

MARINHA DO BRASIL
DIRETORIA DE ENSINO DA MARINHA
CENTRO DE INSTRUÇÃO ALMIRANTE ALEXANDRINO

CURSO DE APERFEIÇOAMENTO AVANÇADO EM
SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES

TRABALHO DE CONCLUSÃO DE CURSO

OS IMPACTOS DA LGPD NA MARINHA DO BRASIL



1ºTEN VICTOR HUGO FERREIRA LOPES

Rio de Janeiro
2023

1ºTEN VICTOR HUGO FERREIRA LOPES

OS IMPACTOS DA LGPD NA MARINHA DO BRASIL

Monografia apresentada ao Centro de Instrução Almirante Alexandrino como requisito parcial à conclusão do Curso de Aperfeiçoamento Avançado em Segurança da Informação e Comunicações.

Orientadores:

CC (T) Cristiane da Silva Rodrigues Pereira

CIAA
Rio de Janeiro
2023

1ºTEN VICTOR HUGO FERREIRA LOPES

OS IMPACTOS DA LGPD NA MARINHA DO BRASIL

Monografia apresentada ao Centro de Instrução Almirante Alexandrino como requisito parcial à conclusão do Curso de Aperfeiçoamento Avançado em Segurança da Informação e Comunicações.

Aprovada em 24 de novembro de 2023.

Banca Examinadora:

CMG (RM1-EN) Gian Karlo Huback Macedo de Almeida. – CIAA _____

CF José Waldomiro Sinico Júnior. – DCTIM _____

CC (T) Cristiane da Silva Rodrigues Pereira, MSc. – DCTIM _____

À minha querida mãe, Marineuza (in memoriam), cujo empenho em me educar sempre veio em primeiro lugar e que não mediu esforços para que eu chegasse até esta etapa de minha vida, aqui estão os resultados dos seus esforços. Com carinho, admiração e saudade.

AGRADECIMENTOS

Agradeço, primeiramente, a Deus, pelo dom da vida, e por me permitir vencer todos os obstáculos encontrados ao longo da realização deste trabalho.

À minha esposa Eduarda, que foi capaz de suportar todos os meus momentos de estresse durante o processo e pelo apoio incondicional oferecido em todos os aspectos. Muito obrigado pela sua presença em minha vida.

Ao meu filho Arthur, razão do meu viver, obrigado por me permitir viver uma experiência única ao poder te ver crescer e por poder zelar diuturnamente por ti.

Ao meu pai Serafim e aos meus irmãos Carlos Eduardo e Rodrigo, pelo apoio e suporte que me deram durante toda a vida e pelas incontáveis horas de ajuda na construção do meu ser.

A todos os instrutores que me influenciaram na minha trajetória. Em especial à CC (T) Cristiane Rodrigues, minha orientadora, que sempre esteve à disposição para me auxiliar na elaboração deste projeto durante todo o processo.

Finalmente, ao coordenador do Curso de Aperfeiçoamento Avançado em Segurança da Informação e Comunicações, CMG (EN-RM1) Huback, pela dedicação e empenho durante o andamento do curso, fazendo sempre o possível para nos auxiliar em nosso processo de aprendizagem, para que fosse mais eficiente e organizado, sempre à disposição para os alunos e nos ouvindo quando necessitávamos de ajuda, nos permitindo lograr êxito nesta missão.

“Com avanço tecnológico e o compartilhamento de informações, não há sequer um segundo em que não estamos vulneráveis e a mercê da violação de dados pessoais, a proteção destes elementos é uma garantia fundamental de todos nós.”

Josiene Rodrigues Rocha

OS IMPACTOS DA LGPD NA MARINHA DO BRASIL

Resumo

O presente trabalho tem por objetivo apresentar a aplicação normativa da Lei Federal n.º 13.709, de 14 de agosto de 2018, a Lei Geral de Proteção de Dados Pessoais (LGPD), na Marinha do Brasil e os impactos causados na instituição. O tratamento de dados é inerente às diversas funções necessárias para o cumprimento da missão da Marinha do Brasil, assim como de todas as entidades da Administração Pública. Objetiva-se, deste modo, apontar os impactos desta lei na Marinha do Brasil de forma a analisar e compreendê-los, buscando fornecer uma visão abrangente dos desafios e oportunidades que a LGPD apresenta para essa instituição e como ela está se adaptando para cumprir as regulamentações de proteção de dados no contexto das suas operações.

Palavras-chave: LGPD. Marinha do Brasil. Proteção de dados pessoais. Tratamento de dados.

LISTAS DE SIGLAS E ABREVIATURAS

ANPD	Agência Nacional de Proteção de Dados
APF	Administração Pública Federal
CDC	Código de Defesa do Consumidor
CF	Constituição Federal
CGI.br	Comitê Gestor da Internet no Brasil
COTIM	Conselho de Tecnologia da Informação da Marinha
DCTIM	Diretoria de Comunicações e Tecnologia da Informação da Marinha
DCTIMARINST	Regulamento publicado pela DCTIM
DGPM	Diretoria-Geral do Pessoal da Marinha
DPO	<i>Data Protection Officer</i> (ou Encarregado de Proteção de Dados)
EMA	Estado-Maior da Armada
ExaCC	<i>Exadata Cloud at Customer</i>
GDPR	<i>General Data Protection Regulation</i>
CHM	Centro de Hidrografia da Marinha
LAI	Lei de Acesso à Informação
LGPD	Lei Geral de Proteção de Dados
MB	Marinha do Brasil
MCI	Marco Civil da Internet
OBTIC	Objetivo Estratégico definido para a área da TIC

OCDE	Organização para a Cooperação e Desenvolvimento Econômico
OM	Organização Militar
PbD	<i>Privacy by Design</i>
PETIM Marinha	Plano Estratégico de Tecnologia da Informação e Comunicações da Marinha
SGBD	Sistemas de Gerenciamento de Banco de Dados
SGM	Secretaria-Geral da Marinha
TIC	Tecnologias da Informação e Comunicações
UE	União Europeia

SUMÁRIO

1 INTRODUÇÃO	11
1.1. Apresentação do Problema	15
1.2. Justificativa e Relevância	16
1.3. Objetivos	17
1.3.1. Objetivo Geral	17
1.3.2. Objetivos Específicos	18
2 REFERENCIAL TEÓRICO	19
2.1. A Lei Geral de Proteção de Dados Pessoais	19
2.2. A Marinha do Brasil e sua política de TIC	22
3 METODOLOGIA	25
3.1. Classificação da Pesquisa	25
3.1.1. Quanto aos fins	25
3.1.2. Quanto aos meios	25
3.2. Limitações do Método	25
3.3. Universo e Amostragem	26
3.4. Coleta e Tratamento de Dados	26
4 DESCRIÇÃO E ANÁLISE DOS RESULTADOS	27
4.1. A Marinha do Brasil e a LGPD	27
4.2. Principais mudanças na MB decorridas da lei	29
4.3. Desafios	32
5 CONCLUSÃO	34

5.1. Sugestões para Futuros Trabalhos	34
REFERÊNCIAS	35

1 INTRODUÇÃO

O tema da proteção de dados pessoais requer uma análise minuciosa no contexto de toda a área que lida com a salvaguarda dos direitos humanos. Portanto, é um dos tópicos mais significativos dos últimos anos em termos de influência nas interações entre pessoas e organizações, uma vez que a sociedade digital depende amplamente do uso de dados como recurso fundamental para facilitar as transações econômicas e sociais.

