ESCOLA NACIONAL DE ADMINISTRAÇÃO PÚBLICA
PROGRAMA DE MESTRADO PROFISSIONAL EM GOVERNANÇA E DESENVOLVIMENTO

A IMPLEMENTAÇÃO DA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS NA GOVERNANÇA DO PROCESSO DE PAGAMENTO DE PESSOAL DO COMANDO DO EXÉRCITO

DISSERTAÇÃO DE MESTRADO

PLÍNIO MARIA CARNEIRO

BRASÍLIA – DF
2023

A IMPLEMENTAÇÃO DA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS NA GOVERNANÇA DO PROCESSO DE PAGAMENTO DE PESSOAL DO COMANDO DO EXÉRCITO

Dissertação apresentada ao Programa de Mestrado em Governança e Desenvolvimento da Escola Nacional de Administração Pública - ENAP como requisito para obtenção do título de Mestre em Governança e Desenvolvimento.

Aluno: PLÍNIO MARIA CARNEIRO
Orientador: PROF. DR. CLÓVIS HENRIQUE LEITE DE SOUZA

Brasília - DF
2023

Ficha catalográfica elaborada pela equipe da Biblioteca Graciliano Ramos da Enap

C289i Carneiro, Plínio Maria
A implementação da Lei Geral de Proteção de Dados Pessoais na governança do processo de pagamento de pessoal do comando do exército / Plínio Maria Carneiro. -- Brasília: Enap, 2023.
134 f. : il.

Dissertação (Mestrado --Programa de Mestrado em Governança e Desenvolvimento) -- Escola Nacional de Administração Pública, 2023.

Orientação: Prof. Dr. Clóvis Henrique Leite de Souza.
1. Segurança de Dados. 2. Lei Geral de Proteção de Dados. 3. Governança de Dados . 4. Dados Pessoais. 5. Centro de Pagamento do Exército. I. Título. II. Souza, Clóvis Henrique Leite de orient.

CDD 658.472

Bibliotecária: Kelly Lemos da Silva – CRB1/1880

ATA DA BANCA DE DEFESA DE TRABALHO DE CONCLUSÃO DO CURSO DE MESTRADO PROFISSIONAL EM GOVERNANÇA E DESENVOLVIMENTO

Aluno (a): Plínio Maria Carneiro

Ano de Ingresso**:** 2022

Título da dissertação: A Implementação da Lei Geral de Proteção de Dados Pessoais na governança do processo de pagamento de pessoal do Comando do Exército

Orientador: Prof. Dr. Clóvis Henrique Leite de Souza

Avaliador:

Prof. Dr. José de Ribamar Sousa Pereira Prof. Dr. Maurício Ebling

Avaliação:

[X Aprovado

]

[Não aprovado. Reapresentação agendada para _____/_____/_____.

]

DocuSigned by:
José de Ribamar Sousa Pereira
B8CF290423EF4F3...

Avaliador

Brasília, 17 de novembro de 2023

DocuSigned by:
Mauricio Ebling
2F1363790D99440...

Avaliador

DocuSigned by:
Clovis Henrique Leite de Souza
CE1C2FDFBED74B5...

Orientador

MINISTÉRIO DA GESTÃO E DA INOVAÇÃO EM SERVIÇOS PÚBLICOS

GOVERNO FEDERAL BRASIL UNIÃO E RECONSTRUÇÃO

BRASÍLIA
2023

Dedico este trabalho a minha amada mãe, Maria Esméria Sobrinho Carneiro, quem foi para mim um exemplo de humildade e de bondade, e quem hoje, lá do plano espiritual, ainda me ensina, enchendo meu coração de gratidão pela oportunidade de ter sido seu filho e de, a cada dia, tentar ser uma pessoa melhor.

AGRADECIMENTOS

A Deus, por sempre ter uma nova oportunidade de reparar os meus erros e por continuar aprendendo todos os dias.

A minha esposa, por ser minha parceira amorosa e apoiadora incondicional, e a minha família, que sempre me deu o suporte necessário.

Aos professores, que se dedicaram em repassar seus conhecimentos.

Ao Exército Brasileiro, que me proporcionou servir a um propósito maior, e à ENAP, por ter me concedido a honra de ser aluno da instituição.

"*Não podemos prever o futuro, mas podemos criá-lo.*"

Peter Drucker

LISTA DE FIGURAS

LISTA DE QUADROS

LISTA DE ABREVIATURAS E SIGLAS

ABNT - Associação Brasileira de Normas Técnicas

ANAC – Agência Nacional de Aviação Civil

ANPD - Autoridade Nacional de Proteção de Dados

ARCO - Acesso, Retificação, Cancelamento

BACEN – Banco Central do Brasil

BEST - *Business Engaged Security Transformation*

BIEG - Banco de Informações Estratégicas e Gerenciais de Remuneração dos Militares

BIOT - Base de Informações de Operações de Tratamento

CAGED - Cadastro Geral de Empregados e Desempregados

CDC - Código de Defesa do Consumidor

CDS - Centro de Desenvolvimento de Sistemas

CITEX - Centro Intregrado de Telemática do Exército

CONARQ - Conselho Nacional de Arquivos

CPEx - Centro de Pagamento do Exército

CPF – Cadastro de Pessoa Física

CTA - Centro Telemática de Área

CTIR Gov - Centro de Tratamento a Resposta a Incidentes Cibernéticos de Governo

DATAPREV - Empresa de Tecnologia e Informações da Previdência Social

DGP – Departamento Geral de Pessoal

DIRF - Declaração do Imposto de Renda Retido na Fonte

DPO - encarregado do tratamento de dados pessoais (Data Protection Officer)

EBconsig - Sistema de Consignações do Exército

EBCORP - Base de Dados Corporativa do Exército

EC - EntidadesConsignatárias

EC-Council - *Cybersecurity Certification, Education, Training, and Services Company*

EME - Estado-Maior do Exército

E-SIC - Sistema Eletrônico do Serviço de Informação ao Cidadão

ETIR - Equipe de Tratamento e Resposta a Incidentes Cibernéticos

FEBRABAN - Federação Brasileira de Bancos

FR – Fator de Risco

GDPR - General Data ProtectionRegulation

GSI - Gabinete de Segurança Institucional

IBCA - Instituto Brasileiro de Conselheiros de Administração

IBGC - Instituto Brasileiro de Governança Corporativa

IBGP - Instituto Brasileiro de Governança Pública

ICN - Índice para Continuidade do Negócio

IDP - Inventário de Dados Pessoais

IL - Índice de importância

INSS – Instituto Nacional de Seguridade Social

ISC – *Intelligence Service Center*

ISO - *International Organization for Standardization*

LGPD - Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018)

LAI - Lei de Acesso à Informação (Lei 12.527/2011)

MD – Ministério da Defesa

NIST - *National Institute of Standards and Technology*

NIT - Número de Inscrição do Trabalhador

OM - Organização Militar

PASEP - Programa de Formação do Patrimônio do Servidor Público

PDA – Plano de Dados Abertos

PDCA - *Plan, Do, Check e Act*

PGP - Programa de Governança em Privacidade

PIS – Programa de Integração Social

PNSI - Política Nacional de Segurança da Informação

PREC/CP – Número de identificação do militar do Exército

PSI - Política de Segurança da Informação

RAIS - Relação Anual de Informações Sociais

RIPD - Relatório de Impacto à Proteção de Dados Pessoais

RPOs - Objetivos de Ponto de Recuperação

RTOs - Objetivos de Tempo de Recuperação

SCPAD - Subcomissão Permanente de Avaliação de Documentos

SEF - Secretaria de Economia e Finanças

SGCSI - Sistema de Gestão de Cibersegurança e Segurança da Informação

SGD - Secretaria de Governo Digital

SIAPPES - Sistema Automático de Pagamento de Pessoal

SIGEPE - Sistema de Gestão de Pessoas do Governo Federal

SINFOEx - Sistema de Informação do Exército

SIPPES - Sistema de Pagamento de Pessoal

SIRC - Sistema Nacional de Informações de Registro Civil

SRE - Sistema de Retribuição no Exterior

STF - Supremo Tribunal Federal

STJ – Superior Tribunal de Justiça

TCU - Tribunal de Contas da União

TI - Tecnologia da Informação

UORg - Unidade Organizacional

RESUMO

CARNEIRO, Plínio Maria. **A implementação da Lei Geral de Proteção de Dados Pessoais na governança do processo de pagamento de pessoal do Comando do Exército**. 2023. 169f. Trabalho de Conclusão de Curso – Mestrado Profissional em Governança e Desenvolvimento – Escola Nacional de Administração Pública, Brasília, Distrito Federal, 2023.

A Lei Geral de Proteção de Dados Pessoais (LGPD) trouxe para os agentes públicos e privados uma nova realidade no tratamento de dados pessoais, o que fez com que este trabalho buscasse avaliar os fatores críticos de sucesso para a implementação da LGPD no processo de pagamento de pessoal do Centro de Pagamento do Exército (CPEx). Foram pesquisadas as medidas necessárias para a implementação contidas na legislação, em modelos teóricos e nos guias da Autoridade Nacional de Proteção de Dados (ANPD), de forma a estabelecer um referencial teórico particularizado para o setor público. Avaliou-se o tratamento de dados no CPEx, identificando medidas que também devem ser cumpridas em função de normativas específicas para esse órgão. Foi analisada a importância da governança da Alta Administração na implementação da LGPD, particularmente a governança de dados, de forma a estabelecer um referencial teórico para essa abordagem. Entrevistas foram realizadas com 5 gestores para comparar os referenciais teóricos com a realidade das instituições e para identificar boas práticas e medidas que impactam diretamente na execução do processo de implementação da lei. Ao final, foi elaborado um modelo de implementação roteirizado que pode ser utilizado não só no processo de adequação da LGPD no CPEx, mas também em outras instituições públicas, de forma a orientar o trabalho dos gestores na implementação da LGPD no setor público, apontando a governança da Alta Administração, as ações educacionais e a atuação de uma equipe multidisciplinar como bases fundamentais para o processo de adequação à lei.

Palavras-chave: LGPD. Implementação. CPEx. Exército. Dados pessoais.

ABSTRACT

CARNEIRO, Plínio Maria. **A implementação da Lei Geral de Proteção de Dados Pessoais na governança do processo de pagamento de pessoal do Comando do Exército**. 2023. 169f. Trabalho de Qualificação de Curso – Mestrado Profissional em Governança e Desenvolvimento – Escola Nacional de Administração Pública, Brasília, Distrito Federal, 2023.

The General Personal Data Protection Law (GPDL) brought a new reality to public and private agents in the processing of personal data, which made this work seek to evaluate the critical success factors for the implementation of GPDL in the payment process of personnel at the Army Payment Center (CPEx). The necessary measures for implementation contained in legislation, theoretical models and National Data Protection Authority (NDPA) guides were identified, in order to establish a specific theoretical framework for the public sector. Data processing at CPEx was evaluated, identifying measures that must also be followed according to specific regulations for this body. The importance of Senior Management governance in the implementation of the GPDL, particularly Data Governance, was analyzed in order to establish a theoretical framework for this approach. Interviews were carried out with 5 managers to compare theoretical references with the reality of the institutions and to identify good practices and measures that directly impact the execution of the law implementation process. In the end, a scripted implementation model was produced that can be used not only in the process of adapting the GPDL at CPEx, but also in other public institutions, in order to guide the work of managers in implementing the GPDL in public sector, pointing out governance of Senior Management, educational actions and the work of a multidisciplinary team as fundamental bases for the process of adapting to the law.

Keywords: GPDL. Implementation. CPEx. Army. Personal data.

SUMÁRIO

1. INTRODUÇÃO

A Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD), trouxe para os diversos agentes de tratamento de dados, públicos e privados, uma nova realidade na execução de suas atividades. Nesse cenário, as exigências de adequação buscam a reflexão sobre as atividades que tratam dados pessoais, se elas são necessárias e adequadas às finalidades que pretendem, se há segurança e transparência nesses processos, se há amparo legal no tratamento e se há a viabilização do exercício dos direitos dos titulares.

Nesse cenário de evolução das normativas legais sobre o tratamento de dados, todos os controladores são, constantemente, obrigados a revisarem seus processos, suas hipóteses e verificarem a adequação do tratamento executado com a finalidade proposta. Nesse contexto evolutivo, a LGPD passa a ditar parâmetros para processos em que não havia adequada regulação ou limitação, implicando na reorganização do fluxo, no uso legítimo de informações pessoais e no estabelecimento de direitos e obrigações aos envolvidos nos tratamentos de dados.

No Comando do Exército, particularmente no Centro de Pagamento do Exército (CPEx), o tratamento de dados é essencial para a execução do pagamento de militares e pensionistas, e a adequada forma como tais informações são utilizadas garante a efetividade da missão institucional, a manutenção do direito dos titulares e a preservação da integridade do Exército, evitando incidentes de segurança, ações judiciais e prejuízos para os proprietários dos dados, de forma que todo processo de pagamento esteja em conformidade com a LGPD.

Avaliando toda essa realidade, surge o questionamento principal: quais seriam os fatores críticos de sucesso para implementar a LGPD no processo de pagamento de pessoal do Comando do Exército? Para responder a essa demanda, foram feitas perguntas secundárias as quais são tomadas como ponto de partida para este trabalho: o que há atualmente de normativo relacionado à implementação LGPD em uma instituição pública? Como o CPEx se encontra nesse processo? Como os modelos teóricos podem auxiliar nessa implementação? Quais medidas foram tomadas por outras instituições nesse processo? Qual o papel da governança institucional na implementação da LGPD? O que o CPEx pode fazer para buscar a conformidade do processo de pagamento de pessoal do Exército?

Desta feita, o objetivo principal do presente estudo foi elaborar projeto de intervenção para propor medidas necessárias para a implementação das diretrizes trazidas pela LGPD, considerando o contexto do processo de pagamento de pessoal do CPEx, os modelos teóricos, as boas práticas existentes, a experiência de outras instituições e as ações de governança

necessárias, de forma a identificar soluções que atendam às exigências da lei na busca da conformidade do tratamento e no alinhamento com as normativas da instituição.

Cabe ressaltar que o presente trabalho não pretende executar o processo de implementação da LGPD no Comando do Exército, tarefa esta que deve ser conduzida, salvo melhor juízo, por uma equipe multidisciplinar nomeada para os trabalhos, sob os parâmetros de governança da instituição. Também não busca avaliar a implementação da LGPD em processos do Comando do Exército que não estejam relacionados ao pagamento de pessoal, como os processos de compra, de gestão de pessoal, de ordem jurídica, nem processos externos ao Exército.

Assim, o foco deste trabalho é propor um modelo teórico roteirizado para viabilizar a implementação da LGPD em um órgão do setor público, particularmente, no processo de pagamento de pessoal do CPEx, de forma a oferecer um direcionamento para a busca da conformidade legal, sem, no entanto, pretender esgotar o assunto ou impedir a elaboraçãode outras propostas relacionadas ao tema.

1.1 Técnicas de pesquisa

Buscando possíveis respostas aos questionamentos do presente trabalho, inicialmente foi feita uma pesquisa bibliográfica nas atuais normativas de tratamento de dados pessoais buscando a referência legal para adoção de medidas de implementação (Capítulo I). De posse de tais conhecimentos, avaliou-se o contexto do tratamento de dados no processo de pagamento de pessoal do Comando do Exército, relacionando-o com as diretrizes da LGPD (Capítulo II).

Em seguida, foi feita uma busca bibliográfica por referências que auxiliassem o processo de implementação da lei, como modelos teóricos que pudessem ser ajustados para o âmbito do setor público. Em complemento, foram entrevistados gestores envolvidos com tratamento de dados pessoais para se obter informações sobre o caminho que cada organização está trilhando no processo de ajuste à LGPD e sobre boas práticas existentes nos setores público e privado.

As entrevistas aconteceram com 1 gestor de uma empresa privada, 1 gestor de órgão público federal, 2 gestores das Forças Armadas e 1 gestor interno do CPEx. Todos atuam na área de proteção de dados, ou na área de TI, ou são DPO em suas instituições. Elas foram feitas presencialmente, por videoconferência e apenas uma por escrito (com o gestor da Aeronáutica). Os entrevistados externos foram selecionados pelo vínculo de suas instituições

com o CPEx e pela similaridade dos tratamentos de dados efetuados. Já o gestor interno foi selecionado em função de suas atividades e responsabilidades envolvendo processos de tratamento de dados no âmbito do CPEx.

Todos os entrevistados foram esclarecidos do escopo do presente trabalho e anuíram em fornecer as informações aqui relatadas. Os nomes, fatos e instituições citados nas entrevistas não foram identificados para preservação da privacidade dos entrevistados. No entanto, tal fato não traz nenhum prejuízo à compreensão ou à interpretação do presente trabalho[1]. Tais entrevistas foram transcritas por meio do App "*Transcribe*" e as principais ideias foram destacadas sem trazer prejuízo ao contexto. Assim, esses destaques foram comparados com as informações obtidas anteriormente na revisão bibliográfica e na observação direta, corroborando ou não os dados previamente levantados.

Ao final, consolidando as informações da revisão bibliográfica da legislação, do estudo dos modelos teóricos e da análise das entrevistas, foi produzido um marco teórico de referência com as medidas necessárias e as boas práticas identificadas até então para servir de base para o estabelecimento do futuro roteiro de implementação (Capítulo III).

Dando continuidade ao trabalho, foi feita uma avaliação sobre arranjos de governança e sobre seus papeis no processo de adequação à LGPD, elaborando um outro marco teórico de referência apenas com as medidas de governança (Capítulo IV). Por fim, consolidando todas as informações e dados colhidos, foi feita uma proposta de implementação da LGPD, na forma de um modelo teórico roteirizado, com as medidas identificadas como necessárias para viabilizar a conformidade do tratamento de dados pessoais em uma instituição pública (Capítulo V).

[1] *A transcrição das entrevistas e os roteiros dos questionários semiestruturados estão no Anexo I.*

2. PROCEDIMENTOS PARA A PROTEÇÃO DE DADOS

2.1. Objetivo

O presente tópico tem por objetivo efetuar um estudo sobre a atual legislação que rege a proteção de dados no país de forma a proporcionar uma visão eficaz sobre os aspectos que exigirão a adoção de medidas por parte do CPEx, de uma forma prática e de fácil compreensão, para viabilizar a futura adequação do processo de tratamento para fins de pagamento de pessoal do Comando do Exército.

O desafio é descrever e compreender as novas exigências legais para refletir sobre a adequação dos processos internos de tratamento de dados, objetivando a conformidade legal, permitindo que os titulares[2] tenham ciência do que está sendo tratado e de que forma podem exercer seus direitos, sem prejudicar a execução da missão institucional do Comando do Exército e sem afetar as ações sob sua responsabilidade.

2.2. Contexto

A proteção de dados pessoais no país somente se estruturou em torno de um normativo unitário muito recentemente (Doneda, 2020). Antes da LGPD o Brasil tinha várias normas que abordavam o tratamento de dados, cada uma regendo um aspecto específico - Código de Defesa do Consumidor (Lei 8.078/1990), o Marco Civil da Internet (Lei 12.965/2014), a Lei de Acesso à Informação (Lei 12.527/2011), a Lei do Cadastro Positivo (Lei 12.414/2011). Em um novo cenário, a LGPD passou a ter a finalidade de ser o referencial normativo do sistema de tratamento e proteção de dados pessoais, o qual era até então regulamentado por leis e decretos setoriais ou temáticos (Tasso, 2020).

A LGPD foi alterada posteriormente pela Medida Provisória 869/2018 e pela Lei nº 13.853/2019, dando a ela sua forma atual. Já a Emenda Constitucional 115/2022 veio inserir o direito à proteção de dados de forma explícita no rol de direitos fundamentais da Carta Magna.

A nova lei foi concebida dentro de um contexto mundial ocupado com a legitimação da utilização de dados pessoais de forma a preservar o direito de privacidade, liberdade e de intimidade dos titulares. Esse movimento é encabeçado pela GDPR - *General Data Protection Regulation* (sigla em inglês para Regulamento Geral de Proteção de Dados, legislação europeia que trata deste tema, em vigor desde 25 de maio de 2018) - normativa que alcança o tratamento de dados independentemente de ter sede dentro dos países signatários.

[2] Titular: pessoa natural a quem se referem os dados pessoais que são objetos de tratamento.

Há uma tendência global de aprovação de leis de proteção aos dados pessoais, uma mudança de filosofia inescapável que acompanha a migração da sociedade para o ambiente virtual, visto que a maior parte das informações das pessoas, instituições e governos passaram a circular na forma digital.

No Brasil, existe um órgão responsável por fiscalizar e normatizar o ecossistema de tratamento de dados, a ANPD (Autoridade Nacional de Proteção de Dados). Ela possui um escopo de atuação não só como órgão central de proteção de dados, mas como instituição responsável pela normatização da LGPD, fiscalização e sancionamento, fixando interpretações e diretrizes, além de possuir um papel informativo e educacional para promover a disseminação de práticas, elaborar guias e executar ações educativas.

2.3. Aspectos relevantes da LGPD

A LGPD não pode ser estereotipada como norma voltada exclusivamente para a segurança da informação e para a proteção de dados. Ela tem um viés muito mais profundo, que é proteger os direitos fundamentais de liberdade, intimidade, privacidade e o livre desenvolvimento da personalidade individual.

A informação, os esclarecimentos e a disponibilização de canais para o exercício do direito são essenciais para que o titular possa assumir o protagonismo no tratamento de dados que é proposto pela LGPD. Tal posição só será possível se esse elemento tiver ciência de quais são os seus dados, de onde eles estão armazenados, de quem tem a sua posse, de que formas eles estão sendo tratados, de qual é o enquadramento legal que está amparando o tratamento, com quem eles estão sendo compartilhados e para qual finalidade eles são necessários.

Ciente de todos esses aspectos, o titular terá condições de decidir quais ações ele pode tomar com relação ao tratamento de seus dados. Por outro lado, o controlador, grande responsável por prestar as informações, os esclarecimentos e por disponibilizar os canais para o exercício de direito, deve apresentar ao titular a necessidade do tratamento, a finalidade e os benefícios oriundos desse processo, bem como os impactos do tratamento parcial ou nulo dentro de determinado contexto.

Nesse cenário, é fundamental que as instituições implantem ou aperfeiçoem seus programas de *compliance*, cujo objetivo é garantir o cumprimento das normativas, regulamentos e leis envolvendo as atividades e os processos internos e externos. A *compliance* é fruto também da ação da governança de dados, incluindo a descrição das

metodologias de processamento e de análise das informações, pois dados têm valor de prova, de evidência, na tomada de decisão (Almeida, 2020). Assim, a implementação da LGPD requer mais que uma apreciação legal, mas principalmente um trabalho que envolve diversos agentes e setores, visto que não é simplesmente um processo de TI nem um processo jurídico, mas sim um conjunto de processos práticos.

A Administração Pública se baliza sempre pelo princípio da legalidade, então qualquer tratamento de dados pessoais por ela executado terá como referência alguma norma legal em algum nível. O próprio Art. 23, caput, da LGPD reforça que qualquer tratamento feito pelo Poder Público "deverá ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público". No entanto, tal prerrogativa não exclui o direito de autodeterminação informativa do titular, nem é justificativa para a falta de observância dos princípios e fundamentos previstos na LGPD.

A LGPD apontou a responsabilização do Poder Público no tratamento de dados pessoais em seu Capítulo IV. Dispensou um conjunto de deveres específicos[3] em decorrência do tratamento e definiu normas reguladoras do uso compartilhado de bases de dados entre órgãos da administração pública e entre estes e instituições privadas. Assim, a responsabilidade estatal foi tida conforme os critérios da responsabilidade objetiva para os atos comissivos, como no tratamento e no compartilhamento irregular de dados. Em se tratando de atos omissivos, entende-se pela responsabilidade subjetiva, como na falta de observância das normas de prevenção e de segurança da informação que venham a ser alvo de vazamento (Tasso, 2020).

2.4. Os atores de tratamento estabelecidos na LGPD

A LGPD estabelece em seu Art. 5º as definições dos atores envolvidos em processos de tratamento de dados. Segundo a lei, o titular é "pessoa natural a quem se referem os dados pessoais que são objeto de tratamento"; já o controlador é "pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais"; e o operador é "pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador".

Nesse cenário, a proteção de dados deve definir a quem cabe o controle sobre os dados pessoais (Doneda, 2020). Assim, o controlador deve decidir em realizar o tratamento dos

[3] Mais detalhes serão apresentados à frente no tópico "Diferenças da LGPD para o Setor Público e para o Setor Privado".

dados na sua organização ou então definir a existência da figura do operador, o qual receberá a delegação total ou parcial para executar as atividades de tratamento (Hang; Kaunert, 2020). No entanto, cabe ressaltar que o controlador pode ser solidariamente responsável conforme previsto no inciso II, §1º do artigo 42, caso ocorram danos ao titular dos dados nas operações de tratamento compartilhado de dados, particularmente entre entes públicos e privados (Tasso, 2020).

Cabe ressaltar que o controlador é também o grande responsável pela governança dos processos de tratamento de dados na sua instituição. Reforça-se novamente a importância dessa governança na observância dos princípios e fundamentos previstos na LGPD, com modelos mais justos, responsáveis e sustentáveis, que protejam e defendam princípios éticos e regulatórios, que ampliem a confiança dos indivíduos e da sociedade na utilização de seus dados para responder a situações de legítimo interesse público (Almeida, 2020).

O controlador é o responsável pela definição da finalidade e dos objetivos do tratamento, de acordo com as bases legais definidas na LGPD, bem como pelo tempo de duração do tratamento e pela definição da natureza dos dados pessoais tratados, a depender do contexto e das peculiaridades do órgão. O operador executa suas atribuições dentro do escopo definido pelo controlador, visto que apenas o último possui poder de decisão no tratamento de dados. Um possui autonomia decisória e o outro possui escopo de executor (Brasil, 2022a).

O CPEx, sendo um órgão despersonalizado, mas vinculado ao Comando do Exército, tem também a função de controlador em razão da desconcentração administrativa (Brasil, 2022a):

> 29. Assim, em conclusão: nas operações de tratamento de dados pessoais conduzidas por órgãos públicos despersonalizados a pessoa jurídica de direito público a que os órgãos sejam vinculados é a controladora dos dados pessoais e, portanto, responsável pelo cumprimento da LGPD.
> 30. Contudo, em razão do princípio da desconcentração administrativa, o órgão público despersonalizado desempenhará funções típicas de controlador de dados, de acordo com as obrigações estabelecidas na LGPD.

O CPEx utiliza o banco de dados do EBcorp e o banco de dados do CITEx para processamento das informações de pagamento do SIPPES e SIAPPES, respectivamente. Tais bancos de dados são utilizados também por outros órgãos vinculados ao Comando do Exército, para finalidades distintas e específicas, não comuns, não convergentes e não complementares. Assim, configura-se a controladoria singular, o que afastaria a incidência do art. 42, §1o, II, da LGPD, que prevê a responsabilização solidária por dano patrimonial, moral, individual ou coletivo (Brasil, 2022a, p. 14). No entanto, caso um titular de dados decida

ajuizar uma ação judicial, questionando o tratamento realizado, deverá ingressar contra o controlador geral, que é a União.

Outro elemento envolvido no processo é o encarregado do tratamento de dados pessoais (*Data Protection Officer* – DPO), um agente importante que possui a missão de ser o elemento de comunicação com os titulares, com o controlador e com a ANPD. Deve prestar esclarecimentos, determinar providências e orientações internas que favoreçam a incorporação da proteção de dados à cultura organizacional, não possuindo responsabilidade pessoal em caso de violação da LGPD (Hang; Kaunert, 2020). Ele é fundamental no sistema de governança dos dados da organização, visto que deve impulsionar e coordenar ações e adotar medidas técnicas e organizacionais para buscar a conformidade da entidade. Ademais, é responsável por sensibilizar, orientar os recursos humanos a respeito das práticas a serem tomadas em relação à proteção de dados pessoais (Hang; Kaunert, 2020).

É importante ressaltar que o desempenho dos atores de tratamento no processo de implementação da LGPD vai além da simples definição formal de suas capacidades e de suas responsabilidades. Como previsto no Art. 50 da referida lei, é importante formular ações educativas para os envolvidos nos processos de tratamento, visto que a mudança de cultura e o estabelecimento de padrões de desempenho necessitam de uma base teórica e técnica de conhecimentos prévios sobre o novo cenário de tratamento de dados no país. Assim, a educação e a capacitação de pessoal é uma boa prática recomendada pela LGPD que envolve diretamente os atores de tratamento, o que a torna uma ação importantíssima para um adequado processo de implementação da lei em uma instituição.

2.5. Os direitos dos titulares

A Administração Pública, por ser uma das maiores controladoras de dados pessoais, deve fornecer obrigatoriamente ao titular informações sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução de suas atividades em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos (Art. 23 da LGPD). Deve divulgar também a identidade do encarregado e as formas de contato do titular com ele, de forma pública e, preferencialmente, no site da entidade, já que ele é o canal de comunicação entre o titular, o controlador e a ANPD (Hang; Kaunert, 2020).

Dessa forma, o Comando do Exército, fazendo parte da Administração Pública, com a LGPD passou a ter novas obrigações relativas ao tratamento de dados no processo de pagamento de pessoal. Obrigações essas não só com o titular dos dados, mas também com a

entidade responsável pela normatização e fiscalização do tratamento de dados no país. Assim, pode também ser solicitado pela ANPD a apresentar informações sobre o âmbito, a natureza dos dados e outros detalhes acerca do tratamento realizado (Dias, 2020).

Muitas dessas obrigações estão expressas no Capítulo III da LGPD, que busca garantir os direitos fundamentais de liberdade, intimidade e privacidade do titular e traz uma série de direitos específicos. São eles (Santos, 2020):

a) A confirmação da existência do tratamento e acesso aos dados (Art. 18, inciso I e II);
b) A correção de dados incompletos, inexatos ou desatualizados (Art. 18, inciso III);
c) A possibilidade de anonimização de dados pessoais desnecessários, excessivos ou tratados em desconformidade (Art. 7, inciso IV, Art. 11, inciso II, c, Art. 13, caput, Art. 16, inciso II, Art. 18, inciso IV); por se tratar de uma possibilidade expressa na lei, o exercício ao direito à anonimização não se dá de forma ilimitada;
d) O bloqueio ou eliminação dos dados desnecessários, excessivos ou tratados em desconformidade: bloqueio consiste em medida temporária e eliminação em medida definitiva (Art. 18, inciso IV);
e) A portabilidade de transferir seus dados pessoais de um controlador para outro;
f) A eliminação dos dados tratados com fundamento na base legal do consentimento, a qual só não poderá ocorrer se houver obrigação legal ou regulatória a ser cumprida pelo controlador (Art. 16);
g) A formalização de reclamações contra o controlador na ANPD ou perante o judiciário.

Deve-se oferecer ao titular formas para o exercício de direitos relativos aos seus dados, mas deve também se deve observar a segurança no processo para evitar incidentes. Por exemplo, caso seja disponibilizado um portal para acesso do titular e o contato com o controlador, é importante que sejam criadas ferramentas de autenticação para verificar se quem está acessando é realmente esse titular ou não, para então apresentar os dados tratados, a sua finalidade, o termo de consentimento, etc. Se o exercício do direito for o fornecimento de informações, deve-se ter preocupação para garantir que é o titular quem realmente receberá a resposta. Também precisam ser analisadas as possibilidades e permissões para a atualização de dados em uma determinada base, de forma a evitar a possibilidade de erros e de fraudes quando o titular ou quem estiver se passando por ele procederem com a alteração das informações diretamente no banco de dados.

O controlador deve observar certo prazo para atendimento do exercício de direitos dos titulares. Em situações em que o titular deseja obter a confirmação da existência de algum tratamento envolvendo seus dados, o controlador, ao confirmar essa existência, deve providenciar imediato acesso do titular a suas informações pessoais. Já em situações em que o titular deseja obter informações sobre a origem dos dados, a inexistência de registro, os critérios utilizados e a finalidade, o controlador deve providenciar a resposta em até 15 dias. (Brasil, 2022d). Já o Art. 18 da LGPD aponta obrigações do controlador que devem ser atendidas a qualquer momento a partir da requisição do titular.

Cabe ressaltar que a garantia legal do acesso do titular aos seus dados não significa que ele se dará sem qualquer critério, podendo os agentes de tratamento solicitarem a apresentação de documentos e de outras informações para assegurar a idoneidade do procedimento pelos titulares (Moura, 2020).

Por fim, em situações que ocorram violações à LGPD, a ANPD poderá enviar informes, com medidas cabíveis para fazer cessar a infração cometida pelo Comando do Exército, solicitar a publicação de relatórios de impacto à proteção de dados pessoais, bem como determinar a adoção de padrões e de boas práticas para os tratamentos de dados.

2.6. As hipóteses de tratamento de dados

O Comando do Exército tem dentre suas missões institucionais a de executar de maneira centralizada o pagamento de pessoal a ele vinculado. Nessa esteira, cabe ao Centro de Pagamento do Exército (CPEx), Organização Militar subordinada à Secretaria de Economia e Finanças (SEF), tratar os dados pessoais dos militares e pensionistas para executar o referido processo de pagamento.

Sendo um órgão da Administração Pública Federal, o Comando do Exército efetua tratamento de dados pessoais, formalizando contratos, por meio de credenciamento público, com bancos de pagamento e com Entidades Consignatárias para amparar o envio de recursos e de informações pessoais para tais instituições, bem como para o cumprimento das atribuições legais.

O tratamento de dados pelo CPEx tem a finalidade de disponibilização de contracheques e de comprovantes de rendimentos pagos para fins de imposto de renda; de envio dos recursos financeiros para os bancos de pagamento; de remessa de informações gerenciais para órgãos do Governo como Receita Federal, INSS e Ministérios da Presidência da República; de envio de informações para órgãos de controle; de remessa de dados para

órgãos do Poder Judiciário; e de formalização de contratos de consignação dos militares e pensionistas com Entidades Consignatárias.

