding**. [s.l.] Monterey, Calif. : Brooks/Cole Pub. Co., 1975.

BANVILLE, C.; LANDRY, M. Can the field of MIS be disciplined? **Communications of the ACM**, v. 32, n. 1, p. 48–60, 1 jan. 1989.

BARTUNEK, J. M. et al. Managers and Project Leaders Conducting Their Own Action Research Interventions. Em: **Handbook of Organizational Consultation**. [s.l.] Routledge, 2019. p. 76–91.

BASKERVILLE, R. L.; WOOD-HARPER, A. T. A critical perspective on action research as a method for information systems research. **Journal of Information Technology (Routledge, Ltd.)**, v. 11, n. 3, p. 235–246, set. 1996.

BRASIL. Lei Nº 13.709, de 14 de agosto de 2018. . 2018, p. 59.

CARTER, T. E. **Privacy Risk Assessment of a DON Digital Contact Tracing System Using the NIST Privacy Framework**. [s.l.] Naval Postgraduate School, 2021.

CARTER, T.; KROLL, J. A.; BRET MICHAEL, J. Lessons Learned From Applying the NIST Privacy Framework. **IT Professional**, v. 23, n. 4, p. 9–13, 1 jul. 2021.

COGHLAN, D.; BRANNICK, T. **DOING ACTION RESEARCH IN YOUR OWN ORGANIZATION**. 2ª ed. Londres: SAGE Publications Ltd, 2005.

CONSELHO NACIONAL DE SEGUROS PRIVADOS. **RESOLUÇÃO CNSP Nº 416, DE 20 DE JULHO DE 2021**. Conselho Nacional de Seguros Privados, , 20 jul. 2021. Disponível em: <https://www2.susep.gov.br/safe/scripts/bnweb/bnmapi.exe?router=upload/25061>

Cyber Risk Institute – Don't risk risk. Disponível em: <https://cyberriskinstitute.org/>. Acesso em: 2 abr. 2023.

DE GUERRE, D. W. Doing action research in one's own organization: An ongoing conversation over time. **Systemic practice and action research**, v. 15, p. 331–349, 2002.

DE HAES, S.; VAN GREMBERGEN, W. **IT Governance Structures, Processes and Relational Mechanisms: Achieving IT/Business Alignment in a Major Belgian Financial Group**. Proceedings of the 38th Annual Hawaii International Conference on System Sciences. **Anais**... Em: 38TH ANNUAL HAWAII INTERNATIONAL CONFERENCE ON SYSTEM SCIENCES. Big Island, HI, USA: IEEE, 2005. Disponível em: <http://ieeexplore.ieee.org/document/1385726/>. Acesso em: 20 jan. 2023

DENNEDY, M. F.; FOX, J.; FINNERAN, T. R. **The Privacy Engineer's Manifesto: Getting from Policy to Code to QA to Value**. [s.l.] Springer Nature, 2014.

Examples of Framework Profiles. Disponível em: <https://www.nist.gov/cyberframework/examples-framework-profiles>. Acesso em: 2 abr. 2023.

FU, X. et al. Data governance in predictive toxicology: A review. **Journal of Cheminformatics**, v. 3, n. 1, p. 24, 13 dez. 2011.

FUKUYAMA, F. What Is Governance? **Governance**, v. 26, n. 3, p. 347–368, 2013.

GAJDA, A. **What if Samuel D. Warren Hadn't Married a Senator's Daughter?: Uncovering the Press Coverage that Led to The Right to Privacy**. Rochester, NY, 5 nov. 2007. Disponível em: <https://papers.ssrn.com/abstract=1026680>. Acesso em: 10 nov. 2022

GILL, R. Change management — or change leadership? **Journal of Change Management**, v. 3, 2003.

GILLAN, S. L. Recent Developments in Corporate Governance: An Overview. **Journal of Corporate Finance**, v. 12, n. 3, p. 381–402, jun. 2006.

GUILHEM. **Artigo - LGPD: etapas da entrada em vigor | FCR Law News**. Disponível em: <https://news.fcrlaw.com.br/artigo-lgpd-etapas-da-entrada-em-vigor/>. Acesso em: 1 dez. 2022.