Estamos vivenciando um período em que se torna vital adotar a "Ética de Dados", a qual incorpora os princípios de transparência, segurança e privacidade, como uma extensão natural da ética empresarial em um cenário de transformação digital. Dada a natureza inovadora desse tópico e sua complexidade, existe uma crescente necessidade de aprofundar a pesquisa na interseção da proteção de dados com outros direitos, a fim de desenvolver um modelo sustentável. É dentro desse cenário que estudos sobre as leis gerais de proteção de dados e seu contexto dentro da atualidade se tornam tão importantes e necessários.

As conversas que começaram no continente europeu tiveram seu primeiro impacto oficial no cenário internacional em 1980, quando a OCDE introduziu as Diretrizes para a Proteção da Privacidade e a Transferência Transfronteiriça de Dados Pessoais, que continuam em vigor até hoje. Apesar de não serem legalmente vinculantes, essas diretrizes estabeleceram os princípios que deveriam orientar o tratamento de dados pessoais e serviram de inspiração para diversos instrumentos legais subsequentemente adotados em todo o mundo.

A lei brasileira foi inspirada no GDPR, que foi aprovado pelo Parlamento Europeu em 14 de abril de 2016 e entrou em vigor em 25 de maio de 2018. A lei revogou a Diretiva 95/46/CE e modificou suas disposições de maneira significativa. O GDPR alcança os seguintes objetivos: define amplamente os dados pessoais; se aplica a empresas e organizações que fazem negócios com pessoas na UE, mesmo que a empresa não tenha uma localização geográfica dentro da UE; enumera o direito de um indivíduo à portabilidade de dados; introduz o papel de DPO e seus requisitos; exige notificações de violações de dados às autoridades de proteção de dados designadas dentro de setenta e duas horas; e impõe multas elevadas em caso de não conformidade com a lei.

A legislação do GDPR levou vários anos para ser elaborada. Foi apresentada pela primeira vez pela Comissão em 2012; o Parlamento propôs uma versão em 2014, e em 2015, o Conselho propôs sua própria versão. As três instâncias se reuniram em 2015 e negociaram o texto do GDPR, que foi aprovado pelo Parlamento em abril de 2016 e entrou em vigor em 25 de maio de 2018. Como um regulamento da União Europeia, o GDPR é vinculativo para todos os Estados membros.

A LGPD é mais curta e menos normativa do que o GDPR. O GDPR é bastante prescritivo, e a UE publicou recitais para explicar as disposições da lei. O Brasil ainda não publicou diretrizes para explicar e interpretar a LGPD. A ANPD possui a autoridade para interpretar a LGPD, mas ainda não o fez; a agência foi estabelecida apenas por decreto executivo em 28 de dezembro de 2018. Erickson sugere que a natureza menos prescritiva da LGPD a torna mais flexível do que o GDPR. No entanto, antes da entrada em vigor da lei, a falta de prescrição e a ausência de textos explicativos podem causar confusão e incerteza para as organizações que visam cumprir.

Assim como o GDPR, a LGPD enumera as bases legais para o tratamento de dados pessoais. A LGPD enumera dez bases legais distintas: (1) consentimento, (2) obrigação legal, (3) implementação de políticas públicas pela administração pública, (4) pesquisa por entidades públicas de estudo, (5) execução de contratos, (6) exercício de direitos em processos legais, (7) proteção da vida, (8) proteção da saúde, (9) interesse legítimo e (10) proteção ao crédito. Os objetivos do texto da LGPD são não apenas garantir direitos individuais, mas também fomentar o desenvolvimento econômico, tecnológico e inovação por meio de regras claras, transparentes e abrangentes para o uso adequado de dados pessoais, o que é semelhante aos objetivos do GDPR. Uma das muitas semelhanças que a LGPD tem com o GDPR é a ampla definição de dados pessoais. A disposição da LGPD é mais concisa do que a definição do GDPR, e dados pessoais são definidos como "informações sobre uma pessoa natural identificada ou identificável."

A promulgação da LGPD, estabeleceu um marco normativo essencial para a nossa adaptação à economia digital. Embora já houvesse regulamentações abrangentes que abordavam a proteção de dados, a LGPD representa um avanço significativo. Na CF, por exemplo, são garantidos direitos à intimidade, à vida privada e ao sigilo de informações. O Código de Defesa do Consumidor (Lei nº 8.078/1990) estabelece importantes direitos relacionados aos cadastros de consumidores, como acesso, comunicação, correção e limitação temporal, prefigurando princípios que hoje são fundamentais nas leis de proteção de dados pessoais. A Lei do Cadastro Positivo (Lei nº 12.414/2011), a LAI (Lei nº 12.527/2011) e o MCI (Lei nº 12.965/2014) também contribuem para a proteção de dados pessoais. Entretanto, a LGPD representa a primeira tentativa no Brasil de abordar de maneira abrangente e sistêmica a proteção de dados pessoais, estabelecendo regras e procedimentos essenciais nesse campo do direito. Isso terá um impacto substancial na vida das pessoas, empresas e entidades dos setores público e privado.

No cenário global, entre os anos de 2012 e 2016, ocorreu a discussão e a aprovação em várias instâncias do GDPR europeu, amplamente reconhecido como a principal influência da LGPD.

Um outro fator que desempenhou um papel importante na formatação e na progressão do desenvolvimento da LGPD, e sua abordagem multissetorial, foi o CGI.br e, mais especificamente, o seu Seminário de Proteção à Privacidade e aos Dados Pessoais.

É importante ressaltar que:

Como um fórum qualificado de discussão sobre privacidade e proteção de dados, em geral, naturalmente o Seminário do CGI.br abrigou, ao longo dos anos, debates sobre o projeto (e Anteprojeto) que viria a se tornar a Lei Geral de Proteção de Dados, bem como sobre certos aspectos da norma após sua aprovação, em 2018. (Bioni, 2021)

Além disso, outros fatores foram essenciais, tanto no Brasil quanto no cenário global, para que a LGPD fosse aprovada, são eles:

- i) O escândalo da Cambridge Analytica, que desencadeou um debate que, embora inicialmente restrito a círculos específicos, rapidamente se expandiu para a grande mídia e o público em geral;
- ii) O desejo declarado do Brasil de se tornar membro da OCDE, que exige a adoção de regulamentações sobre o uso de dados pessoais, juntamente com a criação de um órgão supervisor independente e autônomo; e
- iii) A coordenação interna dentro da Câmara dos Deputados para aprovar alterações na Lei do Cadastro Positivo, que incluía a aprovação da LGPD como um pré-requisito fundamental.

Dito isto, quando se fala em dados pessoais, segundo a LGPD, se trata de toda informação relacionada a uma pessoa identificada ou identificável, não se limitando, portanto, ao nome, sobrenome, apelido, idade, endereço residencial ou eletrônico, mas podendo incluir dados de localização, dados médicos, perfis de compras, IP, dados acadêmicos, histórico de compras, entre outros.

As informações pessoais, ou seja, os dados pessoais são o combustível que permitem ao mercado empreender de forma mais produtiva, descentralizada e eficiente (Bioni, 2021). Assim, entende-se que os dados pessoais são os insumos que permitem o desenvolvimento das atividades empresariais na sociedade da informação. O tratamento dos dados pessoais possibilita que as empresas aprimorem a concepção e a segmentação de um produto ou serviço, desde a sua produção e distribuição até a própria abordagem publicitária para promovê-los.

Os dados pessoais quando cruzados sob o uso de técnicas como *Big Data* e *profiling*, por exemplo, podem gerar perfis que consistem numa representação virtual da pessoa,

o que ocorre muitas vezes sem o conhecimento e consentimento desta, reduzindo sua liberdade de escolha (Doneda, 2019).