Com base na síntese feita nos parágrafos anteriores, é possível buscar, com base na LGPD, o enquadramento do processo de pagamento de pessoal efetuado pelo Comando do Exército na consecução de sua missão institucional, como pode ser visto no Art. 7º:

> Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:
> [...]
> II - para o cumprimento de obrigação legal ou regulatória pelo controlador;
> [...]
> V - quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;

A hipótese do Inciso II dispensa o consentimento do titular do dado, visto que é necessário processar dados pessoais para o cumprimento das obrigações legais e regulatórias específicas do CPEx, que é a de executar, de maneira centralizada, o pagamento de pessoal no Comando do Exército, prevista no Decreto nº 86.979, de 3 de março de 1982.

A hipótese do Inciso V também dispensa o consentimento específico do titular para execução de contrato em que seja parte os militares e pensionistas. O pedido do titular é subentendido pelo ato de formalização do contrato ou termo dele decorrente, abrangido pela autonomia da vontade expressa no momento da sua assinatura, não sendo necessária nova previsão expressa para o tratamento decorrente do negócio jurídico. Como o CPEx processa descontos autorizados em contracheque (consignações), oriundos de contratos particulares firmados entre as Entidades Consignatárias (EC) e os militares/pensionistas, não é necessário, assim, um consentimento específico do titular para processar tais contratos na folha de pagamento.

No mesmo sentido, o Art. 23, caput, da LGPD, aponta que o tratamento de dados pessoais será lícito somente se observar os seguintes propósitos: (i) atendimento da finalidade pública do agente; (ii) persecução do interesse público; e (iii) execução de competência ou atribuições legais do servidor público (Aguilera; Di Biase, 2021).

Dessa forma, outra hipótese de base legal também possível seria o tratamento de dados pela Administração Pública, em cumprimento ao princípio da legalidade, enquadrado na LGPD no Art. 7º:

> Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:
> [...]
> III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e

> regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei.

Cabe ressaltar que, qualquer que seja a base legal utilizada, é necessário observar os princípios da proteção de dados previstos no Art. 6º da LGPD, como o princípio da necessidade, que deve se basear no mínimo necessário para a realização de suas finalidades, sem excessos; o princípio da adequação, que impõe que haja compatibilidade entre o tratamento dos dados e as finalidades desejadas, entre o que é feito com as informações pessoais e o propósito informado ao titular; o princípio da transparência, que permite ao titular obter facilmente informações claras sobre o tratamento de seus dados e os seus respectivos responsáveis; e o princípio do livre acesso, que dá aos titulares a possibilidade de consulta sobre seus próprios dados.

A partir de uma hipótese legal de tratamento, o Poder Público deve seguir determinadas regras previstas no Cap IV da LGPD, dentre elas as previstas no Art. 23, como a informação sobre a legalidade do tratamento em sítio eletrônico e a nomeação de um encarregado:

> Art. 23. O tratamento de dados pessoais pelas pessoas jurídicas de direito público referidas no parágrafo único do art. 1º da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação) , deverá ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público, desde que:
> I - sejam informadas as hipóteses em que, no exercício de suas competências, realizam o tratamento de dados pessoais, fornecendo informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos;
> [...]
> III - seja indicado um encarregado quando realizarem operações de tratamento de dados pessoais, nos termos do art. 39 desta Lei.

No processo de tratamento de dados previsto em leis e regulamentos ou respaldados em contratos, muitas vezes há necessidade de compartilhamento das informações entre órgãos públicos ou entre órgãos públicos e instituições particulares para atingir os propósitos do tratamento. Esse compartilhamento também possui amparo conferido pela LGPD em seu Art. 26, §1º, quando houver previsão legal ou respaldo contratual:

> Art. 26. O uso compartilhado de dados pessoais pelo Poder Público deve atender a finalidades específicas de execução de políticas públicas e atribuição legal pelos órgãos e pelas entidades públicas, respeitados os princípios de proteção de dados pessoais elencados no art. 6º desta Lei.
> § 1º É vedado ao Poder Público transferir a entidades privadas dados pessoais constantes de bases de dados a que tenha acesso, exceto:
> [...]
> IV - quando houver previsão legal ou a transferência for respaldada em contratos, convênios ou instrumentos congêneres.

Saindo do patamar federal da LGPD e adentrando no nível normativo interno do Exército, a Portaria nº 088-EME, de 7 de maio de 2020, aprovou a Diretriz de Orientação para Aplicação da Lei Geral de Proteção de Dados Pessoais no Exército Brasileiro (EB20-D-02.013), e atribuiu ao Estado-Maior do Exército (EME) a função de controlador.

A referida Portaria também delegou responsabilidades a outros órgãos do Comando do Exército na gestão dos dados, bem como destacou a influência da LGPD e a necessidade de observação da referida lei nos processos internos:

> 3. PREMISSAS
> [...]
> e. A gestão da informação é de responsabilidade de todos os órgãos de direção setorial (ODS), do Órgão de Direção Operacional (ODOp) e dos órgãos de assistência direta e imediata (OADI) ao Comandante do Exército. Esses órgãos gerenciam sistemas próprios (sistemas corporativos e/ou sistemas específicos) e são responsáveis pelo ciclo de vida da informação de seu interesse.
> [...]
> h. As unidades do Exército Brasileiro estão diretamente afetadas pela LGPD, pois considera-se que todas realizam tratamento de dados pessoais, nos diversos processos internos que veiculam tais informações.
> [...]
> l. O Comando do Exército passará a observar as disposições da ANPD a partir da entrada em vigor da LGPD.

Assim, o processo de pagamento de pessoal feito pelo CPEx, que utiliza sistemas corporativos específicos para tratar os dados com tal finalidade, necessita se adequar às disposições da LGPD. Tal necessidade de adequação está estabelecida também nos termos da Portaria nº 088-EME:

> 4. OBJETIVOS
> [...]
> d. Analisar, planejar e efetivar alterações nas bases de dados, sistemas, normas e processos, adequando-os às disposições da LGPD.
> [...]
> 5. TRABALHOS DE ADEQUAÇÃO
> a. Reavaliar os processos internos, identificando a necessidade de alterações quanto à adequação das salvaguardas das informações pessoais e demais disposições advindas da LGPD.

Nesse sentido, ao Comando do Exército, particularmente ao CPEx, compete reavaliar todos os processos de tratamento de dados utilizados para efetuar pagamento de pessoal para adequação à LGPD, de forma a analisar os fluxos das informações, sua finalidade, sua adequação, seus riscos, identificar medidas de segurança, técnicas e administrativas para adequação ao novo cenário, além de permitir que os titulares dos dados utilizados no processo de pagamento de pessoal possam ter o protagonismo e o controle de suas informações que estão na posse da instituição.

2.7. O compartilhamento de dados

É importante que o processo de compartilhamento de dados seja formalizado e pautado pela transparência, pela previsibilidade e pela segurança jurídica, para que haja o estabelecimento de uma relação de confiança com os titulares, evitando abusos e desvios de finalidades. O compartilhamento deve ser pautado pela definição formal das obrigações de cada parte no que se refere à divulgação das informações exigidas pela LGPD e às responsabilidades e procedimentos a serem adotados no atendimento de solicitações dos titulares.

Tal compartilhamento de dados deve ser oficializado pelos envolvidos por meio de um ato formal (convênio, contrato, portaria ou similar) ou por meio de uma decisão administrativa de autoridade competente que estabeleça os requisitos definidos como condição para o compartilhamento, além de ser essencial a indicação objetiva e detalhada dos dados pessoais objeto de compartilhamento, dentro do necessário para atender determinada finalidade de tratamento (Brasil, 2022b).

Tais atos formais devem conter também as medidas de segurança, técnicas e administrativas utilizadas para preservar os dados pessoais em incidentes de segurança. Essas medidas serão reavaliadas periodicamente em função da previsão do período de compartilhamento, da necessidade de eliminação após o tratamento ou da possibilidade de conservação dos dados, de possíveis atualizações normativas, dentre outros.

Caso seja necessário um novo compartilhamento, a partir de uma das partes envolvidas, para uma nova instituição pública ou privada, torna-se essencial que o instrumento formal que rege o compartilhamento preveja as condições de tal procedimento dentro das normas aplicáveis. Nele podem ser detalhadas instruções sobre o tratamento e as funções e responsabilidades dos agentes envolvidos.

É imperioso destacar que a informação sobre o compartilhamento deve estar facilmente acessível aos titulares, sendo uma boa prática divulgar na página eletrônica da instituição detalhes sobre tal processo (Brasil, 2022b).

2.8. O Programa de Governança e Privacidade (PGP)

A LGPD, no Art. 50 § 2º, recomenda a implementação de um Programa de Governança em Privacidade (PGP), em que deverão ser especificadas as políticas e práticas para proteger a privacidade do titular, para a adequação dos processos de tratamento de acordo com a lei e para evitar o vazamento das informações.

Por ser um programa (processo que tem continuidade ao longo do tempo), o PGP serve como base permanente para tomada de decisão, para a avaliação de riscos e para melhorias da maturidade institucional. Ele deve ter como objetivo efetuar a proteção dos direitos do cidadão em relação à privacidade da informação, tendo como balizas para o seu desenvolvimento e para sua implementação as normativas legais sobre o tema.

a. Implementação do PGP

A implementação do PGP pode se dar de várias formas, e uma delas é seguir um processo inspirado no ciclo PDCA (*Plan, Do, Check e Act*), dividido em 3 (três) FASES principais (Brasil, 2020a), o qual está representado na figura abaixo:

Figura 1: Modelo de implementação do PGP inspirado no ciclo PDCA
Fonte: Brasil, 2020a.

- **FASE 1 - Iniciação e Planejamento:**

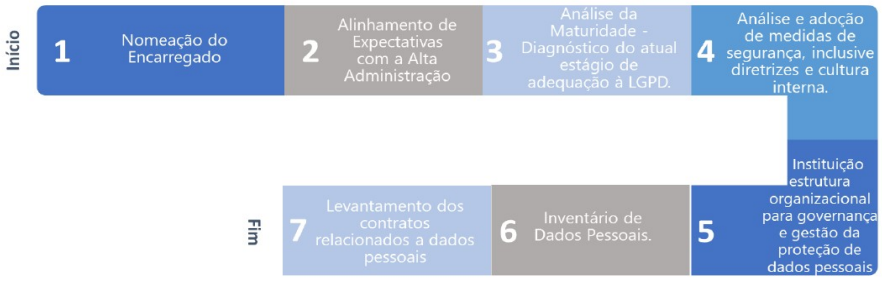

Figura 2: FASE 1 da implementação do PGP
Fonte: Brasil,2020a.

A figura acima aponta a divisão em 7 etapas e cada uma delas contém providências a serem tomadas de acordo com a evolução do processo de implementação do PGP, sendo muitas delas autoexplicativas e outras tendo a necessidade de produção de documentos conforme guias de elaboração expedidos por órgãos competentes.

Por exemplo, na etapa 1 a nomeação do encarregado, elemento com independência e autonomia funcional, deve ser acompanhada da disponibilização de estrutura organizacional

para governança e gestão dos dados pessoais. Ele deverá efetuar a avaliação das atividades de tratamento de dados e encabeçar treinamentos e capacitações voltadas para a segurança da informação e proteção de dados pessoais; deverá também implementar mecanismos para geração de relatórios internos de atividades de processamento de dados pessoais; confeccionará uma minuta de política de privacidade e levantará o orçamento necessário.

A etapa 2 requer o alinhamento dos processos de tratamento com as diretrizes da Alta Administração. Já na etapa 3, deve-se verificar a maturidade da organização conforme ferramenta para a análise da maturidade da Secretaria de Governo Digital – SGD, observando fatores como a rastreabilidade de dados, a comunicação com o cidadão, a transparência, a elaboração da política de privacidade, dos termos de uso e da política de *cookies*.

As medidas de segurança da etapa 4 devem ser analisadas com relação a sua viabilidade pela equipe técnica do órgão antes de sua implementação. Essa etapa também avalia medidas de cultura interna, o que envolve necessariamente a capacitação de pessoal na LGPD, não só dos agentes de tratamento, mas de todos os integrantes de uma instituição, visto que mudanças na cultura interna são viabilizadas por meio de novos comportamentos oriundos da absorção de novos conhecimentos, os quais são transmitidos nas capacitações e treinamentos de recursos humanos. Nesse contexto, podem ser utilizadas as propostas contidas no Guia de Boas Práticas da LGPD feito pela ANPD.

A etapa 5 indica a necessidade da adequação da estrutura organizacional para atender a governança da proteção dos dados, reforçando a proposta contida na etapa 1 desta fase de implementação.

Na etapa 6 é produzido o IDP e na etapa 7 é utilizada a identificação dos processos de tratamento feita no Inventário de Dados Pessoais para viabilizar a realização de uma correlação com os contratos em que estão previstos tratamentos de dados. Assim, torna-se possível efetuar as adequações contratuais necessárias para ajuste com a LGPD.

- **FASE 2 - Construção e Execução**

Figura 3: FASE 2 da implementação do PGP
Fonte: Brasil, 2020a.

Na etapa 1, detalhada na figura acima, as políticas e práticas para proteção da privacidade do cidadão devem definir papéis específicos para os agentes envolvidos no tratamento, bem como devem prever o treinamento e educação desses elementos com relação à proteção da privacidade dos dados e aos direitos dos cidadãos nesse processo. Devem também divulgar informações sobre o tratamento, a finalidade, o ciclo de vida dos dados, tempo de armazenamento, dentre outros.

O desenvolvimento de uma cultura de segurança e proteção de dados e privacidade desde a concepção (*privacy by design*) citado na etapa 2 se inicia pela capacitação de pessoal e disponibilização das informações sobre o PGP de forma clara e acessível aos integrantes do processo de tratamento de dados da instituição. A capacitação e treinamento são fundamentais para a estruturação dessa cultura, juntamente com a adequação dos processos de tratamento, para respeitar os direitos dos titulares dos dados.

Na etapa 3 é produzido o RIPD e na etapa 4 são produzidas a Política de Privacidade e a Política de Segurança da Informação.

Já na etapa 5, de adequação de cláusulas contratuais, é importante que sejam definidos os seguintes termos: delimitações claras e objetivas das responsabilidades do controlador e operador; a forma de coleta e de tratamento de dados; a concessão de direito de acesso dos dados aos titulares; a forma de correção, bloqueio ou eliminação de dados mediante solicitação do titular; a possibilidade de revogação do consentimento dado pelo titular; a identificação de quem tem acesso aos dados, o responsável por seu uso e tratamento, a forma de armazenamento e as particularidades de possíveis auditorias; as medidas de proteção e segurança dos dados.

O último documento a ser produzido nesta fase é o Termo de Uso, o qual deve usar como referência o Guia de elaboração de Termo de Uso e Política de Privacidade para serviços públicos, publicado pela SGD.

- **FASE 3 - Monitoramento**

Figura 4: FASE 3 da implementação do PGP
Fonte: Brasil, 2020a.

A figura acima detalha a fase 3 da implementação da LGPD neste modelo teórico. Já a lista abaixo aponta exemplos de indicadores de performance do PGP para medir e avaliar o resultado da implementação do referido programa:

a) Monitoramento e acompanhamento do número de incidentes de violação de dados pessoais e/ou vazamento de dados pessoais;
b) Resultados do Diagnóstico de Adequação à LGPD - índice de adequação;
c) Índice de serviços com dados pessoais inventariados: número de serviços com dados pessoais inventariados/número de serviços com dados pessoais do órgão x 100;
d) Índice de serviços com termo de uso elaborado: quantidade de serviços com termo de uso elaborado/quantidade de serviços do órgão x 100;
e) Índice de serviços com RIPD elaborado: quantidade de serviços com RIPD elaborado/quantidade de serviços x 100;
f) Índice de conscientização em segurança: quantidade de treinamentos realizados/quantidade de treinamentos previstos x 100;
g) Índice de quantidade de controles de segurança e privacidade implementados para um determinado serviço: quantidade de controles de segurança e privacidade implementados para um determinado serviço/quantidade total de controles de segurança e privacidade identificados para o serviço x 100.

Já na etapa 2, Gestão de Incidentes, são registradas violações de segurança da informação e de privacidade, indicando os sistemas envolvidos, as medidas técnicas utilizadas, as providências para a mitigação dos riscos e evitar novas ocorrências. É importante também a definição de um Plano de Comunicação para divulgar incidentes de forma interna, para evitar reincidências, e de forma externa, para os órgãos responsáveis, para a imprensa e para os titulares.

A análise e o reporte dos resultados observados na etapa 3 são importantes para demonstrar o valor do PGP para a Alta Administração e para avaliar o nível de conformidade em que a instituição pública se encontra.

b. Documentos necessários para a criação do PGP

Observando determinadas etapas nas 3 FASES da implementação citadas anteriormente, é possível identificar que determinados documentos deverão ser produzidos pela instituição pública para a efetiva estruturação interna do PGP (Brasil, 2020a):

1. **Inventário de Dados Pessoais – IDP** (conforme Guia de Elaboração de Inventário de Dados Pessoais da Secretaria Especial de Desburocratização, Gestão e Governo Digital, 2021; e Guia de Avaliação de Riscos de Segurança e Privacidade da Secretaria Especial de Desburocratização, Gestão e Governo Digital, 2020): a produção deste documento é uma forma de efetuar um balanço do que a instituição faz com os dados pessoais, identificando quais dados pessoais são tratados, onde estão e que operações são realizadas com eles.

O IDP auxilia na identificação de quais dados pessoais são tratados, onde eles se localizam e quais as operações de tratamento são efetuadas. Ele descreve informações em relação ao tratamento de dados pessoais realizado pela instituição como (Brasil, 2021a):

a) atores envolvidos (agentes de tratamento e o encarregado);
b) finalidade (o que a instituição faz com o dado pessoal);
c) hipótese (arts. 7o e 11 da LGPD);
d) previsão legal;
e) dados pessoais tratados pela instituição;
f) categoria dos titulares dos dados pessoais;
g) tempo de retenção dos dados pessoais;
h) instituições com as quais os dados pessoais são compartilhados;
i) transferência internacional de dados (art. 33 LGPD); e
j) medidas de segurança atualmente adotadas.

As fases de elaboração do IDP (Brasil, 2021a) estão descritas na figura abaixo:

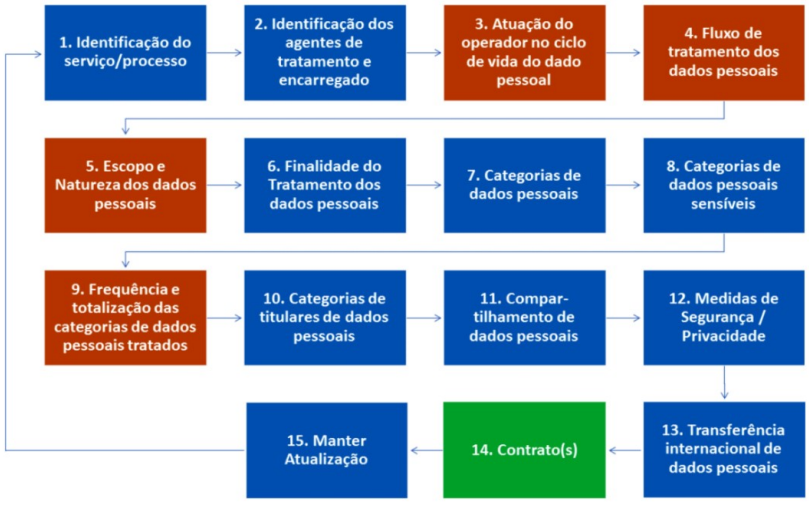

Figura 5: Modelo de implementação do PGP inspirado no ciclo PDCA
Fonte: Brasil, 2020a.

Cabe ressaltar que o tempo de retenção dos dados e o término do tratamento devem marcar um novo momento no ciclo de vida dos dados pessoais. De acordo com cada caso concreto, com as necessidades das instituições públicas e da característica dos dados deve ser avaliado se tais informações serão eliminadas ou se serão armazenadas. Cabe observar que a LGPD determina que os dados sejam eliminados no término do tratamento, com algumas exceções que devem ser avaliadas e harmonizadas com a legislação de arquivos (Lei nº 8.159/1991 e suas regulamentações).

2. **Política de Segurança da Informação** (conforme Instrução Normativa n. 1 de 27 de maio de 2020, do Gabinete de Segurança Institucional da Presidência da República): esse documento tem como objetivo desenvolver e/ou atualizar as diretrizes internas de proteção de dados pessoais, verificando se não há tratamento excessivo de dados, se os controles de segurança são suficientes para os dados tratados, se é necessária à retenção de determinados dados tratados e se é necessário revisar os contratos. Deverá conter pelo menos a definição papéis específicos no processo de tratamento; permitir a educação dos colaboradores; efetuar a divulgação da finalidade do tratamento e da sua base legal na LGPD; determinar os detalhes do ciclo de vida dos dados pessoais (como, onde e por quanto tempo é o armazenamento); definir práticas para proteger a privacidade do cidadão; monitorar a maturidade da organização; e adotar medidas de segurança.

Tal documento deve ser elaborado sob a coordenação do Gestor de Segurança da Informação e divulgado para que todos na instituição pública tomem conhecimento das normas estabelecidas, as quais devem observar a finalidade e o planejamento estratégico da respectiva instituição.

A Política de Segurança da Informação deverá conter, no mínimo, os seguintes itens (Brasil, 2020d):

> I - escopo: descreve o objetivo e a abrangência da Política, definindo o limite dentro do qual as ações de segurança da informação serão desenvolvidas no órgão ou na entidade;
>
> II - conceitos e definições: relaciona e descreve os conceitos e definições a serem utilizados na Política do órgão ou da entidade que possam gerar dificuldade de interpretação ou ambiguidade, devendo ser utilizadas as definições contidas no

> Glossário de Segurança da Informação, aprovado pelo Gabinete de Segurança Institucional da Presidência da República;
> III - princípios: relaciona os princípios que regem a segurança da informação no órgão ou na entidade;
> IV - diretrizes gerais: estabelece diretrizes sobre a implementação, no mínimo, dos seguintes temas:
> a) Tratamento da Informação;
> b) Segurança Física e do Ambiente;
> c) Gestão de Incidentes em Segurança da Informação;
> d) Gestão de Ativos;
> e) Gestão do Uso dos Recursos Operacionais e de Comunicações, como: e-mail, acesso à internet, mídias sociais, computação em nuvem, dentre outros;
> f) Controles de Acesso;
> g) Gestão de Riscos;
> h) Gestão de Continuidade; e
> i) Auditoria e Conformidade.
> V - competências: define as atribuições e as responsabilidades dos envolvidos na estrutura de gestão de segurança da informação;
> VI - penalidades: estabelece as consequências e as penalidades para os casos de violação da Política de Segurança da Informação ou de quebra de segurança, de acordo com as normas já existentes no ordenamento jurídico vigente sobre penalidades ao servidor público federal relativas ao assunto; e
> VII - política de atualização: estabelece a periodicidade máxima para a revisão da Política de Segurança da Informação e dos respectivos instrumentos normativos.

A LGPD dedicou o Capítulo VII de seu texto para apresentar a necessidade de adoção de medidas de segurança, técnicas e administrativas para proteção dos dados pessoais dos titulares. Assim, torna-se essencial buscar identificar melhores práticas sobre privacidade, proteção de dados pessoais e segurança da informação nos normativos atuais.

Para a adequada implementação de medidas de segurança e privacidade, a Alta Administração da instituição pública deve estabelecer uma estrutura básica que contemple papéis importantes em tal processo (Brasil, 2022c):

a) Encarregado pelo Tratamento de Dados Pessoais – conforme a LGPD;

b) Gestor de Segurança da Informação - planejar, implementar e melhorar continuamente os controles de segurança da informação em ativos de informação;
c) Responsável pela unidade de controle interno - assegurar que os controles sejam executados de forma apropriada, por meio do desempenho das funções de apoio, supervisão e monitoramento das atividades desenvolvidas pela primeira linha de defesa;
d) Comitê de Segurança da Informação ou estrutura equivalente - deliberar sobre os assuntos relativos à Política Nacional de Segurança da Informação;
e) Equipe de Tratamento e Resposta a Incidentes Cibernéticos (ETIR) - constituirá a rede de equipes, integrada pelos órgãos e pelas entidades da Administração Pública, coordenada pelo Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo do GSI/PR; e
f) Política de Segurança da Informação - implementada a partir da formalização e aprovação por parte da autoridade máxima da instituição, com o objetivo de estabelecer diretrizes, responsabilidades, competências e subsídios para a gestão da segurança da informação.

Foram estabelecidas 3 categorias de controles para avaliar as medidas a serem adotadas para implementação do PGP: Controles de Estruturação básica de gestão em privacidade e segurança da informação: Controles de CiberSegurança; e Controles de Privacidade (Brasil, 2022c).

3. **Relatório de Impacto à Proteção de Dados Pessoais – RIPD** (conforme Guia de Boas Práticas da LGPD do Comitê Central de Governança de Dados, 2020; e Guia de Avaliação de Riscos de Segurança e Privacidade da Secretaria Especial de Desburocratização, Gestão e Governo Digital, 2020): a produção deste documento não é obrigatória para todas as instituições, no entanto ele é importante para a avaliação dos riscos nas operações de tratamento, do uso e compartilhamento de dados pessoais e das medidas para mitigação dos riscos que possam afetar as liberdades e os direitos dos titulares dos dados. O relatório deverá conter, no mínimo, a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados. Deve identificar os agentes de tratamento

e o encarregado; descrever o tratamento; identificar as partes interessadas; descrever a necessidade e a proporcionalidade do tratamento.

O responsável pela elaboração do relatório será uma pessoa indicada pela instituição que tenha conhecimento técnico para a realização da tarefa, e que será apoiada pelas partes envolvidas nas atividades de tratamento de dados. O encarregado terá a função de apoiar, direcionar e ofertar consultoria durante sua produção, sendo o responsável por aprovar o RIPD ao seu final. Para melhor visualização das etapas de elaboração, elaborou-se a figura a seguir (Brasil 2020e) :

Figura 6: Etapas de implementação do RIPD
Fonte: Brasil, 2020e.

É importante reforçar que a instituição que elabora o RIPD está atenta ao princípio da responsabilização e de prestação de contas, além de promover uma avaliação da conformidade nos processos de tratamento de dados internos, viabilizando a implementação de medidas necessárias para a proteção dos dados e dos direitos dos titulares.

4. **Termo de Uso** (conforme Guia de elaboração de Termo de Uso e Política de Privacidade da Secretaria Especial de Desburocratização, Gestão e Governo Digital, 2022): documento utilizado para fornecer uma descrição detalhada do tratamento, das condições e das regras aplicáveis a ele. É importante que contenha tópicos sobre: aceitação dos termos e da política de privacidade; definições; arcabouço legal; descrição do serviço; direitos do usuário; responsabilidades do usuário e da Administração Pública; mudanças no termo de uso; informações para contato; e foro.

O Termo de Uso informa as regras que o usuário está sujeito ao utilizar o serviço; já a Política de Privacidade deverá ser aplicada sempre que houver tratamento de dados para informar aos usuários os procedimentos e processos adotados no tratamento de dados pessoais realizado pelo serviço, bem como informá-los sobre as medidas de proteção de dados pessoais adotadas. (Brasil, 2022f). A figura abaixo ajuda a visualizar os principais elementos do Termo de Uso:

Figura 7: Elementos do Termo de Uso
Fonte: Brasil,2022f.

As cláusulas do Termo de Uso são definidas pelo controlador de forma unilateral, visto que ele é quem detém condições de avaliar as necessidades para que ocorra o tratamento de dados e de adequar tal processo aos requisitos da LGPD. Assim, o usuário não detém condições concretas de discutir ou modificar substancialmente o conteúdo do Termo de Uso.

5. **A Política de Privacidade** (conforme Guia de elaboração de Termo de Uso e Política de Privacidade da Secretaria Especial de Desburocratização, Gestão e Governo Digital, 2022): documento que compõe o Termo de Uso e que objetiva informar ao titular como é fornecida a privacidade necessária para que a confidencialidade dos dados seja garantida de forma eficiente.

É importante que contenha tópicos sobre: controlador; operador; encarregado; quais dados são tratados; como os dados são coletados; qual o tratamento realizado e para qual finalidade; compartilhamento de dados; segurança dos dados; política de *cookies*; e tratamento posterior dos dados para outras finalidades, conforme explicitado na figura abaixo:

Figura 8: Elementos da Política de Privacidade
Fonte: Brasil, 2022f.

A Política de Privacidade pode se dividir entre interna e externa. A interna apresenta os objetivos, regras, obrigações, restrições e/ou controles para satisfazer os requisitos de privacidade relacionados ao processamento de dados pessoais realizado. A externa apresenta aos elementos externos à instituição informações sobre a identificação e o contato do encarregado; a informação coleta os dados; as operações de tratamento realizadas e o seu tempo (Brasil, 2022f).

Um dos elementos constitutivos da Política de Privacidade são os *cookies*. Eles são arquivos que os sites salvam no dispositivo do usuário enquanto ele navega, coletam informações e tornam o processo mais facilitado, pois guardam dados de *login*, senha, histórico e outras informações que podem ser suficientes para identificar o titular dos dados. Assim, no contexto da LGPD, o uso de *cookies* deve ser informado previamente para que o titular possa ser informado sobre (Brasil, 2022f):

a) Quais cookies são utilizados;
b) Quais dados são coletados;
c) A finalidade do uso de cookies;
d) Informações mais detalhadas sobre os cookies utilizados no serviço.

Uma boa prática é a elaboração de uma Política de *Cookies* e a sua informação ao titular assim que ele acessar o serviço/site, para que ele possa ter conhecimento mais detalhado sobre o uso dos *cookies* e possa optar por desabilitar a coleta de suas informações durante a navegação (Brasil, 2022f).

2.9. Medidas em caso de incidente de segurança

Um incidente de segurança com dados pessoais é qualquer evento relacionado à violação na segurança de informações pessoais: acesso não autorizado, acidental ou ilícito que

resulte em destruição, perda, alteração, vazamento; qualquer forma de tratamento de dados inadequada ou ilícita, os quais possam ocasionar risco para os direitos e liberdades dos titulares. (Brasil, 2021d).

As principais ações a serem tomadas em caso incidente são (Brasil, 2021d):

a) Avaliar internamente o incidente para verificar o impacto do evento; natureza, categoria e quantidade de titulares de dados pessoais afetados; categoria e quantidade de dados afetados, consequências do incidente para os titulares e a entidade, criticidade e probabilidade;
b) Preservar todas as evidências do incidente;
c) Comunicar ao encarregado, ao controlador e à ANPD a existência do incidente;
d) Comunicar à ETIR4 do órgão em caso de incidentes na rede computacional.
e) Comunicar ao CTIR GOV 5 caso a entidade faça parte da administração pública federal, e se necessária, deve ser realizada ação conjunta entre a entidade e o CTIR Gov para a correspondente resolução.
f) Emitir o relatório final com todas as informações coletadas, as ações realizadas para o tratamento do evento para promover a melhoria contínua no atendimento de incidentes e para atualizar o RIPD.

A figura a seguir auxilia na visualização do fluxo das notificações em caso de incidentes de segurança (Brasil, 2021d):

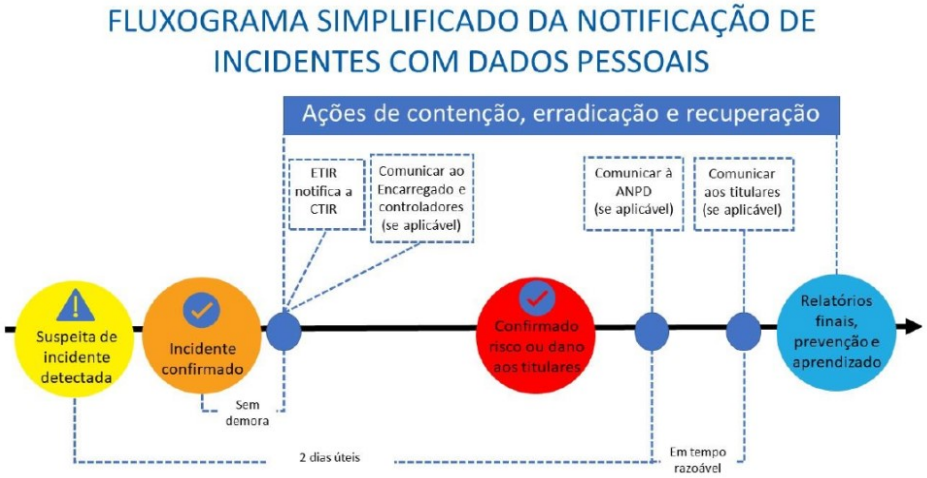

Figura 9: Fluxograma de notificação de incidentes com dados pessoais
Fonte: Brasil,2021d.

[4] *ETIR: equipe de tratamento de incidentes cibernéticos internos de instituições da administração federal.*
[5] *CTIR Gov: o Centro de Tratamento a Resposta a Incidentes Cibernéticos de Governo tem o papel de coordenar e integrar as ações destinadas à gestão de incidentes de TI em órgãos e entidades da administração pública federal. Os incidentes de segurança e de privacidade estão inclusos no escopo de ação do CTIR.*

As diretrizes e o plano de comunicação devem definir quando e como serão realizadas as comunicações de incidentes; a ANPD recomenda que o prazo razoável para a comunicação de incidente seja de 2 (dois) dias úteis.

É uma boa prática que cada instituição tenha uma Política de Gestão de Incidentes com portfólios internos e procedimentos para o tratamento e a resposta a incidentes, procedimentos com ações específicas a serem tomadas por uma determinada equipe para a contenção e mitigação de incidentes e restauração dos serviços, levando em conta aspectos como cultura organizacional, missão, valores e serviços prestados. A Norma Complementar nº 05/IN01/DSIC/GSIPR disciplina a criação de Equipes de Tratamento e Respostas a Incidentes em Redes Computacionais. (Brasil, 2021d).

Cabe ressaltar que todas as medidas de implementação da LGPD devem ser monitoradas e reavaliadas periodicamente, buscando a melhoria constante e a manutenção da conformidade de acordo com a expedição de novas normativas sobre o assunto. Já com relação às medidas de segurança, por ser um tema extremamente técnico, não serão discorridas no presente trabalho as ações a serem tomadas pelas equipes operacionais técnicas para a adequação dos processos de tratamento aos requisitos da lei, visto que as condicionantes para tal adequação dependem de cada processo e da conjuntura de cada órgão/entidade pública.