GUMMESSON, E. **Qualitative methods in management research**. [s.l.] Sage, 2000.

HOLVAST, J. 27 - History of privacy. Em: LEEUW, K. D.; BERGSTRA, J. (Eds.). **The History of Information Security**. Amsterdam: Elsevier Science B.V., 2007. p. 737–769.

HUBERTS, L. **The Integrity of Governance: What it is, What we Know, What is Done and Where to go**. [s.l.] Springer, 2014.

JOINT TASK FORCE. **Control Baselines for Information Systems and Organizations**. [s.l.] National Institute of Standards and Technology, 28 out. 2020a. Disponível em: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53B.pdf>. Acesso em: 28 nov. 2022.

JOINT TASK FORCE. **Security and Privacy Controls for Information Systems and Organizations**. [s.l.] National Institute of Standards and Technology, 10 dez. 2020b. Disponível em: <https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final>. Acesso em: 30 abr. 2023.

JOINT TASK FORCE TRANSFORMATION INITIATIVE. **Guide for conducting risk assessments**. Gaithersburg, MD: National Institute of Standards and Technology, 2012. Disponível em: <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf>. Acesso em: 18 mar. 2023.

KHATRI, V.; BROWN, C. V. Designing Data Governance. **Communications of the ACM**, v. 53, n. 1, p. 148–152, jan. 2010.

KOERNER, KATHARINA. **Standardization landscape for privacy: Part 1 — The NIST Privacy Framework**. **The Privacy Advisor**, 1 dez. 2021. Disponível em: <https://iapp.org/news/a/standardization-landscape-for-privacy-part-1-the-nist-privacy-framework/>. Acesso em: 20 jan. 2023

KRAMER, J.; HOAR, S. **GDPR, Part I: History Of European Data Protection Law.** Disponível em: <https://search.ebscohost.com.sbproxy.fgv.br/login.aspx?direct=true&db=edsvlx&AN=edsvlx.696231625&lang=pt-br&site=eds-live>. Acesso em: 19 abr. 2019.

LEFKOVITZ, N.; BOECKL, K. **Portuguese Translation of the NIST Privacy Framework Version 1.0**. [s.l.] National Institute of Standards and Technology, 1 set. 2021. Disponível em: <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.01162020pt.pdf>. Acesso em: 21 jan. 2023.

LEPORE, J. **Episode 3: The Invisible Lady**. : The Last Archive., 2020. Disponível em: <https://www.thelastarchive.com/season-1/episode-3-the-invisible-lady>. Acesso em: 30 nov. 2021

LIDERANÇA CAPITALIZAÇÃO S.A. **Liderança Capitalização**. Disponível em: <https://lidercap.com.br/>. Acesso em: 30 nov. 2022a.

LIDERANÇA CAPITALIZAÇÃO S.A. **Tele Sena - A Tele Sena**. Disponível em: <https://www.telesena.com.br/#/a-telesena.html>. Acesso em: 30 nov. 2022b.

LUKÁCS, A. WHAT IS PRIVACY? THE HISTORY AND DEFINITION OF PRIVACY. p. 10, 2016.

MONKS, R. A. G.; MINOW, N. **Corporate Governance**. [s.l.] John Wiley & Sons, 2011.

MONTEIRO, R. L. **Lei Geral de Proteção de Dados do Brasil – Análise - Baptista Luz Advogados : Baptista Luz Advogados**. São Paulo: BAPTISTA LUZ ADVOGADOS, 2018. Disponível em: <https://baptistaluz.com.br/institucional/lei-geral-de-protecao-de-dados-do-brasil-analise/>. Acesso em: 10 abr. 2019.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. **NIST PRIVACY FRAMEWORK:: A TOOL FOR IMPROVING PRIVACY THROUGH ENTERPRISE RISK MANAGEMENT, VERSION 1.0**. Gaithersburg, MD: National Institute of Standards and Technology, 16 jan. 2020. Disponível em: <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.01162020.pdf>. Acesso em: 30 jul. 2020.

NILSEN, P. Making sense of implementation theories, models, and frameworks. **Implementation Science 3.0**, p. 53–79, 2020.