Bioni também diferencia dado de informação. Segundo ele, o dado consiste no estado primitivo da informação por não acrescentar conhecimento, pois somente quando processados e organizados convertem-se em algo inteligível, onde se pode extrair uma informação. Ambos os autores concordam que a importância do assunto se insere no contexto da sociedade informacional, considerando os avanços tecnológicos que permitem maior incremento na manipulação, coleta, tratamento e comunicação.

A Lei Federal n.º 13.709, de 14 de agosto de 2018, a LGPD, entrou em vigor no Brasil em setembro de 2020, estabelecendo inúmeras regras para o tratamento de dados pessoais. A lei tem por objetivo proteger a privacidade dos cidadãos e garantir que suas informações sejam tratadas de forma segura e transparente por empresas e instituições. A MB, na figura de instituição pública que lida com dados pessoais de seus membros, bem como de outras pessoas que interagem com a instituição, é impactada diretamente pela LGPD e teve que se adaptar aos novos desafios advindos desta lei.

Macedo comenta que:

Vislumbra-se que diversos são os desafios a serem considerados pelo Poder Público no que concerne ao tratamento, armazenamento e uso de dados pessoais em seus bancos de dados. Tais desafios decorrem de um contexto social onde a informação constitui um ativo de valor econômico, de modo que o próprio Estado precisa considerar esse aspecto, seja na regulação das atividades econômicas, ou no fomento e incentivo a soluções tecnológicas que visem resolver gargalos da comunidade (Macedo, 2022).

A LGPD foi criada para aprimorar um conjunto de leis setoriais de proteção de dados já existentes no Brasil, as quais eram consideradas insuficientes e inadequadas para lidar com a complexidade do cenário atual, em que a economia e a sociedade dependem cada vez mais do uso de dados. Ao estabelecer uma lei de aplicação abrangente, a LGPD visa eliminar a falta de uniformidade que existia devido a uma abordagem fragmentada anterior. Agora, todos os setores econômicos estão sujeitos à regulamentação e existe uma base regulatória central que estabelece um padrão mínimo comum. Isso proporciona segurança jurídica e incentiva a troca de dados em diversas situações, com base em um conjunto compartilhado de regras e definições.

Portanto, os alcances da LGPD são vastos e podem abranger inúmeras ocasiões da vida das pessoas. É desafiador identificar momentos em que não estamos compartilhando dados e, mais importante ainda, quando nossas vidas não são moldadas com base nas informações contidas em bancos de dados. Desde a aprovação de empréstimos e o acesso a benefícios sociais

até o conteúdo exibido nas redes sociais, todas essas atividades são personalizadas automaticamente com base nos dados que nós mesmos geramos. Assim, regulamentações desse tipo, neste estágio, representam essencialmente o nosso próprio contrato social contemporâneo.

A proteção de dados é importante tanto para o cidadão, como para a economia e para a sociedade como um todo. De acordo com a lei, o tratamento de dados pessoais deve ser realizado de forma transparente e segura, garantindo a privacidade e os direitos fundamentais dos titulares dos dados (Brasil, 2018a). A LGPD gerou grandes impactos em todas as organizações, tendo em vista que dispõe sobre o tratamento de dados pessoais por pessoa natural ou por pessoa jurídica de direito público ou privado. Em se tratando das entidades da APF que, em sua essência, lidam com dados pessoais e, por conseguinte, precisam estar em conformidade com os dispositivos da nova lei (Oliveira, 2020). Para as instituições públicas, segundo a ANPD:

De acordo com o princípio da finalidade (art. 6º, i), o tratamento dos dados pessoais deve ser realizado para “propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades”. Adicionalmente, no âmbito do setor público, o tratamento de dados pessoais deve atender a uma “finalidade pública”. (ANPD, 2023).

Além disso, a LGPD possui o capítulo IV, que dispõe exclusivamente sobre o tratamento de dados pelo Poder Público, onde podemos constatar a importância do correto manuseio dos dados que são utilizados pela MB e outras entidades do Poder Público e de se adequarem à esta lei.

A LGPD parte do princípio de que cada organização deve não apenas estar ciente dos dados que possui, mas também convertê-los em informações valiosas. A essência desse sistema gira em torno da ideia de criar uma trilha auditável para os dados, permitindo que cidadãos e outros atores econômicos tenham total transparência sobre o ciclo de vida dos dados e, principalmente, como eles afetam as atividades econômicas e as interações sociais.

Nesse sentido, é fundamental compreender os principais impactos da LGPD na MB, a fim de garantir a proteção dos dados pessoais e a conformidade com a legislação.

1.1. Apresentação do Problema

A LGPD entrou em vigor em setembro de 2020 e impactou empresas e instituições, incluindo as entidades públicas, no sentido de se adequarem às novas regras para evitar sanções e proteger a privacidade dos cidadãos. Na figura de entidade pública, a MB foi uma das instituições afetadas por essa lei e teve que se adequar às suas diretrizes.

Por um lado, a MB precisa realizar o processamento de informações pessoais de seus membros e outros cidadãos que tenham relação direta ou indireta com ela para cumprir suas responsabilidades. Por outro lado, a proteção efetiva desses dados é um direito fundamental e garantia para o indivíduo em relação às possíveis interferências e intervenções do Estado em sua liberdade pessoal. Portanto, é incumbência dos profissionais do campo jurídico resolver essa questão de forma prática, dado que as transferências de informações pessoais entre bancos de dados públicos, bem como entre entidades privadas e agências governamentais, estão se tornando cada vez mais necessárias.

Este trabalho visa responder as seguintes perguntas: Quais foram os impactos dessa lei na MB? Como a MB tem se adaptado à essa lei? Quais soluções estão sendo empregadas pela MB?

1.2. Justificativa e Relevância

O tema proposto se justifica como de grande relevância, considerando que atualmente estamos na era digital e todas as relações entre Estado e indivíduo já se inserem neste contexto. Esta análise é relevante tanto do ponto de vista legal quanto do ponto de vista prático e institucional. Portanto, é notável o aumento dos recursos tecnológicos que o Estado e as entidades governamentais têm empregado para aprimorar e supervisionar a administração pública, como se pode observar nos inúmeros dispositivos legais e regulamentações que apoiam e fomentam empreendimentos tecnológicos no âmbito do setor público (Macedo, 2022).

Vale ressaltar algumas razões pelas quais o tema merece atenção:

Conformidade Legal: A LGPD é uma legislação federal que impõe regras estritas sobre a coleta, processamento e proteção de dados pessoais no Brasil. A MB, como uma instituição pública, está sujeita a essas regulamentações, e a não conformidade pode resultar em sérias sanções. É, portanto, crucial entender e atender aos requisitos legais da LGPD.

Proteção de Dados: A MB lida com uma quantidade significativa de informações pessoais, tanto de seus militares quanto de cidadãos com quem interage. Estas informações podem ser altamente sensíveis e, por isso, é vital garantir a sua proteção adequada. Um vazamento de dados ou uma violação de privacidade pode ter implicações sérias em termos de segurança nacional e comprometimento da missão.

Responsabilidade Institucional: A MB é uma das instituições mais respeitadas e vitais do Brasil, desempenhando um papel fundamental na defesa da nação e na segurança

marítima. Garantir a conformidade com a LGPD é um ato de responsabilidade institucional e demonstra o compromisso da Marinha com a legalidade e a proteção dos direitos dos cidadãos.