Mas para avaliar as medidas necessárias, é essencial primeiro conhecer o ambiente e o contexto em que o CPEx está inserido no processo de tratamento de dados pessoais. Avaliar o cenário, características, medidas existentes e lacunas na conformidade são partes fundamentais da análise do objeto, para que posteriormente possam ser identificadas soluções para a adequação da LGPD no processo de pagamento de pessoal. Assim, o próximo Capítulo do presente trabalho se dedicará a apresentar e detalhar o *status* atual do CPEx nesse novo contexto de tratamento de dados no país.

3. TRATAMENTO DE DADOS NO CPEX

3.1. Governança do tratamento de dados no Exército

A Portaria do Comandante do Exército nº 987, de 18 de setembro de 2020, que institui a Política de Governança do Exército Brasileiro (EB10-P-01.007), conceitua governança como o "conjunto de mecanismos de liderança, estratégia e controle postos em prática para avaliar, direcionar e monitorar a gestão, com vistas à condução de políticas públicas e à prestação de serviços de interesse da sociedade", além de definir também as instâncias e as estruturas internas de governança do Exército envolvidas direta ou indiretamente na avaliação, no direcionamento e no monitoramento da Instituição.

A governança das informações no âmbito do Exército é regulada por meio da Portaria nº 856, de 12 de junho de 2019, que aprovou a Política de Informação do Exército. Um dos objetivos estabelecidos na referida Portaria é adequar a normatização interna referente ao tratamento da informação no Exército aos preceitos legais da administração pública federal. O Estado-Maior do Exército (EME) é o responsável pela governança da informação dentro da instituição.

Nesse sentido, a Portaria nº 1.350, de 29 de agosto de 2019, aprovou a Diretriz Estratégica Organizadora do Sistema de Informação do Exército (SINFOEx). Esta Diretriz detalha os objetivos definidos na Política de Informação do Exército na garantia do correto manuseio dos ativos informacionais. Também ficou definido nesta normativa que a gestão da informação é de responsabilidade de todos os órgãos que gerenciam sistemas próprios (Sistemas Corporativos e/ou Sistemas específicos) e são responsáveis pelo ciclo de vida da informação de seu interesse.

A governança da segurança da informação no âmbito do Exército é feita de forma centralizada pela 2ª Subchefia do Estado-Maior do Exército (EME). As outras Organizações Militares do Exército também podem implementar ações complementares voltadas para a segurança da informação, porém sempre seguindo as diretrizes de governança emanadas pelo EME.

Partindo desse cenário geral de governança de dados, a Portaria nº 088-EME, de 7 de maio de 2020, aprovou a Diretriz de Orientação para Aplicação da Lei Geral de Proteção de Dados Pessoais no Exército Brasileiro, para orientar sua aplicação nos processos internos, nos meios de Tecnologia da Informação e Comunicações (TIC) e na revisão de atos normativos internos do Exército Brasileiro, em conformidade com as disposições da Diretriz Estratégica Organizadora do Sistema de Informação do Exército. Nessa Portaria ficou definido que o

controlador dos dados no âmbito da instituição seria o Estado-Maior do Exército (EME), e as demais diretorias, centros e setores internos da Força seriam os operadores.

Nesse cenário, um dos operadores de dados é o Centro de Pagamento do Exército (CPEx), Órgão de Apoio e Execução diretamente subordinado à Secretaria de Economia e Finanças (SEF) e que tem como missão executar de maneira centralizada o pagamento de pessoal no Comando do Exército, tratando, para tal, os dados pessoais de seus vinculados, enquadrando-se como operador de dados de acordo com a Portaria nº 088-EME.

Buscando se adequar à diretriz do Estado-Maior do Exército, órgão controlador dos dados, o CPEx identificou inicialmente os processos, bancos de dados, sistemas, normas internas e serviços que, no exercício de sua missão institucional, tratem de dados pessoais, atentando para os princípios da finalidade, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação, responsabilização e prestação de contas, previstos no Art. 6º e no Art. 23 da LGPD.

Com base nesse levantamento de informações e na identificação inicial dos processos, posteriormente será possível estudar e propor a implementação de novas medidas de tratamento de dados adequadas à Lei de Proteção de Dados Pessoais de forma a manter a conformidade com as diretrizes trazidas pela referida norma legal.

3.2. Processos de tratamento de dados do CPEx

O acesso às informações sobre pagamento de pessoal é o processo com maior número de procura dentro dos canais do Exército, cujos usuários usam os serviços do CPEx em busca de informações sobre seus pagamentos. Para exemplificar, só nos últimos 3 anos a quantidade de acessos ao sítio eletrônico do CPEx foi acima de 4.696.000[6] (quatro milhões, seiscentos e noventa e seis mil acessos), sendo por esse motivo fundamental que os sistemas ofereçam um equilíbrio entre a autodeterminação informativa, a privacidade e a segurança necessárias às novas demandas da LGPD.

Com esse objetivo, o CPEx realiza tratamento de dados em vários processos, todos voltados para a sua missão institucional, isto é, executar pagamento de pessoal previsto em legislação específica, efetuando o tratamento das informações pessoais contidas na EBCORP (base de dados corporativa do Exército composta por diversos sistemas informatizados, incluindo os voltados para pagamento de pessoal), repassando recursos a serem

[6] *Fonte: contador de acessos do site <https://cpex.eb.mil.br/>.*

disponibilizados pelas instituições bancárias aos seus vinculados (militares, civis e pensionistas).

O CPEx realiza, também, o tratamento de dados para o processamento de consignações em contracheque, situação específica em que há a formalização de contratos particulares entre militares/pensionistas e Entidades Consignatárias (EC), permitindo a execução dos contratos consignados.

Tanto nas situações de envio de recursos de pagamento para os bancos quanto no processamento dos contratos consignados há o compartilhamento de dados pessoais dos titulares com instituições públicas e privadas, para o cumprimento de obrigação legal (pagamento de pessoal vinculado) e para a execução contratual (consignações).

Além disso, o CPEx possui processos de tratamento para disponibilizar aos seus vinculados informações relativas ao pagamento de pessoal, como contracheques, ficha financeira e Declaração de Imposto de Renda Retido na Fonte. Há também processos de tratamento e compartilhamento de informações com outros órgãos governamentais como INSS, Ministério da Defesa, Receita Federal e Ministério do Trabalho, contendo dados sobre pagamentos e dados empregatícios, bem como processo de consulta de informações junto a instituições como a DATAPREV.

Nesse cenário, para buscar implementar a LGPD no macroprocesso de pagamento de pessoal, foi feita inicialmente uma observação direta da atividade fim e das atividades meios do CPEx que envolvem tratamento de dados pessoais. A partir desse levantamento inicial, foi possível identificar sumariamente os fluxos de informações existentes em processos de pagamento específicos, processos de compartilhamento de informações, processos de consulta, processos que viabilizam a formalização de contratos particulares e processos de decisões judiciais.

Observou-se que o CPEx faz o tratamento de dados pessoais em 14 processos com finalidades variadas, mas todas ligadas ao macroprocesso pagamento de pessoal do Exército. Os objetivos desses processos vão desde a geração do pagamento mensal de militares e pensionistas até o compartilhamento de informações com instituições públicas e privadas, tendo diversos atores e sistemas informatizados envolvidos, conforme demonstrado no quadro abaixo, que identifica sumariamente os fluxos das informações no macroprocesso pagamento de pessoal:

PROCESSO	BANCO DE DADOS	QUEM ACESSA	FINALIDADE	INFORMAÇÕES CONTIDAS NO BANCO DE DADOS
Pagamento SIAPPES	CITEx[7] / 7º CTA[8]	CITEx / 7º CTA, CDS[9], OM e CPEx	Gerar o pagamento de militares de carreira e pensionistas.	Nome, CPF, identidade, PREC/CP, data nascimento, estado civil, gênero, PIS/PASEP, informações bancárias
Pagamento SIPPES	CITEx / 7º CTA	CITEx / 7º CTA, CDS, DGP[10], OM e CPEx	Gerar o pagamento de militares temporários.	Nome, CPF, identidade, PREC/CP, data nascimento, estado civil, gênero, PIS/PASEP, informações bancárias
Pagamento SER	CITEx / 7º CTA	CITEx / 7º CTA, CDS, OM e CPEx	Gerar o pagamento de militares em missão no exterior.	Nome, CPF, identidade, PREC/CP, data nascimento, estado civil, gênero, PIS/PASEP, informações bancárias
Pagamento SIGEPE	Ministério do Planejamento	Instituições vinculadas ao Ministério do Planejamento, OM e CPEx	Gerar o pagamento de servidores civis	Nome, CPF, identidade, matrícula, carteira de trabalho, data nascimento, e-mail, PIS/PASEP/NIT, informações bancárias, endereço, estado civil, nome da mãe, telefone
Consignações	Sistema EBconsig	OM, EC, militar/pens e CPEx	Permitir a contratação entre a EC e os militares/pensionistas, processando os descontos em contracheque	Nome, cpf, PREC/CP, e-mail, telefone
Acesso ao contracheque	CITEx / 7º CTA	militar/pens e CPEx	Acessar o contracheque, ficha financeira e Comprovante de Rendimentos Pagos (CRP)	Nome completo, CPF, PREC/CP, Posto/Grad, identidade, e-mail
Sistema de atendimento ao usuário	CITEx / 7º CTA	militar/pens e CPEx	Orientar e tirar dúvidas dos usuários	Nome, CPF, PREC/CP, identidade, nome da mãe, e-mail, telefone, cidade, selfie

[7] *Centro Intregrado de Telemática do Exército: gerenciar a infraestrutura física e lógica de tecnologia da informação do Sistema de Informação do Exército e hospedar os sistemas corporativos do Exército.*

[8] 7º Centro Telemática de Área: OM subordinada ao CITEx que hospeda sistemas corporativos.

[9] *Centro de Desenvolvimento de Sistemas: OM responsável por conceber, analisar, desenvolver, integrar, aperfeiçoar, avaliar, manter e sustentar produtos de software e estruturas de dados de sistemas corporativos.*

[10] *Departamento Geral de Pessoal: responsável por todo efetivo de pessoal do Exército.*

BIEG	CITEx / 7º CTA	CPEx e Ministério da Defesa (MD)	Reunir informações gerenciais das folhas de pagamento dos militares das Forças Armadas para apoio à tomada de decisão sobre recursos humanos e remuneração	Nome, PREC/CP, cpf, data de nascimento, local de nascimento, nome da mãe, local de trabalho, número de dependentes, tempo de serviço, data de ingresso, gênero, remuneração
PASEP	CITEx / 7º CTA	Ministério do Trabalho	Custear o seguro-desemprego, o abono de empregados e programas de desenvolvimento econômico por meio do BNDES permitir a geração de abono aos trabalhadores que ganham menos que dois salários mínimos por mês.	Nome, cpf, data de nascimento, gênero, remuneração, grau de instrução
DIRF	CITEx / 7º CTA	RECEITA FEDERAL	Permitir o controle tributário dos rendimentos auferidos por militares e pensionistas e recolhimento de tributos	Nome, cpf, remuneração
CAGED	CITEx / 7º CTA	Ministério do Trabalho	Permitir ao Governo acompanhar e fiscalizar processos de admissão e de demissão de trabalhadores celetistas	Nome, cpf, data de nascimento, gênero, remuneração, grau de instrução
RAIS	CITEx / 7º CTA	Ministério do Trabalho	Prover dados para a elaboração de estatísticas do trabalho e a disponibilização de informações do mercado de trabalho às entidades governamentais	Nome, cpf, data de nascimento, gênero, remuneração, grau de instrução
SIRC	DATAPREV	CPEx	Compartilhar informação de óbitos	Nome, cpf, nome da mãe, local e data do falecimento, número da certidão

Processos judiciais	CITEx / 7º CTA DATAPREV, EBconsig, Ministério do Planejamento	CPEx	Efetuar o cumprimento de demandas judiciais.	Nome, CPF, identidade, PREC/CP, data nascimento, estado civil, gênero, PIS/PASEP, informações bancárias, nome da mãe, local e data do falecimento, número da certidão, remuneração, grau de instrução, local de trabalho, número de dependentes, tempo de serviço, data de ingresso, identidade, nome da mãe, e-mail, telefone, cidade

Quadro 1: Processos de tratamento do CPEx
Fonte: Elaboração própria.

De acordo com as hipóteses de tratamento contidas no Art. 7º da LGPD, a maioria dos processos de tratamento de dados do CPEx possui enquadramento que dispensa a obtenção de um Termo de Consentimento dos militares e pensionistas. Apenas o processo do Sistema de Atendimento ao Usuário foi identificado inicialmente como enquadrado no Art. 7º, Inciso I, demandando o fornecimento de um Termo de Consentimento, visto que este é um canal aberto para a manifestação de qualquer indivíduo, e para isso o CPEx necessita que seus dados pessoais sejam fornecidos para validar se as informações solicitadas podem ser repassadas ou não.

Assim, há possibilidade de enquadramento dos processos de tratamento de dados em mais de uma hipótese prevista no Art. 7º da LGPD. No entanto, com a regulação mais detalhada da lei trazida pela ANPD por meio do Guia Orientativo de Tratamento de Dados Pessoais pelo Poder Público (2022), Item 30, verifica-se que a quase totalidade dos processos do CPEx possuem base legal de tratamento estabelecida no Art. 7º, Inciso II, qual seja, o cumprimento de obrigação legal ou regulatória pelo controlador, visto que decorre de normas de organização (normas que estruturam órgãos e entidades e estabelecem suas competências e atribuições).

Conforme previsto no Guia Orientativo supracitado, no contexto normativo das normas de organização o tratamento de dados pessoais é parte essencial do exercício de prerrogativas estatais típicas, uma vez que necessário para viabilizar a própria execução das atribuições, competências e finalidades públicas da entidade ou do órgão público.

Dessa feita, o Regimento Interno do Centro de Pagamento do Exército, aprovado pela Portaria – SEF/C Ex nº 149, de 16 de agosto de 2021, é uma norma de organização que estabeleceu as competências que amparam o tratamento de dados em cada processo citado anteriormente (Art. 4º, 6º, 7º, 8º, 11, 14, 18 e 19).

Cabe ressaltar que todo integrante das Seções do CPEx passa por uma análise de perfil antes de ser admitido na atividade de pagamento, momento esse em que são verificadas as habilitações do militar e se há algum tipo de restrição junto ao Centro de Inteligência e ao Centro de Controle Interno. Após essa aprovação, o militar assina um Termo de Compromisso de Manutenção de Sigilo, no qual ele se responsabiliza em manter conduta adequada ao nível de atividades críticas que executa, de forma a introduzir esse novo integrante no ambiente de segurança da informação e proteção de dados existente no CPEx.

3.3. Processos de compartilhamento externo de dados do CPEx

O CPEx faz o compartilhamento de dados pessoais em 12 (doze) processos que estão dentro de suas atribuições legais como órgão público, conforme o seguinte quadro:

PROCESSO	BANCO DE DADOS	AGENTE EXTERNO QUE RECEBE OS DADOS	FINALIDADE DO COMPARTILHAMENTO DOS DADOS
Pagamento SIAPPES	CITEx / 7º CTA	Bancos de pagamento	Enviar dados de pagamento para os bancos para permitir que militares de carreira e pensionistas possam receber sua remuneração, proventos e pensão
Pagamento SIPPES	CITEx / 7º CTA	Bancos de pagamento	Enviar dados de pagamento para os bancos para permitir que militares temporários possam receber sua remuneração
Pagamento SRE	CITEx / 7º CTA	Bancos de pagamento	Enviar dados de pagamento para os bancos para permitir que militares no exterior possam receber sua remuneração
Pagamento SIGEPE	Ministério do Planejamento	Bancos de pagamento	Enviar dados de pagamento para os bancos para permitir que servidores civis possam receber sua remuneração

BIEG	CITEx / 7º CTA	Ministério da Defesa (MD)	O Banco de Informações Estratégicas e Gerenciais de Remuneração dos Militares (BIEG) busca reunir informações gerenciais das folhas de pagamento dos militares das Forças Armadas para apoio à tomada de decisão sobre recursos humanos e remuneração
PASEP	CITEx / 7º CTA	Ministério do Trabalho	O Programa de Formação do Patrimônio do Servidor Público (Pasep) busca custear o seguro-desemprego, o abono de empregados e programas de desenvolvimento econômico por meio do BNDES permitir a geração de abono aos trabalhadores que ganham menos de dois salários mínimos por mês. A alimentação desse banco de dados ocorre por meio de arquivo enviado ao Banco do Brasil.
DIRF	CITEx / 7º CTA	RECEITA FEDERAL	A Declaração do Imposto de Renda Retido na Fonte (DIRF) permite o controle tributário dos rendimentos auferidos por militares e pensionistas e recolhimento de tributos
Consignações	Sistema EBconsig	Entidades Consignatárias Credenciadas	Permitir a contratação entre a EC e os militares/pensionistas, processando os descontos em contracheque
CAGED	CITEx / 7º CTA	Ministério do Trabalho	O Cadastro Geral de Empregados e Desempregados (CAGED) busca permitir ao Governo acompanhar e fiscalizar processos de admissão e de demissão de trabalhadores celetistas. O CPEx não alimenta o banco de dados de forma direta, mas por meio da RAIS.
RAIS	CITEx / 7º CTA	Ministério do Trabalho	A Relação Anual de Informações Sociais (RAIS) busca prover dados para a elaboração de estatísticas do trabalho e a disponibilização de informações do mercado de trabalho ao Governo.

SIRC	DATAPREV	DATAPREV	O Sistema Nacional de Informações de Registro Civil (SIRC) efetua o compartilhamento de informação de óbitos. São baixadas as informações dos falecidos e cruzados com o nosso banco de dados. Essas informações também são compartilhadas com a Marinha para cruzamento das informações com o seu banco de dados.
Processos judiciais	CITEx / 7º CTA DATAPREV, EBconsig, Ministério do Planejamento	CPEx	Efetuar o cumprimento de demandas judiciais.

Quadro 2: Processos de compartilhamento externo de dados
Fonte: Elaboração própria.

OCPEx possui uma cultura de proteção de dados intrínseca aos seus integrantes, particularmente quanto ao compartilhamento de informações. Apesar de não existir um código de condutas devidamente normatizado e publicado em forma de regras explícitas, a cultura auxilia no uso ético e seguro das informações, de forma que elas sejam tratadas ou compartilhadas estritamente em atendimento aos requisitos legais, regulatórios e normativos. Por exemplo, uma OM efetuou a solicitação ao CPEx da relação nominal dos militares que estão endividados para evitar que eles ocupem cargos sensíveis. Tal solicitação foi negada em função de que, apesar de haver razoabilidade na demanda, não seria ético expor a situação financeira dos militares, pois estaríamos adentrando na esfera de privacidade deles.

3.4. O arquivamento de dados no Comando do Exército

A informação pessoal pode ser agrupada em subcategorias relativas a aspectos determinados da vida do titular, o que faz com que uma classificação deste gênero pode ser o pressuposto para apontar as normas a serem adotadas (Doneda, 2020). Assim, o Comando do Exército efetua sua atividade de tratamento de dados para fins de pagamento de pessoal com base na legislação federal relativa ao armazenamento e arquivamento de dados. Tal legislação pode ser mais bem especificada pelas seguintes normativas legais:

a) Lei nº 8.159, de 8 de janeiro de 1991. Dispõe sobre a política nacional de arquivos públicos e privados;

b) Decreto nº 4.073, de 3 de janeiro de 2002, que regulamenta a política nacional de arquivos públicos e privados;
c) Decreto nº 4.915, de 12 de dezembro de 2003, que dispõe sobre o Sistema de Gestão de Documentos e Arquivos da Administração Pública Federal;
d) Código de classificação e tabela de temporalidade e destinação de documentos relativos às atividades-meio do Poder Executivo Federal, de 2020, que aprovou o Código de Classificação e Tabela de Temporalidade referentes à Subclasse 080 - Pessoal Militar;
e) Resolução CONARQ nº 40, de 9 de dezembro de 2014, que dispõe sobre os procedimentos para a eliminação de documentos no âmbito dos órgãos e entidades integrantes do Sistema Nacional de Arquivos (SINAR);
f) Instruções CONARQ de Preenchimento da "Listagem de Eliminação de Documentos" pelos Órgãos e Entidades Integrantes do Sistema de Gestão de Documentos de Arquivo (SIGA), de 16 de janeiro de 2015;
g) Portaria Normativa nº 1.235/MD, de 11 de maio de 2012, que estabelece normas para o funcionamento e a tramitação de demandas do Sistema de Informações ao Cidadão no âmbito da administração central do Ministério da Defesa (SIC-MD);
h) Portaria Normativa nº 2.975/MD, de 24 de outubro de 2013, que disciplina no âmbito do Ministério da Defesa, os procedimentos de lavratura do Termo de Classificação de Informação (TCI).

Com base nas normativas supracitadas, o Comando do Exército expediu a Portaria – C Ex n° 1878, de 30 de novembro de 2022, que aprovou a Política de Gestão Documental do Exército Brasileiro, e a Portaria Cmt Ex nº 1.702, de 22 de outubro de 2019, que aprovou as Instruções Gerais para Avaliação de Documentos do Exército, dentre outros cadernos e orientações internas sobre o armazenamento de dados.

Assim, o Comando do Exército lida com o armazenamento de dados em três condições: arquivo corrente, arquivo intermediário e arquivo permanente. Tais divisões são replicações da separação prevista na legislação federal sobre o tema, conforme ilustrado abaixo:

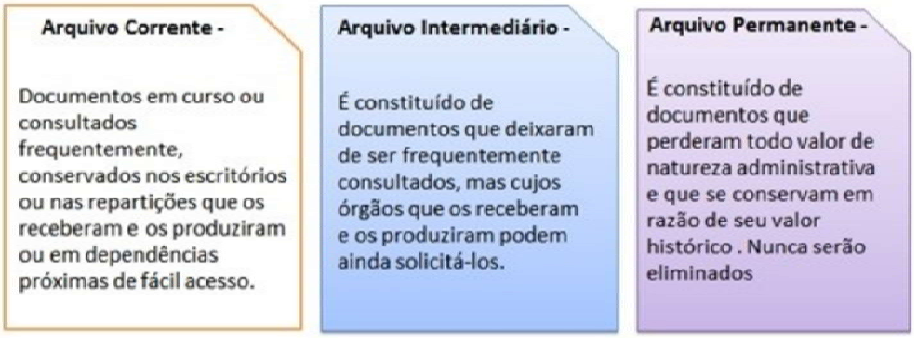

Figura 10: Tipos de arquivos
Fonte: Cartilha Básica sobre Gestão de Arquivos de Organizações Militares, 2019.

No âmbito do Exército o arquivamento obrigatório mínimo é de 5 anos, contados a partir da data de produção do documento, prazo este que varia de acordo com a utilização dos dados (arquivo corrente). Após o prazo de armazenamento no arquivo corrente, o documento é movido para o arquivo intermediário e lá permanecerá de acordo com o prazo determinado pela Tabela de Temporalidade de Documentos. Por fim, o documento é avaliado pela Subcomissão Permanente de Avaliação de Documentos (SCPAD) de cada Organização Militar, que proporá a sua destinação final (arquivo permanente ou eliminação).

O objetivo aqui não é aprofundar sobre as normativas nem sobre o arquivamento em si, mas sim apontar como elas influenciam no armazenamento dos dados pessoais utilizados no processo de pagamento de pessoal tratado pelo Comando do Exército.

Assim, de acordo com o Código de classificação e tabela de temporalidade e destinação de documentos relativos às atividades-meio do Poder Executivo Federal, que aprovou a Tabela de Temporalidade referentes à Subclasse 080 - Pessoal Militar, as informações de pagamento de pessoal devem ser armazenadas em períodos que variam entre 52 até 125 anos ou falecimento do titular dos dados, conforme cada caso específico observado nos extratos dos quadros abaixo:

ASSUNTO	Prazo de guarda		Destinação Final
	Fase corrente	Fase intermediária	
085.61 – REMUNERAÇÃO NA ATIVA	5 anos		Eliminação
fichas financeiras e folhas de pagamento	5 anos	125 anos	Eliminação
085.611 – ADICIONAIS	5 anos		Eliminação
militar de habilitação de tempo de serviço de compensação orgânica de permanência	5 anos	47 anos	Eliminação

085.62 -PROVENTOS NA INATIVIDADE	5 anos		Eliminação
fichas financeiras e folhas de pagamento	5 anos	125 anos	Eliminação
085.621 – ADICIONAIS	5 anos		Eliminação
militar de habilitação de tempo de serviço de compensação orgânica de permanência	5 anos	47 anos	Eliminação
085.63 – DESCONTOS			
085.631 – OBRIGATÓRIOS	5 anos		Eliminação
contribuição para a assistência médico-hospitalar e social (prestada por entidade militar) impostos incidentes sobre a remuneração ou proventos indenização pela assistência médico-hospitalar (prestada por entidade militar) indenização à Fazenda Nacional multa por ocupação irregular de próprio nacional residencial pensão alimentícia ou judicial contribuição para a pensão militar taxa de uso por ocupação de próprio nacional residencial	5 anos	47 anos	Eliminação
085.632 – AUTORIZADOS	5 anos		Eliminação
descontos em favor de entidades consignatárias, de terceiros ou benefício família	5 anos	47 anos	Eliminação
086 – INATIVOS E PENSIONISTAS			
086.1 – INATIVOS			
086.11 – RESERVA			
086.111 – REMUNERADA	5 anos		Eliminação
processo de transferência para a reserva remunerada	5 anos	Até a reforma ou falecimento do militar	*
086.112 – NÃO REMUNERADA	5 anos		Eliminação
processo de transferência para a reserva não remunerada	5 anos	47 anos	Eliminação
086.2 – PENSIONISTAS			
086.21 – PENSÕES			
086.211 – TEMPORÁRIA	5 anos		Eliminação
processos de solicitação /concessão de pensão militar temporária	5 anos	95 anos	Eliminação
086.212 – VITALÍCIA	5 anos		Eliminação
processos de solicitação /concessão de pensão militar vitalícia	5 anos	125 anos	Eliminação

Quadro 3: Tabela de Temporalidade referente à Subclasse 080 - Pessoal Militar

Fonte: Código de classificação e tabela de temporalidade e destinação de documentos relativos às atividades-meio do Poder Executivo Federal, 2020.

O armazenamento demanda custos de manutenção de servidores de banco de dados com grande capacidade e demanda medidas de segurança por parte do controlador para garantir a integridade das informações e, consequentemente, o direito dos titulares. Assim, é importante efetuar o mapeamento de todos os dados armazenados e a avaliação pormenorizada sobre a natureza sensível e sobre a real necessidade de coleta e manutenção desses dados, de forma a verificar se eles são realmente imprescindíveis para atingir o objetivo do tratamento de dados feito pelo CPEx, ou se eles podem ser eliminados. Essa medida, além de proporcionar uma maior adequação do processo de tratamento à LGPD, reduz o ônus e o risco potencial intrínseco no armazenamento de informações.

Dessa forma, é possível observar que o tratamento de dados feito pelo CPEx para fins de pagamento de pessoal necessita também da manutenção das informações dos titulares armazenadas por períodos superiores a meio século. A preservação dos dados deve ocorrer então pelo prazo necessário ao cumprimento da atividade administrativa e legal do CPEx, cujo valor permanente tenha sido previamente definido na Tabela de Temporalidade. Tal fato levanta particularidades na adequação do processo de pagamento de pessoal do Exército com os requisitos da LGPD.

3.5. A Lei de Acesso à Informação e a Política de Dados Abertos do Poder Executivo Federal nos processos de pagamento do CPEx

O CPEx, como integrante da Administração Pública, deve seguir os procedimentos observados na Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação – LAI), sancionada em 18 de novembro de 2011, que regulamentou o direito constitucional de acesso à informação aos cidadãos.

A LAI é estruturada com base no direito público e no princípio da transparência, já que assegura o direito fundamental de acesso à informação aos cidadãos com base nas atividades das instituições públicas, no princípio da publicidade dos atos administrativos nos três poderes. Assim, qualquer pessoa pode requerer informações de cunho público às instituições governamentais. Por outro lado, e de forma complementar, a LGPD é estruturada com base no princípio do acesso livre aos dados pessoais por interesse do titular. Isto é, o próprio titular, em regra, tem o direito de requerer informações e de autorizar o tratamento de seus dados. Assim, a transparência é base tanto da LAI quanto da LGPD, no entanto a transparência na LAI é para conteúdo coletivo e a transparência na LGPD é para conteúdo particular.

Cabe ressaltar que dentro dos dados a serem disponibilizados pelas instituições públicas podem existir dados pessoais de cidadãos e de servidores, os quais não entram no escopo da LAI. Assim, a instituição pública deve avaliar as requisições com base na LAI e tem autonomia de negar acesso a uma informação caso considere que ela não se enquadra no interesse público.

No mesmo sentido da transparência e da publicidade da LAI, a Política de Dados Abertos (PDA) do Poder Executivo Federal, instituída por meio do Decreto no 8.777, de 11 de maio de 2016, definiu regras para disponibilização ativa de dados abertos governamentais no âmbito do Poder Executivo Federal.

Segundo o Manual de Elaboração de Planos de Dados Abertos da Controladoria-Geral da União (CGU, 2020, p. 5), os dados abertos "são dados que podem ser livremente acessados, utilizados, modificados e compartilhados por qualquer pessoa, estando sujeito a, no máximo, exigências que visem preservar sua proveniência e abertura".

Assim, a Política de Dados Abertos tem como principal objetivo promover a publicação de dados contidos em bases de dados de órgãos e entidades da administração pública federal direta, autárquica e fundacional sob a forma de dados abertos; aprimorar a cultura de transparência pública; e franquear aos cidadãos o acesso, de forma aberta, aos dados produzidos ou acumulados pelo Poder Executivo Federal (Decreto nº 8.777/2016).

No âmbito do Exército, a Portaria - EME/C Ex nº 360, de 31 de março de 2021, aprovou o atual Plano de Dados Abertos e busca promover na instituição a abertura de dados produzidos, em formato que permita seu uso e reuso, zelando pelos princípios da publicidade, da transparência, da eficiência e do controle social, como forma de integração com a sociedade brasileira.

Também a Portaria C Ex n° 1878, de 30 de novembro de 2022, considera em sua composição a obrigação de facilitar à sociedade o acesso à informação, conforme previsto na LAI. Assim, toda pessoa física ou jurídica pode requerer as informações desejadas eletronicamente, que deve feito por meio do Sistema Eletrônico do Serviço de Informação ao Cidadão, o e-SIC[11], ou pessoalmente por meio do Serviço de Informações ao Cidadão (SIC) diretamente nas dependências do Comando do Exército[12].

Dentro desse contexto de publicidade e transparência, conforme previsto no art. 7°, § 3°, VI, do Decreto nº 7.724/2012, que regulamenta a Lei nº 12.527, de 18 de novembro de 2011, que dispõe sobre o acesso a informações previsto no inciso XXXIII do caput do art. 5º

[11] *Acesso por meio do endereço <https://landpage.cgu.gov.br/redirectfalabr/index.html>.*
[12] *Todas orientações constam no link <https://www.eb.mil.br/acesso-a-informacao>.*

no inciso II do § 3º do art. 37, e no § 2º do art. 216 da Constituição Federal, toda instituição pública deve divulgar de forma individualizada a remuneração e subsídio recebidos por ocupante de cargo, posto, graduação, função e emprego público, incluindo outras vantagens pessoais. A divulgação dessas informações se baseia no fato de que os valores recebidos pelos agentes públicos são informações de interesse público e que devem ser transparentes, conforme entendimento do Supremo Tribunal Federal no julgamento em 2015 do Recurso Extraordinário com Agravo (ARE 652777).

Desta feita, a Portaria – EME/C Ex nº 360 buscou também de forma ativa atender aos princípios previstos na LAI e na Política de Dados Abertos com relação à divulgação dos dados relativos ao pagamento de pessoal no Exército, visto que essas duas normativas foram utilizadas na elaboração da referida Portaria. Nela o Tema "Pagamento de Pessoal", contido no Anexo C, contém a descrição do catálogo de dados, o prazo de abertura das informações e a responsabilidade sobre as informações dos dados abertos de pagamento de pessoal[13], conforme detalhado na figura a seguir:

TEMA	DESCRIÇÃO	PERÍODO/PRAZO PARA ABERTURA	ÓRGÃOS RESPONSÁVEIS
Racionalização e otimização da gestão dos recursos das Unidades Orçamentárias Cmdo do Exército e Fundo do Exército	1. Controle e acompanhamento dos recursos financeiros do Fundo do Exército aplicados nos bancos no Módulo de Aplicações Financeiras	NOV 21	D Cont/SEF
	2. Sub-repasses para pagamento das despesas liquidadas da Gestão Fundo do Exército no Módulo de Movimentações Financeiras	AGO 22	
	3. Sub-repasses para pagamento das despesas liquidadas da Gestão Tesouro no Módulo Numerário	NOV 22	
Execução orçamentária, financeira e patrimonial	1. Movimentação dos bens, direitos e obrigações	AGO 21	
	2. Mutação do patrimônio	NOV 21	
Execução financeira	Descentralização de numerário por meio de Programações Financeiras (PF)	NOV 21	
Gestão de Custos	Custos das Organizações Militares do Exército com serviço, material e pessoal	MAR 22	
Pagamento de Pessoal	1. Pagamento de Militares de Carreira e Temporários da Ativa (quantitativo físico de pessoal e remuneração/posto/graduação)	NOV 21	CPEx/SEF
	2. Pagamento de Militares Inativos (quantitativo)	MAR 22	
	3. Pagamento de Pensionistas Militares (quantitativo)	NOV 22	

Quadro 4*: Abertura de Dados de Pagamento de Pessoal*
Fonte: Portaria – EME/C Ex nº 360, 2021.