OECD. **Guidelines governing the protection of privacy and transborder flows of personal data**. [s.l.] Organisation for Economic Cooperation and Development, 1980. . Acesso em: 19 abr. 2019.

OECD. **OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data**. [s.l.] OECD, 2002.

OECD. **Princípios de Governo das Sociedades do G20/OCDE**. [s.l.] OECD Publishing, 2016.

OPICE BLUM, BRUNO E VAINZOF ADVOGADOS ASSOCIADOS. **LGPD em Vigor? | Report informativo e LIVE hoje às 13h30**. Disponível em: <https://mailchi.mp/opiceblum/lgpd-aguarda-sancao-presidencial-para-entrar-em-vigor?e=d54077e2a1>. Acesso em: 1 dez. 2022.

PrivacyEngCollabSpace/tools/risk-assessment/NIST-Privacy-Risk-Assessment-Methodology-PRAM at master · usnistgov/PrivacyEngCollabSpace. Disponível em: <https://github.com/usnistgov/PrivacyEngCollabSpace>. Acesso em: 30 abr. 2023.

SAMSET, K.; VOLDEN, G. H. Front-end definition of projects: Ten paradoxes and some reflections regarding project management and project governance. **International Journal of Project Management**, v. 34, n. 2, p. 297–313, 1 fev. 2016.

SHLEIFER, A.; VISHNY, R. W. A Survey of Corporate Governance. **The Journal of Finance**, v. 52, n. 2, p. 737–783, 1997.

SOLOVE, D. J. A Brief History of Information Privacy Law. p. 47, 2006.

SUPERINTENDÊNCIA DE SEGUROS PRIVADOS. **CIRCULAR SUSEP Nº 612, DE 18 DE AGOSTO DE 2020**. , 18 ago. 2020.

SUPERINTENDÊNCIA DE SEGUROS PRIVADOS. **10º RELATÓRIO DE ANÁLISE E ACOMPANHAMENTO DOS MERCADOS SUPERVISIONADOS**. , 30 maio 2022. Disponível em: <https://www.gov.br/susep/pt-br/central-de-conteudos/dados-estatisticos/Relat_Acomp_Mercado_2022.pdf>. Acesso em: 7 abr. 2023

SWARTZ, P.; DA VEIGA, A.; MARTINS, N. **A conceptual privacy governance framework**. 2019 Conference on Information Communications Technology and Society (ICTAS). **Anais**... Em: 2019 CONFERENCE ON INFORMATION COMMUNICATIONS TECHNOLOGY AND SOCIETY (ICTAS). Durban, South Africa: IEEE, mar. 2019. Disponível em: <https://ieeexplore.ieee.org/document/8703636/>. Acesso em: 1 nov. 2022

SWARTZ, P.; DA VEIGA, A.; MARTINS, N. Validating an information privacy governance questionnaire to measure the perception of employees. **Information & Computer Security**, v. 29, n. 5, p. 761–786, 1 jan. 2021.

TEFFÉ, C. S. DE; VIOLA, M. Tratamento de dados pessoais na LGPD: estudo sobre as bases legais. **civilistica.com**, v. 9, n. 1, p. 1–38, 9 maio 2020.

VAN EYNDE, D. F.; BLEDSOE, J. A. The Changing Practice of Organisation Development. **Leadership & Organization Development Journal**, v. 11, n. 2, p. 25–30, 1 jan. 1990.

WARREN, S. D.; BRANDEIS, L. D. The Right to Privacy. **Harvard Law Review**, v. 4, n. 5, p. 193–220, 1890.

WEILL, P. D.; ROSS, J. W. **IT Governance : How Top Performers Manage IT Decision Rights for IT Governance :** 1. ed. Boston, MA, EUA: Harvard Business Review Press, 2004.

WESTIN, A. F. **Privacy and freedom**. [s.l.] New York, Atheneum, 1967.

Whitepaper: Survey Report: Trends in Security Framework Adoption. Disponível em: <https://www.tenable.com/whitepapers/trends-in-security-framework-adoption>. Acesso em: 20 jan. 2023.

ZUBER-SKERRITT, O.; PERRY, C. Action research within organisations and university thesis writing. **The learning organization**, v. 9, n. 4, p. 171–179, 2002.