Desafios de Implementação: A adaptação à LGPD pode ser um processo complexo que exige mudanças substanciais na forma como os dados são gerenciados. Compreender os desafios específicos que a MB enfrenta ao implementar as diretrizes da LGPD é fundamental para garantir uma transição eficiente e eficaz.

Reputação e Confiança Pública: A confiança do público na MB é essencial para o cumprimento de suas missões. O cumprimento rigoroso da LGPD contribui para manter e fortalecer essa confiança, mostrando o compromisso da MB com a ética, a transparência e a proteção dos direitos dos cidadãos.

Portanto, a análise dos impactos da LGPD na Marinha do Brasil não é apenas relevante, mas também fundamental para garantir o funcionamento adequado da instituição, a proteção dos dados pessoais e a manutenção da integridade institucional e legal.

Este trabalho explora os diversos aspectos e desafios que a LGPD impõe à MB, analisando como esta instituição se adapta a essa nova legislação para cumprir suas missões e, ao mesmo tempo, proteger os dados pessoais de forma eficaz e em conformidade com a lei.

1.3. Objetivos

Nesta seção serão apresentados os objetivos que fundamentaram a produção deste trabalho. Inicialmente, apresentar-se-á o objetivo geral, descrevendo em um alto nível de abstração o objetivo principal do estudo propriamente dito. Sequencialmente, apresentar-se-á os objetivos específicos, listando o que se espera tanto da apresentação dos conceitos relacionados à importância da LGPD na MB, os principais impactos da LGPD na MB, bem como exemplos práticos de como a instituição vem lidando com a lei até o momento.

1.3.1. Objetivo Geral

O principal objetivo deste trabalho é analisar e compreender os impactos da Lei Geral de Proteção de Dados (LGPD) na Marinha do Brasil. Buscamos fornecer uma visão abrangente dos desafios e oportunidades que a LGPD apresenta para essa instituição e como ela está se adaptando para cumprir as regulamentações de proteção de dados no contexto das suas operações.

1.3.2. Objetivos Específicos

Analisar os impactos operacionais: Apontar como a LGPD afeta as operações e os processos internos da MB, incluindo a coleta, processamento e armazenamento de dados pessoais, e quais ajustes foram necessários para cumprir as regulamentações.

Identificar desafios específicos da MB: Identificar desafios específicos que a Marinha enfrenta ao implementar a LGPD, considerando a natureza sensível das informações que lida e suas missões críticas de segurança.

Apresentar as medidas de segurança e proteção de dados: Apresentar as medidas de segurança de dados implementadas pela MB para garantir a proteção efetiva das informações pessoais, incluindo políticas de segurança cibernética e de privacidade.

Destacar as oportunidades e benefícios: Identificar as oportunidades e benefícios que a conformidade com a LGPD pode trazer para a MB, como o fortalecimento da segurança de dados, a proteção da privacidade dos membros e cidadãos, e a melhoria da reputação institucional.

Ao alcançar esses objetivos, este estudo visa oferecer informações valiosas sobre como a MB está se adaptando às regulamentações de proteção de dados, os desafios que enfrenta e as oportunidades que podem surgir no contexto da LGPD.

2 REFERENCIAL TEÓRICO

É um fato que o referencial legal para a proteção de dados no Brasil é mais abrangente do que simplesmente uma lei geral. Esse arcabouço regulatório foi moldado ao longo de décadas por meio de pilares significativos, incluindo o CDC, a Lei nº 12.965/2014 (Marco Civil da Internet), a Lei nº 12.414/2011 (conhecida como Lei do Cadastro Positivo), além de outras normas específicas de setores diversos.

A aprovação de uma lei representa apenas o estágio inicial na construção de uma cultura de proteção de dados pessoais no Brasil. Tomando como exemplo a promulgação do CDC na década de 90, a sociedade, as entidades de fiscalização e as próprias empresas demoraram um certo tempo para aderir efetivamente às diretrizes do CDC. Após quase quatro décadas, é evidente que o CDC foi amplamente aceito e contribuiu para tornar o mercado de produtos e serviços mais seguro, promovendo um ambiente mais civilizado.

Da mesma forma, as organizações que perceberam a nova legislação como uma oportunidade para agregar valor e melhorar sua reputação continuam a colher os benefícios até hoje, incluindo a incorporação desses princípios em suas estratégias de comunicação.

As organizações que optarem por estabelecer processos sólidos de governança de dados, investindo não apenas em tecnologia, mas também em capital humano, como parte fundamental de sua missão institucional, estarão à frente e poderão capitalizar sobre a formação de uma cultura de proteção de dados pessoais que ainda está em desenvolvimento no Brasil.

2.1. A Lei Geral de Proteção de Dados Pessoais

É importante notar que a LGPD não visa restringir o fluxo de informações, mas, ao contrário, incentiva-o, desde que siga uma lógica de sustentabilidade que beneficie tanto quem produz os dados quanto quem os utiliza (Bioni, 2019). Por exemplo, ela estipula que todas as atividades de tratamento de dados, desde a coleta até o descarte, devem, entre outros princípios, ter uma finalidade específica claramente definida. Isso contribui para uma organização eficaz das informações. Infelizmente, muitas organizações ainda têm o hábito de coletar dados em excesso, sem considerar sua real utilidade. Basta observar a quantidade de aplicativos em nossos smartphones que solicitam acesso a recursos como lista de contatos, câmera e microfone, muitas vezes sem necessidade para o funcionamento do serviço. Isso não apenas resulta na subutilização dos dados, mas também os transforma em um risco potencial, como vimos em vazamentos de dados que causaram graves problemas na economia movida a informações. Um

caso recente que exemplifica isso foi o vazamento de dados pessoais de cerca de 4 milhões de beneficiários do Auxílio-Brasil, que ocorreu em outubro de 2022.

Em seu artigo 2º, podemos observar os princípios fundamentais que a lei visa assegurar:

Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos:

I - o respeito à privacidade;

II - a autodeterminação informativa;

III - a liberdade de expressão, de informação, de comunicação e de opinião;

IV - a inviolabilidade da intimidade, da honra e da imagem;

V - o desenvolvimento econômico e tecnológico e a inovação;

VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e

VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais. (Brasil, 2018a)

Esses princípios constam em outras leis, como a CF, o CDC, etc., e são reforçados nesta lei para que possa dar amplo conhecimento da necessidade de proteção desses direitos num mundo globalizado onde os dados são a principal fonte.

O artigo 3 define que essa legislação é relevante para todas as ações de manipulação de dados realizadas por pessoas físicas ou entidades jurídicas, seja de natureza pública ou privada, sem importar o meio ou o país onde têm sua sede ou onde os dados estejam situados, desde que:

I - a operação de tratamento seja realizada no território nacional;

II - a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional;
ou

III - os dados pessoais objeto do tratamento tenham sido coletados no território nacional.

§ 1º Consideram-se coletados no território nacional os dados pessoais cujo titular nele se encontre no momento da coleta.

§ 2º Exceção-se do disposto no inciso I deste artigo o tratamento de dados previsto no inciso IV do caput do art. 4º desta Lei. (Brasil, 2018a)

Das principais estratégias para cumprir a nova lei seguem a seguinte abordagem: a análise abrangente dos dados e programas de governança. Primeiro, a organização precisa realizar uma análise completa de seu repositório de informações, identificando quais práticas precisam ser mantidas ou modificadas para garantir conformidade com as regulamentações. Quando realizado de maneira apropriada, esse processo pode gerar novas ideias, especialmente em relação a dados que não estão sendo utilizados plenamente, mas que têm o potencial de informar ações tanto no setor público quanto no privado.