Os dados de pagamento de pessoal dos vinculados ao Comando do Exército também estão disponíveis no Portal da Transparência do Governo Federal[14], de forma detalhada, mas com os dados de documentos do titular pseudoanonimizados, constando apenas o nome completo de forma expressa, como demonstrado na figura abaixo:

[13] *Acesso por meio do endereço <https://www.eb.mil.br/acesso-a-informacao/dados-abertos>.*
[14] *Acesso por meio do endereço <https://portaldatransparencia.gov.br/>.*

Servidor Público Federal ORIGEM DOS DADOS

Nome	CPF	UF
ABADI PEREIRA DA SILVA	***.519.870-**	RIO GRANDE DO SUL

Data da Reforma/Reserva:
05/03/1982

Posto de pagamento:
MAJOR

Regime Jurídico:
ESTATUTO DOS MILITARES

Situação Vínculo:
MILITAR REFORMADO

Jornada de Trabalho:
DSPN. PERMANENTE

Matrícula
007****

FEVEREIRO 2023 | JANEIRO 2023 | DEZEMBRO 2022 | NOVEMBRO 2022 | OUTUBRO 2022 | SETEMBRO 2022

Remuneração

Remuneração básica	Valor (R$)
REMUNERAÇÃO BÁSICA BRUTA:	21.954,24
Deduções obrigatórias (-)	
IRRF (IMPOSTO DE RENDA RETIDO NA FONTE):	- 3.777,27
PSS/RPGS (PREVIDÊNCIA OFICIAL):	0,00
PENSÃO MILITAR:	- 2.305,19
FUNDO DE SAÚDE:	- 658,62
Total da Remuneração Após Deduções:	**15.213,16**

Quadro 5: Dados de Pagamento de Pessoal
Fonte: Portal da Transparência do Governo Federal, 2023.

Apesar de não haver previsão na legislação de como as informações sobre valores e vantagens pecuniárias recebidas pelos agentes públicos devem ser publicados, tais dados devem ser transparentes e abrangentes, da forma completa e detalhada, excetuando os dados de natureza particular e íntima, como documentos pessoais, descontos consignados, endereços, telefones e pensões alimentícias, por exemplo.

Tanto as demandas oriundas da LAI como as informações fornecidas em função da PDA passam por uma criteriosa avaliação por parte dos integrantes responsáveis no CPEx, cuidado esse que já faz parte da cultura da instituição. Cada setor que recebe uma demanda da LAI, por exemplo, avalia se ela é pertinente e se as informações solicitadas podem ser fornecidas, registrando em documento formal as respostas, seja atendendo ou negando os dados, com seu devido amparo legal e motivo. Já o setor responsável pelo fornecimento dos dados da PDA se atém exclusivamente às informações necessárias, sem apresentar outras que não estejam dentro do escopo da normativa.

Pelo exposto, as informações de pagamento de pessoal do Comando do Exército possuem obrigação legal de serem divulgadas de forma ativa, por meio da Política de Dados Abertos e do Portal da Transparência, e de forma passiva nos canais de atendimento à sociedade. No entanto, a divulgação de tais informações deve também atender ao direito de

privacidade dos titulares com relação aos seus dados pessoais, o que levanta uma particularidade no processo de implementação da LGPD no processo de pagamento de pessoal do Comando do Exército.

3.6. Problemas dos processos do CPEx à luz da LGPD

O CPEx possui processos de tratamento de dados pessoais bem estruturados e com resultados que demonstram sua eficácia, visto que nunca houve atraso nos últimos 20 anos no pagamento dos mais de 400 mil militares e pensionistas. Tal fato ressalta que a missão institucional do Centro vem sendo cumprida de forma assertiva com o modelo atual de tratamento de dados.

No entanto, para se estabelecer um sistema de proteção de dados pessoais, com todas as suas implicações, faz-se necessário um determinado grau de elaboração conceitual a fim de abranger de forma adequada a problemática abordada (Doneda, 2020). Assim, com a vigência da LGPD, toda a estrutura de tratamento deve ser reavaliada para atender aos requisitos e princípios trazidos pela nova lei, buscando uma forma adequada de integrá-la às demais normativas legais que já regem o tratamento de dados para fins de pagamento de pessoal no âmbito do Comando do Exército.

Em uma avaliação inicial feita no presente trabalho, verificou-se que o CPEx já possui um direcionamento que facilitará a implementação por completo da LGDP, dado que existem diversos protocolos de segurança no acesso aos dados, segregações de funções, documentação de orientação que estão em conformidade parcial com os requisitos trazidos pela Lei de Proteção de Dados Pessoais.

Inicialmente o Comando do Exército, por meio da Portaria nº 088 - EME, de 7 de maio de 2020, aprovou a Diretriz de Orientação para Aplicação da Lei Geral de Proteção de Dados Pessoais no Exército Brasileiro. Com base nele, foi feito um mapeamento superficial dos dados utilizados no processo de pagamento de pessoal do CPEx, o qual foi consolidado por meio do Relatório sobre a Lei Geral de Proteção de Dados no CPEx/2020.

A Portaria SEF/C Ex nº 149, de 16 de agosto de 2021, aprovou o novo Regimento Interno do Centro de Pagamento do Exército, em que constam responsabilidades sucintas dos operadores de tratamento no âmbito do CPEx.

Em 2022 o CPEx disponibilizou em seu sítio eletrônico[15] informações sobre a LGPD e já em 2023 expediu sua Política de Privacidade dos Dados, elaborada de acordo com o que

[15] *Acesso por meio do endereço* < https://cpex.eb.mil.br/ >.

prescreve a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet), e em cumprimento ao que determina a LGPD, em que apresenta como as informações pessoais são coletadas, utilizadas e protegidas, bem como quais são os direitos individuais dos titulares e como eles poderão ser exercidos.

No entanto, existem medidas a serem tomadas para permitir que todos os requisitos da lei sejam cumpridos no tratamento de dados pessoais feitos pelo CPEx, e com o estudo singular feito no presente trabalho foi possível identificar alguns pontos de atenção no que diz respeito à conformidade dos processos à luz da LGPD:

a) Há necessidade do envolvimento do Alto Comando para iniciar um processo adequado de implementação;
b) Não existe um programa de treinamento e capacitação voltado para a LGPD;
c) Não existe um comitê (GOVERNANÇA) nem uma equipe técnica voltados para os trabalhos de implementação;
d) Não existe um mapeamento completo dos fluxos de dados de pagamento de pessoal;
e) Não existe um Programa de Privacidade implementado;
f) Não existe atribuição formal detalhada de responsabilidades para os operadores de tratamento;
g) Não existem políticas, normas e procedimentos de GOVERNANÇA para o tratamento de dados pessoais:
h) Não existe um inventário de dados;
i) Não existe um mapeamento da segurança da informação do processo de tratamento;
j) Não existe um mapeamento de contratos e de compartilhamentos e transferência de dados;
k) Não existe uma matriz de compliance e de riscos legais voltadas para a proteção de dados;
l) Não existe um Relatório de Impacto à Proteção de Dados Pessoais (RIPD);
m) Não existe um mecanismo ou orientação para o direcionamento da comunicação e das requisições dos titulares para o controlador (Estado-Maior do Exército);
n) Não existe um processo de obtenção do consentimento e de guarda de provas para o tratamento de dependentes menores de idade;
o) Não existe um adequado monitoramento, registro e auditoria das ações de tratamento de dados por meio de um software;

p) Não há uma Política de Segurança da Informação (PSI) voltada para o tratamento de dados no processo de pagamento de pessoal:
q) Não há a informação ativa ao titular sobre o tratamento e o compartilhamento dos dados;
r) Não há um plano de respostas a incidentes de segurança;
s) Não há uma Equipe de Tratamento e Resposta a Incidentes Cibernéticos (ETIR).

Cabe ressaltar que essas inconformidades iniciais levantadas apenas indicam o tópico principal de cada tema/área do tratamento de dados, o qual pode se desdobrar em diversas medidas necessárias, podendo aumentar consideravelmente o rol apontado. Da mesma forma, outras medidas e outras inconformidades poderão ser identificadas por uma equipe multidisciplinar dedicada ao processo de implementação da LGPD.

Assim, a ação dessa equipe, com acesso irrestrito a todos os processos e com conhecimento técnico dos tratamentos efetuados no CPEx, poderá confirmar ou não as inconformidades apontadas, bem como poderá apontar outras que não tenham sido identificadas na observação direta, de forma a inseri-las nos trabalhos de implementação da LGPD no processo de pagamento de pessoal.

De qualquer forma, inconformidades relativas à LGPD no processo de pagamento de pessoal podem gerar impactos em grande escala no Exército, visto que envolve a totalidade do efetivo da instituição, particularmente quanto à reparação e responsabilização dos agentes de tratamento, quanto à imagem da instituição perante os seus militares e pensionistas vinculados, perante os órgãos reguladores e de controle e perante a sociedade como um todo, visto que o Exército é das mais antigas instituições no Brasil, com mais de 375 anos de história.

Assim, é necessário buscar referências para sanar esse cenário de inconformidades, tanto na literatura quanto em outras instituições. Por meio de uma verificação de modelos teóricos e de soluções adotadas por gestores de tratamento de dados em outras instituições, podem ser obtidas informações importantes para auxiliar o processo de implementação da LGPD no CPEx. Dessa feita, os ensinamentos colhidos com essa verificação serão apresentados no Capítulo seguinte do presente trabalho.

4. REFERÊNCIAS PARA A IMPLEMENTAÇÃO DA LGPD

4.1. Apontamentos iniciais

Por se tratar um novo patamar no tratamento de dados, a adequação legal de processos às diretrizes da LGPD trouxe um novo desafio obrigatório a ser enfrentado por todos os agentes de tratamento para a conformidade de suas ações.

Assim, tanto os agentes de tratamento do setor público como do setor privado vêm buscando informações e formas sobre como implementar a LGPD para atingir a conformidade de seus processos, mas existe um hiato de conhecimento entre o que está previsto na lei e a aplicação prática dos seus preceitos nas atividades diárias das instituições, provocando uma leve sensação de desorientação no processo de implementação.

O que fazer e por onde começar a implementar a LGPD? Talvez essa seja a pergunta que muitos gestores enfrentam atualmente. Talvez também ela possa ser respondida pelo presente trabalho, visto que nele se buscam medidas que podem ser replicadas em outras instituições além do Comando do Exército.

Alguns modelos teóricos de implementação da nova lei e a experiência de outras instituições nesse processo podem auxiliar a responder ao questionamento principal do presente trabalho. Cabe ressaltar que não há receita de bolo que seja adequada para todas as instituições. Há sim a busca de referências e de experiências obtidas no processo de implementação da LGPD que possam servir de norteadoras para a avaliação das particularidades e da conjuntura de cada instituição. Afinal, as exigências da adequação passam necessariamente pela reflexão sobre as atividades cotidianas nas quais se tratam os dados pessoais; sobre a necessidade e adequação às finalidades pretendidas; e sobre a transparência e a segurança exigidas.

Cabe ressaltar que a implementação da LGPD não é um processo de TI; a abrangência da lei é muito maior que, simplesmente, processos informáticos. A implementação da LGPD também não é um processo jurídico; os advogados serão muito bem-vindos, com seu conhecimento sobre leis e detalhes técnicos sobre contratos e coisas correlatas, mas a LGPD pressupõe um conjunto de processos práticos em que o setor jurídico será apenas mais um dos envolvidos no processo, e não o responsável principal pela implementação.

É importante que exista uma comissão multidisciplinar, encabeçada pelo Encarregado, que possa reunir todos os setores das instituições que se relacionem com os processos de tratamento de dados para que, conjuntamente, sejam definidas as melhores formas de implementar a LGPD. Assim, poderão ser identificadas, em modelos teóricos sobre a

implementação, diversas boas práticas aplicadas nos processos de tratamento, nas políticas de governança, de conformidade e de gestão de riscos, o que auxiliará na obtenção dos objetivos estratégicos de cada órgão/entidade responsável pelo tratamento de dados.

4.2. Diferenças da LGPD para o Setor Público e para o Setor Privado

Existem peculiaridades que envolvem o tratamento de dados pessoais pelo Poder Público e que decorrem da necessidade de compatibilização entre o exercício das prerrogativas estatais típicas e os princípios, regras e direitos estabelecidos na LGPD (Brasil, 2022b), para que haja segurança jurídica nas operações de tratamento realizadas por instituições públicas. Nesse sentido, a LGPD dedicou o Capítulo IV, Art. 23 a 30, para definir normas específicas direcionadas ao Poder Público.

A LGPD é uma normativa que deve ser seguida obrigatoriamente tanto pelo setor público como pelo setor privado, mas apesar desse aspecto igualitário, tais setores são diferentes em seus princípios e propósitos, o que faz com que a implementação da referida lei seja feita também de forma diferente em cada um deles. Ademais, em função do regramento imposto por outras normativas legais ao setor público ou ao privado, a LGPD acaba tendo reflexos diferentes para cada tipo de instituição, o que reflete também na sua forma de implementação.

Inicialmente, a LGPD cita que outros princípios não expressos em seu texto, mas presentes no ordenamento jurídico pátrio, também devem ser observados (Art. 64). Assim, incluem-se os princípios da Administração Pública, os quais são de observância obrigatória para o setor público, mas não para o privado. Por exemplo, o princípio da publicidade é muito mais amplo e abrangente no âmbito do setor público, que obriga muitas vezes o repasse de informações entre órgãos hierarquicamente subordinados para coordenação de medidas, e na publicidade de dados pessoais dos servidores responsáveis pela assinatura de contratos, exigência oriunda da Lei de Acesso à Informação.

Para o setor privado, o cumprimento dos requisitos da LGPD é uma forma de agregar valor à instituição, sendo também um meio de preservação da imagem e da reputação de uma empresa. Já para uma instituição pública, esse cumprimento é o atendimento a uma obrigação legal, dentre as tantas outras reguladoras do seu setor, para a manutenção da moralidade e da legalidade.

A nomeação do encarregado de dados no setor privado possui certa flexibilização, ao contrário do setor público, visto que a Resolução CD/ANPD nº 2, de 27 de janeiro de 2022,

que aprova o Regulamento de Aplicação da LGPD para Agentes de Tratamento de Pequeno Porte, traz hipótese de dispensa da necessidade dessa nomeação para algumas instituições privadas.

No setor público existem restrições de nomeação do encarregado pela Instrução Normativa SGD/ME Nº 117, de 19 de novembro de 2020, que dispõe sobre a indicação do Encarregado pelo Tratamento dos Dados Pessoais no setor público, apontando que o encarregado nomeado não pode pertencer aos quadros de pessoal de unidades de Tecnologia da Informação nem ser gestor responsável por sistemas de informação.

A própria atribuição de responsabilidades do controlador no setor público é diferente do setor privado. A União é controladora e responsável perante a LGPD, conforme estabelecido na Resolução CD/ANPD nº 2, mas em função da desconcentração administrativa as atribuições de controlador são exercidas pelos órgãos públicos hierarquicamente subordinados, respeitando a distribuição interna de competências.

A gestão de riscos no setor privado pode ser feita por qualquer ferramenta, já no setor público a instituição deve verificar se já existem indicadores objetivos estabelecidos previamente, como alguns disponibilizados por tribunais ou órgãos de controle.

As próprias bases legais ou hipóteses de tratamento utilizadas para enquadrar os processos dos setores são diferentes. O consentimento, por exemplo, é muito mais comum como hipótese de tratamento do setor privado, enquanto o cumprimento de obrigação legal é mais utilizado no setor público.

As sanções previstas LGPD são aplicadas de forma diferente a depender se a instituição pertence ao setor público ou ao privado. Assim, a responsabilização por violação das normas de proteção de dados pessoais é distinta, apesar de ambos os setores se sujeitarem ao poder fiscalizatório da Autoridade Nacional de Proteção de Dados (ANPD). Por exemplo, o setor público não está suscetível a receber sanções previstas nos Incisos II e III do Art. 52 da LGPD, no entanto, existe a possibilidade de aplicação de sanções disciplinares previstas nos estatutos e normativas dos servidores públicos em caso de condutas inapropriadas, fato este que não ocorre no setor privado.

Assim, por possuírem diferenças básicas na sua finalidade, objetivo, estrutura, regulação e responsabilização, os setores público e privado naturalmente são impactados de forma distinta pelos requisitos da LGPD, além do fato da própria lei e das regulamentações expedidas pela ANPD estabelecerem diferenças de aplicação entre eles. Dessa forma, naturalmente a implementação da LGDP também será diferente a depender se uma instituição estiver ligada à iniciativa privada ou ao serviço público, o que ressalta a necessidade de

particularização do processo em cada situação. Por fim, cabe ressaltar que se deve considerar o regime de proteção de dados pessoais de forma diversa entre o Estado e um ente privado no tratamento de dados pessoais que tiver como objetivo a obtenção de um patamar idêntico de proteção para o titular (Doneda, 2020).

4.3. Modelos teóricos de implementação

A implementação da LGPD não deve se restringir apenas aos processos que envolvem tratamento de dados. Ela deve marcar um novo paradigma das instituições, uma mudança de cultura e de enfoque que se dá aos dados pessoais de forma mais abrangente. Assim, a implementação pode atuar em quatro frentes no processo de transformação (Hang, Kaunert, 2020):

a) Pessoas – com a capacitação de pessoal interno e de terceiros;
b) Jurídico – com a adequação e elaboração de contratos, políticas de segurança, de privacidade e de uso, assim como demais documentos que envolvam a privacidade de dados pessoais;
c) Tecnologia – com o uso de ferramentas digitais de segurança e privacidade (arquitetura de software desenhada considerando conceitos como “Privacy by Design” e “Privacy by Default”);
d) Processos – com a revisão e criação de processos ao adequado ciclo dos dados.

O caminho mais adequado para conduzir a implementação da LGPD em uma instituição talvez seja obter, primeiramente, conhecimento sobre a lei e sobre sua normatização, para depois focar em cada uma das quatro frentes supracitadas e adaptar os modelos sugeridos às realidades e peculiaridades de cada órgão/entidade. No entanto, existem alguns modelos teóricos sobre a implementação da LGPD que também podem auxiliar nesse processo de busca da conformidade dos processos de tratamento de dados pessoais, os quais passarão a ser apresentados nos próximos tópicos. Assim, serão descritos alguns modelos que se distinguiram pelos aspectos abordados e que mais se aproximaram do processo de pagamento de pessoal do Comando do Exército.

4.3.1. Modelo 1 de implementação (Pohlmann, 2019)

Neste modelo, voltado para empresas privadas, os setores envolvidos na implementação terão responsabilidades primárias (atividades que o setor deve encabeçar, ou

seja, como o responsável principal da atividade) e secundárias (o setor atuará em apoio a outra área que atuará como responsável).

Compilação das medidas apontadas no modelo 1 de implementação:

- ➔ Preparação inicial
  - ✔ Definição dos setores envolvidos na implementação com suas responsabilidades primárias e secundárias;
  - ✔ Difusão do conhecimento sobre a LGPD para os integrantes da instituição por meio de treinamentos, palestras, cursos e atualizações;
  - ✔ Confecção do Catálogo de Dados inicial;
  - ✔ Definição de como serão obtidos os consentimentos;
  - ✔ Avaliação dos setores de TI de segurança, infraestrutura e sistema sobre as melhores medidas e ações que podem ser tomadas para garantir a proteção dos dados;
  - ✔ Definição do mecanismo que o titular dos dados poderá utilizar para solicitar informações, modificações ou exclusões de seus dados;
  - ✔ Preparação dos especialistas em segurança da informação de um plano de resposta voltado para os requisitos estabelecidos na LGPD;
  - ✔ Preparação do Relatório de Impacto de Dados Pessoais.
- ➔ Conhecer o contexto da instituição e sua estrutura
  - ✔ Conhecimento da estrutura básica da instituição (organograma);
  - ✔ Definição do escopo do projeto;
  - ✔ Definição da equipe que trabalhará no projeto;
  - ✔ Obtenção dos dados prévios;
  - ✔ Conhecimento da cultura da instituição.
- ➔ Organizar um *roadmap*
- ➔ Realizar uma auditoria de *compliance*
- ➔ Efetuar o cálculo do Fator de Risco
- ➔ Catalogar todos os dados de todos os setores
- ➔ Determinar tratamentos e procedimentos
- ➔ Projetar um processo de acompanhamento das atividades realizadas
- ➔ Determinar pontos chave para que a *compliance* possa ser mantida
- ➔ Confeccionar os documentos: Consultoria ou Auditoria de *Compliance* com a LGPD; Declaração de Conformidade; Catálogo de Dados; Relatório de Impacto aos Dados Pessoais; Políticas de Segurança da Informação; Consentimento para acesso à rede de Visitantes; Termos de Uso.

4.3.2. Modelo 2 de implementação (Lamboy; Leite; Lapolla, 2019)

Os itens sugeridos neste modelo, também voltado para a iniciativa privada, buscam estabelecer um programa de *compliance*, chamado pela LGPD de programa de governança em privacidade. Para sua aplicação, é necessário que os responsáveis estruturem o programa de acordo com os recursos disponíveis, o grau de complexidade do negócio e os objetivos a serem atingidos, observando os preceitos estabelecidos na LGPD.

Compilação das medidas apontadas no modelo 2 de implementação:

- ➔ Indicação pela Alta Administração do encarregado, responsável pelo tratamento dos dados na instituição;
- ➔ Indicação de área da instituição responsável pela governança e pelos controles internos do tratamento de dados;
- ➔ Identificação dos setores que devem ser adaptados à LGPD;
- ➔ Identificação das normas correlatas de proteção de dados relacionadas com as atividades da instituição;
- ➔ Estabelecimento de políticas, normas e procedimentos para tratamento dos dados;
- ➔ Avaliação da natureza, do escopo, da finalidade e da gravidade dos riscos e dos benefícios decorrentes do tratamento de dados
- ➔ Mapeamento do ciclo de vida do dado;
- ➔ Mapeamento da segurança da informação do processo de tratamento;
- ➔ Mapeamento de contratos e de modelo de negócios;
- ➔ Mapeamento de compliance, controles internos e de riscos;
- ➔ Confecção da matriz de *compliance* e de riscos legais à proteção de dados;
- ➔ Confecção de Planos de resposta a incidentes e remediação;
- ➔ Confecção do Relatório de informações obrigatórias ou por solicitação da ANPD ou do titular do dado;
- ➔ Confecção do Relatório de Impacto à Proteção de Dados Pessoais (RIPD);
- ➔ Estabelecimento de fluxo de comunicação (interna e externa, RIPD, relatório de informações obrigatórias por solicitação da ANPD ou do titular do dado, planos de resposta a incidentes e remediação, ouvidoria da ANPD);
- ➔ Estabelecimento de Programa de Compliance para Proteção de Dados;
- ➔ Estabelecimento de critérios para ações comerciais e de marketing que não firam os direitos dos titulares dos dados;
- ➔ Estabelecimento de treinamento na instituição;
- ➔ Implementação de ferramenta de armazenamento de dados e de extração de informações;
- ➔ Estabelecimento de regras para compartilhamento e transferência de dados;
- ➔ Estabelecimento de controles internos por meio de 7 testes para a implementação de ações de proteção de dados e para validação da conformidade dos processos de uma instituição;
- ➔ Manutenção da conformidade da relação comercial com clientes e fornecedores;
- ➔ Revisão periódica dos pilares do programa de compliance.

4.3.3. Modelo 3 de implementação (Aguilera-Fernandes, 2020)

Neste modelo, também voltado para o auxílio de empresas privadas no atendimento aos requisitos da LGPD, busca-se a implementação inicial da lei de forma que também possam ser feitas evoluções futuras advindas de novas regulações expedidas pela ANPD e de inovações tecnológicas.

A implementação sustentável dos requisitos da LGPD depende que todas as áreas da instituição sejam envolvidas (negócio, processos, pessoas e tecnologias). Assim, este modelo usa como referência uma determinada metodologia de gestão de projetos, a metodologia BEST (*Business Engaged Security Transformation*), a qual faz uma abordagem holística,

sustentável e adaptável para implementação da LGPD, independentemente do porte das operações ou área de atuação da instituição.

Compilação das medidas apontadas no modelo 3 de implementação:

- ➔ Implementação por meio da metodologia BEST, com foco em pessoas e interações ao invés de processos e ferramentas;
- ➔ Execução das atividades por meio de *Sprints* de 15 dias corridos envolvendo as Equipes de Transformação;
- ➔ Sequência das ações de implementação da LGPD definidas como controles:
  - ✔ Definir o Sistema de Gestão de Cibersegurança e Segurança da Informação (SGCSI)
  - ✔ Definir a Política de Cibersegurança e Segurança da Informação (PCSI)
  - ✔ Definir o calendário de implantação
  - ✔ Acompanhar a implantação do SGCSI
  - ✔ Revisar processos, políticas e normas de acordo com seu calendário
  - ✔ Divulgação de políticas e normas
  - ✔ Determinar classes de valor das informações caracterizando minimamente os dados pessoais e dados pessoais sensíveis
  - ✔ Caracterizar a arquitetura funcional, identificando a descrição dos tratamentos de dados
  - ✔ Caracterizar a arquitetura técnica, identificando o país onde acontecem os tratamentos
  - ✔ Indicar o Encarregado pelo tratamento de Dados Pessoais
  - ✔ Divulgar informações do Encarregado pelo tratamento de dados pessoais
  - ✔ Indicação dos Operadores e do escopo de tratamento de cada um
  - ✔ Indicar os Controladores e o escopo de tratamento de cada um
  - ✔ Manter o inventário de informações armazenadas, processadas, compartilhadas ou transmitidas
  - ✔ Informar tratamentos e compartilhamentos ao Titular
  - ✔ Obter consentimento do Titular ou responsável por menor
  - ✔ Caracterizar captura para finalidades privadas ou específicas
  - ✔ Manter a lista de acesso às informações
  - ✔ Prover mecanismo gratuito e facilitado para revogação do consentimento de acesso
  - ✔ Garantir ao Titular o livre acesso, facilitado e gratuito, sobre finalidade, forma e duração do tratamento
  - ✔ Comunicar mudanças no tratamento de dados
  - ✔ Elaborar Relatório de Impacto à Proteção de Dados Pessoais
  - ✔ Registrar e atender a solicitações da Autoridade Nacional de Proteção de Dados (ANPD) e de organismos de defesa do consumidor
  - ✔ Realizar backup de dados automaticamente
  - ✔ Realizar treinamento em Segurança da Informação
- ➔ Produção de documentação: Políticas de Segurança da Informação (PSI); processos e procedimentos-padrão formalmente definidos; registros de auditoria; relação de riscos de falha de atendimento de requisitos avaliados e tratados; descrição de controles de riscos implantados; documentos de suporte à operação e tomada de decisões; bases de dados de controle das operações de segurança; relatórios de auditorias realizadas com a relação de não conformidades encontradas; relatórios e materiais de divulgação de cibersegurança.

4.3.4. Modelo 4 de implementação (Donda, 2020)

O presente modelo foi idealizado para a iniciativa privada e é bastante direto em sua metodologia. Segundo o autor, apesar de existirem muitos materiais que ajudam no entendimento da LGPD, compreender como ela pode ser aplicada na prática nas atividades da empresa privada torna-se o desafio mais complexo.

Compilação das medidas apontadas no modelo 4 de implementação:

- ➔ Criação de um comitê (governança) para análise e tomadas de decisão;
- ➔ Designação do encarregado/DPO (oficial de proteção de dados);
- ➔ Mapeamento do ciclo de vida dos dados;
- ➔ Confecção de documentação de análise do risco;
- ➔ Monitoramento do tratamento dos dados;
- ➔ Adoção da política de segurança da informação;
- ➔ Monitoramento, registro e auditoria das ações de tratamento por meio de um software de auditoria para facilitar o processo;
- ➔ Produção do Relatório de Impacto à Proteção de Dados;
- ➔ Produção de um plano de ação para situações de emergência.

4.3.5. Modelo 5 de implementação (Kohls, 2021)

O presente modelo, voltado para a iniciativa privada, avalia inicialmente que é preciso conscientizar e capacitar os recursos humanos da instituição para fazer com que haja o entendimento da responsabilidade de gerir dados pessoais, o que é a LGPD e de que forma ela influencia as atividades das organizações e o direito dos cidadãos.

Compilação das medidas apontadas no modelo 5 de implementação:

- ➔ Elaboração de normas de governança para o tratamento de dados pessoais;
- ➔ Definição do encarregado e da equipe do projeto de implementação;
- ➔ Execução do mapeamento de dados;
- ➔ Obtenção do consentimento e de como proceder com a guarda de provas;
- ➔ Confecção de documento para compor a Política de Gestão de Riscos da organização;
- ➔ Formalização de um instrumento de ajuste de conduta (como um contrato) em caso de compartilhamento e transferência de dados;
- ➔ Estabelecimento da Política de Segurança da Informação (PSI);
- ➔ Disponibilização de um canal aberto de comunicação direta com os titulares;
- ➔ Desenvolvimento do Plano de Continuidade de Negócios;
- ➔ Estabelecimento do Relatório de Impacto de Proteção de Dados (RIPD);
- ➔ Promoção de treinamento e da cultura de proteção de dados;
- ➔ Adoção de modelo de gestão da proteção de dados para melhoria contínua;
- ➔ Estabelecimento de sistema de gestão da proteção de dados e da segurança da informação.

4.3.6. Modelo 6 de implementação (Cierco; Mendes; Santana, 2022)

O presente modelo, voltado para a implementação da LGPD em organizações privadas, apresenta o conceito de Privacidade Ágil, que aplica técnicas de desburocratização na criação e manutenção de sistemas de gestão da privacidade, baseado no Manifesto Ágil e em seus valores e princípios. A mentalidade Ágil é uma maneira de pensar e agir que prioriza transparência, inspeção e adaptação. É baseada em ciclos curtos, entregas iterativas e incrementais, resolução rápida de problemas, estímulo aos feedbacks, entrega de valor de negócios aos clientes, com foco nas pessoas, na colaboração e na interação.

Compilação das medidas apontadas no modelo 6 de implementação:

- ➔ Implementação por meio de técnicas, valores e princípios do conceito de Privacidade Ágil;
- ➔ Uso da metodologia *Scrum* para o desenvolvimento do Programa de Privacidade;
- ➔ Definição dos papéis e componentes da equipe *Scrum* (*Product Owner*, *Scrum Master* e Time);
- ➔ Realização do primeiro encontro dos especialistas em privacidade (consultores externos ou internos) e a equipe da organização que será primariamente envolvida no programa (*kick-off*);
- ➔ Oferta de palestras de conscientização ou pequenos treinamentos para o resto da organização para o início de uma ambientação cultural sobre os temas;
- ➔ Realização do Reconhecimento para a produção do *Backlog* do Produto
- ➔ Execução da primeira *Sprint* de implantação para início do ciclo de *Sprint*s, para que as seguintes usem o que foi aprendido e construído nas *Sprint*s anteriores;
- ➔ Execução da análise de gaps para avaliar a maturidade dos setores e dos processos;
- ➔ Definição da gestão de riscos (análise de riscos por maturidade versus importância, análise por gaps de maturidade ou outro de tipo de avaliação de riscos);
- ➔ Produção da documentação mínima necessária para o Sistema de Privacidade:
    - ✔ Visão geral de como a organização lida com dados pessoais, com definição de responsabilidades e com compromisso com a privacidade;
    - ✔ Política para o Encarregado de Dados (finalidade, responsabilidade e funções);
    - ✔ Política de tratamento de dados pessoais (orientações sobre como efetuar o tratamento de dados);
    - ✔ Política para exercício de direitos do titular (pedido de informações, correções de dados, restrição de tratamento, eliminação de dados, portabilidade de dados, revisão de decisão automatizada, recepção de solicitação, identificação do titular, execução da solicitação, resposta ao titular, monitoramento e registro);
    - ✔ Política de gestão de incidentes de privacidade (fluxos de trabalho e ferramentas para agir em incidentes);
    - ✔ Política para dados sensíveis;
    - ✔ Política de consentimento (orientações sobre obtenção, armazenamento e revogação do consentimento);
    - ✔ Política de legítimo interesse;
    - ✔ Política de retenção de dados (padrões e prazos para o armazenamento de dados);

- ✔ Política de dados pessoais e cookies na Internet;
- ✔ Política de Privacyby Design (para novos fluxos e processos de tratamento);
- ✔ Política de avaliação e monitoramento da gestão de privacidade (define responsabilidades, períodos de avaliação, orientações para produção do Relatório de Impacto de Dados – RIPD);
- ✔ Política de treinamento e conscientização;
- ✔ Avisos de privacidade aos titulares, aos colaboradores e a clientes e parceiros.

➔ Implementação da Base de Informações de Operações de Tratamento (BIOT) para manter o registro das operações de tratamento de dados pessoais;

➔ Implementação de ciclos de melhoria do Sistema de Privacidade conduzidos por um profissional experiente.

4.3.7. Modelo 7 de implementação (Xavier, 2022)

O presente modelo foi elaborado para o setor público, particularmente para os Tribunais de Contas, trazendo recomendações e boas práticas para o processo de implementação, a qual ainda está nos estágios iniciais na maioria das organizações públicas, segundo um levantamento feito pelo Tribunal de Contas da União[16].

Compilação das medidas apontadas no modelo 7 de implementação:

➔ Implementação de Medidas Administrativas (política de segurança da informação, conscientização e treinamento, gerenciamento de contratos) e Técnicas (controles de acesso, segurança dos dados pessoais armazenados, segurança das comunicações, programa de gerenciamento de vulnerabilidades) na área de Segurança da Informação.

➔ Avaliação de boas práticas de proteção de dados (monitoramento de contas de usuário privilegiadas, monitoramento do acesso e uso de bancos de dados, implementação de *hardening* de servidores, encriptação de dados pessoais, autenticação multifator, controle de acesso rígido, teste de invasão, não armazenamento de senhas em texto claro em arquivos não criptografados, registro de tentativas de login sem sucesso).