A jornada de conformidade não deve ser vista como um custo, e muito menos como uma tarefa meramente burocrática para cumprir uma lista de obrigações legais. Pelo contrário, deve ser considerada um investimento que pode otimizar e tornar mais eficientes as atividades das organizações sujeitas à regulação.

Para tal, faz-se mister seguir estritamente os princípios definidos no artigo 6º da LGPD:

Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:

I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;

II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;

III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;

IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;

V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;

VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;

VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;

VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;

IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;

X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas. (Brasil, 2018a)

Além dos benefícios internos que esse processo de conformidade traz, ele pode ser um ponto crucial para as organizações no contexto de um mercado altamente competitivo e global. A maioria das leis de proteção de dados pessoais, como o GDPR europeu e a lei brasileira, estabeleceu uma relação de responsabilidade conjunta entre o controlador dos dados

e seus terceirizados, conhecidos como processadores. Se um terceirizado causar algum dano, o controlador pode ser diretamente responsabilizado por repará-lo.

Isso implica que os controladores devem contratar apenas processadores que estejam em conformidade com as regras de proteção de dados pessoais, direta ou indiretamente. Como resultado, os diversos participantes na cadeia de tratamento de dados, em vez de simplesmente fiscalizarem uns aos outros, tendem a deixar de lado aqueles que não estão em conformidade. Portanto, estar em conformidade passa a conferir uma vantagem competitiva sobre os concorrentes que não adotaram medidas similares, podendo inclusive resultar na valorização dos serviços e produtos da organização.

Ao incorporar metas, como a integração da *PbD*, nas regulamentações de proteção de dados pessoais, as novas leis enfatizam cada vez mais a colaboração dos responsáveis pelo desenvolvimento de produtos e serviços na redução dos riscos associados às suas próprias atividades. Em contraste com a antiga abordagem em que todas as atividades de tratamento de dados eram obrigadas a ser notificadas às autoridades reguladoras, a regulamentação atual da UE exige a comunicação somente quando uma atividade específica apresenta um risco elevado para os titulares de dados. Esse sistema é calibrado com base na confiança depositada nesse processo e por meio de ferramentas que permitem que os agentes de tratamento de dados demonstrem a eficácia das medidas adotadas para cumprir as normas de proteção de dados pessoais.

2.2. A Marinha do Brasil e sua política de TIC

A MB, como uma instituição pública com uma longa história, tem lidado com dados pessoais de militares e civis desde o seu estabelecimento, e sua política de tratamento desses dados sempre tem sido moldada pelas leis vigentes. É crucial destacar que o direito ao sigilo de informações é uma parte fundamental da CF, conforme estabelecido em seu artigo 5º, destacando sua importância, mesmo no passado. Com a entrada em vigor da LGPD, a relevância desse direito foi ainda mais fortalecida e reforçada.

As políticas de TIC da MB refletem a importância estratégica da segurança e do gerenciamento eficaz dos recursos tecnológicos em uma organização tão abrangente e multifacetada. Essas políticas visam garantir a integridade, confidencialidade e disponibilidade dos dados e dos sistemas da Marinha, abrangendo desde as operações navais até a administração interna. Para atingir esses objetivos, são adotadas medidas rigorosas de segurança cibernética,

como a criptografia de dados, a autenticação de usuários e o monitoramento constante de ameaças.

Além disso, elas visam promover a modernização e a inovação tecnológica, permitindo que a organização acompanhe as demandas em constante evolução de uma força naval moderna. Isso inclui a implementação de sistemas avançados de comunicação, navegação e gerenciamento de informações, bem como a capacitação dos membros da MB em competências de TIC relevantes. O foco na cibersegurança, aliado à busca pela eficiência operacional, demonstra o compromisso da MB em garantir que suas políticas de TIC estejam alinhadas com as melhores práticas globais e as necessidades de uma força naval do século XXI.

As políticas de TIC também desempenham um papel fundamental na eficiência operacional e na segurança das comunicações em uma instituição militar de importância estratégica. No entanto, a entrada em vigor LGPD introduziu um novo conjunto de desafios e responsabilidades para a Marinha e causou mudanças em suas políticas de TIC. A LGPD estabelece diretrizes rígidas para o tratamento de dados pessoais, incluindo questões de privacidade e segurança. Portanto, a MB precisa ajustar constantemente suas políticas de TIC para garantir o cumprimento da LGPD e a proteção adequada dos dados pessoais que podem ser tratados em suas operações.

Os impactos da LGPD nas políticas de TIC incluem a necessidade de implementar medidas de segurança mais robustas para proteger os dados pessoais que possam ser coletados e armazenados em suas operações. Isso envolve a revisão das práticas de criptografia, o monitoramento de ameaças cibernéticas e a garantia de que os membros da Marinha estejam cientes das normas de privacidade e proteção de dados. Além disso, a LGPD exige a nomeação de um DPO para supervisionar a conformidade com a lei, bem como a atualização das políticas de retenção de dados e a documentação adequada das atividades de tratamento de dados.

As políticas de TIC também precisam estar bem definidas para ajudar a lidar com a responsabilidade legal e as penalidades associadas ao não cumprimento da LGPD. A lei prevê multas significativas para violações de dados e falta de conformidade. Portanto, a Marinha deve estar preparada para evitar sofrer as implicações legais e financeiras decorrentes de eventuais violações. Além disso, a LGPD exige transparência nas atividades de tratamento de dados, o que significa que a Marinha deve estar preparada para fornecer informações sobre como os dados pessoais são tratados e protegidos.

No geral, os impactos da LGPD nas políticas de TIC da Marinha do Brasil refletem a necessidade de maior atenção à privacidade e à segurança dos dados pessoais, com a

implementação de medidas de proteção e a conformidade estrita com a regulamentação. Essa adaptação é essencial para garantir que a Marinha cumpra a lei e proteja os dados pessoais dos indivíduos envolvidos em suas operações.

3 METODOLOGIA

A metodologia utilizada para elaborar esse trabalho tem um caráter qualitativo, já que as informações foram obtidas a partir de livros, artigos, teses e dissertações a respeito do assunto em questão. Não foram utilizados experimentos laboratoriais ou em campo, além de não se fazer uso de métodos numéricos ou matemáticos para encontrar soluções para o problema em análise.

Ao longo deste trabalho serão abordados os princípios básicos da LGPD, sua importância para a MB e sua implementação e a adequação por parte da MB, a fim de identificar os impactos desta lei na MB.

3.1. Classificação da Pesquisa

Este subitem do trabalho foi destinado ao enquadramento da pesquisa. Uma pesquisa pode ser feita de diversas maneiras e possui algumas classificações que podem enquadrá-la. Ela pode ser classificada quanto aos fins e quanto aos meios.

3.1.1. Quanto aos fins

Segundo Vergara (1998) podemos classificar essa pesquisa quanto aos fins como explicativa, pois visa esclarecer quais fatores contribuem, de alguma forma, para a necessidade de adequação da MB com relação à LGPD.

3.1.2. Quanto aos meios

Quanto aos meios, a pesquisa pode ser classificada como bibliográfica, de acordo com Vergara (1998), já que foi realizada com base em trabalhos publicados de amplo acesso, como teses de doutorado, dissertações de mestrado, artigos, livros e pesquisas.

3.2. Limitações do Método

Foi proposta apenas uma visão teórica acerca do assunto, visto que não haveria tempo hábil para uma abordagem mais prática do tema estudado. A limitação do método escolhido é o fato de não haver bibliografias mais abrangentes e específicas acerca do assunto em lide.

3.3. Universo e Amostragem

O universo da pesquisa estará referido aos grupos diretamente envolvidos com a Marinha do Brasil, como seus membros e outros cidadãos cujos dados são tratados por ela. Com relação a estes, o tipo de amostragem utilizada será a probabilística por conglomerados, que parece ser a mais adequada no presente caso.

3.4. Coleta e Tratamento de Dados

Os dados serão coletados por meio de pesquisa bibliográfica em trabalhos publicados de amplo acesso, como teses de doutorado, dissertações de mestrado, artigos, livros e pesquisas, onde serão levantadas as mudanças causadas pela LGPD na Marinha. Em virtude da natureza do problema investigado, o tratamento e a análise dos dados, realizados com base nos dados primários obtidos quando da revisão bibliográfica, recaíram sobre uma abordagem mais qualitativa.

4 DESCRIÇÃO E ANÁLISE DOS RESULTADOS

Esse capítulo será dedicado à análise dos impactos da LGPD na MB e como ela está se adaptando às regulamentações de proteção de dados, os desafios que enfrenta e as oportunidades que podem surgir no contexto da LGPD.

4.1. A Marinha do Brasil e a LGPD

Desde que foi promulgada, a LGPD tem apresentado uma série de desafios que devem ser enfrentados por todas as empresas e organizações que lidam com informações de cidadãos brasileiros. A MB, como uma dessas instituições afetadas, enfrentou dificuldades iniciais em seu processo de adaptação, em grande parte devido à falta de uma cultura de segurança mais forte, que é algo predominante no país. Fato este que pode ser comprovado pelo Relatório de Feedback da Auditoria de Diagnóstico para Adequação à LGPD realizado pelo TCU no Comando da Marinha (CM), entre novembro de 2020 e maio de 2021, disponível na página da Marinha¹, onde podemos constatar que, naquele período onde fora avaliada, a MB ainda estava longe de alcançar um grau mais elevado de conformidade com a lei, pois teve seu grau de adequação considerado em fase inicial, conforme o relatório:

A partir dos valores do indicador, foram definidos quatro níveis de adequação à LGPD: “Inexpressivo” (indicador menor ou igual a 0,15), “Inicial” (indicador maior do que 0,15 e menor ou igual a 0,5), “Intermediário” (indicador maior do que 0,5 e menor ou igual a 0,8) e “Aprimorado” (indicador maior do que 0,8). Assim, conforme o valor do indicador obtido, as organizações foram classificadas em um desses níveis de maturidade.

A organização CM obteve o valor 0,21 para o indicador de adequação, o que corresponde ao nível “Inicial”. (Brasil, 2022)

Nessa primeira avaliação, podemos constatar que a grande maioria das OM da MB ainda estava iniciando seu processo de adequação, como mostra a Figura 1.

¹ Cf. em: <https://www.marinha.mil.br/protecao-de-dados-pessoais-lgpd>.

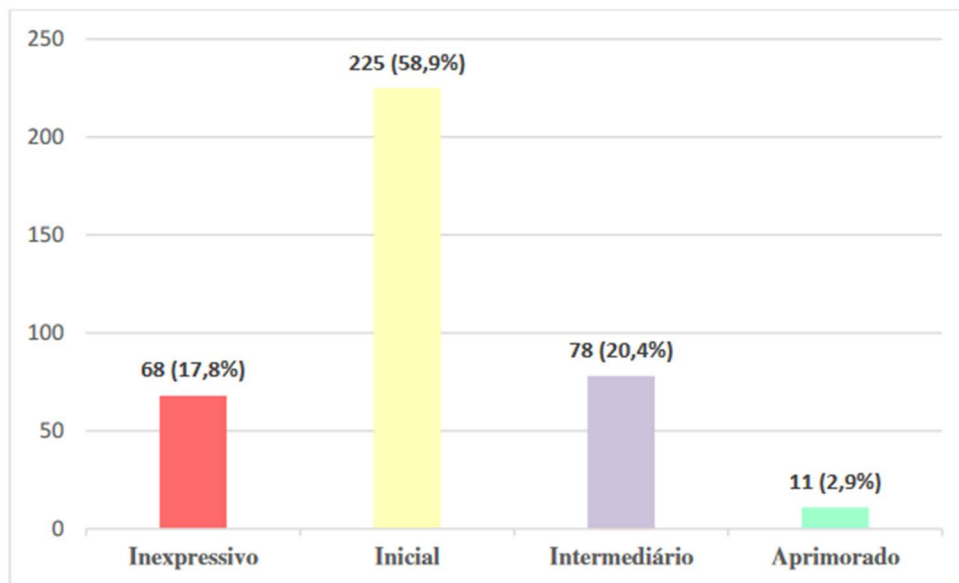


Figura 1 - Distribuição das organizações por níveis de adequação à LGPD

Fonte: Relatório de feedback do TCU

Isso se deve, principalmente, devido ao fato de que a MB ainda não havia publicado de fato diretrizes mais específicas de forma a padronizar como cada OM deveria iniciar seu processo de conformidade com a lei. Sendo assim, cada OM acabou por implementar, à luz de suas interpretações da lei, as medidas que acharam mais adequadas para tal.

Cabe ressaltar também que a própria agência reguladora, a ANPD, só iniciou suas atividades efetivamente em 06 de novembro de 2020, o que também contribuiu para essa “demora”, já que a ANPD é a responsável por elaborar as diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade, além de outros documentos primordiais para o correto entendimento das “lacunas” que a lei deixou a cargo da agência.

Entretanto, após receber o relatório, verificou-se a necessidade de maior comprometimento por parte da MB para o correto cumprimento da lei e então o EMA, na figura de órgão de governança de dados da MB, divulgou por meio de sua circular nº 6/2021, a “Implantação da Lei Geral de Proteção de Dados (LGPD) na Marinha do Brasil”, o primeiro passo para o início da adequação da MB à LGPD.

Diversos outros documentos foram publicados desde então, como a DCTIMARINST 30-17 (Norma sobre a adequação dos Sistemas Digitais e Banco de Dados existentes na MB às boas práticas de segurança para proteção dos Dados Pessoais), e outros ainda necessitam de atualizações, como o EMA-416 (Doutrina de Tecnologia da Informação da Marinha), para que a normatização de seus regulamentos internos possa transformar as

políticas de TIC da MB em algo mais próximo do que a LGPD almeja: assegurar a proteção dos dados pessoais.

No que se refere à implementação de regulamentos, de acordo com a Doutrina de Tecnologia da Informação da Marinha, o EMA, por meio do COTIM, é encarregado de aprovar diretrizes doutrinárias. Enquanto isso, a DCTIM tem a responsabilidade de "desenvolver regulamentos, orientações técnicas e procedimentos padronizados relacionados a áreas de conhecimento ligadas ao uso de Tecnologia da Informação na MB". Essas áreas incluem notavelmente a segurança da informação digital e a guerra cibernética. As demais ações, que compõem esta ação estratégica, são atribuições da DCTIM.

Em se tratando da Circular nº 6/2021 do EMA, ela determinou a designação de um DPO para cada OM, possibilitando a descentralização e maior controle dos procedimentos adotados, o que facilita, a longo prazo, o incremento da mentalidade de segurança e a adequação de cada OM à lei.

Um outro documento publicado, o PETIM 2022-2025, estabelece um OBTIC para os próximos anos, estabelecendo um percentual de atendimento ao índice de atendimento ao formulário de conformidade com a LGPD para proteção de dados pessoais em meio digital, principalmente, em banco de dados da MB (Brasil, 2021b). Esse formulário, que consta como anexo em outra publicação da Marinha, a DCTIMARINST 30-17, possui perguntas sobre medidas de segurança e medidas de privacidade que as OM devem ter para alcançar maior adequação com a LGPD.