➔ Seis ações mínimas para implementação da LGPD:

1. Criação de um Programa de Governança em Privacidade (PGP)
   - ✔ Designar o encarregado;
   - ✔ Alinhar as expectativas com a Alta Administração;
   - ✔ Analisar a maturidade da instituição;
   - ✔ Analisar as medidas de segurança;
   - ✔ Definir uma estrutura organizacional para governança, gestão e proteção de dados;
   - ✔ Realizar o inventário de dados;
   - ✔ Identificar contratos que envolvam dados pessoais.
   - ✔ Elaborar políticas e práticas para proteção da privacidade;
   - ✔ Implantar cultura de proteção e privacidade desde a concepção;
   - ✔ Elaborar RIPD;
   - ✔ Verificar as medidas e políticas de segurança da informação e criar uma política de privacidade;
   - ✔ Adequar cláusulas contratuais;

[16] *Fonte: <https://irbcontas.org.br/tribunais-de-contas-avancam-na-implementacao-da-lgpd/>.*

- ✔ Elaborar termos de uso.
- ✔ Definir indicadores de performance para o PGP;
- ✔ Implantar processo de gestão de incidentes;
- ✔ Analisar e reportar os resultados

2. Definição do encarregado
3. Inventário de dados
4. Fortalecimento da segurança da informação
   - ✔ I - o estabelecimento de controle estrito sobre o acesso aos dados mediante a definição de responsabilidades das pessoas que terão possibilidade de acesso e de privilégios de acesso exclusivo para determinados usuários;
   - ✔ II - a previsão de mecanismos de autenticação de acesso aos registros, usando, por exemplo, sistemas de autenticação dupla para assegurar a individualização do responsável pelo tratamento dos registros;
   - ✔ III - a criação de inventário detalhado dos acessos aos registros de conexão e de acesso a aplicações, contendo o momento, a duração, a identidade do funcionário ou do responsável pelo acesso designado pela empresa e o arquivo acessado, inclusive para cumprimento do disposto no art. 11, § 3°, da Lei n° 12.965, de 2014; e
   - ✔ IV - o uso de soluções de gestão dos registros por meio de técnicas que garantam a inviolabilidade dos dados, como encriptação ou medidas de proteção equivalentes.
5. Revisão de contratos e convênios.
6. Programa de capacitação continuada.

4.3.8. Quadro comparativo das medidas (marco teórico de referência)

Após a análise dos modelos encontrados e da legislação sobre o tema, buscou-se reunir as principais medidas identificadas de forma que elas pudessem compor o quadro comparativo abaixo. Naturalmente, muitas medidas similares apareceram com redações diferentes em cada modelo, mas que podem ser reunidas se tomarmos como referência sua essência e sua intenção. Para isso, foi necessário redigir as medidas com palavras que pudessem englobar o objetivo principal da medida apresentada por cada modelo.

Cabe ressaltar que medidas muito técnicas, principalmente aquelas voltadas para a área de segurança e tecnologia da informação, não serão objeto de comparação, visto que, justamente por serem extremamente técnicas, devem ser avaliadas por uma equipe especializada e que compreenda o contexto, a estrutura e os recursos de cada instituição.

Assim, o quadro abaixo apresenta uma forma de visualização comparativa das medidas, as quais estão ordenadas em uma sequência inicialmente pensada como adequada para um projeto de implementação, englobando tanto aquelas voltadas para o setor privado quanto as direcionadas para o setor público:

Medidas identificadas na legislação e nos modelos		**Modelo 1**	**Modelo 2**	**Modelo 3**	**Modelo 4**	**Modelo 5**	**Modelo 6**	**Modelo 7**
1	Execução de ações de Governança da Alta	1	2	3	4	5	6	7

	Administração para a implementação							
2	Estabelecimento de estrutura de governança para proteção de dados				4			7
3	Criação de um Comitê de Privacidade e Proteção de Dados Pessoais							7
4	Estabelecimento do controlador, encarregado e operador	1	2	3	4	5	6	7
5	Estabelecimento das bases legais e finalidades para o processo de tratamento	1	2	3	4	5	6	7
6	Divulgação de informações sobre agentes de tratamento, os dados tratados, as finalidades e as mudanças no tratamento aos titulares			3		5		7
7	Formalização de instrumento de ajuste de conduta entre controlador e operador	1		3		5		7
8	Estabelecimento de regras pelo controlador para determinar as condutas dos operadores			3		5		7
9	Mapeamento dos dados de todos os setores	1	2	3	4	5	6	7
10	Mapeamento do ciclo de vida dos dados	1	2		4	5		7
11	Confecção o documento de arquitetura técnica, com a determinação da localização geográfica dos elementos de computação e de armazenamento			3		5	6	
12	Determinação classes de valor das informações			3				7
13	Avaliação da necessidade de armazenamento e retenção dos dados		2	3	4	5		7
14	Normatização das regras e procedimentos sobre os tratamentos	1	2	3	4	5	6	7
15	Estabelecimento de controles de acompanhamento das atividades de tratamento	1		3		5		7
16	Identificação de normas correlatas de processos de tratamento	1						
17	Estabelecimento de ferramenta de registro de acesso, logs, tratamento e extração de informações	1	2	3	4	5	6	7
18	Avaliação dos compartilhamentos de dados	1	2			5	6	7
19	Divulgação dos compartilhamentos aos titulares			3		5	6	
20	Formalização/adequação de contratos/instrumentos de ajuste de conduta entre instituições sobre o compartilhamento de dados		2	3		5	6	7
21	Disponibilização de canais para exercício de direitos do	1	2	3	4	5	6	7

	titular							
22	Monitoramento dos tempos de resposta e de atendimento de solicitação dos titulares				4			
23	Estabelecimento de canal de comunicação com ANPD	1	2	3				7
24	Viabilização da criação de uma cultura organizacional de gestão e governança de dados	1	2	3	4	5	6	7
25	Implementação de um Programa de Governança em Privacidade (PGP)						6	7
26	Implementação de um Programa de *compliance*	1	2	3	4	5		
27	Estabelecimento de pontos de controle para manutenção da *compliance*	1	2					
28	Definição da Base de Informações de Operações de Tratamento (BIOT)						6	
29	Confecção do Inventário de Dados Pessoais (IDP)	1	2	3	4	5	6	7
30	Confecção da Política de Segurança da Informação	1	2	3	4	5	6	7
31	Confecção do Relatório de Impacto à Proteção de Dados Pessoais (RIPD)	1	2	3	4	5	6	7
32	Confecção do Termo de Uso	1				5	6	7
33	Confecção da Política de Privacidade	1	2	3	4	5	6	7
34	Confecção da Política de Cookies		2				6	
35	Divulgação interna do PGP							7
36	Divulgação externa das Políticas de Privacidade, de Cookies e do Termo de Uso			3			6	
37	Implementação de cultura de segurança e proteção de dados e privacidade desde a concepção (*privacyby design*)		2			5	6	7
38	Confecção de relatórios de resultados do PGP para a Alta Administração							7
39	Implementação de indicadores de performance do PGP							7
40	Verificação da maturidade da organização na proteção de dados						6	7
41	Criação de um Plano de Comunicação com os titulares					5	6	
42	Confecção de uma Política de Gestão de Incidentes	1	2	3	4	5	6	7
43	Confecção de uma Política para o encarregado de dados						6	
44	Confecção de uma Política para o exercício de direitos do titular						6	
45	Confecção de uma Política de Tratamento de Dados Pessoais						6	
46	Confecção de uma Política de Dados Sensíveis						6	
47	Confecção de uma Política de consentimento						6	
48	Confecção de uma Política de retenção de dados						6	

49	Confecção de uma Política do legítimo interesse						6	
50	Definição dos setores envolvidos na implementação com suas responsabilidades primárias e secundárias	1	2			5	6	7
51	Confecção do Catálogo de Dados Inicial	1					6	
52	Obtenção do conhecimento da estrutura básica da instituição	1		3				7
53	Obtenção sobre o conhecimento da cultura da instituição	1		3		5	6	7
54	Definição do escopo do projeto	1						
55	Organização de um *roadmap*	1						
56	Realização de auditoria de *compliance*	1						
57	Estabelecimento de processo de gestão de risco complementar ao RIPD	1	2		4	5	6	
58	Implementação de medidas de segurança e proteção de dados	1	2	3	4	5	6	7
59	Divulgação de informações na rede de comunicação interna sobre proteção de dados		2	3		5	6	7
60	Realização de treinamentos e capacitações	1	2	3	4	5	6	7
61	Confecção de relatórios internos de atividades de tratamento					5		
62	Definição de como os consentimentos serão obtidos, armazenados e eliminados	1		3		5	6	
63	Confecção da Declaração de Conformidade	1						
64	Confecção de consentimento para acesso à rede de visitantes	1						
65	Avaliação periódica das políticas, normas e procedimentos		2	3		5		7
66	Estabelecimento de canal de denúncias		2					
67	Declaração da prestação imediata, facilitada e gratuita de informações sobre dados pessoais ao titular ou reguladores		2					
68	Estabelecimento de critérios para ações comerciais e de marketing que não prejudiquem os direitos dos titulares		2					
69	Manutenção da conformidade da relação comercial com clientes e fornecedores		2			5	6	
70	Manutenção da conformidade da relação com empregados e terceirizados		2			5	6	
71	Definição do Sistema de Gestão de Cibersegurança e Segurança da Informação (SGCSI)			3		5		
72	Definição do calendário de implementação			3				

73	Viabilização da eliminação, anonimização ou pseudoanonimização dos dados	1	2	3		5		
74	Desenvolvimento do Plano de Continuidade de Negócios,					5		
75	Adoção de modelo de gestão da proteção de dados para melhoria contínua					5	6	

Quadro 6: Comparação das medidas de implementação
Fonte: Elaboração própria.

Avaliando o quadro acima, pode-se verificar que algumas medidas foram previstas pela totalidade dos modelos, isto é, há uma relevância consensual entre os autores; já outras foram abordadas apenas por um determinado modelo; algumas ainda foram abordadas apenas pelo modelo voltado para o setor público, enquanto outras foram específicas para determinados modelos de implementação no setor privado. Nesse cenário, foi necessário avaliar cada medida para verificar se ela se adequaria a um processo de implementação voltado para o setor público, mesmo que ela tenha sido indicada unicamente por um modelo voltado para o setor privado, ou que tenha sido citada em todos modelos. O objetivo é aproveitar ao máximo todas as informações coletadas para enquadrar ou não as medidas em um novo modelo voltado para o setor público.

Assim, é possível considerar o rol do quadro comparativo acima como um marco teórico de referência das medidas de implementação da LGPD. Cabe ressaltar que certas medidas podem ser interpretadas como o cerne da implementação, independente da instituição que realizará a atividade, e outras que podem ser utilizadas de acordo com cada contexto e situação organizacionais, configurando-se em boas práticas a serem avaliadas por cada instituição. No entanto, é importante observar a obrigação legal estabelecida por determinadas medidas, principalmente aquelas apresentadas no Capítulo 2 do presente trabalho.

Com a compilação das medidas e com a avaliação delas sob a lente da governança, será possível identificar quais as mais adequadas para compor uma proposta de implementação da LGPD no âmbito do CPEx, considerando a estrutura institucional, o contexto de tratamento, as legislações correlatas sobre dados nos processos de pagamento de pessoal e a cultura organizacional, o que será feito ao final do presente trabalho.

4.4. A implementação da LGPD em outras instituições

Os tratamentos de dados pessoais por empresas e instituições públicas em algum momento deverão ser readequados ou reestruturados em função da LGPD. A necessidade de ações para a implementação dos requisitos de proteção de dados proporciona não só a

conformidade legal dos processos de tratamento como também o fortalecimento da credibilidade de cada instituição. No entanto, para atingir esse objetivo, cada organização percorrerá um caminho particular de acordo com sua maturidade com relação à privacidade de dados, seus processos internos de tratamento, sua gestão de riscos, sua cultura organizacional e sua responsabilidade social.

Nesse contexto, o TCU efetuou uma auditoria[17] para elaborar um diagnóstico sobre os controles e medidas implementadas por organizações públicas federais para adequação à LGPD. Nesse trabalho, constatou-se que mais que 75% das instituições se encontram com nível inexpressivo ou inicial no processo de implementação, o que pode ser interpretado como uma situação de alto risco à privacidade dos titulares dos dados. Assim, cabe a cada instituição tomar medidas para implementar a LGPD e atingir um nível viável de *compliance* de adequação à lei, conforme suas particularidades, recursos e setores internos envolvidos.

São diversas as áreas das instituições abrangidas na adequação à LGPD, o que exige uma multidisciplinaridade de conhecimentos que se entrelaçam por meio da governança. Tais setores, de acordo com cada instituição, terão que efetuar ajustes nas políticas internas, na capacitação de pessoal, em ferramentas e sistemas de TI, na área jurídica, nos instrumentos contratuais e nos canais de comunicação com os titulares. Assim, algumas medidas tomadas serão exclusivas de determinadas instituições, e outras poderão servir de *benchmarking* para o processo de implementação em diferentes organizações.

Com o objetivo de obter informações sobre medidas adotadas por outras instituições, dificuldades encontradas, lições aprendidas e sobre o caminho que algumas delas estão trilhando no processo de implementação, foram feitas entrevistas com gestores envolvidos no processo de adequação à LGPD, tanto do setor público como do privado.

Optou-se por separar cada entrevista em uma seção para que fosse possível consolidar melhor as informações mais importantes colhidas de cada entrevistado. Essa forma de consolidar as informações também facilitou a comparação do *status* de implementação entre as instituições entrevistadas, bem como serviu de referência para a adequação a ser feita nos processos do CPEx.

4.4.1. Entrevista com gestora da empresa ZETRASOFT

A entrevista com a ZETRASOFT trouxe a informação de que o processo de implementação da LGPD na empresa foi facilitado em função de sua Certificação ISO 9001 e

[17] *Fonte: <https://portal.tcu.gov.br/imprensa/noticias/tcu-verifica-risco-alto-a-privacidade-de-dados-pessoais-coletados-pelo-governo.htm>.*

da Certificação ISO 27.001, que se referem respectivamente à Gestão da Qualidade e Segurança da Informação, o que contribuiu para a existência de uma cultura prévia de proteção de dados e por diversos processos já estarem congruentes ao exigido pela nova lei (linhas 51-55, 58-60 e 73).

O processo utilizado para obter as certificações foi feito por meio da contratação de uma consultoria para mapeamento, adequação dos processos e produção de políticas e normativas internas. Tudo isso foi aproveitado no processo de implementação da LGPD, aliado a um treinamento constante para os funcionários, o que se refletiu em uma nova cultura na empresa com gestão de riscos, revisão de processos, capacitações e treinamentos periódicos (linhas 207-213, 218-227, 228-232).

Com o advento da LGDP, a empresa proativamente procurou cursos e modelos teóricos sobre o tema, mas na época ambos eram muito escassos. Por isso fizeram cursos que encontraram sobre a GDPR e para formação de DPO, e cursos de interpretação de requisitos da ISO 27.001e da ISO 27.701 (Gestão de Privacidade da Informação), os quais ajudaram na adequação dos processos da empresa. Encontraram materiais em outros idiomas e começaram a seguir pedaços de cada *framework* encontrado, pois, a ANPD nem tinha começado a produzir a regulamentação da lei (linhas 109-118, 160-161, 163-164, 445-450, 452-453, 456-459, 728).

Mapearam os fluxos de dados, verificaram os contratos com os parceiros, fizeram diligências e tomaram diversas ações por mais ou menos um ano e meio para adequar todos os processos envolvendo a empresa. Viram que em alguns deles ela seria a controladora dos dados, particularmente quanto à estrutura e recursos internos, e em outros ela seria operadora, nas atividades envolvendo sua área de negócios. Assim, tomaram medidas para coletar o consentimento nos processos em que era controladora e ajustaram os contratos com os parceiros dos quais era operadora (linhas 462-467, 469-470, 482-485, 500-502, 522-527).

No mesmo sentido, designaram as responsabilidades atinentes à LGPD à equipe e ao comitê de segurança e privacidade da empresa. Por meio dessas equipes, ajustaram ferramentas de TI para registro das informações de tratamento, cuidando para que tais informações fossem preservadas enquanto durarem seus contratos como operadora. Outras ferramentas já foram implementadas para a segregação de acessos aos dados, para impedir vazamentos, para monitoramento e para garantir a proteção e registro dos tratamentos feitos pelos funcionários (linhas 588-590, 607-611, 739-742, 276-278, 372-374).

Produziram seu RIPD, apesar de não ser uma exigência obrigatória, disponibilizaram canal para receber demandas dos titulares relativas aos seus dados, e disponibilizam formas

para que os próprios funcionários registrem incidentes ou fatos que pudessem comprometer a segurança dos dados para que, posteriormente, fossem objetos de avaliação, retificação ou melhoria dos procedimentos (linhas 699-701, 547-556, 814-820, 266-268).

Hoje a empresa entende estar plenamente adequada à LGPD e busca a Certificação da ISO 27.701 para ter a validação de um organismo externo que ateste que ela cumpre os requisitos da lei, já que a ANPD não faz esse tipo de verificação. Com isso, ela faz avaliações periódicas de seus processos que acabam por se transformar em um programa contínuo voltado para a privacidade e proteção dos dados (linhas 728-731, 749-750, 430-431).

4.4.2. Entrevista com gestor do STJ

O STJ começou a se adequar à LGPD por uma determinação *top-down*, conforme algumas demandas sobre o tema foram surgindo e porque foi obtido o diagnóstico de que o tribunal não estava com maturidade suficiente para as novas demandas. Iniciaram então a divulgação de informações sobre a nova lei nos painéis digitais e com alertas sobre a LGPD espalhados pelo órgão, mas viram que não estavam tendo resultado efetivo. Com isso, a escola corporativa do STJ começou a criar e disponibilizar vários cursos sobre a LGPD para capacitação de pessoal em diversas áreas. Assim, criaram pontos focais que auxiliam na disseminação de boas práticas sobre a LGPD e que atuam também na governança de dados (linhas 29-33,49-50, 69-75, 12-126).

O tribunal trabalha com muitos dados pessoais envolvendo os processos judiciais, os quais são solicitados constantemente por partes interessadas e por terceiros, o que reforça a necessidade de avaliação se as informações solicitadas podem ser compartilhadas ou não. As informações pessoais só são compartilhadas se o solicitante tiver um e-mail cadastrado no tribunal para autenticar que ele é o titular dos dados, ou conforme protocolos padrões já estabelecidos. Por isso a orientação geral é para a proteção das informações e, caso haja dúvida, os pontos focais com conhecimento sobre a LGPD sejam consultados antes de compartilhar os dados (linhas 112-115, 119-120, 140-142, 163-165, 178-179).

Há documentos e normativos produzidos pelo tribunal voltados para a LGPD, ajustados para complementar as exigências de outras normas, como a LAI e tabelas de temporalidade de armazenamento das informações. Há uma preocupação em revisar essas normativas, tanto as novas como as antigas, em função das constantes atualizações expedidas sobre a LGPD. Todos esses documentos são produzidos e avaliados pela assessoria de conformidade e integridade digital e pelo comitê de LGPD do STJ, setores focados na

governança de dados e no atendimento aos requisitos da nova lei, com a participação de representantes de vários setores que tratam dados pessoais, sendo uma equipe multidisciplinar. Também fizeram a adequação dos contratos e estabelecimento de responsabilidades por meio dele e por meio de normativas voltadas para os operadores (linhas 222-230, 249-256, 265, 271-275, 281-286, 308-312, 547-554, 606-611).

Para a implementação, o STJ buscou em 2021 o apoio dos elementos que participaram da confecção da LGPD, capacitando a equipe que iria fazer a implementação nos processos de tratamento do tribunal. Importantíssima foi a atuação da TI nos processos, tanto na melhoria quanto na identificação de pontos fracos nas ações de tratamento, visto que há uma maior preocupação interna com fragilidades desde o problema de vazamento de dados ocorrido em 2020-2021 (linhas 340-343, 383-385, 391-394, 465-469, 478-481).

Foi utilizado como modelo teórico um manual sobre a LGPD expedido pelo Ministério da Economia em 2020, uma cartilha do TJ-MG e documentos da ANAC. Começaram a fazer a inventariança dos dados, o que foi um trabalho exaustivo que demorou vários meses e que foi feito por uma equipe multidisciplinar. Como foi analisado todo o fluxo das informações e dos processos, foram identificados problemas nos tratamentos, como a coleta excessiva de dados pessoais. Nesse processo utilizaram um sistema temporário para localizar, identificar e classificar as informações conforme as hipóteses de tratamento previstas na LGPD, com a participação direta de cada setor responsável pelos dados (linhas 394-397, 413-419, 437-441, 497-508, 577-583).

A pessoa entrevistada considera que o tribunal já possui uma boa base no tema LGPD e que está em processo de implementação e de melhoria constante, e que atualmente possui um nível 7 em uma escala de 0 a 10, nota que vai aumentar ao longo do ano. Por receberem dados de diversas frentes, por serem demandados a fornecer informações e a produzi-las, há um aprimoramento interno constante sobre a LGPD. Por fim, ressaltou que a implementação da LGPD auxiliou também na melhoria de outros processos do STJ (linhas 161-162, 184-193, 201-208, 448-450, 457-459).

4.4.3. Entrevista com gestor da MARINHA DO BRASIL

Nessa instituição, um militar da Divisão de Infraestrutura de TI teve a iniciativa de buscar capacitação na LGPD, visto que não houve inicialmente nenhum envolvimento do Alto Comando da Marinha na implementação da nova lei. A difusão do conhecimento e a tentativa de conscientização sobre o tema dentro do setor de pagamento da instituição estão sendo

encabeçadas pelo militar atualmente, mas com o envolvimento do escalão superior a partir do final de 2021, e com a preparação de documentação voltada para a proteção de dados pessoais (linhas 51-58, 70-74, 108-111, 149-153, 172).

A instituição possui uma preocupação com a proteção dos dados pessoais, e já existe uma cultura interna voltada para isso, mas de forma genérica. Estão sendo feitos alguns cursos, produzidos pelo próprio militar, focados nos requisitos da LGPD, bem como a definição de responsabilidades no processo de tratamento de dados pessoais na área de pagamento. Assim, o processo de implementação gera muitas dúvidas ainda sobre os papeis, os responsáveis, os procedimentos a serem tomados (linhas 84-87, 123-125, 143, 172-177, 194-201).

Ainda não existe um DPO nomeado nem um setor responsável pela LGPD na Marinha, apenas a Assessoria de Gestão está à frente das ações de implementação no momento, que está ainda em fase inicial, dado que as diretrizes do escalão superior são muito recentes (linhas 208-210, 217, 230-233).

O processo de tratamento envolve diversos setores internos na Marinha, e nele há também a necessidade de observância de outras normas legais no processo de tratamento, como a LAI e normativas internas sobre arquivamento e manutenção dos dados pessoais de pagamento para fins de histórico. Sobre o compartilhamento de dados, ele existe com uma empresa que gerencia as consignações e com outros órgãos governamentais, como Receita Federal, TCU, Ministério da Defesa. No entanto, apenas com a ZETRASOFT há um instrumento de ajuste de conduta sobre o compartilhamento das informações (linhas 242-258, 294-296, 299, 332-333).

O processo de tratamento possui infraestrutura de TI voltada para a proteção de dados e registro das informações de tratamento, mas não possui um canal para o exercício dos direitos do titular sobre seus dados (linhas 346-352, 388-391, 408-410).

Os trabalhos de implementação estão ainda no início, mas que já existe uma idealização do caminho a ser percorrido. Para isso, sugeriu-se o envolvimento e coordenação do Ministério da Defesa, para ajustar as condutas no âmbito das três Forças, bem como uma maior interação entre elas para auxiliar nos trabalhos de implementação da LGPD (linhas 442-445).

4.4.4. Entrevista com gestor do SIAPPES

O entrevistado informou que existe uma cultura de proteção aos dados na instituição, mas que não existem programas informativos nem de capacitação voltados para a LGPD em

si (linhas 43-54), e que a preocupação em buscar informações depende da ação individual de cada militar interessado (linhas 60 e 61). Da mesma forma, informou que não existe no CPEx normativas sobre proteção e política de privacidade (linha 73), nem um setor específico que trata desse assunto (linhas 76-78), mas apenas em um nível mais alto, âmbito Exército, como no CCIEx, CITEx e CTA (linhas 89 e 90). Desconhece também qualquer definição formal das responsabilidades dos agentes de tratamento no CPEx (linha 135).

Informou que existem subsistemas que armazenam os dados pessoais de pagamento de militares e pensionistas (linhas 96-101) e que a coleta desses dados é feita por meio do sistema FAP Digital, por onde as diversas OM espalhadas pelo país coletam e enviam as informações de pagamento para processamento centralizado no CPEx (linhas 111-131). Apresentou ainda a informação de que tais dados também são compartilhados externamente com outros órgãos governamentais, para fins de cumprimento legal, e com instituições financeiras para viabilizar as atividades de pagamento em si (linhas 138-143).

Citou que existe todo o registro e controle das operações de tratamento de dados no processo de pagamento de pessoal (linhas 162-179) e que tais informações são armazenadas por 130 anos em função de obediência a uma resolução do CONARQ (linhas 230-232).

O chefe do SIAPPES disse não saber responder sobre a existência de um plano de gestão de risco envolvendo o processo de pagamento e desconhece um plano de resposta a incidentes de segurança relativos ao tratamento de dados feitos no CPEx (linhas 182, 183 e 192). Por fim, citou que seria importante a execução de treinamentos com todo pessoal do CPEx e a elaboração de plano de resposta a incidentes (linhas 214-216).

4.4.5. Entrevista com gestor da FORÇA AÉREA DO BRASIL

O assessor do encarregado de dados da FAB informou que a instituição está desenvolvendo uma cultura de proteção de dados (linha 24), mas que já há um plano formal aprovado para adoção de um programa de educação voltado para a LGPD na instituição (linha 28). Ademais, a instituição citou o referencial teórico que está sendo utilizado no processo de implementação (linhas 126-137) e que a grande dificuldade nesse processo é a resistência a mudanças internas (linha 56).

A instituição possui normativas voltadas para a proteção de dados (linha 31), há definição formal sobre responsabilidades dos agentes de tratamento (linha 75), há compartilhamento de dados com outras instituições, formalizado por meio de instrumentos de

ajuste de conduta (linha 78, 83 e 86), e que há um setor específico que trate desse assunto na FAB (linha 34 e 35).

O DPO nomeado é o responsável pela implementação da LGPD (linha 43) e que estão com 50% do processo executado (linha 46). Para isso, foi contratada uma consultoria que resultou em um plano de ação com controles para o processo de adequação (linhas 50-53, 90 e 91). Com isso, estão desenvolvendo um RIPD (linha 94), um canal para o exercício de direitos pelo titular (linhas 108 e 109) e um sistema de registro das operações de tratamento para armazenamento e extração de informações (linha 98). Já possuem um plano de gestão de riscos (linha 101) e um plano de resposta a incidentes (linha 104).

Por fim, citou que há um plano aprovado para permitir a anonimização e eliminação dos dados (linha 112), mas que tal medida deve também seguir as tabelas de temporalidade previstas na legislação arquivística vigente (linhas 119-122). Ressaltou ainda que o processo de implementação deve envolver a Alta Administração, pois a chance de insucesso se for um processo *bottom-up* é muito grande (linhas 50-53).

4.4.6. Considerações a respeito das entrevistas

Observou-se nas entrevistas que algumas instituições estão no estado da arte perante os requisitos da LGPD, como a empresa ZETRA, e outras estão ainda no estágio inicial da implementação, como a Marinha. No entanto, encontraram dificuldades no processo de implementação, seja pela quantidade de adequações exigidas pela lei para serem feitas, seja por não encontrarem um modelo ou roteiro particularizado para implementação em seus processos internos de tratamento de dados pessoais.

As certificações ISO obtidas pela ZETRA proporcionaram uma base quase que completa para os requisitos da LGPD, necessitando apenas de ajustes pontuais em um ambiente onde a cultura de proteção de dados já fazia parte do escopo da empresa. No entanto, a falta de informações e materiais mais detalhados sobre o tema à época também foram citados como dificuldade pela empresa.

Já o STJ utilizou como modelo teórico principal um manual produzido pelo Ministério da Economia, mas se amparou bastante no conhecimento das pessoas que participaram do processo de redação da LGPD e que proporcionaram o treinamento dos elementos que implementaram a referida lei no tribunal.

A capacitação de pessoal foi um ponto unânime entre os entrevistados. Os cursos sobre a LGPD são fundamentais para criar um ambiente e uma cultura voltados para a proteção de

dados pessoais. Sem eles, não há base para uma implementação efetiva dos requisitos da lei. A escola corporativa do STJ pode ser citada como uma importante agente nesse processo, desenvolvendo materiais e cursos particularizados para a própria instituição.

O estabelecimento de pontos focais com conhecimento na LGPD no STJ também foi outra ação que se mostrou interessante para a difusão dos conhecimentos e auxílio diretos nos problemas e dúvidas envolvendo o tratamento e compartilhamento de dados.

A documentação normativa interna também foi outro ponto citado entre os entrevistados que como fundamental para a conformidade das medidas de implementação, ajustando os processos internos de forma particularizada aos requisitos da LGPD, determinando responsabilidade e norteando as ações. No sentido de ajuste particularizado dos processos internos, a FAB citou que a eliminação dos dados segue também a legislação arquivística vigente, o que ressalta a necessidade de compatibilização das normas que regulem os tratamentos de dados.

Um ponto fundamental da LGPD, que pode ser considerado como o objetivo principal dela, é proporcionar ao titular dos dados o controle de seus dados, dando a ele o direito de gerenciamento de suas informações pessoais junto às instituições. Com isso, um canal específico para o titular exercer seus direitos torna-se uma medida essencial e importantíssima no processo de implementação. No entanto, nas entrevistas pode ser verificado que algumas instituições sequer criaram um canal inicial para permitir ao titular tomar qualquer ação ou solicitar qualquer tipo de informação.

A formação de equipes multidisciplinares, com elementos de diversos setores, também foi um dos pontos citados pelos entrevistados como importantes no processo de implementação. As ações da área de Tecnologia da Informação também foi outro tópico levantado nas entrevistas como fundamental para garantir a efetividade das medidas do processo de implementação.

A maturidade da instituição com relação à LGPD só realmente avança a partir do início das ações de implementação, o que faz com que as próprias atividades de tratamento da instituição gerem questionamentos e dúvidas sobre os tratamentos, o que provoca a mobilização dos elementos com conhecimento técnico e, consequentemente, a descoberta de soluções e a adequação dos processos conforme os requisitos da lei. Assim, observou-se que cada instituição entrevistada está em um grau diferente no processo de implementação, não havendo uma homogeneidade com relação à adoção de medidas de adequação à LGPD.

O compartilhamento de dados também foi citado como ponto importante a ser observado, principalmente quanto ao amparo do processo por meio de um termo de ajuste de conduta que identifique os dados compartilhados e as responsabilidades de cada parte.

Particularmente com relação ao CPEx, foi observado que há uma cultura de proteção de dados inerente ao tratamento de dados pessoais executado pelo Centro, mas que não há programas de capacitação voltados para a LGPD, não há adequado envolvimento da Alta Administração, não há normativas adequadas voltadas para a implementação da lei nem ações educacionais sobre o tema.

O envolvimento da Alta Administração de cada instituição foi outro ponto fundamental citado para impulsionar as ações iniciais e para a manutenção do ciclo de conformidade com a lei, e que a chance de insucesso aumenta se o processo de implementação for *bottom-up*, como citado pela FAB.

Nesse sentido, novamente a governança desponta com pilar essencial para a adequação dos processos de tratamento de dados, o que a ratifica como um dos fatores críticos de sucesso para a implementação da LGPD. Assim, faz-se necessário avaliar qual o papel da governança nesse processo, quais suas características e como ela atua nesse novo cenário de proteção de dados, o que será analisado no próximo Capítulo do presente trabalho.

5. GOVERNANÇAPARA IMPLEMENTAÇÃO DA LGPD

5.1. Histórico

A governança começou a se estruturar de forma mais evidente e com bases em estudos mais sólidos a partir do final da década de 1980, particularmente nos EUA e na Europa. Esse movimento surgiu em função de escândalos financeiros ocorridos em grandes empresas e pela discordância de interesses que investidores e acionistas tinham em relação à forma como as grandes corporações estavam sendo administradas.

Para melhorar o entendimento, pode-se imaginar um cenário em que uma empresa é dirigida por administradores que receberam poder e recursos para conduzir os rumos de uma organização e alcançar os objetivos almejados pelos proprietários e pelos acionistas do quadro societário. Nesse contexto, levantam-se diversas questões: os interesses das partes envolvidas estão sendo atendidos? O direcionamento dado pelos administradores está em conformidade com os objetivos da empresa e das partes interessadas? Como definir melhor esse direcionamento? Como saber se a organização está sendo bem administrada?

Os administradores, devido aos seus interesses e preferências particulares, podem agir de maneira distinta daquela esperada pelos proprietários, gerando o que se chama de conflito agente-principal ou conflito de agência, que é quando os interesses do principal (sociedade, acionistas, proprietários) não são adequadamente atendidos pelos agentes (administradores) incumbidos de respeitá-los e atendê-los (Jensen; Meckling, 2008). Para solucionar esses conflitos e essas questões é que surgiu a governança, primariamente definida como a forma de governar (administrar, regular, conduzir, dirigir) sistemas corporativos privados, estabelecendo boas práticas e mecanismos para direcionar a organização, monitorar suas atividades para que as decisões estejam voltadas para o melhor desempenho da corporação.

A governança ganhou mais luz a partir da década de 1990 em função de escândalos financeiros ocorridos em grandes empresas americanas por demonstrações financeiras forjadas. Fatos assim despertaram debates envolvendo acadêmicos, legisladores e investidores sobre a necessidade imprescindível de definição sobre as práticas de governança corporativa, o que acarretou anos depois na criação da Lei *Sarbanes-Oxley* (SOx) naquele país em 2002.

Ainda nos EUA, a *General Motors* criou o primeiro código de governança corporativa de uma empresa, o que foi seguido por grande parte das grandes empresas americanas. Já na Inglaterra foi criado o Relatório *Cadbury*, primeiro código de boas práticas de governança corporativa na Europa. Nesse contexto, as boas práticas de governança corporativa passaram a ser evidenciadas por todo o mundo, particularmente em função da valorização financeira das

empresas que seguiam essa linha, já que investidores passaram a ser atraídos mais por companhias que se planejavam e se preocupavam com a governança e com resultado sustentável dos negócios ao longo dos anos.

O Brasil seguiu um caminho semelhante ao dos outros países, criando, em 1995, o Instituto Brasileiro de Conselheiros de Administração (IBCA), atual Instituto Brasileiro de Governança Corporativa (IBGC). A Administração Pública brasileira também passou por mudanças e evoluções no mesmo período, o que contribuiu para trazer e adaptar os princípios e boas práticas da governança corporativa para o âmbito do Estado. Esse movimento se deu pela necessidade natural de melhor emprego dos recursos públicos, pela cobrança social de maior efetividade das políticas públicas e pela evolução da própria Administração Pública, de modo a incorporar as práticas de governança no planejamento estatal.

Esse cenário contribuiu para a implementação da governança no setor público, o qual se baseou nos princípios e diretrizes evidenciados pela governança corporativa, mas com suas devidas adequações, visto que o conflito de agência no âmbito do setor público é ainda mais evidente e complexo que no setor privado, já que envolve interesses diversos de toda uma sociedade. Ademais, o próprio desenvolvimento do modelo de administração pública gerencial, com a proposta de tornar o Estado mais eficiente e mais capaz de atender às crescentes demandas por mais e melhores serviços (Matias-Pereira, 2018), propiciou um ambiente para a disseminação do debate sobre governança pública.

5.2. Definições de governança

A governança possui definições diversificadas, plurais e com variadas aplicações, com natureza múltipla e dinâmica, o que dá a ela um espectro teórico mais abrangente. Por se tratar de um campo em constante desenvolvimento e em consolidação, ela não tem uma definição única e consensual aceita entre estudiosos da área. No entanto, as definições existentes atualmente, apesar de diferentes, são convergentes e somam forças em uma mesma direção, voltadas para atingir os objetivos organizacionais e dos atores interessados com o melhor resultado possível.

Assim, para melhor auxiliar o entendimento desse conceito multivariado e por este trabalho ser direcionado para a implementação da LGPD em um órgão público, serão apresentadas definições existentes sobre a governança pública ou voltada para o setor público. Cabe ressaltar que, em função dos conceitos plurais, dos níveis de análise e dos fatores

considerados, torna-se difícil definir uma teoria geral que possa ser aplicada a todas as formas de governança.

A governança pública pode ser dita como a gestão de redes complexas, com atores diferentes (governo nacional, provincial e local, grupos políticos e sociais, grupos de pressão, grupos de ação e interesse, instituições sociais, organizações privadas), para influenciar processos sociais de políticas públicas (Kickert, 1997).

Governança pública pode ser definida também como uma teoria política de caráter interorganizacional voltada para uma forma emergente, democrática e estratégica de governar o serviço público, com a participação de entes sociais, por meio de redes, como as parcerias público-privadas e a inclusão da sociedade civil organizada na união de esforços e associação de recursos (Peters e Pierre, 1998).

O Instituto Brasileiro de Governança Pública (IBGP, 2014, p. 1) aponta que governança pública é o "sistema que compreende os mecanismos institucionais para o desenvolvimento de políticas públicas que garantam que os resultados desejados pelos cidadãos, e demais entes da vida pública, sejam definidos e alcançados".

Outro interessante conceito é o de que a governança pública é um campo de estudo interdisciplinar centrado nas relações de poder entre as autoridades governamentais, a sociedade civil e o mercado, em um contexto de transformações na capacidade das comunidades políticas legitimamente se governarem e agirem efetivamente (Lynn e Malinowska, 2018).

O Tribunal de Contas da União (TCU) vem evoluindo os conceitos de governança na Administração Pública ao longo dos anos. Inicialmente, indicava que governança pública era a forma pela qual as organizações públicas são avaliadas, monitoradas e controladas, o que envolve o relacionamento entre a sociedade, a alta administração e os servidores públicos para a consecução dos objetivos do governo de atender as demandas sociais (Brasil, 2014a).

Posteriormente, conceituou governança como mecanismos de liderança, estratégia e controle postos em prática para avaliar, direcionar e monitorar a atuação da gestão, com vistas à condução de políticas públicas e à prestação de serviços de interesse da sociedade (Brasil, 2018d).

Recentemente o TCU explicitou seu novo conceito de governança pública:

> [...] a aplicação de práticas de liderança, de estratégia e de controle, que permitem aos mandatários de uma organização pública e às partes nela interessadas avaliar sua situação e demandas, direcionar a sua atuação e monitorar o seu funcionamento, de modo a aumentar as chances de entrega de bons resultados aos cidadãos, em termos de serviços e de políticas públicas (Brasil, 2020h, p. 15).

Já a Portaria do Comandante do Exército nº 987, de 18 de setembro de 2020, conceitua governança como o "conjunto de mecanismos de liderança, estratégia e controle postos em prática para avaliar, direcionar e monitorar a gestão, com vistas à condução de políticas públicas e à prestação de serviços de interesse da sociedade". Esse será o conceito adotado pelo presente trabalho, visto que necessita de alinhamento doutrinário e estratégico com as diretrizes expedidas pelo Comando do Exército, particularmente aquelas voltadas para o tratamento de dados para fins de pagamento de pessoal.

5.3. Princípios, funções e mecanismos de governança

Apesar de classificações conceituais diversas para a governança no campo teórico, não há distinção no seu escopo de aplicação nas diferentes áreas em que seus mecanismos são implementados. Assim é importante que a governança seja uma forma de atribuir responsabilidades, normatizar diretrizes, estabelecer redes entre elementos vinculados, gerenciar recursos e obter efetividade nas entregas. Desta feita, é essencial definir princípios que sejam a sustentação das bases da governança, que sejam as suas balizas teóricas para a sua implementação nas organizações.

A governança é influenciada de uma forma multidimensional que varia de acordo com o ambiente, a cultura, a estrutura socioeconômica, as regulações normativas, os estímulos, a articulação, a rede dos envolvidos, o nível de responsabilidade e integridade dos atores, os processos existentes, as políticas públicas e os interesses das partes. Toda essa dinâmica e todas essas variáveis influenciarão no modo como a governança vai direcionar a condução das ações de todo um setor ou de toda uma instituição.

Os princípios da governança são como um arcabouço normativo-prescritivo para o seu desenvolvimento que auxiliam na delimitação das competências dos atores e das estruturas envolvidas (Paludo, 2021). O Banco Mundial aponta que os princípios de boa governança são a legitimidade, a equidade, a responsabilidade, a eficiência, a probidade, a transparência e a *accountability*. Para a instituição, a efetividade da governança depende da presença do Estado de direito, de uma sociedade engajada, de ética profissional, de planejamento político aberto e transparente e de execução responsável das ações (World Bank, 2007).

O Decreto 9.023/2017, que dispõe sobre a política de governança da Administração Pública Federal, aponta que a governança é orientada pelos princípios da capacidade de resposta, integridade, confiabilidade, melhoria regulatória, prestação de contas, responsabilidade e transparência (Brasil, 2017a). Já o TCU adota os princípios da capacidade

de resposta, integridade, transparência, equidade e participação, *accountability*, confiabilidade e melhoria regulatória (Brasil, 2020h).

A orientação com base nos princípios da governança é o passo inicial para o processo de implementação organizacional da LGPD. Eles servirão de direcionadores para o planejamento estratégico, para a execução dos processos e para o envolvimento das partes interessadas.

Assim, imersa no rol de princípios norteadores, a governança possui as funções de avaliar, direcionar e monitorar as atividades organizacionais. Avaliar as demandas das partes interessadas e estabelecer as prioridades; direcionar a capacidade de realização da organização para a efetiva resolução das prioridades; monitorar a gestão da organização para garantir o cumprimento das direções estabelecidas, permitir os ajustes de percurso e evitar que os riscos impeçam ou prejudiquem a consecução dos objetivos (Brasil, 2020h).

Para proporcionar mais concretude para a parte teórica, as funções de governança (avaliar, direcionar e monitorar) podem ser mais bem detalhadas por meio das seguintes medidas (Paludo, 2021):

a) Avaliar o ambiente, cenários, desempenho e resultados;
b) Alinhar as funções organizacionais às necessidades das partes interessadas;
c) Assegurar às partes interessadas o governo estratégico da organização;
d) Assegurar o alcance dos objetivos estabelecidos;
e) Auditar e avaliar o sistema de gestão e controle;
f) Confrontar os resultados com as metas estabelecidas e as expectativas das partes interessadas;
g) Definir o direcionamento estratégico;
h) Determinar o gerenciamento de riscos estratégicos;
i) Direcionar e orientar a preparação, a articulação e a coordenação de políticas e planos;
j) Envolver as partes interessadas nas decisões;
k) Garantir que as ações estejam alinhadas com o interesse público;
l) Instituir mecanismos de gestão para melhorar o desempenho;
m) Monitorar o desempenho, os resultados e o cumprimento de políticas e planos;
n) Orientar aspectos essenciais da gestão;
o) Promover a coordenação entre agências;
p) Promover a transparência e a accountability;
q) Resolver conflitos internos;

r) Responsabilizar os agentes com poder de decisão;
s) Supervisionar a gestão.

Para assegurar o cumprimento de tais funções, a governança adota os mecanismos de liderança, estratégia e controle (Paludo, 2021). A liderança é composta por pessoas e competências, princípios e comportamentos, liderança organizacional e sistema de governança. A estratégia é composta por relacionamento com as partes interessadas, estratégia organizacional e alinhamento transorganizacional. O controle se refere à gestão de riscos e controle interno, auditoria interna, *accountability* e transparência.

Cabe ressaltar que os elementos de cada um dos mecanismos citados não abrangem todos aqueles aplicáveis à diversidade de organizações públicas existentes, sendo apenas um rol conceitual apresentado pelo autor. A própria evolução das normas e da literatura sobre o assunto, juntamente com as características de cada organização fazem com que novos elementos sejam criados ou adaptados.

Por fim, com a efetividade na implementação podem-se enumerar possíveis benefícios que uma boa governança traz para uma organização pública (Brasil, 2020h):

a) Garantir a entrega de benefícios econômicos, sociais e ambientais para os cidadãos;
b) Garantir que a organização seja e pareça responsável para com os cidadãos;
c) Ter clareza acerca de quais são os produtos e serviços efetivamente prestados para cidadãos e usuários, e manter o foco nesse propósito;
d) Ser transparente, mantendo a sociedade informada acerca das decisões tomadas e dos riscos envolvidos;
e) Possuir e utilizar informações de qualidade e mecanismos robustos de apoio às tomadas de decisão;
f) Dialogar com a sociedade e a ela prestar contas;
g) Garantir a qualidade e a efetividade dos serviços prestados aos cidadãos;
h) Promover o desenvolvimento contínuo da liderança e dos colaboradores;
i) Definir claramente processos, papéis, responsabilidades e limites de poder e de autoridade;
j) Institucionalizar estruturas adequadas de governança;
k) Selecionar a liderança tendo por base aspectos como conhecimento, habilidades e atitudes (competências individuais);

l) Avaliar o desempenho e a conformidade da organização e da liderança, mantendo um balanceamento adequado entre eles;
m) Garantir a existência de um sistema efetivo de gestão de riscos;
n) Utilizar-se de controles internos para manter os riscos em níveis adequados e aceitáveis;
o) Controlar as finanças de forma atenta, robusta e responsável; e
p) Prover aos cidadãos dados e informações de qualidade (confiáveis, tempestivas, relevantes e compreensíveis).

5.4. Estrutura, implementação e diretrizes de governança

O planejamento estratégico em órgãos e entidades públicas é o instrumento central de governança organizacional na busca dos objetivos almejados. O planejamento estratégico efetua a avaliação da situação da organização pública e do ambiente onde ela se encontra, indicando para a gestão as balizas que deverão ser seguidas nas metas e nos planos de ações para alcançar os objetivos. Esse planejamento é essencial para que o setor público possa lidar com as novas demandas impostas pela sociedade, com a escassez de recursos, com as inovações e tecnologias que constantemente impõem mudanças na prestação dos serviços públicos.

A governança não propõe a criação de mais controles e de mais burocracia, mas sim buscar formas de descobrir oportunidades e de remover controles desnecessários, visto que seu objetivo é a melhoria do desempenho da organização e a entrega de valor. Assim, não há efetividade na tentativa de incorporação de práticas de boa governança sem foco nos resultados (Brasil, 2020h).

Antes de tudo, é importante localizar a governança na estrutura sistêmica criada para direcionar e conduzir o novo ambiente organizacional. Ela não pode ser confundida nem com governo, nem com administração, nem com gestão. Como pode ser observado na figura abaixo, a governança está acima da gestão e é uma ferramenta ligada diretamente ao nível estratégico organizacional, isto é, de uso essencial da Alta Administração, Assim, a governança age como ligação entre a Alta Administração e a gestão.

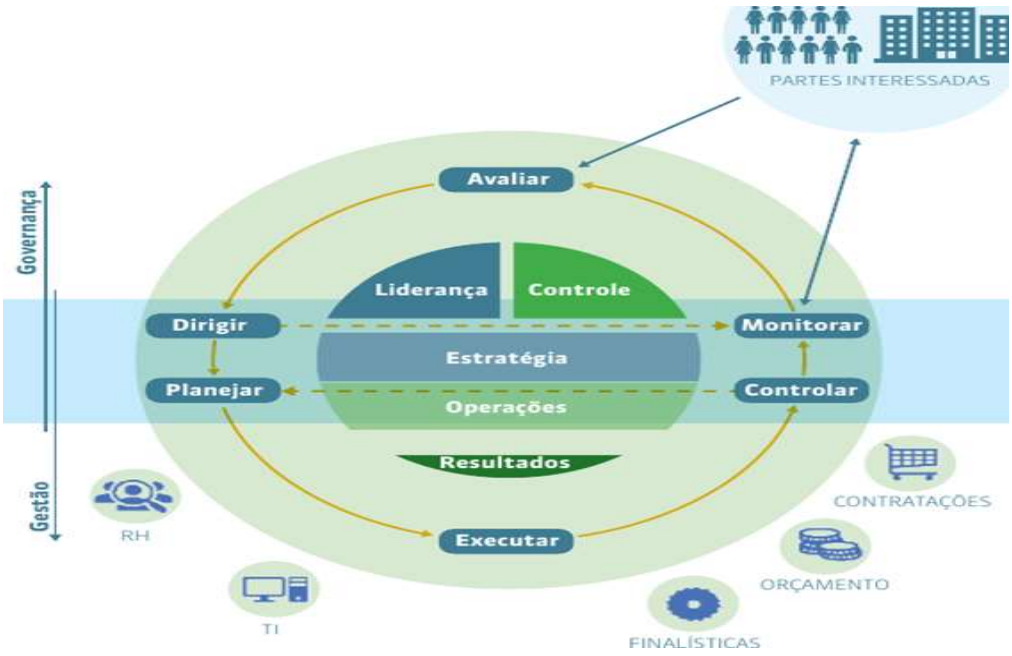

Figura 11: Modelo de Governança e Gestão
Fonte: Brasil, 2020a.

A governança age na avaliação, no direcionamento e no monitoramento da gestão e dos gestores, os quais planejam, executam e controlam os processos. Na figura abaixo, Paludo (2021) apresenta que a Alta Administração usa a governança (nível estratégico) para fazer com que a gestão (nível operacional) execute suas principais funções. Assim, a governança exerce o direcionamento e a gestão exerce a realização.

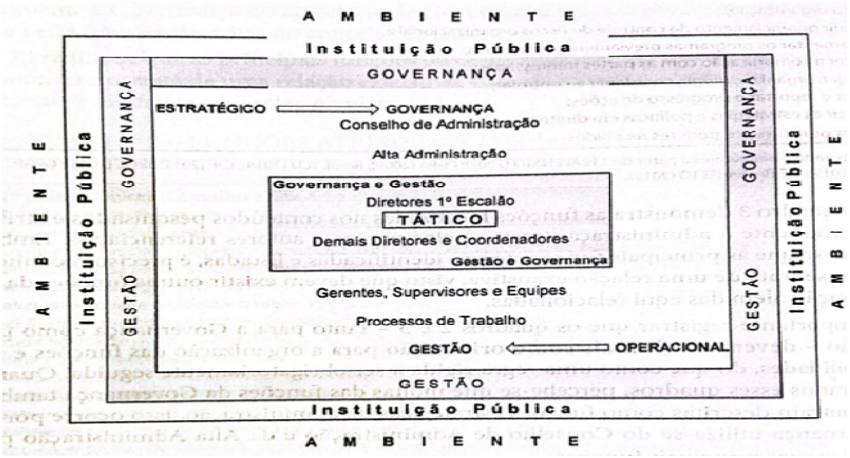

Figura 12: Posicionamento da Governança e da Gestão no ambiente organizacional
Fonte: Paludo, 2021.

A governança e a gestão acabam se tocando em determinadas funções, integrando os círculos de forma harmônica. Por exemplo, o direcionamento do planejamento estratégico e o monitoramento das atividades são dados pela governança; já o planejamento da execução e o controle da gestão geram informações para o monitoramento da governança, com o objetivo

de identificar o atendimento dos interesses das partes interessadas e permitir ajustes na execução dos processos. Apesar dessa aproximação, cada função deve manter-se separada para que suas atividades cumpram suas finalidades específicas dentro de cada organização.

Dado que a governança e a gestão se localizam em níveis distintos dentro de uma organização, faz-se necessário buscar a implementação da governança de forma a criar um ambiente harmônico para a integração dos processos, para o envolvimento dos atores e para a entrega de mais resultados. Mas para isso, a governança depende do cumprimento dos seguintes pontos (IFAC, 2014):

a) Garantia do comportamento ético, íntegro, responsável, comprometido e transparente da liderança;
b) Controle da corrupção;
c) Implementação efetiva de um código de conduta e de valores éticos;
d) Observação e garantia da aderência das organizações às regulamentações, códigos, normas e padrões;
e) Garantia da transparência e da efetividade das comunicações;
f) Balanceamento dos interesses e envolvimento efetivo dos stakeholders (cidadãos, usuários de serviços, acionistas, iniciativa privada).

Devido aos diversos conceitos envolvendo a governança e suas formas de aplicação e atuação, foram compiladas algumas diretrizes que representam ações para viabilizar a sua implementação nas organizações (Brasil, 2020h):

a) Definir formalmente e comunicar claramente os papéis e responsabilidades das instâncias internas e de apoio à governança, e assegurar que sejam desempenhados de forma efetiva;
b) Estabelecer processos decisórios transparentes, baseados em evidências e orientados a riscos, motivados pela equidade e pelo compromisso de atender ao interesse público;
c) Promover valores de integridade e implementar elevados padrões de comportamento, começando pela demonstração de conduta exemplar da liderança da organização e de apoio às políticas e programa de integridade;
d) Aprimorar a capacidade da liderança da organização, garantindo que seus membros tenham habilidade, conhecimentos e experiências necessários ao desempenho de suas funções; avaliando o desempenho deles como indivíduos e como grupo; e equilibrando, na composição da liderança, continuidade e renovação;

e) Desenvolver continuamente a capacidade da organização, assegurando a eficácia e eficiência da gestão dos recursos organizacionais, como a gestão e a sustentabilidade do orçamento, das pessoas, das contratações e da tecnologia e segurança da informação;
f) Apoiar e viabilizar a inovação para agregar valor público e lidar com as limitações de recursos e com novas ameaças e oportunidades;
g) Estabelecer um sistema eficaz de gestão de riscos e controles internos;
h) Estabelecer objetivos organizacionais alinhados ao interesse público, e comunicá-los de modo que o planejamento e a execução das operações reflitam o propósito da organização e contribuam para alcançar os resultados pretendidos;
i) Monitorar o desempenho da organização e utilizar os resultados para identificar oportunidades de melhoria e avaliar as estratégias organizacionais estabelecidas;
j) Considerar os interesses, direitos e expectativas das partes interessadas nos processos de tomada de decisão;
k) Implementar boas práticas de transparência;
l) Prestar contas às partes interessadas e implementar mecanismos eficazes de responsabilização dos agentes;
m) Apoiar o uso das ferramentas digitais para aumentar e facilitar a participação das partes interessadas nas decisões públicas e aprimorar a prestação de serviços públicos;
n) Promover a simplificação administrativa, a modernização da gestão pública e a integração dos serviços públicos, especialmente aqueles prestados por meio eletrônico;
o) Editar e revisar atos normativos, pautando-se pelas boas práticas regulatórias e pela legitimidade, estabilidade e coerência do ordenamento jurídico e realizando consultas públicas, sempre que conveniente.

Assim, diretrizes de governança se apresentam como necessidades do processo de implementação da LGPD, podendo atingir níveis de profundidade e de complexidade variáveis, dependendo do foco, do ambiente, dos riscos, da maturidade e da necessidade de cada organização.

Cabe à autoridade máxima da organização, principal responsável pela governança, e aos gestores/administradores de nível estratégico que estiverem ligados à autoridade máxima o estabelecimento das políticas e dos objetivos para o direcionamento da organização e pela implementação das boas práticas de governança.

5.5. A governança de dados e a LGPD

A LGPD, em seu Art. 50, aponta que regras e boas práticas de governança poderão ser formuladas pelas instituições para estabelecer condições de organização, regime de funcionamento, procedimentos, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos elementos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos.

A partir desse regramento trazido pela LGPD, é possível analisar um dos braços da governança, a chamada governança de dados. Ela dá direcionamento aos processos compostos por fluxos de informações que permeiam um ente/órgão/instituição, alinha-se diretamente à estratégia de negócio da organização de forma a garantir a conformidade dos processos de tratamento de dados, a incentivar que as pessoas passem a adotar as práticas de governança e a identificar riscos e problemas de gestão das informações.

A governança de dados então representa o exercício da autoridade, o controle de estratégias, políticas, regras, procedimentos, papéis e atividades envolvidos com os processos de dados. Ela se inicia na mais alta esfera da organização, envolve interface com diversas outras funções e estabelece políticas e diretrizes corporativas para governar os dados, além de atribuir papéis e responsabilidades (Rêgo, 2013).

Para isso, ela busca responder a diversos questionamentos como: qual a política adotada pela empresa sobre o uso dos dados e informações? Quais são as responsabilidades e os papéis envolvidos no uso dos dados e informações? Quais os processos utilizados para gerir dados e informações? Quais os padrões e procedimentos utilizados? Quem são os gestores das informações? A clareza e o conteúdo das respostas refletem diretamente a maturidade de governança de dados de uma instituição (Rêgo, 2013).

Assim, respondendo aos questionamentos supracitados, a governança de dados pode definir diretrizes estratégicas dos processos de tratamento de dados que são adequados para a missão da organização; os dados que são necessários; as responsabilidades e os responsáveis pelo tratamento das informações; o prazo de armazenamento dos dados, quem poderá acessá-los e onde eles ficam armazenados; a forma como eles são coletados, a sua finalidade e o amparo legal de todo processo, mantendo assim um alinhamento com as diretrizes da própria LGPD.

Nesse sentido, a governança de dados necessita então se alinhar diretamente à estratégia de negócio da organização, visto que, quanto mais resolver problemas de gestão de dados, maior será a probabilidade de gerar mudança de comportamento nas pessoas e fazer

com que elas adotem as práticas de governança. Para isso, a governança deve estabelecer formas e mecanismos, por meio da adoção de uma Política de governança de dados, para solucionar problemas e atender às necessidades das partes interessadas (DAMA-DMBOK, 2017), buscando sempre:

a) Avaliar os requisitos de conformidade regulatória (Compliance Policy);
b) Definir uma política de dados;
c) Documentar como os dados serão gerenciados e compartilhados;
d) Identificar as licenças e acordos de compartilhamento vinculados aos dados coletados;
e) Identificar as restrições que a organização deve aderir;
f) Apontar quais os aspectos legais e éticos de restrições de acesso e uso de dados confidenciais;
g) Certificar que todas as políticas de dados sejam aplicadas de forma adequada.

Existem três componentes comuns em programas de governança de dados: pessoas, processos e tecnologia. Tais componentes necessitam atuar deforma integrada para estabelecer a política e a estratégia de dados do programa de governança. Assim, eles devem ser avaliados por ocasião do estabelecimento do programa, dos objetivos, das principais premissas e das direções para traçar planos de ação de estratégicos que possibilitem atingir as metas acerca dos dados (Rêgo, 2013).

A governança de dados deve efetuar também o gerenciamento de conflitos, o que significa identificar, quantificar, priorizar e resolver questões envolvendo dados. O gerenciamento de conflitos compreende (DAMA-DMBOK, 2017):

a) Autoridade: questões relativas à decisão, direitos e procedimentos;
b) Contratos/acordos: negociação e revisão de dados compartilhados, monetização de dados e armazenamento;
c) Segurança: privacidade e questões de confidencialidade, desastres ou falhas de segurança;
d) Qualidade de dados: detecção e resolução de problemas.

A governança de dados deve ser considerada, então, como um programa institucional, pois deve ser um processo contínuo, e não deve ser vista como um projeto com características temporárias. Ela deve possibilitar que a organização atinja seus objetivos estratégicos e cumpra sua missão institucional, bem como deve estabelecer uma Política de Dados, que em

geral são regras que devem ser adotadas pelos envolvidos no tratamento dos dados, desde sua coleta até sua eliminação, com processos formais de controle, tendo como base as normativas legais e as diretrizes internas sobre tratamento de dados.

Assim, é possível fazer uma relação entrea normatização contida na LGPD com as medidas de governança de dados recomendadas pelo DAMA-DMBOK (2017) para que instituições possam efetuar um adequado planejamento estratégico da gestão de dados e a implementação da referida lei:

a) Entender as necessidades estratégicas de dados da organização;
b) Desenvolver e manter a estratégia de dados;
c) Estabelecer os papéis dos profissionais e das organizações de dados;
d) Identificar e apontar os gestores dos dados;
e) Estabelecer organizações de gestão e governança de dados;
f) Desenvolver e aprovar políticas, padrões e procedimentos de dados;
g) Supervisionar equipes e organizações profissionais de dados;
h) Coordenar atividades de governança de dados;
i) Gerenciar e resolver questões relacionadas aos dados;
j) Monitorar e forçar o cumprimento dos regulatórios.

Nesse contexto, com a governança de dados a organização passa a ter conhecimento completo dos fluxos de tratamento de dados, ter condições de se adequar às novas legislações e normativas e ter uma ferramenta para disseminar sua Política de Dados. Ela consegue obter subsídios para tomada de decisões com base em informações corretas e obtidas de forma mais rápida e eficiente. Por fim, a governança de dados traz para a organização um perfil de confiabilidade e seriedade, visto que dá aos titulares dos dados a segurança de que suas informações pessoais são tratadas de forma idônea.

A governança de dados é, então, uma ferramenta importante para a adequação das organizações à LGPD. Ela está expressa na Seção II, Das Boas Práticas e da governança, Art. 50, § 2º, com as determinações para a implementação de um Programa de Governança em Privacidade (PGP) nos sistemas utilizados para tratamento de dados pessoais, conforme as particularidades dos componentes pessoas, processos e tecnologias da instituição.

Também é abordado o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os

mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais (Brasil, 2018d).

Assim, para qualquer organização que busque a conformidade de seus processos com a Lei Geral de Proteção de Dados, é essencial que inicialmente haja a avaliação das pessoas, dos processos e da tecnologia da instituição voltada para a governança de dados. Com isso, a Alta Administração deve viabilizar a implantação de uma da Política de Dados, dos fluxos das informações, da infraestrutura, da capacitação e da responsabilização de pessoal, de forma que os dados sejam tratados dentro dos requisitos da LGPD. A governança de dados atuará, assim, de cima para baixo na organização, considerando a natureza, o escopo, a finalidade e efetuando a gestão de riscos do tratamento de dados efetuado, além de fomentar mecanismos para que o titular das informações possa exercer seus direitos garantidos na referida normativa legal.

Dessa forma, a governança e a LGPD possuem laços indissociáveis que devem ser fortalecidos por todas as organizações públicas nesse novo cenário de tratamento de dados pessoais no país. Como o presente trabalho buscará avaliar as implicações, as medidas necessárias para a implementação da LGPD, é relevante que a governança seja a norteadora para a plena conformidade do tratamento de dados no CPEx. Por meio dela, a Alta Administração utiliza sua liderança estabelecendo as diretrizes para que a lei seja implementada, viabilizando a introdução de uma cultura de privacidade e proteção dos dados na organização, bem como mobilizando a estrutura necessária para as adequações, o monitoramento e a constante evolução da conformidade dos processos de tratamento para fins de pagamento de pessoal.

5.6. A governança de dados da LGPD no Exército

Conforme previsto na Portaria nº 088 EME, de 7 de maio de 2020, que aprovou a diretriz de orientação para aplicação da LGPD no Exército, a governançade dados do processo de implementação da lei ficou a cargo do EME, o qual faz a ligação entre a Alta Administração, representada pelo Comandante do Exército, e a gestão dos processos de tratamento de dados pessoais, representados pelos demais órgãos do Comando do Exército, dentre eles o CPEx.

A referida Portaria, em resumo, atribuiu responsabilidades aos elementos subordinados e expediu ordens para que eles inventariassem seus processos de tratamento, implementassem medidas de adequação e remetessem relatórios das atividades executadas ao EME. Também

estabeleceu ações para viabilizar que os titulares pudessem exercer seus direitos perante o controlador, divulgando informações sobre o tratamento, finalidade, previsão legal, bem indicando que o próprio EME seria o responsável por tais medidas, bem como por ser o elemento de ligação com a ANPD.

Verificou-se que foi disponibilizado pelo EME um canal para o exercício dos direitos dos titulares, conforme previsto na Portaria nº 088, mas que não contêm nenhuma informação sobre os tratamentos dos dados, além do fato de que o encarregado lá indicado não mais está em atividade no Exército[18]. Ademais, o e-mail de contato disponibilizado não atende às demandas dos titulares, visto que, 10 pessoas foram solicitadas a enviar mensagens pelo referido canal, solicitando informações sobre seus dados, e algumas sequer foram respondidas e outras receberam respostas automatizadas que não corresponderam ao solicitado[19]. Cabe ressaltar que a resposta automática foi recebida mais de 4 meses depois do questionamento apresentado pelos titulares.

Atendendo ao previsto na Portaria nº 088 EME, o CPEx confeccionou um Relatório de Inventário, apontando algumas medidas idealizadas como necessárias para implementar a LGPD e identificando de forma sucinta apenas 6 processos de tratamento de dados[20]. Tal relatório foi produzido de forma a cumprir a determinação do EME, sem ocorrer uma capacitação prévia de pessoal para executar o trabalho e sem o estabelecimento de um programa de instrução ou de estudo que viabilizasse a difusão de informações e de conhecimentos sobre a LGPD no âmbito da instituição.

Sobre esse aspecto, constata-se que houve deficiência na confecção do referido relatório por falta de capacitação de recursos humanos sobre o tema e pela falta de medidas de governança da Alta Administração, que delegou suas atribuições aos elementos subordinados e não observou a complexidade e a necessidade de empenho efetivo do Comando do Exército no processo de implementação da LGPD. Cabe ressaltar que a Portaria nº 088 EME foi o único documento formal produzido pela Alta Administração do Exército sobre a LGPD, e que após o envio do Relatório de Inventário pelo CPEx nenhuma nova diretriz ou determinação foi recebida com relação à referida lei.

Analisando as diretrizes contidas na Portaria nº 088 EME, nota-se que há uma delegação das medidas de implementação aos elementos subordinados e, consequentemente, uma falta de envolvimento do controlador no processo. Tal aspecto pode ser relacionado com

---

[18] <https://www.eb.mil.br/acesso-a-informacao/protecao-de-dados-lgpd>.
[19] *Exemplo de mensagem disponibilizada no Anexo II.*
[20] *Relatório disponível no Anexo III*

a situação atual da adequação da LGPD no processo de pagamento de pessoal do CPEx, em que há também uma ausência quase que total de medidas de implementação. Assim, a referida Portaria tem apenas 3 medidas de governança apresentadas para o processo de adequação:

> 5. TRABALHOS DE ADEQUAÇÃO
>
> a. Reavaliar os processos internos, identificando a necessidade de alterações quanto à adequação das salvaguardas das informações pessoais e demais disposições advindas da LGPD.
>
> b. Auditar os Bancos de Dados Corporativo do Exército assim como as demais bases de dados e sistemas por onde tramitam informações pessoais, verificando sua conformidade com as disposições da LGPD, regulamentos e orientações advindas da ANPD.
>
> c. Identificar as normas internas que tratam de dados pessoais, analisando a sua adequação às disposições da LGPD, do Decreto nº 9.191, de 1º de novembro de 2017 e do Decreto nº10.139, de 28 de novembro de 2019.

Cabe ressaltar que atualmente existe uma Política de Privacidade produzida por iniciativa própria do CPEx ainda em 2023, bem como outras normativas internas voltadas para a Política de Segurança da Informação. No entanto, observou-se que todas normativas produzidas pelo Exército no âmbito da Segurança da Informação, disponível na intranet da 2ª Subchefia do EME[21], são de data anterior à vigência da LGPD, o que retrata que o arcabouço normativo interno da instituição não foi adaptado para os requisitos da referida lei.

Dessa forma, analisando o cenário atual no âmbito do processo de pagamento de pessoal do CPEx e a Portaria nº 088 EME, medida singular tomada pelo controlador para implementação da LGPD, é possível identificar que EME deixou lacunas na governança de dados que não viabilizaram adequadamente o processo de implementação da lei na instituição, dado que, conforme demonstrado no presente trabalho, medidas *bottom-up* e adotadas de formas pontuais e descentralizadas, sem a governança da Alta Administração agindo como força motriz do processo, não trazem efetividade adequada às medidas de implementação.

5.7. Marco teórico de referência de governança de dados na LGPD

A governança de dados entra no processo de implementação da LGPD como o elemento motriz que irá liderar os trabalhos a serem executados. Por meio de uma avaliação organizacional e de um planejamento estratégico efetuados pela governança, que direcionarão as ações, serão atribuídas responsabilidades, expedidas diretrizes, estabelecidas redes de interação entre os elementos envolvidos, geridos os riscos e mobilizada estrutura para obter

[21] *<http://intranet.eme.eb.mil.br/emenet/sites/2sch/index.php/legislacao-2sch>, Anexo IV.*

efetividade na implementação, além de implementar controles para monitorar e manter a conformidade obtida ao final.