4.2. Principais mudanças na MB decorridas da lei

Do ponto de vista dos titulares de dados pessoais, pouco mudou de fato. Resumidamente, aumentou-se a consciência da importância da correta utilização de seus dados pessoais para evitar acúmulo desnecessário de informações, criou-se o termo de consentimento do titular (pois é exigido pelo artigo 7º, item I da lei, que haja consentimento do titular para que possa haver o tratamento de dados)², documento formal onde o titular autoriza ao DPO de sua OM a realizar o tratamento de seus dados para os fins necessários, desde que cumpridas as exigências do artigo 6º:

Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:

² Cf. o artigo 11º da lei, que fala sobre as hipóteses de tratamento sem o consentimento do titular.

I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;

II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;

III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;

IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;

V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;

VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;

VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;

VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;

IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;

X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas. (Brasil, 2018a)

Além disso, de acordo com a lei, sempre que houver necessidade de compartilhamento ou tratamento dos dados, o mesmo é informado imediatamente sobre os motivos que justificam tais medidas; e, no caso de vazamento de dados do titular, também serão comunicados: as medidas adotadas para reverter ou mitigar o prejuízo, os riscos relacionados e as medidas técnicas e de segurança utilizados para a proteção dos dados.

A lei também definiu e tornou necessário para o correto tratamento dos dados pessoais, a exigência dos chamados agentes de tratamento (controlador e operador) e do encarregado. Estas funções são definidas no artigo 5º:

VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;

VII - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;

VIII - encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD); (Redação dada pela Lei nº 13.853, de 2019) Vigência

IX - agentes de tratamento: o controlador e o operador. (Brasil, 2018a)

Por estes serem ligados diretamente ao tratamento de dados, também lhes foram atribuídas diversas responsabilidades legais:

- Ao controlador compete:
 1. Elaborar relatório de impacto à proteção de dados pessoais;
 2. Comprovar que o consentimento obtido do titular atende às exigências legais;
 3. Comunicar à ANPD a ocorrência de incidentes de segurança;
 4. Fornecer informações relativas ao tratamento;
 5. Assegurar a correção e a eliminação de dados pessoais; e
 6. Receber requerimento de oposição a tratamento.
- Ao operador compete:
 1. Realizar o tratamento segundo as instruções fornecidas pelo controlador;
 2. Firmar contratos que estabeleçam, dentre outros assuntos, o regime de atividades e responsabilidades com o controlador; e
 3. Dar ciência ao controlador em caso de contrato com suboperador (ANPD, 2021).
- Ao encarregado compete (de acordo com o § 2º do art. 41):
 1. Aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;
 2. Receber comunicações da autoridade nacional e adotar providências;
 3. Orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e
 4. Executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.

Essas funções são elementos essenciais para o cumprimento legal da lei e exercem papel de elevada responsabilidade perante a lei. Para tal, foi determinado que o controlador de cada OM é o titular da OM (em caso de ser Almirante, essa função é delegada para um outro oficial). Além disso, teve que indicar seus respectivos encarregados e operadores, para se reportarem aos controladores e assegurarem o correto manuseio dos dados pessoais dos titulares. Devido a isso, eles acabaram por se tornar os principais difusores de informação sobre a lei e de mentalidade de segurança, itens iniciais requeridos para aprimorar a gestão dos dados.

Com relação às medidas de segurança, podemos citar a aquisição da solução de nuvem privada do banco de dados Oracle, denominada ExaCC, a qual abrange os sistemas digitais dos setores da SGM e da DGPM, hospedados no CD-MB, e também os sistemas digitais do CHM.

A adoção do ExaCC permitiu a redução dos custos com licenciamento da Oracle e aprimorou a segurança dos dados, tendo em vista que as bases de dados do ExaCC não são acessíveis pela internet e essa tecnologia oferece vários controles para garantir a integridade, a confidencialidade, o privilégio mínimo de acesso e a auditoria dos registros de acesso. Cabe ressaltar que todas as bases de dados são criptografadas em atendimento às diretrizes da LGPD.

Além disso, a DCTIM publicou a DCTIMARINST 30-17 com o objetivo de recomendar as melhores práticas para o tratamento dos dados pessoais que estão armazenados em banco de dados. Vale ressaltar que durante o processo de conformidade de um sistema digital, deve ser preenchido o Formulário LGPD, Anexo da referida norma, com as medidas de segurança que foram adotadas durante o desenvolvimento do sistema.

Com as mudanças elencadas, podemos identificar algumas oportunidades e benefícios que a conformidade com a lei pode e tem trazido resultados para a MB, como o fortalecimento da segurança de dados, o aumento da mentalidade de segurança, a proteção da privacidade dos membros e cidadãos e a melhoria da reputação institucional.

4.3.Desafios

Em seu artigo 7º a lei explicita em quais hipóteses poderá ser realizado o tratamento de dados, sendo elas:

- I - mediante o fornecimento de consentimento pelo titular;
- II - para o cumprimento de obrigação legal ou regulatória pelo controlador;
- III - **pela administração pública**, para o tratamento e uso compartilhado de dados necessários à **execução de políticas públicas previstas em leis e regulamentos** ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei. (Brasil, 2018a, grifo nosso)

Porém, o termo “políticas públicas” é um termo que ficou vago – de fato, este foi o intuito da utilização do termo, de modo a permitir que as outras leis fossem atualizadas com o passar dos anos sem que essa lei tivesse que ser alterada – e acabou por dar margem a interpretações mais abstratas da realidade (antes da criação da ANPD e de suas publicações complementares à lei), tendo em vista que, inicialmente, qualquer operação realizada pela MB seria considerada uma política pública, por se tratar de órgão da APF no cumprimento de seus deveres. Todavia, apesar de o Guia Orientativo para o Tratamento de dados pessoais pelo Poder Público não definir o que seriam as “políticas públicas” nas quais há embasamento legal para o tratamento dos dados, ele diz que “recomenda-se que sejam consideradas as definições usuais

do termo, conforme a praxe administrativa e as orientações a seguir apresentadas” (ANPD, 2023).

A adequação da MB à LGPD envolve também:

- **Conscientização e Treinamento:** Garantir que todos os servidores estejam cientes das obrigações impostas pela LGPD e estejam devidamente treinados para cumprir as diretrizes de proteção de dados; e
- **Segurança de Dados:** Implementar medidas de segurança de dados robustas para proteger as informações pessoais dos indivíduos e evitar violações de dados.

Além desses desafios, a MB também deve considerar as implicações específicas da LGPD para suas operações e políticas, bem como a necessidade de cooperação com outras entidades governamentais para garantir a conformidade com a lei.

5 CONCLUSÃO

Com base no referencial teórico e nos fatos apresentados, é possível constatar que, apesar da LGPD ter proposto diversas regulações e imposto novos desafios, a MB tem se empenhado constantemente para se manter atualizada e de acordo com as normas vigentes, mesmo que ainda não se encontre totalmente em conformidade com a lei, além de necessitar manter continuada verificação de procedimentos em busca de melhorias em prol da conformidade, haja vista que há um longo caminho a trilhar em busca de aprimoramento de segurança, face ao mundo digital em que vivemos, e proteção de dados pessoais.