Assim, com base na revisão particularizada feita sobre a governança no presente trabalho, é possível estabelecer um marco teórico de referência para orientar o olhar sobre a atual realidade do processo de pagamento de pessoal do CPEx e sintetizar medidas da Alta Administração que serão necessárias para a adequação à LGPD, sem excluir outras medidas que possam também ser identificadas pela equipe multidisciplinar de implementação:

a) Comprometimento da Alta Administração para o alcance dos objetivos estabelecidos;
b) Avaliação do ambiente organizacional, dos possíveis cenários e dos resultados esperados;
c) Direcionamento estratégico do processo de implementação;
d) Direcionamento de objetivos organizacionais alinhados com os direitos dos titulares dos dados para alcançar os resultados pretendidos;
e) Direcionamento do gerenciamento de riscos estratégicos e de controles internos;
f) Direcionamento da preparação, da articulação e da coordenação de políticas e planos;
g) Viabilização do contínuo desenvolvimento dos processos de capacitação de pessoal e de aplicação de tecnologia e segurança da informação;
h) Coordenação das atividades entre os diferentes órgãos e setores;
i) Resolução de divergências e de conflitos internos;
j) Definição e comunicação formal dos papéis e responsabilidades de forma a assegurar que sejam desempenhados de forma efetiva;
k) Promoção de valores de integridade e de elevados padrões de comportamento, com exemplo dado pela liderança da organização e com apoio às políticas e programa de integridade;
l) Aprimoramento da capacidade da liderança da instituição, garantindo que seus integrantes tenham competência necessária para o processo de implementação e para difusão de conhecimentos;
m) Viabilização de inovações para lidar com as limitações de recursos e com novas ameaças e oportunidades;
n) Inserção dos direitos dos titulares nos processos de tomada de decisão sobre tratamento de dados, com base em evidências e em gestão de riscos;
o) Implementação da transparência no processo de tratamento e compartilhamento dos dados, com prestação de informações aos titulares;

p) Viabilização do uso das ferramentas digitais para facilitar o exercício de direito dos titulares;
q) Avaliação da adequação e da real necessidade da coleta e do armazenamento dos dados tratados;
r) Avaliação e revisão dos atos normativos, pautando-se pelas boas práticas regulatórias e pela legitimidade;
s) Monitoramento do desempenho, dos resultados e do cumprimento de políticas e planos.

Cabe ressaltar que o cerne das medidas de governança da Alta Administração é ligeiramente diferente das medidas comparadas no Quadro 7 (marco teórico de referência); as medidas comparadas no capítulo anterior possuem um caráter mais objetivo, operacional, voltadas muitas vezes para a consecução de uma determinada tarefa específica, como a elaboração de um determinado documento; já as medidas de governança possuem um caráter mais fluido, estratégico, com variadas formas de execução, de acordo com a análise e a viabilidade da conjuntura organizacional, podendo apresentar muitas vezes resultados diferentes, mas que atingem perfeitamente os fins pretendidos.

As medidas de governança podem, nesse sentido, ser integradas ao planejamento estratégico da instituição, sem a necessidade de se efetuar todo um trabalho em separado, focado especificamente no tratamento de dados e na LGPD. Na verdade, é interessante que haja a incorporação da governançada LGPD em um escopo estratégico já existente, permitindo uma integração entre diferentes setores envolvidos, de forma a reforçar a relevância do tema e a fundamentar a cultura de proteção de dados pessoais dentro da organização.

Assim, após o levantamento de todas as informações do Capítulo atual e dos anteriores do presente trabalho, de toda a análise do objeto e do problema existente, do estabelecimento de marcos teóricos de referência e do delineamento de possíveis medidas de adequação, é possível apresentar uma proposta de implementação da LGPD no processo de pagamento de pessoal do CPEx. Desta feita, no próximo Capítulo serão apresentadas as conclusões finais do presente trabalho, com um novo modelo teórico de adequação à lei voltado para o setor público, que poderá ser utilizado pelo CPEx para alcançar soluções para conformidade legal dos seus processos de tratamento de dados.

6. PROPOSTA DE MEDIDAS PARA IMPLEMENTAR A LGPD NO CPEX

6.1. Conclusões parciais

A adequação dos processos de pagamento de pessoal à nova realidade de tratamento de dados pessoais deve ser uma obrigação irrevogável por parte do CPEx, o qual ainda se encontra em um estágio primário do processo de implementação da LGPD. Foi observado no presente trabalho que algumas poucas medidas foram adotadas para a implementação da LGPD no Comando do Exército, tanto por parte do CPEx quanto pelo EME, e que elas não estão totalmente adequadas ao novo cenário de tratamento de dados trazido pela lei.

No mesmo sentido, os problemas encontrados nos processos de tratamento de dados do CPEx à luz da LGPD foram apresentados definindo o seu escopo principal, isto é, o elemento central do problema, podendo haver assim o seu desdobramento em diversas outras inconformidades de acordo com o tema/área do tratamento de dados. Tal fato pode aumentar consideravelmente o rol de problemas apontados, bem como a quantidade de medidas necessárias para a adequação à lei.

Por outro lado, o CPEx já possui um direcionamento que facilitará a implementação da LGDP, dado que existem protocolos de segurança no acesso aos dados, segregações de funções e documentação de orientação que contribuem para uma cultura intrínseca de proteção de dados existente na instituição.

Partindo da análise situacional do CPEx e adentrando no contexto da LGPD, durante os estudos foi identificado que informações sobre o processo de implementação encontram-se dispersas em várias peças normativas, desde a lei propriamente dita até guias e manuais expedidos por entes governamentais. Tal fato dificulta o estabelecimento de um roteiro ou de uma sequência de atividades que possa contribuir para a avaliação do cenário, o planejamento do trabalho e a execução das medidas de adequação. Em função disso, buscou-se apoio na literatura sobre o tema, com o objetivo de identificar modelos teóricos que pudessem auxiliar o gestor público na missão de implementar a LGPD em sua instituição.

Ao fim da análise dos modelos teóricos, observou-se que existe uma lacuna importante: a pouca disponibilidade de modelos voltados para a implementação da LGPD no setor público, visto que, dos 7 encontrados, apenas 1 não era voltado para o setor privado. Tal constatação também foi observada durante a pesquisa bibliográfica na literatura que aborda a implementação da LGPD. Os estudos existentes vêm focando seus esforços em obras

doutrinárias e em modelos destinados à implementação da LGPD no setor privado, o que faz com que não haja muitos modelos direcionados para o setor público.

Assim, os modelos teóricos contribuíram com a possibilidade de se estabelecer um sequenciamento de ações, além de apresentar diversas medidas para a implementação, as quais variaram conforme o escopo priorizado pelos autores. Desta feita, por meio da listagem e da comparação dessas medidas, somadas àquelas citadas nas normativas legais, foi possível configurar um marco teórico de referência, identificando as medidas que mais se adequam ao setor público e que poderão compor a proposta de implementação do presente trabalho.

Já as entrevistas serviram como uma nova fonte de identificação de fatores críticos de sucesso para a implementação da LGPD, mais voltada para a aplicação concreta na realidade, saindo da previsão literária das medidas apontadas nas normativas legais e nos modelos teóricos. O diálogo com outras instituições foi importante também para avaliar o cenário das instituições no processo de adequação, as dificuldades observadas, os ensinamentos colhidos e as etapas futuras, de forma a efetuar uma replicação de conhecimentos que favoreça o processo de implementação da lei.

Por fim, após todo o estudo feito no presente trabalho, é possível afirmar que os fatores críticos de sucesso para implementar a LGDP no processo de pagamento de pessoal do CPEx são representados por ações de governança e por medidas de implementação identificadas como adequadas ao contexto de tratamento de dados no setor público.

6.2. As ações de governança

As ações de governança podem ser tidas como o conjunto de mecanismos de liderança, estratégia e controle, ligados à Alta Administração, utilizados para implementação de medidas de segurança, técnicas e administrativas da governança de dados. Assim, as ações de governança podem ser designadas como a força motriz de todo processo, isto é, o mecanismo de liderança que conduzirá a instituição, estabelecendo a estratégia adequada para atingir os objetivos da implementação e para controlar, avaliar, direcionar e monitorar a busca pela conformidade legal, viabilizando tanto a execução da missão da instituição pública como a garantia dos direitos dos titulares dos dados.

Como exposto no marco teórico de referência de governança, suas ações devem ser o início de todo o processo de implementação, principalmente na avaliação do *status* do ambiente organizacional, na viabilização da incorporação de novas informações e conhecimentos, por meio de ações educacionais, e no direcionamento estratégico do processo.

Assim, em todo processo de execução das medidas de implementação a governança deve se fazer presente, desde as etapas iniciais até a avaliação e o monitoramento posterior para manutenção da conformidade e do novo *status* de adequação da instituição.

No mesmo sentido, a governança deve agir na resolução de divergências e de conflitos internos; na promoção de valores de integridade e de elevados padrões de comportamento; na liderança da organização e no apoio às políticas e programa de integridade; na viabilização de que os integrantes da instituição tenham competência necessária para o processo de implementação e para a difusão de conhecimentos; na inovação para lidar com as limitações de recursos, com novas ameaças e oportunidades; na inserção dos direitos dos titulares nos processos de tomada de decisão sobre tratamento de dados, com base em evidências e em gestão de riscos; na avaliação e na revisão dos atos normativos, pautando-se pelas boas práticas regulatórias e pela legitimidade; e no monitoramento do desempenho, dos resultados e do cumprimento de políticas e planos.

Como o EME é o controlador dos dados no âmbito do Comando do Exército, cabe a ele a análise do ambiente institucional e o envolvimento direto nas ações de governança, com o direcionamento estratégico dos seguintes tópicos:

a) Ações educacionais;
b) Processo de implementação;
c) Regras de tratamentos de dados;
d) Normatização dos processos;
e) Definição de atribuições, das políticas e planos;
f) Atribuição de responsabilidades;
g) Gestão de riscos;
h) Estabelecimento de controles;
i) Definição dos padrões de comportamento;
j) Coordenação e resolução de conflitos;
k) Gerenciamento de redes de comunicação;
l) Monitoramento da conformidade e da integridade.

Já o CPEx, estabelecido atualmente como operador, também possui a função de controlador em razão da desconcentração administrativa, o que viabiliza por ele a execução das mesmas ações de governança contidas no marco teórico de referência apresentado no capítulo anterior, apenas restringindo o escopo para o seu ambiente operacional. Nesse caso,

apenas algumas medidas ficariam prejudicadas, particularmente aquelas que extrapolam o escopo do ambiente operacional do processo de pagamento de pessoal, como na coordenação de medidas que envolvam o CPEx e o CDS, por exemplo. Entretanto, ainda assim considera-se viável que a implementação da LGPD no processo de pagamento de pessoal seja conduzida sob a liderança do próprio CPEx, o que melhoraria sobremaneira o atual *status* de adequação à lei sem a necessidade e dependência de ações governança do EME.

Nesse caso, para se evitar qualquer tipo de conflito interno de competências e de atribuições hierárquicas, é interessante que as ações executadas pelo CPEx para implementação das medidas sejam reportadas formalmente ao EME, para que ele também possa monitorar as atividades. Nesse reporte também pode constar uma solicitação de coordenação de medidas que extrapolam o escopo do processo de pagamento de pessoal, como aquelas que envolvam a participação de mais de um órgão, de forma a evitar que a implementação fique em parte prejudicada. Por fim, o reporte ao EME seria uma boa prática adotada nesse cenário e com possibilidade de replicação em outros processos de tratamento de dados dentro da própria instituição, que tenham particularidades como as do pagamento de pessoal.

6.3. As medidas de implementação adequadas

As medidas tidas como adequadas para a implementação da LGPD foram listadas a partir de sua identificação nas normativas legais, nos modelos teóricos, nas entrevistas realizadas e na observação direta dos processos do CPEx. Algumas se mostraram recorrentes ao longo do trabalho, enquanto outras foram desconsideradas por não serem muito adequadas ao setor público, de forma que, ao final, foi possível estabelecer um rol daquelas entendidas como essenciais para o sucesso do processo de implementação da LGPD.

Assim, para viabilizar a adequação dos processos CPEx à luz da LGPD, foi proposto um novo marco teórico normativo de referência para a implementação da lei no setor público, isto é, de forma mais genérica, para que ele também possa, dentro da conveniência e oportunidade, ser utilizado por outra instituição pública que necessite de um modelo teórico roteirizado para buscar a conformidade de seus processos de tratamento de dados.

A linguagem utilizada na descrição das medidas buscou a simplicidade e a generalidade, de forma a identificar objetivamente o que deve ser feito, para que qualquer indivíduo que tenha conhecimentos básicos sobre a LGPD possa compreender aquilo que deve ser executado. Essa abordagem é importante em função da multidisciplinaridade atinente

à lei, isto é, as várias áreas do conhecimento que ela aborda e, consequentemente, as diferentes áreas de formação dos recursos humanos envolvidos no processo de implementação. Assim, as medidas tornam-se compreensíveis para os elementos de uma equipe multidisciplinar voltada para a implementação da LGPD, evitando abordagens e termos técnicos que dificultariam sua interpretação e prejudicariam a fluidez dos trabalhos a serem executados.

Nesse modelo as medidas foram propostas de uma forma que possam servir também como um roteiro de atividades sequenciais, para facilitar o processo de implementação, mas sem a necessidade de obedecer a ordem sugerida, já que algumas medidas podem ter a viabilidade de execução simultânea por diferentes elementos/setores. A forma de roteiro de atividades serve também para que a instituição verifique item a item a real necessidade de implementação de cada uma das medidas, ou então que analise e ratifique/retifique a conformidade delas, de forma a se debruçar na implementação da medida subsequente.

As medidas serão citadas no quadro a seguir contendo detalhes importantes que foram colhidos durante o processo de pesquisa, com a identificação da área de conhecimento envolvida (ADM – administração; GOV – governança; TI – tecnologia da informação; JUR – jurídica):

Nº	MEDIDA DE IMPLEMENTAÇÃO DA LGPD	ÁREA
1	**Identificação de um núcleo de mudanças na instituição** - elemento ou equipe envolvidos ou não no tratamento de dados, que tenham conhecimento básico da estrutura da organização e que alertem para a necessidade de adequação à LGPD.	GOV
2	**Conscientização e envolvimento da Alta Administração** - planejamento de ações educacionais e de diretrizes *top-down* para o processo de implementação e de mudança da cultura organizacional.	GOV
3	**Difusão do conhecimento sobre a LGPD para os integrantes da instituição** - por meio de capacitação, treinamentos, palestras e atualizações; criação de um programa contínuo de ações educacionais para viabilizar uma mudança cultural no tratamento de dados, comparando, de forma concreta, as atividades executadas pela instituição com o cenário adequado de um ambiente de proteção de dados.	GOV
4	**Nomeação de um Comitê de Governança, Privacidade e Proteção de Dados Pessoais ou estrutura equivalente para deliberação sobre a implementação da LGPD e sobre assuntos relativos à proteção de dados e segurança da informação** - deverá conter elementos da Alta Administração, do setor jurídico, do setor de tratamento de dados, do setor de Tecnologia da Informação e de auditoria.	GOV

5	**Nomeação do encarregado/DPO** - elemento que possui a missão de ser o elemento de comunicação com os titulares, com o controlador e com a ANPD; não pode pertencer aos quadros de pessoal de unidades de Tecnologia da Informação nem ser gestor responsável por sistemas de informação, e deve impulsionar e coordenar ações e adotar medidas técnicas e organizacionais para buscar a conformidade da instituição.	GOV
6	**Nomeação da equipe multidisciplinar que trabalhará na implementação** - grupo que deverá congregar conhecimentos da área jurídica, de tecnologia da informação, de processos de tratamento de dados e de segurança da informação.	GOV
7	**Contratação de auditoria externa para avaliação dos processos de tratamento da instituição, da *compliance* e do *status* de adequação à LGPD** - é importante a divulgação prévia desse tipo de auditoria para que haja a colaboração dos integrantes da instituição por ocasião do fornecimento de informações à equipe responsável.	GOV
8	**Elaboração do Inventário de Dados Pessoais (IDP)** - máximo de informações sobre os dados existentes, seu ciclo de vida e sobre os processos de tratamento da instituição. O IDP conterá o mapeamento de dados e do seu ciclo de vida nos processos de tratamento existentes; mapeamento dos itens de segurança da informação existentes no processo de tratamento; mapeamento de contratos e de compartilhamentos e transferência de dados; mapeamento de *compliance*, controles internos e de riscos. Conterá também: • Atores envolvidos (agentes de tratamento e o encarregado); • Finalidade (o que a instituição faz com o dado pessoal); • Hipóteses; • Previsão legal; • Dados pessoais tratados pela instituição; • Categoria dos titulares dos dados pessoais; • Tempo de retenção dos dados pessoais; • Instituições com as quais os dados pessoais são compartilhados; • Transferência internacional de dados; • Medidas de segurança atualmente adotadas.	ADM JUR TI
9	**Identificação e avaliação de normativas legais correlatas aos processos de tratamento de dados na instituição** - descrição das particularidades dos processos de retenção e de arquivamento de dados, bem como do fornecimento de informações em detrimento da LAI e da Política de Dados Abertos (PDA). Deverá conter: • Atores envolvidos (agentes de arquivamento e responsáveis por atendimentos da LAI e da PDA); • Previsão legal; • Dados pessoais que são arquivados;	ADM JUR TI

	• Dados que podem conter nos atendimentos da LAI e PDA; • Tipos de arquivamento e locais utilizados, físicos e virtuais; • Tempo de arquivamento dos dados pessoais; • Elementos e instituições para quem os atendimentos da LAI e PDA são feitos; • Medidas de segurança adotadas para o arquivamento; • Controles de conformidade para avaliação das respostas dos atendimentos da LAI e PDA; • Informações sobre outras normativas legais correlatas ao processo de tratamento.	
10	**Apresentação do IDP e da avaliação das normativas legais correlatas ao processo de tratamento de dados ao Comitê de governança para avaliação das próximas etapas da implementação** - identificação dos setores que devem ser adaptados à LGPD; definição dos Controladores e do escopo de tratamento de cada um; definição dos Operadores e do escopo de tratamento de cada um; as hipóteses de tratamento, bases legais e finalidades; e definição do escopo do projeto de implementação do Programa de Privacidade.	GOV ADM JUR TI
11	**Elaboração do Planejamento Estratégico de implementação da LGPD-** • Avaliação do ambiente organizacional, dos possíveis cenários e dos resultados esperados; • Direcionamento estratégico do processo de implementação; • Direcionamento de objetivos organizacionais alinhados com os direitos dos titulares dos dados para alcançar os resultados pretendidos; • Direcionamento do gerenciamento de riscos estratégicos e de controles internos; • Direcionamento da preparação, da articulação e da coordenação de políticas e planos; • Viabilização do contínuo desenvolvimento de ações educacionais dos processos de capacitação de pessoal e de aplicação de tecnologia e segurança da informação; • Coordenação das atividades entre os diferentes órgãos e setores; • Estabelecimento de um calendário de implementação; • Definição e comunicação formal dos papéis e responsabilidades de forma a assegurar que sejam desempenhados de forma efetiva; • Promoção de valores de integridade e de elevados padrões de comportamento; • Implementação da transparência no processo de tratamento e compartilhamento dos dados, com prestação de informações aos titulares; • Viabilização do uso das ferramentas digitais para facilitar o exercício de direito dos titulares; • Direcionamento para a adequação da coleta e do	GOV ADM JUR TI

	armazenamento dos dados tratados. • Nomeação dos Controladores e Operadores. • Definição de ordens aos elementos subordinados para o processo de implementação.	
12	**Nomeação do Gestor de Segurança da Informação** - planejar, implementar e melhorar continuamente os controles de segurança da informação, o qual poderá ter o apoio de um Comitê de Segurança da Informação ou estrutura equivalente.	GOV
13	**Avaliação da implementação pelo setor de TI de segurança, infraestrutura e sistemas** – identificar as melhores medidas que podem ser adotadas para garantir a proteção dos dados e do processo de tratamento.	TI
14	**Nomeação da Equipe de Tratamento e Resposta a Incidentes Cibernéticos (ETIR)-** constituirá a rede de equipes, integrada pelos órgãos e pelas entidades da Administração Pública, coordenada pelo Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo do GSI/PR.	GOV TI
15	**Formalização de um instrumento de ajuste de conduta** – estabelecimento de termo entre o Controlador e o Operador (contrato, convênio) ou publicação de documento com atribuições de competência e responsabilidades entre instituições ligadas hierarquicamente (portaria, normativa, circular).	JUR ADM
16	**Divulgação do nome do encarregado/DPO e das formas de contato com ele em sítio eletrônico** –viabilizar canal para que tanto os titulares quanto a ANPD possam solicitar informações acerca do tratamento realizado.	GOV TI
17	**Disponibilização ao titular de informações para exercício de direito -** canal de fácil acesso, preferencialmente em sítio eletrônico, com a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução das atividades de tratamento, bem como com a metodologia utilizada para garantir a segurança das informações e os compartilhamentos efetuados.	GOV JUR
18	**Estabelecimento de um processo de atualização de informações ao titular**– forma de divulgação caso haja alguma alteração na finalidade, no tratamento dos dados ou a necessidade de um novo compartilhamento.	ADM TI
19	**Elaboração e divulgação interna dos procedimentos-padrão de tratamento de dados, das responsabilidades dos agentes de tratamento, da finalidade e dos objetivos do tratamento** - bases legais, do tempo de duração do tratamento, da natureza dos dados pessoais e da correlação com outras normativas sobre tratamento a depender do contexto e das peculiaridades da instituição e do escopo definido pelo controlador.	GOV ADM
20	**Elaboração e divulgação de Código de Conduta da instituição com os fundamentos e princípios legais atinentes aos processos de tratamento de dados** - reger as atividades e o comportamento tanto dos integrantes da	GOV ADM

	instituição quanto dos elementos externos, fornecedores e prestadores de serviços.	
21	**Inserção dos riscos envolvendo os tratamentos de dados na Política de Gestão de Riscos da organização, com matriz de *compliance* e riscos legais à proteção de dados** - identificar lacunas de segurança da informação e de privacidade no tratamento de dados nos sistemas, contratos e processos da instituição.	ADM JUR
22	**Elaboração da Política de Segurança da Informação (PSI)**- implementada a partir da formalização e aprovação por parte da autoridade máxima da instituição, contendo regramentos descritos em documentos de acordo com as particularidades de cada instituição: • Visão geral de como a organização lida com dados pessoais, com definição de responsabilidades e com compromisso com a privacidade; • Política para o Encarregado de Dados (finalidade, responsabilidade e funções); • Política de tratamento de dados pessoais (orientações sobre como efetuar o tratamento de dados); • Política para exercício de direitos do titular (pedido de informações, correções de dados, restrição de tratamento, eliminação de dados, portabilidade de dados, revisão de decisão automatizada, recepção de solicitação, identificação do titular, execução da solicitação, resposta ao titular, monitoramento e registro); • Política de gestão de incidentes de privacidade (fluxos de trabalho e ferramentas para agir em incidentes); • Política para dados sensíveis (caso existam dados sensíveis); • Política de consentimento (orientações sobre obtenção, armazenamento e revogação do consentimento); • Política de legítimo interesse; • Política de retenção de dados (padrões e prazos para o armazenamento de dados); • Política de dados pessoais e de cookies na Internet; • Política de *Privacyby Design* (para novos fluxos e processos de tratamento); • Política de avaliação e monitoramento da gestão de privacidade (define responsabilidades, períodos de avaliação, orientações para produção do Relatório de Impacto de Dados – RIPD); • Política de treinamento e conscientização; • Avisos de privacidade aos titulares, aos integrantes da instituição e aos elementos externos; • Política de compartilhamento e transferência de dados.	ADM TI
23	**Formalização de um instrumento de ajuste de conduta (contrato, convênio, portaria, normativa, circular) em caso de compartilhamento e transferência de dados com outras instituições, ou adequação dos**	ADM JUR

	instrumentos já existentes - estabelecer as condições e instruções para o tratamento e compartilhamento; as medidas de segurança, técnicas e administrativas utilizadas para preservar os dados pessoais em incidentes de segurança; a necessidade de eliminação após o tratamento ou da possibilidade de conservação dos dados; as possíveis atualizações normativas e as responsabilidades dos agentes envolvidos.	
24	**Estabelecimento do processo de obtenção do consentimento e de guarda de provas** - dar amparo ao tratamento efetuado pela instituição, caso seja necessário.	ADM JUR TI
25	**Elaboração do Relatório de Impacto à Proteção de Dados Pessoais (RIPD) -** atender ao princípio da responsabilização e de prestação de contas; apesar de não ser obrigatório para todas as instituições, ele é importante para a avaliação dos riscos nas operações de tratamento, do uso e compartilhamento de dados pessoais e das medidas para mitigação dos riscos que possam afetar as liberdades e os direitos dos titulares dos dados. O relatório deverá conter, no mínimo: • Descrição dos dados coletados; • Metodologia utilizada para a coleta e para a garantia da segurança das informações; • Identificação dos agentes de tratamento e do encarregado; • Identificação das partes interessadas; • Descrição do tratamento; • Descrição da necessidade e da proporcionalidade do tratamento; • Identificação dos riscos de todo o ciclo de vida dos dados e dos processos de tratamento; • Análise das medidas, salvaguardas e mecanismos de mitigação de risco adotados; • Viabilização da implementação de medidas necessárias; • Revisão e avaliação da conformidade nos processos de tratamento de dados.	GOV ADM JUR TI
26	**Elaboração do Termo de Uso** - informar as regras que o usuário está sujeito ao utilizar o serviço; documento utilizado para fornecer uma descrição detalhada do tratamento, das condições e das regras definidas pelo controlador de forma unilateral, devendo conter tópicos sobre: • Descrição dos serviços; • Aceitação dos termos e da política de privacidade; • Definições; • Arcabouço legal; • Descrição do serviço; • Direitos do usuário; • Responsabilidades do usuário e da Administração Pública; • Mudanças no termo de uso; • Informações para contato e foro.	GOV ADM JUR TI

27	**Elaboração da Política de Privacidade** - documento que compõe o Termo de Uso e que objetiva informar ao titular como é fornecida a privacidade necessária para que a confidencialidade dos dados seja garantida de forma eficiente. Deve conter tópicos sobre: • Objetivos, regras, obrigações, restrições e/ou controles para satisfazer os requisitos de privacidade relacionados ao processamento de dados pessoais realizado; • Controlador; • Operador; • Encarregado; • Dados tratados; • Forma de coleta dos dados; • Tratamento realizado, sua finalidade e por quanto tempo; • Compartilhamento de dados; • Segurança dos dados; • Política de cookies; • Tratamento posterior dos dados para outras finalidades.	GOV ADM JUR TI
28	**Elaboração de um plano de resposta a incidentes de segurança da informação**- voltado para os requisitos estabelecidos na LGPD, contendo as ações a serem tomadas e os elementos envolvidos.	TI
29	**Estabelecimento de um processo de reparação de danos**– processo para retificação de problemas causados em razão do tratamento ou por violação à legislação.	ADM JUR
30	**Estabelecimento de fluxo de comunicação interna e externa** - divulgar informações e atender demandas oriundas da ANPD, do titular do dado e de planos de resposta a incidentes e remediação.	ADM TI
31	**Monitoramento, registro e auditoria das ações de tratamento de dados**- por meio de um *software* de auditoria para facilitar o processo (implementação de ferramenta de registro de dados e de extração de informações).	ADM TI
32	**Consolidação formal de um Programa de Governança em Privacidade (PGP) -**especificação das políticas e práticas para proteger a privacidade do titular, para a adequação dos processos de tratamento e para evitar o vazamento de dados, contendo: • Análise de maturidade (diagnóstico do estágio de adequação à LGPD); • Análise e adoção de medidas e diretrizes de segurança; • Instituição de estrutura organizacional para governança e gestão da proteção dos dados; • IDP; • Levantamento e adequação de contratos; • Políticas e práticas para proteção da privacidade; • Viabilização de uma cultura de segurança e proteção; • RIPD; • Política de privacidade e Política de Segurança da	GOV ADM JUR TI

	Informação; • Termo de Uso; • Estabelecimento de indicadores de performance; • Gestão de incidentes; • Análise de resultados; • Reporte de resultados para a Alta Administração por meio da produção de documentos como: registros de auditoria; relação de riscos de falha de atendimento de requisitos avaliados e tratados; descrição de controles de riscos implantados; documentos de suporte à operação e tomada de decisões; bases de dados de controle das operações de segurança; relatórios de auditorias realizadas com a relação de não conformidades encontradas; relatórios e materiais de divulgação de cibersegurança.	
33	**Conscientização e envolvimento dos integrantes da instituição**- buscar a colaboração na melhoria dos processos de tratamento por meio de sugestões *bottom-up,* utilizando os conhecimentos e melhorias oriundas dos escalões mais baixos de tratamento de dados, a partir do momento em que eles estiverem capacitados na LGPD.	GOV ADM
34	**Estabelecimento de pontos de controle para manutenção da *compliance*** – processo de avaliação constante do tratamento de dados por meio de controles, particularmente pelo setor jurídico, para perfeita conformidade entre as ações e o regramento normativo.	ADM
35	**Revisão periódica dos pilares do programa de *compliance* e da documentação envolvendo o tratamento de dados pessoais** – observação e atualização dos processos e documentos internos em função de mudanças na legislação de tratamento de dados.	GOV ADM JUR TI

Quadro 7: Medidas para implementação da LGPD
Fonte: Elaboração própria.

Após observar as medidas do quadro anterior, a instituição pode decidir a melhor forma de como proceder com a implementação do roteiro sugerido. Ela pode iniciar pelos processos que apresentem o maior risco, de acordo com o que foi levantado no mapeamento e no plano de gestão de riscos da instituição; pode separar as medidas pela área do conhecimento envolvida; pode ainda executar os requisitos que tiverem melhores condições de serem implementados, ou da maneira como o roteiro melhor se enquadrar no contexto da instituição.

Nesse sentido, a liberdade de execução do roteiro de implementação sugerido está direcionada para sequenciamento de ações com uma ordenação lógica, facilitando o planejamento dos gestores e proporcionando autonomia na divisão e na execução das atividades, sem pretender estabelecer um procedimento rígido de implementação. Ademais,

destaca-se que o objetivo maior do processo de implementação é fazer com que a instituição se aproxime ao máximo da conformidade com a lei, cenário este que o roteiro pode proporcionar na medida em que apresenta a ela um caminho orientado a ser seguido.

6.4. Apontamentos finais

Ao longo do estudo feito no presente trabalho, foram identificadas três medidas importantes para o processo de adequação à LGPD em uma instituição: o envolvimento da governança da Alta Administração, as ações educacionais e a atuação de uma equipe multidisciplinar na implementação. Tais medidas foram reiteradamente observadas, sendo citadas no texto da própria lei, nos normativos estudados, em todos os modelos teóricos avaliados e também nas entrevistas com os gestores. Assim, dada à recorrência com que foram observadas, e particularmente pela fala dos gestores nas entrevistas, foi possível delinear uma fundamentação para elas se tornassem bases estruturantes para o processo de implementação da lei

A primeira base, a governança da Alta Administração, é a grande força motriz do processo de implementação na instituição, devendo estar comprometida com o alcance dos objetivos estabelecidos. As medidas propostas para a adequação à LGPD necessitam ser conduzidas por ela, fato este ressaltado pela experiência na prática dos gestores entrevistados, os quais observaram que a efetividade da implementação vai depender do envolvimento direto da Alta Administração e de suas intervenções *top-down*.

Já as ações educacionais, a segunda base, são também de grande relevância para todo processo de implementação, visto que a confecção de todo um rol procedimental e normativo interno de nada serve se não houver a absorção e o entendimento das informações por parte dos integrantes da instituição. Isso pode ser proporcionado por meio da capacitação e da educação dos recursos humanos, inserindo na cultura organizacional novos conhecimentos e novos comportamentos. Nesse sentido, a capacitação e a conscientização de recursos humanos aparentam ser essenciais na implementação da LGPD, tanto nas atividades relacionadas ao tratamento e à privacidade de dados quanto nos processos de segurança da informação, viabilizando ao final o estabelecimento de um Programa de Governança e Privacidade (PGP) em toda a instituição.

A terceira base, a utilização de equipes multidisciplinares no processo de implementação, é necessária em função de que a própria LGPD aborda em seu texto diferentes áreas do conhecimento, que acabam envolvendo diversos setores de uma instituição,

como o jurídico, o de administração, de gerenciamento de processos/projetos, de gestão de riscos, de tecnologia e de segurança da informação, todos unidos e relacionados por meio da governança da Alta Administração. Por esse motivo é interessante que o processo de implementação seja conduzido por uma equipe multidisciplinar, que terá condições de avaliar sucintamente os aspectos atinentes a cada setor, bem como somar conhecimentos para a particularização das medidas ao contexto organizacional.

Assim, é possível inferir que essas três bases estruturantes proporcionariam uma melhoria no *status* de adequação à lei, o que levaria a afirmar que elas representam os fatores críticos de sucesso para que uma instituição pública possa implementar a LGPD. Com elas, mesmo que o processo seja demorado, poderão ser plantadas bases para uma mudança de comportamento dos integrantes de uma instituição e para a adequação dos processos de tratamento de dados, o que acarretaria, de uma forma ou de outra, em uma melhoria na conformidade da organização.

A partir dessas três medidas tidas como bases estruturantes, foi proposto um novo modelo teórico roteirizado para o processo de implementação da LGPD no CPEx, de forma a guiar as ações dos gestores com organização e sequenciamento, em um processo gradual de mudança que viabilizaria a construção de uma nova cultura de proteção de dados com bases mais sólidas.

Cabe ressaltar que as medidas propostas do novo modelo teórico podem ser implementadas gradualmente na organização, por etapas, de forma que possa ser construído um novo ambiente de proteção de dados por meio do PGP e que envolva os integrantes da instituição. Com isso, viabilizaria uma mudança na cultura organizacional conforme os conhecimentos e informações sobre a lei forem sendo incorporados pelos integrantes da instituição por meio das ações educacionais, o que consequentemente incentivaria a adoção de medidas de adequação impulsionadas pela governança da Alta Administração.