5.1. Sugestões para Futuros Trabalhos

Diante do exposto, a Marinha do Brasil tem envidado esforços no sentido de atender as diretrizes da LGPD. Portanto, com o intuito de aprimorar a conformidade da MB com a LGPD, os seguintes tópicos poderiam ser estudados:

- Aprimoramento da governança de dados na MB, com o objetivo de mapear todos os dados pessoais que estão armazenados em diversas bases de dados;
- Ampliar os estudos referentes à migração de sistemas digitais da MB para a nuvem pública; e
- Tendo em vista que a maioria dos dados pessoais estão armazenados digitalmente, seria interessante automatizar a verificação da conformidade do tratamento dos dados pessoais com a LGPD, por meio da aquisição ou desenvolvimento de um sistema digital.

REFERÊNCIAS

ANPD – AGÊNCIA NACIONAL DE PROTEÇÃO DE DADOS. **Guia Orientativo para Definição dos Agentes de Tratamento de Dados Pessoais e do Encarregado**. Brasília, mai. 2021. Disponível em: <https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/guia-poder-publico-anpd-versao-final.pdf>. Acesso em: 20 jul. 2023.

_____. **Guia Orientativo para o Tratamento de dados pessoais pelo Poder Público**. Brasília, jun. 2023. Disponível em: <https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/guia-poder-publico-anpd-versao-final.pdf>. Acesso em: 20 jul. 2023.

BIONI, Bruno Ricardo. **Proteção de Dados Pessoais: a função e os limites do consentimento**. 3. ed. Rio de Janeiro: Forense, 2019.

_____. **Proteção de dados: contexto, narrativas e elementos fundantes**. São Paulo: Sociedade Individual de Advocacia, 2021.

BRASIL. Constituição da República Federativa do Brasil de 1988. **Diário Oficial**, Brasília, 05 out. 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 12 abr. 2023.

_____. Lei nº 10.406, de 10 de janeiro de 2002. Institui o Código Civil. **Diário Oficial**, Brasília, 10 jan. 2002. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/2002/110406compilada.htm. Acesso em: 13 abr. 2023.

_____. Ministério da Defesa. **Política de Segurança da Informação para o Sistema Militar de Comando e Controle**. (MD31-P-03). Brasília, 29 out. 2015. Disponível em: https://www.gov.br/defesa/pt-br/arquivos/File/doutrinamilitar/listadepublicacoesEMD/md31a_p03a_pola_sega_infoa_sismc_2a_2eda_2015.pdf/view. Acesso em: 19 jul. 2023.

_____. Lei nº 13.709 de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais. **Diário Oficial**, Brasília, 15 ago. 2018a. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/113709.htm. Acesso em: 12 abr. 2023.

_____. Decreto Presidencial Nº 9.637, de 26 de dezembro de 2018. Institui a Política de Segurança da Informação, dispõe sobre a governança da segurança da informação. **Diário Oficial**, Brasília, 2018b. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/decreto/D9637.htm. Acesso em: 14 abr. 2023.

_____. Lei nº 13.853, de 8 de julho de 2019. Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências. **Diário Oficial**, Brasília, 19 dez. 2019. Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Lei/L13853.htm. Acesso em: 12 abr. 2023.

_____. Marinha do Brasil. **Norma sobre a adequação dos Sistemas Digitais e Banco de Dados existentes na MB às boas práticas de segurança para proteção dos Dados Pessoais.** (DCTIMARINST 30-17). Rio de Janeiro, 22 jun. 2021a.

_____. Marinha do Brasil. **Plano Estratégico de Tecnologia da Informação e Comunicações da Marinha (2022-2025).** Brasília, 26 out. 2021b.

_____. Decreto nº 11.529, de 16 de maio de 2023. Institui o Sistema de Integridade, Transparência e Acesso à Informação da Administração Pública Federal e a Política de Transparência e Acesso à Informação da Administração Pública Federal. **Diário Oficial**, Brasília, 16 mai. 2023. Disponível em http://www.planalto.gov.br/ccivil_03/_Ato2023-2026/2023/Decreto/D11529.htm#art19. Acesso em: 18 jul. 2023.

_____. Tribunal de Contas da União. **Relatório de Feedback do Comando da Marinha sobre a auditoria para elaborar diagnóstico acerca dos controles implementados pelas organizações públicas federais para adequação à LGPD.** [2022]. Disponível em: https://www.marinha.mil.br/sites/default/files/relatorio_de_feedback_do_tcu.pdf. Acesso em: 22 jun. 2023.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais: fundamentos da Lei Geral de Proteção de Dados.** 2. ed. São Paulo: Revista dos Tribunais, 2019.

ERICKSON, Abigayle. **Comparative Analysis of the EU's GDPR and Brazil's LGPD: Enforcement Challenges with the LGPD,** 44 Brook. J. Int'l L. 859 (2019). Disponível em: <https://brooklynworks.brooklaw.edu/bjil/vol44/iss2/9>. Acesso em: 03 ago. 2023.

FERNANDES, Renan Camejo. **A importância do princípio da publicidade e da transparência da administração para a credibilidade do Exército Brasileiro.** Trabalho de Conclusão de Curso (Bacharel em Ciências Militares). Resende: AMAN, 2017. Disponível em: <https://bdex.eb.mil.br/jspui/bitstream/1/1089/1/TCC%204286%20CAMEJO.pdf>. Monografia.

BARZOTTO, Luciane Cardoso; COSTA, Ricardo Hofmeister de Almeida Martins. **Estudos sobre LGPD – Lei Geral de Proteção de Dados – lei nº 13.709/2018:** doutrina e aplicabilidade no âmbito laboral. Porto Alegre: Escola Judicial do Tribunal Regional do Trabalho da 4ª Região. Diadorim Editora, 2022. Disponível em: <https://cdea.tche.br/site/wp-content/uploads/2022/05/Estudos-sobre-LGPD.pdf>. Acesso em: 23 set. 2023.

MACEDO, Nathália Brito de. **A proteção de dados pessoais em banco de dados públicos no atual contexto da sociedade da informação:** reflexões sobre o tratamento de dados pessoais pelo poder público brasileiro. Natal-RN, 2022.

OLIVEIRA, Geveson de Souza. **Os impactos da Lei Geral de Proteção de Dados (LGPD) na Administração Pública Federal.** Conteúdo Jurídico, Brasília-DF: 13 out. 2020. Disponível em: <https://conteudojuridico.com.br/consulta/artigos/55320/os-impactos-da-lei-geral-de-proteo-de-dados-lgpd-na-administracao-pblica-federal>. Acesso em: 17 mai. 2023.

PIMENTEL, F. F. R. **Os desafios da Marinha do Brasil com a LGPD.** Revista de Direito Militar, v. 80, n. 1, 2021.

RODRIGUES, Valquíria de Lima. **A Lei de Acesso à Informação na Marinha: limites e possibilidades das relações com a comunicação.** Dissertação (Mestrado em Comunicação) - Universidade de Brasília, Brasília, 2019. Disponível em: <https://repositorio.unb.br/handle/10482/38208>. Acesso em: 15 ago. 2023.

SILVA, Alexandre; LUCCAS, Victor. Público, Porém Não Disponível: **Os Limites de Tratamento do Dado Pessoal Público.** In: RAIS, Diogo; FILHO, Francisco. Direito Público Digital - Ed. 2020. São Paulo: Editora Revista dos Tribunais. 2020. Disponível em: <https://thomsonreuters.jusbrasil.com.br/doutrina/1212768862/direito-publico-digital-ed-2020>. Acesso em: 27 abr. 2023.

VERGARA, Sylvia Constant. **Projetos e Relatórios de Pesquisa em Administração.** 2. ed. São Paulo: Atlas, 1998.