Em um outro viés, devem-se observar também as medidas particularizadas aos processos de tratamento do CPEx, como a necessidade de armazenamento de dados e o arquivamento das informações, conforme prazos estabelecidos nas tabelas de temporalidade envolvendo dados de pagamento de pessoal militar. As normativas sobre retenção e arquivamento não podem ser consideradas como contrárias às medidas de eliminação ou anonimização dos dados, mas sim como regras internas que devem ser harmonizadas com os demais mandamentos da LGPD, buscando a conformidade por meio da integração das normativas correlatas nos processos de tratamento de dados. Assim, a equipe multidisciplinar de implementação necessitaria estabelecer a complementaridade das medidas da LGPD com

as normativas de retenção e arquivamento de informações, bem como com outras que porventura existirem, em uma sinergia que tenha como foco a proteção de dados e a conformidade legal.

Sobre a obrigatoriedade de divulgação de determinadas informações dos titulares por meio da Lei de Acesso à Informação (LAI) e da Política de Dados Abertos (PDA), cabe ressaltar que tais dados devem também ser protegidos e que não podem ser utilizados para uma finalidade diversa. Assim, o CPEx não pode compartilhar informações com terceiros com a alegação de que elas já possuem publicidade por meio do portal da transparência ou por meio de alguma solicitação com base na LAI. O compartilhamento dessas informações com as instituições governamentais é justificado por força da legislação, mas não mais o será se o compartilhamento for com terceiros para outro fim.

Além de medidas pontuais de adequação, existem tarefas que necessitam observação contínua como: atualização de documentos e políticas de tratamento; atualização das regras de arquivamento das informações; avaliação de novos processos no desenvolvimento de seus sistemas e serviços; implementação de novas medidas de segurança da informação; renovação da comunicação aos titulares sobre alterações na finalidade ou nas operações de tratamento; e sobre um novo compartilhamento/transferência de dados com outra instituição.

Observando o que foi exposto, o CPEx, de posse do modelo teórico de implementação proposto, utilizando suas ferramentas dentro de um ambiente que já possui uma cultura de proteção de dados, teria condições de atingir a plena conformidade do processo de pagamento de pessoal, executando as medidas na função de controlador, ou mantendo sua condição de operador e viabilizando a implementação das medidas que forem adequadas a esse contexto.

Assim, ao utilizar o modelo proposto, seja como controlador ou como operador, o *status* de adequação do Centro de Pagamento do Exército estaria em constante elevação, dado que a execução das próprias medidas realimenta todo o processo em um ciclo de constante aprimoramento, proporcionando proteção aos dados dos titulares e à própria instituição Exército Brasileiro. A possibilidade de utilização do modelo é também uma forma de mitigação de riscos, visto que atualmente o processo de pagamento de pessoal não atende aos requisitos da LGPD, o que pode acarretar em auditoria e autuação da ANPD.

Por fim, é importante ressaltar que a proposta apresentada também poderia ser utilizada como um modelo teórico voltado para implementação da LGPD em outras instituições no setor público, pois, como citado, a grande maioria dos modelos teóricos encontrados são voltados para a iniciativa privada. Tal utilização pode ser entendida como uma possível extensão do presente trabalho, em que poderia ser avaliada a aplicação do

modelo de implementação proposto para análise futura de sua efetividade e também para o seu aperfeiçoamento.

REFERÊNCIAS

AGUILERA, Daniel Fortes; DI BIASE, Nicholas Furlan. **Dificuldades interpretativas no regime de tratamento de dados pelo poder público: Lacunas, contradições e técnicas na LGPD**. Revista Eletrônica da Procuradoria Geral do Estado do Rio de Janeiro - PGE-RJ, Rio de Janeiro, v. 4, n. 2, maio/ago. 2021. Disponível em: <https://revistaeletronica.pge.rj.gov.br/index.php/pge/article/view/238>. Acessso em: 13/01/23.

AGUILERA-FERNANDES, Edson. et al. **Lei Geral de Proteção de Dados Pessoais (LGPD): guia de implantação**. Editora Edgard Blücher Ltda. São Paulo – SP. 2020.

ALMEIDA, Bethania de Araújo et al. **Preservação da privacidade no enfrentamento da COVID-19: dados pessoais e a pandemia global. 2020**. Ciência e Saúde Coletiva 25. 2487-2492. Disponível em: <https://www.scielo.br/j/csc/a/T6rwdhnTNzp5vYr84w9xthB/?lang=pt>. Acesso em: 15/10/22.

BRASIL. Casa Civil da Presidência da República. **Guia da Política de Governança Pública**. 2018a. Disponível em: <https://www.gov.br/casacivil/pt-br/centrais-de-conteudo/downloads/guia-da-politica-de-governanca-publica>. Acesso em: 10 junho 2021.

_____. Lei nº 13.709, de 14 de agosto de 2018. **Lei geral de proteção de dados pessoais (LGPD).** 2018b. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: 10 junho 2021.

_____. **Lei nº 13.726, de 8 de outubro de 2018**. Racionaliza atos e procedimentos administrativos dos Poderes da União, dos Estados, do Distrito Federal e dos Municípios e institui o Selo de Desburocratização e Simplificação. 2018c. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13726.htm>. Acesso em: 20 junho 2021.

_____. Autoridade Nacional de Proteção de Dados. **Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado**. 2022a. Disponível em: <https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia_agentes_de_tratamento_e_encarregado___defeso_eleitoral.pdf>. Acesso em 26/01/23.

_____. Ministério da Economia. Secretaria Especial de Desburocratização, Gestão e Governo Digital. **Guia de Elaboração de Programa de Governança em Privacidade**. 2020a. Disponível em: <https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/ppsi/guia_programa_governanca_privacidade.pdf>. Acesso em 16/05/22.

_____. Ministério da Economia. Secretaria Especial de Desburocratização, Gestão e Governo Digital. **Guia de Avaliação de Riscos de Segurança e Privacidade. Lei Geral de Proteção de Dados Pessoais**. 2020b. Disponível em: <https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_avaliacao_riscos.pdf/view>. Acesso em 16/05/22.

_____. Autoridade Nacional de Proteção de Dados (ANPD). **Guia Orientativo de Tratamento de Dados Pessoais pelo Poder Público.** 2022b. Disponível em:

<https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-poder-publico-anpd-versao-final.pdf>. Acesso em 16/05/22.

_____. Comitê Central de Governança de Dados. **Guia de Boas Práticas para Implementação na Administração Pública Federal. Lei Geral de Proteção de Dados (LGPD).** 2020c. Disponível em: <https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_lgpd.pdf>. Acesso em 03/04/22.

_____. Secretaria Especial de Desburocratização, Gestão e Governo Digital. **Guia de Elaboração de Inventário de Dados Pessoais. Lei Geral de Proteção de Dados Pessoais**. 2021a. Disponível em: < https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/ppsi/guia_inventario_dados_pessoais.pdf >. Acesso em 16/05/22.

_____. Secretaria Especial de Desburocratização, Gestão e Governo Digital. **Programa de Privacidade e Segurança da Informação (PPSI). Guia do Framework de Privacidade e Segurança da Informação.** 2022c. Disponível em: <https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/ppsi/guia_framework_psi.pdf >. Acesso em 10/12/22.

_____. Autoridade Nacional de Proteção de Dados. **Guia orientativo sobre segurança da informação para agentes de tratamento de pequeno porte. Lei Geral de Proteção de Dados Pessoais.** 2021c. Disponível em: <https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-vf.pdf >. Acesso em 16/05/22.

_____. Autoridade Nacional de Proteção de Dados; Secretaria Nacional do Consumidor. **Como proteger seus dados pessoais: Guia do Núcleo de Proteção de Dados do Conselho Nacional de Defesa do Consumidor em parceria com a ANPD e a SENACON. Lei Geral de Proteção de Dados Pessoais**. 2022d. Disponível em: <https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/arquivos-de-documentos-de-publicacoes/guia-do-consumidor_como-proteger-seus-dados-pessoais-final.pdf>. Acesso em 10/12/22.

_____. Autoridade Nacional de Proteção de Dados. **Guia orientativo de Cookies e proteção de dados pessoais.** 2022e. Disponível em: <https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-orientativo-cookies-e-protecao-de-dados-pessoais.pdf>. Acesso em 16/05/22.

_____. Presidência da República. Gabinete de Segurança Institucional**. Instrução Normativa nº 1, de 27 de Maio de 2020.** Dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal. 2020d. Disponível em: <https://www.in.gov.br/en/web/dou/-/instrucao-normativa-n-1-de-27-de-maio-de-2020-258915215>. Acesso em 16/05/22.

_____. Ministério da Economia. Secretaria Especial de Desburocratização, Gestão e Governo Digital. **Guia de elaboração de Termo de Uso e Política de Privacidade para serviços públicos.** 2022f. Disponível em: <https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/ppsi/guia_termo_uso_politica_privacidade.pdf>. Acesso em 16/05/22.

_____. Ministério da Economia. Secretaria Especial de Desburocratização, Gestão e Governo Digital. **Guia de resposta a incidentes de segurança.** 2021d. Disponível em: <

https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/ppsi/guia_resposta_incidentes.pdf >. Acesso em 16/05/22.

_____. Ministério da Economia. Secretaria Especial de Desburocratização, Gestão e Governo Digital. **Oficina dirigida sobre a elaboração do Relatório de Impacto de Proteção de Dados. Lei Geral de Proteção de Dados Pessoais (LGPD).** 2020e. Disponível em: <https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/apresentacoes/apresentacao_ripd.pdf>. Acesso em: 15/02/23.

_____. **Decreto nº 9.203, de 22 de novembro de 2017**. Dispõe sobre a política de governança da administração pública federal direta, autárquica e fundacional. 2017a. Disponível em <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2017/decreto/d9203.htm>. Acesso em: 03/12/21.

_____. **Portaria - C Ex n º 987, de 18 de setembro de 2020.** Institui a Política de Governança do Exército Brasileiro (EB10-P-01.007). 2020f. Disponível em < http://www.sgex.eb.mil.br/sg8/006_outras_publicacoes/05_politicas/port_n_987_cmdo_eb_18set2020.html>. Acesso em: 03/12/21.

_____. **Portaria nº 856, de 12 de junho de 2019**. Aprova a Política de Informação do Exército. 2019a. Disponível em: <http://www.sgex.eb.mil.br/sg8/006_outras_publicacoes/05_politicas/port_n_856_cmdo_eb_12jun2019.html>. Acesso em: 13/06/23.

_____. Tribunal de Contas da União. **Governança Pública.** Brasília, 2014a. Disponível em: <http://portal.tcu.gov.br/biblioteca-digital>. Acesso em: 25/04/2022.

_____. Tribunal de Contas da União. **Perfil integrado de governança pública e governança e gestão de pessoas, tecnologia da informação e contratações, das organizações da administração pública federal.** Brasília, 2018d. Disponível em: < https://portal.tcu.gov.br/governanca/governancapublica/organizacional/levantamento-de-governanca/levantamento-de-governanca.htm >. Acesso em: 25/04/2022

_____. Tribunal de Contas da União. **Referencial básico de governança aplicável a organizações públicas e outros entes jurisdicionados ao TCU.** Secretaria de Controle Externo da Administração do Estado – Secex Administração, Edição 3. Brasília, 2020g. Disponível em: < https://portal.tcu.gov.br/lumis/portal/file/fileDownload.jsp?fileId=8A81881F7595543501762EB92E957799 >. Acesso em: 10/03/2022.

_____. **Decreto nº 86.979, de 3 de março de 1982.** Cria a Diretoria de Auditoria no Ministério do Exército, as Inspetorias de Contabilidade e Finanças, o Centro de Pagamento do Exército, e dá outras providências. Disponível em: <https://www2.camara.leg.br/legin/fed/decret/1980-1987/decreto-86979-3-marco-1982-436515-publicacaooriginal-1-pe.html>. Acesso em: 08/09/22.

_____. **Decreto nº 7.845, de 14 de novembro de 2012.** Regulamenta procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo, e dispõe sobre o Núcleo de Segurança e Credenciamento. 2012a. Brasília, DF: Diário Oficial da União, 16 nov. 2012. Seção 1. Disponível em:

<http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/Decreto/D7845.htm>. Acesso em: 13/01/23.

_____. **Decreto no 8.777, de 11 de maio de 2016.** Institui a Política de Dados Abertos do Poder Executivo federal. Brasília, DF. 2016. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/d8777.htm>. Acesso em: 13/01/23.

_____. **Decreto nº 7.724, de 16 de maio de 2012.** Regulamenta a Lei nº 12.527, de 18 de novembro de 2011, que dispõe sobre o acesso a informações previsto no inciso XXXIII do caput do art. 5º , no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição.2012b. Brasília, DF. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/decreto/d7724.htm>. Acesso em: 13/01/23.

_____. **Decreto nº 4.073, de 3 de janeiro de 2002**. Regulamenta a Lei no 8.159, de 8 de janeiro de 1991. Dispõe sobre a política nacional de arquivos públicos e privados. 2002. Brasília, DF. Disponível em: <https://www.planalto.gov.br/ccivil_03/decreto/2002/d4073.htm>. Acesso em: 13/01/23.

_____. **Decreto nº 4.915, de 12 de dezembro de 2003**. Dispõe sobre o Sistema de Gestão de Documentos e Arquivos da Administração Pública Federal. 2003. Brasília, DF. Disponível em: <https://www.planalto.gov.br/ccivil_03/decreto/2003/d4915.htm>. Acesso em: 13/01/23.

_____. Gabinete de Segurança Institucional da Presidência da República. **Padrões Mínimos de Segurança da Informação e Comunicações para os Sistemas Estruturantes da Administração Pública Federal** - NC19/IN01/DSIC/GSIPR de 15 JUL 14C. 2014b. Norma complementar. Disponível em: <https://datasus.saude.gov.br/wp-content/uploads/2019/08/Norma-Complementar-n%C2%BA-19IN01DSICGSIPR.pdf >. Acesso em: 13/01/23.

_____. **Instruções de Preenchimento da "Listagem de Eliminação de Documentos" pelos Órgãos e Entidades Integrantes do Sistema de Gestão de Documentos de Arquivo (SIGA)**, de 16 de janeiro de 2015. Conselho Nacional de Arquivos – CONARQ. 2015. Disponível em: <http://www.ahex.eb.mil.br/docs/dgad/Legislacoes-Basicas-sobre-Eliminacao-de-Documentos/1-instrucoes-preenchimento-listagem-eliminacao-SIGA.pdf>. Acesso em: 13/01/23.

_____. **Lei nº 12.527, de 18 de novembro de 2011**. Lei de Acesso à Informação – LAI, Regula o acesso a informações previsto no inciso XXXIII do art. 5º , no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. Brasília, DF. 2011. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm>. Acesso em: 13/01/23.

_____. **Lei nº 8.159, de 8 de janeiro de 1991**. Dispõe sobre a política nacional de arquivos públicos e privados. Brasília, DF. Disponível em: <https://www.planalto.gov.br/ccivil_03/leis/l8159.htm >. Acesso em: 13/01/23.

_____. Controladoria-Geral da União. Secretaria de Transparência e Prevenção da Corrupção. **Manual de Elaboração de Planos de Dados Abertos da CGU**. 2020h. Brasília, DF. Disponível em: <https://www.gov.br/cgu/pt-br/centrais-de-conteudo/publicacoes/transparencia-publica/arquivos/manual-pda.pdf>. Acesso em: 13/01/23.

_____. Ministério da Transparência e Controladoria-geral da União. Secretaria Federal de Controle Interno. **Manual de orientações técnicas da atividade de auditoria interna governamental do poder executivo federal: Glossário**. Brasília: CGU, 2017b. p. 142. Disponível em: <https://www.gov.br/cgu/pt-br/centrais-de-conteudo/publicacoes/auditoria-e-fiscalizacao/arquivos/manual-de-orientacoes-tecnicas-1.pdf>. Acesso em: 13/01/23.

_____. **Nota Informativa CPEx 006/2023 – Consignações**. Regular os procedimentos e divulgar informações envolvendo descontos autorizados em contracheque (consignações), orientando Unidades Gestoras (UG) pagadoras, Entidades Consignatárias (EC) e militares e pensionistas vinculados ao Comando do Exército. 2023a. Disponível em: <https://cpex.eb.mil.br/categorias/154-consignacoes/69-legislacao-sobre-consignacao>. Acesso em: 15/01/23.

_____. **Política de Privacidade dos Dados do CPEx**. 2023b.

_____. **Portaria SEF/C Ex nº 149, de 16 de agosto de 2021**. Aprova o Regimento Interno do Centro de Pagamento do Exército. 2021e. Disponível em: <http://www.sgex.eb.mil.br/sg8/001_estatuto_regulamentos_regimentos/03_regimentos/port_n_149_sef_16ago2021.html>. Acesso em: 15/01/23.

_____. **Portaria 1.271-C Ex, de 13 de agosto de 2018**. Aprova as Instruções Gerais para Consignação de Descontos em Folha de Pagamento (EB10-IG08.002), 2ª Edição. 2018e.Disponível em: <https://cpex.eb.mil.br/categorias/154-consignacoes/69-legislacao-sobre-consignacao>. Acesso em: 15/01/23.

_____. **Portaria 124-SEF, de 20 de fevereiro de 2019**. Aprova as Instruções Reguladoras para Consignação de Descontos em Folha de Pagamento (EB90-IR02.001). 2019b.Disponível em: <https://cpex.eb.mil.br/categorias/154-consignacoes/69-legislacao-sobre-consignacao>. Acesso em: 15/01/23.

_____. **Portaria nº 1.350, de 29 de agosto de 2019**. Aprova a Diretriz Estratégica Organizadora do Sistema de Informação do Exército. 2019c. Disponível em: < http://www.sgex.eb.mil.br/sg8/006_outras_publicacoes/01_diretrizes/01_comando_do_exercito/port_n_1350_cmdo_eb_29ago2019.html>. Acesso em: 15/05/23.

_____. **Portaria – C Ex n° 1878, de 30 de novembro de 2022**. Aprova a Política de Gestão Documental do Exército Brasileiro. 2022g. Disponível em: <http://www.sgex.eb.mil.br/sg8/006_outras_publicacoes/05_politicas/port_n_1878_cmdo_eb_30nov2022.html>. Acesso em: 15/01/23.

_____. **Portaria - EME/C Ex nº 360, de 31 de março de 2021**. Aprova o Plano de Dados Abertos do Exército Brasileiro para o exercício 2021/2022. 2021f. Disponível em: <http://www.sgex.eb.mil.br/sg8/006_outras_publicacoes/04_planos/port_n_360_eme_31mar2021.html>. Acesso em: 15/01/23.

_____. **Portaria Normativa nº 1.235/MD, de 11 de maio de 2012**. Estabelece normas para o funcionamento e a tramitação de demandas do Sistema de Informações ao Cidadão no âmbito da administração central do Ministério da Defesa (SIC-MD). 2012c. Disponível em: <https://www.gov.br/defesa/pt-br/arquivos/lai/sobre_a_LAI/pn1235.pdf >. Acesso em: 15/01/23.

_____. **Portaria Normativa nº 2.975/MD, de 24 de outubro de 2013**. Disciplina no âmbito do Ministério da Defesa, os procedimentos de lavratura do Termo de Classificação de Informação (TCI). Disponível em: <https://www.gov.br/defesa/pt-br/arquivos/lai/sobre_a_LAI/porta_normativaa_2975a_24102013.pdf>. Acesso em: 15/01/23.

_____. **Portaria nº 088 - EME, de 7 de maio de 2020**. Aprova a Diretriz de Orientação para Aplicação da Lei Geral de Proteção de Dados Pessoais no Exército Brasileiro. 2020i. Disponível em: <http://www.sgex.eb.mil.br/sg8/006_outras_publicacoes/01_diretrizes/04_estado-maior_do_exercito/port_n_088_eme_07maio2020.html>. Acesso em: 15/01/23.

_____. **Relatório sobre a Lei Geral de Proteção de Dados no CPEx**. 2020j.

_____. Arquivo Nacional. **Código de classificação e tabela de temporalidade e destinação de documentos relativos às atividades-meio do Poder Executivo Federal**. Rio de Janeiro, 2020k. Disponível em: <https://www.gov.br/arquivonacional/pt-br/centrais-de-conteudo-old/cod-classif-e-tab-temp-2019-m-book-digital-25jun2020-1-pdf/view>. Acesso em: 15/01/23.

_____. **Resolução nº 40, de 9 de dezembro de 2014**. Conselho Nacional de Arquivos - CONARQ. Dispõe sobre os procedimentos para a eliminação de documentos no âmbito dos órgãos e entidades integrantes do Sistema Nacional de Arquivos (SINAR). 2014c. Disponível em: <https://www.gov.br/conarq/pt-br/legislacao-arquivistica/resolucoes-do-conarq/resolucao-no-40-de-9-de-dezembro-de-2014-alterada >. Acesso em: 15/01/23.

CARIO, S. A. F.; DIAS, T.; **Governança pública: ensaiando uma concepção**. Revista Contabilidade, Gestão e Governança, v. 17, nº 3, pág. 89-108. 2014.

CAVALCANTE, P. **Gestão pública contemporânea: do movimento gerencialista ao pós-NPM**. Brasília: Ipea, 2017. Disponível em: < https://repositorio.ipea.gov.br/bitstream/11058/8027/1/td_2319.pdf >. Acesso em: 02/04/22.

CIERCO, Agliberto; MENDES, João Ricardo B.; SANTANA, Priscila. **Privacidade Ágil: implantação da LGPD de forma ágil**. Editora Brasport, 1ª Edição. Rio de Janeiro – RJ. 2022.

COIMBRA, Marcelo de A.; MANZI, Vanessa A. **Manual de *compliance*: preservando a boa governança e a integridade das organizações.** São Paulo: Atlas, 2010. Disponível em: <https://books.google.com.br/books/about/MANUAL_DE_*COMPLIANCE*_PRESERVANDO_A_BOA.html?id=9DE3SgAACAAJ&redir_esc=y>. Acesso em: 08/01/23.

DIAS, Jorge Alves. **O que esperar do poder público com a LGPD? Comentários à Lei Geral de Proteção de Dados**. Comissão de Direito Digital, Tecnologia e Inteligência Artificial. OAB-SP 116ª Subseção Jabaquara – Saúde. São Paulo. 2020. Disponível em:

<https://www.passeidireto.com/arquivo/80538589/comentarios-a-lei-geral-de-protecao-de-dados-oab-sao-paulo-2020>. Acesso em: 15/10/22.

DONDA, Daniel. **Guia prático de implementação da LGPD: tudo o que sua empresa precisa saber para estar em conformidade.** São Paulo – SP. Editora Labrador, 2020.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais: fundamentos da lei geral de proteção de dados.** Thomson Reuters Revista dos Tribunais. 2ª Edição. São Paulo – SP. 2020. Disponível em: <https://www.lexml.gov.br/urn/urn:lex:br:rede.virtual.bibliotecas:livro:2020;001161708>. Acesso em: 15/10/22.

GUERRA, Sérgio. **Discricionariedade, regulação e reflexividade: uma nova teoria sobre as escolhas administrativas**. Belo Horizonte: Fórum, 2013.

HANG, Cristina; KAUNERT, Jane. **Dos agentes de tratamento de dados. Comentários à Lei Geral de Proteção de Dados**. Comissão de Direito Digital, Tecnologia e Inteligência Artificial. OAB-SP 116ª Subseção Jabaquara – Saúde. São Paulo. 2020. Disponível em: <https://www.passeidireto.com/arquivo/80538589/comentarios-a-lei-geral-de-protecao-de-dados-oab-sao-paulo-2020>. Acesso em: 15/10/22.

HENDERSON, Deborah. **DAMA-DMBOK. Data Management Body of Knowledge.Technics Publications.** Second Edition. Basking Ridge, USA. 2017.

HORRIGAN, Bryan; NICOLL, Geoffrey; HALLIGAN, John; EDWARDS, Meredith. **Public Sector Governance in Australia.** 2012. Disponível em: <https://press.anu.edu.au/publications/series/anzsog/public-sector-governance-australia>. Acesso em 01/04/22.

IFAC, **The International Federation of Accountants**; CIPFA, The Chartered Institute of Public Finance & Accountancy. International Framework: Good Governance in the Public Sector, 2014. Disponível em: <https://forum.ibgp.net.br/p-ifac-2014/>. Acesso em: 12/11/22.

INSTITUTO BRASILEIRO DE GOVERNANÇA PÚBLICA (IBGP). **Conceitos de Governança no Setor Público**. 2012. Disponível em: <https://forum.ibgp.net.br/conceitos-de-governanca-no-setor-publico/>. Acesso em: 10/03/22.

JENSEN, C; MECKLING, W. H. **Teoria da Firma: comportamento dos administradores, custos de agência e estrutura de propriedade**, 2008. Disponível em: <https://www.scielo.br/pdf/rae/v48n2/v48n2a13.pdf>. Acesso em: 31/11/22.

KICKERT, W. J. M. **Public governance in the Netherlands: an alternative to Anglo-American 'managerialism'**. PublicAdministration, 1997. Disponível em <https://books.google.com.br/books?id=9sZTDAAAQBAJ&pg=PA5&lpg=PA5&dq=KICKERT,+W.+J.+M.+(1997).+Public+governance+in+the+Netherlands:+an+alternative+to+Anglo%E2%80%90American+%E2%80%98managerialism%E2%80%99.+Public+Administration&source=bl&ots=B2zE2JJFBQ&sig=ACfU3U13_cSzaXXVxf5wDJ912UjjnUeo4Q&hl=pt-BR&sa=X&ved=2ahUKEwiq34bHjtD3AhXOA7kGHcOiAYsQ6AF6BAgDEAM#v=onepage&q=KICKERT%2C%20W.%20J.%20M.%20(1997).%20Public%20governance%20in%20the%20Netherlands%3A%20an%20alternative%20to%20Anglo%E2%80%90American%20%

E2%80%98managerialism%E2%80%99.%20Public%20Administration&f=false >. Acesso em: 22/04/22.

KOHLS, Cleize; DUTRA, Luiz Henrique; WELTER, Sandro. **LGPD: da teoria à implementação nas empresas.** São Paulo - SP. Editora Rideel, 2021.

LAMBOY, Christian de; LEITE, Luciano Vasconcelos; LAPOLLA, Marcelo. **Manual de implementação da Lei Geral de Proteção de Dados.** 1ª Edição. Editora Via Ética. São Paulo - SP. 2019.

LÓPEZ, Núria; BLUM, Renato Opice. **Lei Geral de Proteção de Dados no setor público: transparência e fortalecimento do Estado Democrático de Direito**. Cadernos Jurídicos da Escola Paulista de Magistratura. São Paulo, ano 21, nº 53, Janeiro-Março/2020. Disponível em: <https://www.tjsp.jus.br/download/EPM/Publicacoes/CadernosJuridicos/ii_7_cadernos_juridicos_epm.pdf?d=637250348268501368>. Acessoem: 12/12/22.

MALINOWSKA, A.; LYNN, L. E., Jr.; **How are patterns of public governance changing in the US and the EU?** It's complicated. Journal of Comparative Policy Analysis: Research and Practice, 2018. Disponível em <https://www.researchgate.net/publication/323671862_How_are_Patterns_of_Public_Governance_Changing_in_the_US_and_the_EU_It's_Complicated>. Acesso em: 22/04/22.

MARQUES, E. **Governo, atores políticos e governança em políticas urbanas no Brasil e em São Paulo: conceitos para uma agenda de pesquisa futura**. In: MENICUCCI, T. M.; GONTIJO, J. G. (Orgs.). Gestão e políticas públicas no cenário contemporâneo: tendências nacionais e internacionais. Rio de Janeiro: Fiocruz, 2016. Disponível em: <https://pesquisa.bvsalud.org/portal/resource/pt/biblio-983452>. Acesso em: 22/04/22.

MARTINS, Humberto F., Marini, Caio. **Um Guia de Governança para Resultados na Administração Pública.** Brasília, Instituto Publix, Editora Publix, 2010.

MATIAS-PEREIRA, J. **A governança corporativa aplicada no setor público brasileiro**. Administração Pública e Gestão Social. 2010. Disponível em: <https://periodicos.ufv.br/apgs/article/view/4015>. Acesso em: 01/05/22.

_____. **Curso de Administração Pública: foco nas instituições e ações governamentais**. 5. ed. São Paulo: GEN-Atlas, 2018.

MEDAUAR, Odete. **Direito administrativo moderno**. São Paulo: Ed. Revista dos Tribunais, 2009.

MOURA, Marcel Brasil de Souza. **As disposições preliminares da LGPD. Comentários à Lei Geral de Proteção de Dados.** Comissão de Direito Digital, Tecnologia e Inteligência Artificial. OAB-SP 116ª Subseção Jabaquara – Saúde. São Paulo. 2020. Disponível em: <https://www.passeidireto.com/arquivo/80538589/comentarios-a-lei-geral-de-protecao-de-dados-oab-sao-paulo-2020>. Acesso em: 15/10/22.

PALUDO, Agostinho V.; OLIVEIRA, Antônio G. **Governança organizacional pública e planejamento estratégico para órgãos e entidades públicas**. Indaiatuba - SP. Editora Foco. 2021. (pág 1 - 5; 8 – 51)

PEDERSEN, K. H.; JOHANNSEN, L. **New public governance in the Baltic States: flexible administration and rule bending**. Public Performance & Management Review, 2018. Disponível em: <https://www.tandfonline.com/doi/abs/10.1080/15309576.2018.1465828>. Acesso: em 22/04/22

PETERS, Guy; PIERRE, John. **Governance without governement? Rethinking public administration**. Journal of Public Administration Research and Theory. 1998. Disponível em: < https://www.jstor.org/stable/1181557>. Acesso em: 15/04/22.

POHLMANN, Sérgio Antônio. **LGPD Ninja: Entendendo e Implementando a Lei Geral de Proteção de Dados nas empresas**. Editora Fross. Nova Friburgo – RJ. 2019.

RÊGO, Bergson Lopes. **Gestão e Governança de Dados: promovendo dados como ativos de valor nas empresas**. Brasport. Rio de Janeiro - RJ. 2013. (pág 37 a 46, 48-56, 93-117).

SANTOS, Andréia da Costa Pereira dos. **Finalmente o empoderamento dos indivíduos enquanto titulares de seus dados. Comentários à Lei Geral de Proteção de Dados**. Comissão de Direito Digital, Tecnologia e Inteligência Artificial. OAB-SP 116ª Subseção Jabaquara – Saúde. São Paulo. 2020.

TASSO, Fernando Antônio. **A responsabilidade civil na Lei Geral de Proteção de Dados e sua interface com o Código Civil e o Código de Defesa do Consumidor**. Cadernos Jurídicos da Escola Paulista de Magistratura. São Paulo, ano 21, nº 53, Janeiro-Março/2020. Disponível em: <https://www.tjsp.jus.br/download/EPM/Publicacoes/CadernosJuridicos/ii_1_interface_entre_a_lgpd.pdf?d=637250344175953621>. Acesso em: 15/10/22.

Yin, R. K. **Estudo de caso: planejamento e métodos**. Porto Alegre: Bookman, 2010.

WIMMER, Miriam. **Proteção de dados pessoais no Poder Público: incidência, bases legais e especificidades**. Revista do Advogado, São Paulo, v. 39, n. 144, p. 126-133, nov. 2019.

WORLD BANK. **Governance and management. In Independent Evaluation Group, Sourcebook for evaluating global and regional partnership programs: indicative principles and Standards**. 2007. Washington, DC. Disponível em: < https://www.oecd.org/development/evaluation/dcdndep/37981082.pdf >. Acesso em: 02/04/22.

XAVIER, Fábio Corrêa. **LGPD no setor público: boas práticas para a jornada de adequação**. ISNB: 979-84-430-9883-8. Publicação independente. 2022.

ANEXO I

Transcrição das entrevistas e questionários semiestruturados (Arquivos externos)

ANEXO II

Exemplo de resposta recebida para questionamento feito por titular no canal disponibilizado pelo EME

---------- Forwarded message ---------
De: <lgpd.eb@ccomsex.eb.mil.br>
Date: ter., 8 de ago. de 2023 10:41
Subject: Re: LGPD
To: [redacted]>

Prezada [redacted]

A respeito do assunto, esclarecemos que a Portaria nº 088 - EME, de 7 de maio de 2020, aprovou a Diretriz de Orientação para Aplicação da Lei Geral de Proteção de Dados Pessoais no Exército Brasileiro.
Uma das premissas desta Portaria é que a gestão da informação é de responsabilidade de todos os Órgãos de Direção Setorial (ODS), do Órgão de Direção Operacional (ODOp) e dos Órgãos de Assistência Direta e Imediata (OADI) ao Comandante do Exército. Esses órgãos gerenciam sistemas próprios (sistemas corporativos e/ou sistemas específicos) e são responsáveis pelo ciclo de vida da informação de seu interesse.
Assim, a Senhora precisa indicar para qual Organização Militar (OM) do Exército Brasileiro cedeu seus dados pessoais. Dessa forma, teremos condições de lhe indicar o controlador responsável pelo tratamento de seus dados pessoais. Ainda, é fundamental que informe o sistema, o processo ou o contexto no qual Vossa Senhoria foi instado a compartilhar seus dados pessoais (exigência legal) ou mesmo motivado a compartilhar, em razão de interesse de ordem particular. Tais informações também são úteis para que a Instituição seja capaz de indicar o controlador correto.

Atenciosamente,

Encarregado de Dados do Exército Brasileiro

De: [redacted]>
Para: "lgpd eb" <lgpd.eb@ccomsex.eb.mil.br>
Enviadas: Segunda-feira, 3 de abril de 2023 10:24:52
Assunto: LGPD

Bom dia!

Já recebi ligações com oferta de produtos de pessoas que tinham informações pessoais minhas.
Assim, gostaria de saber quais dados pessoais meus são tratados pelo Exército, conforme previsto no Artigo 18 da Lei Geral de Proteção de Dados, e quais as medidas de segurança existentes para evitar o vazamento dessas informações?

Muito obrigado pela ajuda!

ANEXO III

Relatório de Inventário do CPEx encaminhado ao EME (arquivo externo)

ANEXO IV

Normativas do EME sobre Segurança da Informação